19. Wahlperiode

Drucksache **19/5728**

HESSISCHER LANDTAG

05. 12. 2017

Gesetzentwurf
der Fraktionen der CDU und BÜNDNIS 90/DIE GRÜNEN

für ein Hessisches Gesetz zur Anpassung des Hessischen Datenschutzrechts an die Verordnung (EU) Nr. 2016/679 und zur Umsetzung der Richtlinie (EU) Nr. 2016/680 und zur Informationsfreiheit

A. Problem

1. Die Verordnung (EU) Nr. 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung) (ABl. EU Nr. L 119 S. 1, Nr. L 314 S. 72) gilt nach Art. 2 Abs. 1 für die ganz oder teilweise automatisierte Verarbeitung personenbezogener Daten sowie für die nicht automatisierte Verarbeitung personenbezogener Daten, die in einem Dateisystem gespeichert sind oder gespeichert werden sollen. Nach Art. 288 Abs. 2 des Vertrags über die Arbeitsweise der Europäischen Union (AEUV) haben Verordnungen allgemeine Geltung, sind in allen ihren Teilen verbindlich und gelten unmittelbar in jedem Mitgliedstaat.

   Am 25. Mai 2018 wird die Verordnung (EU) Nr. 2016/679 unmittelbar geltendes Recht in allen Mitgliedstaaten der Europäischen Union sein. Ihrem Charakter als Grundverordnung folgend sieht sie jedoch Öffnungsklauseln für den nationalen Gesetzgeber vor. Zugleich enthält sie konkrete, an die Mitgliedstaaten gerichtete Regelungsaufträge. Daraus ergibt sich in Bund und Ländern gesetzlicher Anpassungs- und Ausgestaltungsbedarf im Datenschutzrecht.

2. Zeitgleich mit der Verordnung (EU) Nr. 2016/679 in Kraft getreten ist die Richtlinie (EU) Nr. 2016/680 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zweck der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung sowie zum freien Datenverkehr und zur Aufhebung des Rahmenbeschlusses 2008/977/JI des Rates (ABl. EU Nr. L 119 S. 89). Nach deren Art. 63 sind die der Richtlinie (EU) Nr. 2016/680 unterfallenden Staaten verpflichtet, bis zum 6. Mai 2018 die Rechts- und Verwaltungsvorschriften zu erlassen, die erforderlich sind, um dieser Richtlinie nachzukommen.

3. Das Verwaltungshandeln soll in Hessen für die Bürgerinnen und Bürger offener und transparenter gestaltet werden. Zurzeit gibt es eine Reihe von Vorschriften in unterschiedlichen Gesetzen, die den Zugang zu Akten und behördlichen Informationen eröffnen. Der Informationszugang ist dabei mit Ausnahme des Umweltinformationsrechts jeweils von der Erfüllung bestimmter Voraussetzungen abhängig. Einen allgemeinen Anspruch auf Informationszugang gibt es in Hessen bislang nicht.

B. Lösung

1. Das Hessische Datenschutzgesetz wird neu gefasst, um es an die Vorschriften der Verordnung (EU) Nr. 2016/679 anzupassen. Dabei werden Öffnungsklauseln für den Gesetzgeber genutzt, soweit entsprechende Regelungen nicht aufgrund ihres Bezugs den Fachgesetzen vorbehalten sind, und Regelungsaufträge aus der Verordnung umgesetzt.

   Im Rahmen der Neufassung werden zugleich Vorschriften zur Umsetzung der Richtlinie (EU) Nr. 2016/680 in das neue Hessische Datenschutz- und Informationsfreiheitsgesetz aufgenommen, soweit der Gegenstand der Regelung fachbereichsübergreifend von Bedeutung ist. Das Hessische Datenschutzgesetz bündelt damit auch zukünftig die allgemeinen Rechtsgrundlagen für die Verarbeitung personenbezogener Daten durch die öffentlichen Stellen in Hessen, sowohl für die Verwaltung im Geltungsbereich der Verordnung (EU) Nr. 2016/679 als auch für die Behörden im Geltungsbereich der Richtlinie (EU) Nr. 2016/680.

Eingegangen am 5. Dezember 2017 · Eilausfertigung am 6. Dezember 2017 · Ausgegeben am 9. Januar 2018
Herstellung: Kanzlei des Hessischen Landtags · Postfach 3240 · 65022 Wiesbaden · www.Hessischer-Landtag.de

2. Die Bürgerinnen und Bürger in Hessen erhalten einen gesetzlichen Anspruch auf Zugang zu den bei öffentlichen Stellen des Landes vorhandenen amtlichen Informationen. Dabei bleibt nicht nur der Schutz von Betriebs- oder Geschäftsgeheimnissen gewährleistet, sondern insbesondere auch von personenbezogenen Daten. Aufgrund des engen Zusammenhangs zwischen dem Informationszugangsrechts auf der einen Seite und dem Datenschutz auf der anderen Seite werden die Regelungen zum Informationszugang als weiterer Teil in das Hessische Datenschutz- und Informationsfreiheitsgesetz eingefügt.
3. Zur Anpassung der Vorschriften über die Verarbeitung personenbezogener Daten in den hessischen Fachgesetzen an die Verordnung (EU) Nr. 2016/679 und zur Umsetzung der Richtlinie (EU) Nr. 2016/680 werden darüber hinaus 28 weitere Gesetze geändert, u.a. das Strafvollzugsgesetz, das Jugendstrafvollzugsgesetz und das HSOG.

C. Befristung

Eine Befristung ist nicht vorgesehen. Das Hessische Datenschutz- und Informationsfreiheitsgesetz dient dem Schutz des informationellen Selbstbestimmungsrechts und enthält Vorschriften zur Konkretisierung und Umsetzung des EU-Datenschutzrechts durch die öffentlichen Stellen des Landes, der Gemeinden und Gemeindeverbände. Vorhandene Befristungen in den weiteren geänderten Gesetzen bleiben unberührt.

D. Alternativen

Keine. Die Anpassung der datenschutzrechtlichen Vorschriften im Landesrecht an die Datenschutz-Grundverordnung ist geboten, um einen rechtssicheren Vollzug des unmittelbar geltenden europäischen Rechts zu gewährleisten.

Die Richtlinie (EU) Nr. 2016/680 verpflichtet die Mitgliedstaaten zum Erlass der für die Umsetzung der Regelungen notwendigen Gesetze.

E. Finanzielle Auswirkungen

1. Auswirkungen auf die Liquiditäts- oder Ergebnisrechnung

   Die finanziellen Auswirkungen der Vorschriften zum Datenschutz lassen sich gegenwärtig nicht beziffern. Der Aufwand der öffentlichen Stellen des Landes für den Vollzug wird im Wesentlichen unmittelbar durch die europarechtlichen Vorschriften bzw. die europarechtlichen Vorgaben für die landesrechtlichen Umsetzungsregelungen bestimmt.

   Der Vollzug der neuen Vorschriften zum Informationszugangsrecht wird bei den Landesbehörden zu einem gegenwärtig nicht zu beziffernden Mehraufwand führen. Wie hoch dieser sein wird, hängt vom Antragsaufkommen insgesamt und dem Bearbeitungsaufwand in den jeweiligen Einzelfällen ab. Teilweise wird dieser Aufwand durch die vorgesehene Erhebung von Gebühren für die Gewährung des Informationszugangs ausgeglichen.

2. Auswirkungen auf die Vermögensrechnung

   Keine.

3. Berücksichtigung der mehrjährigen Finanzplanung

   Keine.

4. Auswirkungen für hessische Gemeinden und Gemeindeverbände

   Hinsichtlich der Auswirkungen des Gesetzes auf die Gemeinden und Gemeindeverbände wird zunächst auf die Ausführungen zu Nr. 1 verwiesen. Anders als bei den Landesbehörden wird die Entscheidung über die Anwendung des neuen Informationszugangsrechts jedoch in das Ermessen der Kommunen gestellt. Aufgrund dieser Befugnis, die auch die Regelung der Kostenerhebung für den Informationszugang einschließt, bemisst sich der Aufwand für den Vollzug insoweit nach Maßgabe der Entscheidung der jeweiligen Kommune.

F. Unmittelbare oder mittelbare Auswirkungen auf die Chancengleichheit von Frauen und Männern

Keine.

G. Besondere Auswirkungen auf behinderte Menschen

Keine. Das Hessische Datenschutz- und Informationsfreiheitsgesetz wurde am Maßstab der UN-Behindertenkonvention überprüft. Es besteht kein Änderungsbedarf.

Der Landtag wolle das folgende Gesetz beschließen:

**Hessisches Gesetz
zur Anpassung des Hessischen Datenschutzrechts
an die Verordnung (EU) Nr. 2016/679 und zur
Umsetzung der Richtlinie (EU) Nr. 2016/680
und zur Informationsfreiheit**

Vom

Inhaltsübersicht

[1] Ändert FFN 24-39
[2] Ändert FFN 24-42
[3] Ändert FFN 24-43
[4] Ändert FFN 24-46
[5] Ändert FFN 24-49
[6] Ändert FFN 26-5
[7] Ändert FFN 43-25
[8] Ändert FFN 50-35
[9] Ändert FFN 50-51
[10] Ändert FFN 60-6
[11] Ändert FFN 60-31
[12] Ändert FFN 72-123
[13] Ändert FFN 74-2
[14] Ändert FFN 89-37
[15] Ändert FFN 230-198
[16] Ändert FFN 304-32
[17] Ändert FFN 310-63
[18] Ändert FFN 312-12
[19] Ändert FFN 316-34
[20] Ändert FFN 325-30
[21] Ändert FFN 326-9
[22] Ändert FFN 350-6
[23] Ändert FFN 350-94
[24] Ändert FFN 351-84
[25] Ändert FFN 351-90
[26] Ändert FFN 352-3

[27] Ändert FFN 352-6
[28] Ändert FFN 363-34
[29] Hebt FFN 300-28 auf

Artikel 1
Hessisches Datenschutz- und Informationsfreiheitsgesetz
(HDSIG)

INHALTSVERZEICHNIS

ERSTER TEIL
Gemeinsame Bestimmungen

Erster Abschnitt
Anwendungsbereich und Begriffsbestimmungen

§ 1
Anwendungsbereich

(1) Dieses Gesetz gilt für die Verarbeitung personenbezogener Daten durch die öffentlichen Stellen des Landes, der Gemeinden und Landkreise.

(2) Andere Rechtsvorschriften über den Datenschutz gehen vorbehaltlich des Abs. 3 den Vorschriften dieses Gesetzes vor. Regeln sie einen Sachverhalt, für den dieses Gesetz gilt, nicht oder nicht abschließend, finden die Vorschriften dieses Gesetzes Anwendung. Die Verpflichtung zur Wahrung gesetzlicher Geheimhaltungspflichten oder von Berufs- oder besonderen Amtsgeheimnissen, die nicht auf gesetzlichen Vorschriften beruhen, bleibt unberührt.

(3) Die Vorschriften dieses Gesetzes gehen denen des Hessischen Verwaltungsverfahrensgesetzes vor, soweit bei der Ermittlung des Sachverhalts personenbezogene Daten verarbeitet werden.

(4) Die Vorschriften dieses Gesetzes, ausgenommen § 28, finden keine Anwendung, soweit der Hessische Rundfunk personenbezogene Daten zu journalistischen Zwecken verarbeitet.

(5) Die Vorschriften dieses Gesetzes finden keine Anwendung, soweit das Recht der Europäischen Union, insbesondere die Verordnung (EU) Nr. 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung) (ABl. EU Nr. L 119 S. 1, Nr. L 314 S. 72) in der jeweils geltenden Fassung, unmittelbar gilt.

(6) Bei Verarbeitungen zu den in Art. 2 der Verordnung (EU) Nr. 2016/679 genannten Zwecken stehen die Vertragsstaaten des Abkommens über den Europäischen Wirtschaftsraum und die Schweiz den Mitgliedstaaten der Europäischen Union gleich. Andere Staaten gelten insoweit als Drittländer.

(7) Bei Verarbeitungen zu den in Art. 1 Abs. 1 der Richtlinie (EU) Nr. 2016/680 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung sowie zum freien Datenverkehr und zur Aufhebung des Rahmenbeschlusses 2008/977/JI des Rates (ABl. EU Nr. L 119 S. 89) genannten Zwecken stehen die bei der Umsetzung, Anwendung und Entwicklung des Schengen-Besitzstandes assoziierten Staaten den Mitgliedstaaten der Europäischen Union gleich. Andere Staaten gelten insoweit als Drittländer.

(8) Für Verarbeitungen personenbezogener Daten durch öffentliche Stellen im Rahmen von Tätigkeiten, die nicht in den Anwendungsbereich der Verordnung (EU) Nr. 2016/679 und der Richtlinie (EU) Nr. 2016/680 fallen, finden die Verordnung (EU) Nr. 2016/679 sowie der Erste und Zweite Teil entsprechende Anwendung, soweit gesetzlich nichts anderes bestimmt ist.

(9) Die Vorschriften dieses Gesetzes finden keine Anwendung auf anonyme Informationen oder anonymisierte Daten.

§ 2
Begriffsbestimmungen

(1) Öffentliche Stellen sind die Behörden, die Organe der Rechtspflege und andere öffentlich-rechtlich organisierte Einrichtungen des Landes, der Gemeinden und Landkreise oder sonstige deren Aufsicht unterstehende juristische Personen des öffentlichen Rechts sowie deren Vereinigungen ungeachtet ihrer Rechtsform. Nimmt eine nicht öffentliche Stelle hoheitliche Aufgaben der öffentlichen Verwaltung wahr, ist sie insoweit öffentliche Stelle im Sinne dieses Gesetzes.

(2) Öffentliche Stellen gelten als nicht öffentliche Stellen, soweit sie als öffentlich-rechtliche Unternehmen am Wettbewerb teilnehmen. Insoweit finden die für nicht öffentliche Stellen geltenden Vorschriften des Bundesdatenschutzgesetzes und die §§ 5 bis 18 und 23 Anwendung.

(3) Vereinigungen des privaten Rechts von öffentlichen Stellen, die Aufgaben der öffentlichen Verwaltung wahrnehmen, gelten ungeachtet der Beteiligung nicht öffentlicher Stellen als öffentliche Stellen, wenn einer oder mehreren öffentlichen Stellen die absolute Mehrheit der Anteile

gehört oder der Stimmen zusteht. Beteiligt sich eine Vereinigung des privaten Rechts, die nach Satz 1 als öffentliche Stelle gilt, an einer weiteren Vereinigung des privaten Rechts, so finden Satz 1 und Abs. 2 entsprechende Anwendung.

(4) Anonyme Informationen sind solche Informationen, die sich nicht auf eine identifizierte oder identifizierbare natürliche Person beziehen. Personenbezogene Daten, die in einer Weise anonymisiert worden sind, dass die betroffene Person nicht oder nicht mehr identifiziert werden kann, sind anonymisierte Daten. Eine natürliche Person ist identifizierbar, wenn sie unter Berücksichtigung aller Mittel, die von dem Verantwortlichen oder einer anderen Person nach allgemeinem Ermessen wahrscheinlich genutzt werden, um die Identität der natürlichen Person direkt oder indirekt zu ermitteln, identifiziert werden kann. Bei der Feststellung, ob Mittel nach allgemeinem Ermessen wahrscheinlich zur Identifizierung der natürlichen Person genutzt werden, sollten alle objektiven Faktoren, insbesondere die Kosten der Identifizierung und der dafür erforderliche Zeitaufwand, herangezogen werden, wobei die zum Zeitpunkt der Verarbeitung verfügbare Technologie und technologische Entwicklungen zu berücksichtigen sind.

Zweiter Abschnitt
Rechtsgrundlagen für die Verarbeitung personenbezogener Daten

§ 3
Verarbeitung personenbezogener Daten, Auftragsverarbeitung

(1) Die Verarbeitung personenbezogener Daten durch eine öffentliche Stelle ist zulässig, wenn sie zur Erfüllung der in der Zuständigkeit des Verantwortlichen liegenden Aufgabe oder in Ausübung öffentlicher Gewalt, die dem Verantwortlichen übertragen wurde, erforderlich ist.

(2) Der Verantwortliche ist verpflichtet, sicherzustellen, dass ein Auftragsverarbeiter, auf den dieses Gesetz keine Anwendung findet, dessen Vorschriften beachtet. Als Auftragsverarbeiter gelten auch Personen und Stellen, die im Auftrag Wartungsarbeiten und vergleichbare Hilfstätigkeiten bei der Verarbeitung personenbezogener Daten erledigen.

§ 4
Videoüberwachung öffentlich zugänglicher Räume

(1) Die Beobachtung öffentlich zugänglicher Räume mit optisch-elektronischen Einrichtungen (Videoüberwachung) ist nur zulässig, soweit sie

1. zur Aufgabenerfüllung öffentlicher Stellen,
2. zur Wahrnehmung des Hausrechts oder
3. zur Wahrnehmung berechtigter Interessen für konkret festgelegte Zwecke

erforderlich ist und keine Anhaltspunkte bestehen, dass schutzwürdige Interessen der Betroffenen überwiegen.

(2) Der Umstand der Beobachtung sowie der Name und die Kontaktdaten des Verantwortlichen sind durch geeignete Maßnahmen zum frühestmöglichen Zeitpunkt erkennbar zu machen.

(3) Die Speicherung oder Verwendung von nach Abs. 1 erhobenen Daten ist zulässig, wenn sie zum Erreichen des verfolgten Zwecks erforderlich ist und keine Anhaltspunkte bestehen, dass schutzwürdige Interessen der Betroffenen überwiegen. Für einen anderen Zweck dürfen sie nur weiterverarbeitet werden, soweit dies zur Abwehr von Gefahren für die staatliche und öffentliche Sicherheit sowie zur Verfolgung von Straftaten und nicht geringfügigen Ordnungswidrigkeiten erforderlich ist.

(4) Die Daten sind zu löschen, sobald sie zur Erreichung des Zwecks nicht mehr erforderlich sind oder wenn schutzwürdige Interessen der Betroffenen einer weiteren Speicherung entgegenstehen.

Dritter Abschnitt
Datenschutzbeauftragte öffentlicher Stellen

§ 5
Benennung

(1) Öffentliche Stellen benennen eine Datenschutzbeauftragte oder einen Datenschutzbeauftragten sowie deren oder dessen Vertreterin oder Vertreter.

(2) Für mehrere öffentliche Stellen kann unter Berücksichtigung ihrer Organisationsstruktur und ihrer Größe eine gemeinsame Datenschutzbeauftragte oder ein gemeinsamer Datenschutzbeauftragter benannt werden.

(3) Die oder der Datenschutzbeauftragte wird auf der Grundlage ihrer oder seiner beruflichen Qualifikation und insbesondere ihres oder seines Fachwissens benannt, das sie oder er auf dem Gebiet des Datenschutzrechts und der Datenschutzpraxis besitzt, sowie auf der Grundlage ihrer oder seiner Fähigkeit zur Erfüllung der in § 7 genannten Aufgaben.

(4) Die oder der Datenschutzbeauftragte kann Beschäftigte oder Beschäftigter der öffentlichen Stelle sein oder ihre oder seine Aufgaben auf der Grundlage eines Dienstleistungsvertrags erfüllen.

(5) Die öffentliche Stelle veröffentlicht die Kontaktdaten der oder des Datenschutzbeauftragten und teilt diese Daten der oder dem Hessischen Datenschutzbeauftragten mit.

§ 6
Rechtsstellung

(1) Die öffentliche Stelle stellt sicher, dass die oder der Datenschutzbeauftragte ordnungsgemäß und frühzeitig in alle mit dem Schutz personenbezogener Daten zusammenhängenden Fragen eingebunden wird.

(2) Die öffentliche Stelle unterstützt die Datenschutzbeauftragte oder den Datenschutzbeauftragten bei der Erfüllung ihrer oder seiner Aufgaben nach § 7, indem sie die für die Erfüllung dieser Aufgaben erforderlichen Ressourcen und den Zugang zu personenbezogenen Daten und Verarbeitungsvorgängen sowie die zur Erhaltung ihres oder seines Fachwissens erforderlichen Ressourcen zur Verfügung stellt. Insbesondere ist die oder der Datenschutzbeauftragte im erforderlichen Umfang von der Erfüllung anderer Aufgaben freizustellen.

(3) Die öffentliche Stelle stellt sicher, dass die oder der Datenschutzbeauftragte bei der Erfüllung ihrer oder seiner Aufgaben keine Anweisungen bezüglich der Ausübung dieser Aufgaben erhält. Die oder der Datenschutzbeauftragte untersteht und berichtet unmittelbar der höchsten Leitungsebene der öffentlichen Stelle. Die oder der Datenschutzbeauftragte darf von der öffentlichen Stelle wegen der Erfüllung ihrer oder seiner Aufgaben nicht abberufen oder benachteiligt werden.

(4) Beschäftigte der öffentlichen Stellen können sich ohne Einhaltung des Dienstwegs in allen Angelegenheiten des Datenschutzes an die oder den Datenschutzbeauftragten wenden. Betroffene Personen können die Datenschutzbeauftragte oder den Datenschutzbeauftragten zu allen mit der Verarbeitung ihrer personenbezogenen Daten und mit der Wahrnehmung ihrer Rechte nach der Verordnung (EU) Nr. 2016/679, diesem Gesetz sowie anderen Rechtsvorschriften über den Datenschutz im Zusammenhang stehenden Fragen zu Rate ziehen. Die oder der Datenschutzbeauftragte ist zur Verschwiegenheit über die Identität der betroffenen Person verpflichtet, die ihr oder ihm in der Eigenschaft als Datenschutzbeauftragte oder Datenschutzbeauftragter Tatsachen anvertraut hat. Die Verschwiegenheitspflicht erstreckt sich auch auf die Umstände, die Rückschlüsse auf die betroffene Person zulassen, sowie auf diese Tatsachen selbst, soweit die oder der Datenschutzbeauftragte nicht durch die betroffene Person davon befreit wird.

(5) Wenn die oder der Datenschutzbeauftragte bei ihrer oder seiner Tätigkeit Kenntnis von Daten erhält, für die der Leitung oder einer bei der öffentlichen Stelle beschäftigten Person aus beruflichen Gründen ein Zeugnisverweigerungsrecht zusteht, steht dieses Recht auch der oder dem Datenschutzbeauftragten und den ihr oder ihm unterstellten Beschäftigten zu. Über die Ausübung dieses Rechts entscheidet die Person, der das Zeugnisverweigerungsrecht aus beruflichen Gründen zusteht, es sei denn, dass diese Entscheidung in absehbarer Zeit nicht herbeigeführt werden kann. So weit das Zeugnisverweigerungsrecht der oder des Datenschutzbeauftragten reicht, unterliegen ihre oder seine Akten und andere Dokumente einem Beschlagnahmeverbot.

§ 7
Aufgaben

(1) Der oder dem Datenschutzbeauftragten obliegen neben den in der Verordnung (EU) Nr. 2016/679 genannten Aufgaben zumindest folgende Aufgaben:

1. Unterrichtung und Beratung der öffentlichen Stelle und der Beschäftigten, die Verarbeitungen durchführen, hinsichtlich ihrer Pflichten nach diesem Gesetz und sonstigen Vorschriften über den Datenschutz, einschließlich der zur Umsetzung der Richtlinie (EU) Nr. 2016/680 erlassenen Rechtsvorschriften,
2. Überwachung der Einhaltung dieses Gesetzes und sonstiger Vorschriften über den Datenschutz, einschließlich der zur Umsetzung der Richtlinie (EU) Nr. 2016/680 erlassenen Rechtsvorschriften, sowie der Strategien der öffentlichen Stelle für den Schutz personenbezogener Daten einschließlich der Zuweisung von Zuständigkeiten, der Sensibilisierung und der Schulung der an den Verarbeitungsvorgängen beteiligten Beschäftigten und der diesbezüglichen Überprüfungen,

3. Beratung im Zusammenhang mit der Datenschutz-Folgenabschätzung und Überwachung ihrer Durchführung nach § 62,
4. Zusammenarbeit mit der oder dem Hessischen Datenschutzbeauftragten,
5. Tätigkeit als Anlaufstelle für die oder den Hessischen Datenschutzbeauftragten in mit der Verarbeitung zusammenhängenden Fragen, einschließlich der vorherigen Konsultation nach § 64, und gegebenenfalls Beratung zu allen sonstigen Fragen.

Im Fall einer oder eines bei einem Gericht bestellten Datenschutzbeauftragten beziehen sich diese Aufgaben nicht auf das Handeln des Gerichts im Rahmen seiner justiziellen Tätigkeit.

(2) Die oder der Datenschutzbeauftragte kann andere Aufgaben und Pflichten wahrnehmen. Die öffentliche Stelle stellt sicher, dass derartige Aufgaben und Pflichten nicht zu einem Interessenkonflikt führen.

(3) Die oder der Datenschutzbeauftragte trägt bei der Erfüllung ihrer oder seiner Aufgaben dem mit den Verarbeitungsvorgängen verbundenen Risiko gebührend Rechnung, wobei sie oder er die Art, den Umfang, die Umstände und die Zwecke der Verarbeitung berücksichtigt.

Vierter Abschnitt
Die oder der Hessische Datenschutzbeauftragte

§ 8
Rechtsstellung und Unabhängigkeit

(1) Die oder der Hessische Datenschutzbeauftragte ist eine oberste Landesbehörde.

(2) Die oder der Hessische Datenschutzbeauftragte handelt in Ausübung ihres oder seines Amtes unabhängig und ist nur dem Gesetz unterworfen. Sie oder er unterliegt bei der Erfüllung ihrer oder seiner Aufgaben und bei der Ausübung ihrer oder seiner Befugnisse weder direkter noch indirekter Beeinflussung von außen und ersucht weder um Weisung noch nimmt sie oder er Weisungen entgegen.

(3) Die oder der Hessische Datenschutzbeauftragte unterliegt der Rechnungsprüfung durch den Hessischen Rechnungshof.

(4) Die oder der Hessische Datenschutzbeauftragte ist berechtigt, an den Sitzungen des Landtags und seiner Ausschüsse nach Maßgabe der Geschäftsordnung des Landtags teilzunehmen und sich zu Fragen zu äußern, die für den Datenschutz von Bedeutung sind. Der Landtag und seine Ausschüsse können die Anwesenheit der oder des Hessischen Datenschutzbeauftragten verlangen.

§ 9
Wahl

(1) Der Landtag wählt auf Vorschlag der Landesregierung die Hessische Datenschutzbeauftragte oder den Hessischen Datenschutzbeauftragten.

(2) Die Präsidentin oder der Präsident des Landtags verpflichtet die Hessische Datenschutzbeauftragte oder den Hessischen Datenschutzbeauftragten vor dem Landtag, ihr oder sein Amt gerecht und unparteiisch zu führen und die Verfassung des Landes Hessen und das Grundgesetz für die Bundesrepublik Deutschland und die Gesetze getreulich zu wahren.

§ 10
Persönliche Voraussetzungen

Die oder der Hessische Datenschutzbeauftragte muss bei ihrer oder seiner Wahl das 35. Lebensjahr vollendet haben. Sie oder er muss über die für die Erfüllung ihrer oder seiner Aufgaben und die Ausübung ihrer oder seiner Befugnisse erforderliche Qualifikation, Erfahrung und Sachkunde insbesondere im Bereich des Schutzes personenbezogener Daten verfügen und die Befähigung zum Richteramt oder zum höheren Dienst haben.

§ 11
Amtsverhältnis

(1) Die oder der Hessische Datenschutzbeauftragte steht nach Maßgabe dieses Gesetzes zum Land in einem öffentlich-rechtlichen Amtsverhältnis. Sie oder er übt ihre oder seine Tätigkeit hauptamtlich aus. Die oder der Hessische Datenschutzbeauftragte sieht von allen mit den Aufgaben ihres oder seines Amtes nicht zu vereinbarenden Handlungen ab und übt während der Amtszeit keine mit dem Amt nicht zu vereinbarende entgeltliche oder unentgeltliche Tätigkeit aus. Die oder der Hessische Datenschutzbeauftragte erteilt dem Landtag jährlich Auskunft über

Art und Umfang der von ihr oder ihm im Kalenderjahr ausgeübten Nebentätigkeiten sowie über die dafür erhaltenen Vergütungen.

(2) Die oder der Hessische Datenschutzbeauftragte wird für die Dauer von fünf Jahren gewählt. Das Amtsverhältnis endet mit Ablauf der Amtszeit oder mit dem Rücktritt. Die oder der Hessische Datenschutzbeauftragte bleibt bis zur Neuwahl im Amt. Die Wiederwahl ist zulässig. Durch Urteil des Staatsgerichtshofs können ihr oder ihm das Amt und die Rechte aus dem Amt abgesprochen werden, wenn Tatsachen vorliegen, die bei einer Beamtin oder einem Beamten die Entlassung nach den §§ 22 und 23 Abs. 1 und 3 Nr. 1 des Beamtenstatusgesetzes vom 17. Juni 2008 (BGBl. I S. 1010), geändert durch Gesetz vom 8. Juni 2017 (BGBl. I S. 1570), oder die Beendigung des Dienstverhältnisses nach § 24 des Beamtenstatusgesetzes rechtfertigen. Der Antrag auf Erhebung der Klage muss von mindestens 15 Mitgliedern des Landtags unterzeichnet sein und bedarf der Zustimmung von zwei Dritteln der gesetzlichen Zahl seiner Mitglieder. Die §§ 31 bis 35 des Gesetzes über den Staatsgerichtshof in der Fassung der Bekanntmachung vom 19. Januar 2001 (GVBl. I S. 78), zuletzt geändert durch Gesetz vom 28. März 2015 (GVBl. S. 158), sind entsprechend anzuwenden.

(3) Die oder der Hessische Datenschutzbeauftragte kann jederzeit von ihrem oder seinem Amt zurücktreten.

(4) Die oder der Hessische Datenschutzbeauftragte ernennt für den Fall der Verhinderung oder des vorzeitigen Ausscheidens aus dem Amt für die Zeit bis zur Wahl einer oder eines neuen Hessischen Datenschutzbeauftragten eine Beschäftigte oder einen Beschäftigten ihrer oder seiner Dienststelle zur Vertreterin oder zum Vertreter. Als Verhinderung gilt auch, wenn im Einzelfall in der Person der oder des Hessischen Datenschutzbeauftragten Gründe vorliegen, die bei einer Richterin oder einem Richter zum Ausschluss von der Mitwirkung oder zur Ablehnung wegen Besorgnis der Befangenheit führen können.

(5) Die oder der Hessische Datenschutzbeauftragte erhält vom Beginn des Kalendermonats an, in dem das Amtsverhältnis beginnt, bis zum Ende des Kalendermonats, in dem das Amtsverhältnis endet, als Amtsbezüge ein Amtsgehalt in Höhe des Grundgehalts der Besoldungsgruppe B 7 sowie einen Familienzuschlag in entsprechender Anwendung des Hessischen Besoldungsgesetzes vom 27. Mai 2013 (GVBl. S. 218, 256, 508), zuletzt geändert durch Gesetz vom 30. Juni 2017 (GVBl. S. 114), in der jeweils geltenden Fassung. Für Reise- und Umzugskosten, Trennungsgeld, Beihilfen und Urlaubsangelegenheiten der oder des Hessischen Datenschutzbeauftragten gelten die für die Beamtinnen und Beamten des Landes geltenden Vorschriften entsprechend.

(6) Zuständig für die Festsetzung, Berechnung und Anordnung der Zahlung der Amtsbezüge einschließlich der Sonderzahlungen sowie der Rückforderung zu viel gezahlter Amtsbezüge ist die Hessische Bezügestelle im Auftrag der oder des Hessischen Datenschutzbeauftragten. Zuständig für die Festsetzung von Reise- und Umzugskosten sowie Trennungsgeld ist die Dienststelle der oder des Hessischen Datenschutzbeauftragten. Zuständig für die Festsetzung der Beihilfe ist die Kanzlei des Hessischen Landtags.

(7) Die oder der Hessische Datenschutzbeauftragte und deren oder dessen Hinterbliebene erhalten Versorgung in entsprechender Anwendung der in Hessen für die Mitglieder der Landesregierung geltenden Bestimmungen. Zuständig für die Festsetzung der Versorgungsbezüge ist das Regierungspräsidium Kassel im Auftrag der oder des Hessischen Datenschutzbeauftragten.

§ 12
Verschwiegenheitspflicht

Die oder der Hessische Datenschutzbeauftragte ist, auch nach Beendigung ihres oder seines Amtsverhältnisses, verpflichtet, über die ihr oder ihm bei ihrer oder seiner amtlichen Tätigkeit bekannt gewordenen Angelegenheiten Verschwiegenheit zu bewahren. Dies gilt nicht für Mitteilungen im dienstlichen Verkehr oder über Tatsachen, die offenkundig sind oder ihrer Bedeutung nach keiner Geheimhaltung bedürfen. Satz 1 und 2 gelten entsprechend für ihre oder seine Beschäftigten. Die oder der Hessische Datenschutzbeauftragte gilt als oberste Dienstbehörde im Sinne des § 96 der Strafprozessordnung. Sie oder er entscheidet entsprechend den Bestimmungen über die Vorlage- und Auskunftspflichten von Behörden in den gerichtlichen Verfahrensordnungen. Die oder der Hessische Datenschutzbeauftragte trifft die Entscheidungen nach § 37 Abs. 3 des Beamtenstatusgesetzes und § 46 des Hessischen Beamtengesetzes für sich und die bei ihr oder ihm tätigen Beamtinnen und Beamten.

§ 13
Zuständigkeit und Aufgaben

(1) Die oder der Hessische Datenschutzbeauftragte überwacht bei den öffentlichen und nicht öffentlichen Stellen sowie deren Auftragsverarbeitern die Anwendung dieses Gesetzes, der Ver-

ordnung (EU) Nr. 2016/679 und sonstiger Vorschriften über den Datenschutz, einschließlich der zur Umsetzung der Richtlinie (EU) Nr. 2016/680 erlassenen Rechtsvorschriften.

(2) Neben den Aufgaben nach Art. 57 der Verordnung (EU) Nr. 2016/679 hat die oder der Hessische Datenschutzbeauftragte die Aufgaben,

1. die Anwendung dieses Gesetzes und sonstiger Vorschriften über den Datenschutz, einschließlich der zur Umsetzung der Richtlinie (EU) Nr. 2016/680 erlassenen Rechtsvorschriften, zu überwachen und durchzusetzen,
2. die Öffentlichkeit für die Risiken, Vorschriften, Garantien und Rechte im Zusammenhang mit der Verarbeitung personenbezogener Daten zu sensibilisieren und sie darüber aufzuklären, wobei spezifische Maßnahmen für Kinder und Jugendliche besondere Beachtung finden,
3. den Landtag, die im Landtag vertretenen Fraktionen, die Landesregierung, die Kommunen und andere Einrichtungen und Gremien über legislative und administrative Maßnahmen zum Schutz der Rechte und Freiheiten natürlicher Personen in Bezug auf die Verarbeitung personenbezogener Daten zu beraten,
4. die Verantwortlichen und die Auftragsverarbeiter für die ihnen aus diesem Gesetz und sonstigen Vorschriften über den Datenschutz, einschließlich der zur Umsetzung der Richtlinie (EU) Nr. 2016/680 erlassenen Rechtsvorschriften, entstehenden Pflichten bei der Verarbeitung personenbezogener Daten zu sensibilisieren,
5. auf Anfrage jeder betroffenen Person Informationen über die Ausübung ihrer Rechte aufgrund dieses Gesetzes und sonstiger Vorschriften über den Datenschutz, einschließlich der zur Umsetzung der Richtlinie (EU) Nr. 2016/680 erlassenen Rechtsvorschriften, zur Verfügung zu stellen und gegebenenfalls zu diesem Zweck mit den Aufsichtsbehörden in anderen Mitgliedstaaten zusammenzuarbeiten,
6. sich mit Beschwerden einer betroffenen Person oder Beschwerden einer Stelle, einer Organisation oder eines Verbandes nach Art. 55 der Richtlinie (EU) Nr. 2016/680 zu befassen, den Gegenstand der Beschwerde in angemessenem Umfang zu untersuchen und den Beschwerdeführer innerhalb einer angemessenen Frist über den Fortgang und das Ergebnis der Untersuchung zu unterrichten, insbesondere, wenn eine weitere Untersuchung oder Koordinierung mit einer anderen Aufsichtsbehörde notwendig ist,
7. mit anderen Aufsichtsbehörden zusammenzuarbeiten, auch durch Informationsaustausch, und ihnen Amtshilfe zu leisten, um die einheitliche Anwendung und Durchsetzung dieses Gesetzes und sonstiger Vorschriften über den Datenschutz, einschließlich der zur Umsetzung der Richtlinie (EU) Nr. 2016/680 erlassenen Rechtsvorschriften, zu gewährleisten,
8. Untersuchungen über die Anwendung dieses Gesetzes und sonstiger Vorschriften über den Datenschutz, einschließlich der zur Umsetzung der Richtlinie (EU) Nr. 2016/680 erlassenen Rechtsvorschriften, durchzuführen, auch auf der Grundlage von Informationen einer anderen Aufsichtsbehörde oder einer anderen Behörde,
9. maßgebliche Entwicklungen zu verfolgen, soweit sie sich auf den Schutz personenbezogener Daten auswirken, insbesondere die Entwicklung der Informations- und Kommunikationstechnologie und
10. Beratung in Bezug auf die in § 64 genannten Verarbeitungsvorvorgänge zu leisten.

Im Anwendungsbereich der Richtlinie (EU) Nr. 2016/680 nimmt die oder der Hessische Datenschutzbeauftragte zudem die Aufgaben nach § 52 Abs. 7 auch in Verbindung mit § 51 Abs. 4, § 53 Abs. 7 und § 55 wahr.

(3) Die oder der Hessische Datenschutzbeauftragte beobachtet die Auswirkungen der automatisierten Datenverarbeitung auf die Arbeitsweise und die Entscheidungsbefugnisse der öffentlichen Stellen, insbesondere ob diese zu einer Verschiebung in der Gewaltenteilung zwischen den Verfassungsorganen des Landes, zwischen den Organen der kommunalen Selbstverwaltung oder zwischen der staatlichen Verwaltung und der kommunalen Selbstverwaltung führen. Sie oder er soll Maßnahmen anregen, die geeignet erscheinen, derartige Auswirkungen zu verhindern.

(4) Die oder der Hessische Datenschutzbeauftragte ist

1. zuständige Behörde für die Verfolgung und Ahndung von Ordnungswidrigkeiten nach
   a) § 38 und
   b) Art. 83 Abs. 4 bis 6 der Verordnung (EU) Nr. 2016/679 sowie
2. zuständige Stelle für die Leistung von Hilfe nach Art. 13 Abs. 2 Buchst. a des Übereinkommens zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten vom 28. Januar 1981 (BGBl. 1985 II S. 538, 539).

(5) Abs. 2 Nr. 1 gilt nicht für das Handeln der Gerichte im Rahmen ihrer justiziellen Tätigkeit.

(6) Zur Erfüllung der in Abs. 2 Satz 1 Nr. 3 genannten Aufgabe kann die oder der Hessische Datenschutzbeauftragte von sich aus oder auf Anfrage Stellungnahmen an den Landtag oder einen seiner Ausschüsse, die Landesregierung, die Kommunen, sonstige Einrichtungen und Stellen sowie an die Öffentlichkeit richten. Auf Ersuchen des Landtags oder eines seiner Ausschüsse, der Landesregierung, der Kommunen, sonstiger Einrichtungen und Stellen geht die oder der Hessische Datenschutzbeauftragte ferner Hinweisen auf Angelegenheiten und Vorgänge des Datenschutzes nach.

(7) Die oder der Hessische Datenschutzbeauftragte erleichtert das Einreichen der in Abs. 2 Satz 1 Nr. 6 genannten Beschwerden durch Maßnahmen wie etwa die Bereitstellung eines Beschwerdeformulars, das auch elektronisch ausgefüllt werden kann, ohne dass andere Kommunikationsmittel ausgeschlossen werden.

(8) Zur Erfüllung der in Abs. 2 Satz 1 Nr. 7 genannten Aufgabe kann die oder der Hessische Datenschutzbeauftragte anderen Aufsichtsbehörden Informationen übermitteln und ihnen Amtshilfe leisten.

(9) Für die Erfüllung der Aufgaben und Gewährung der Auskunft nach § 80 Abs. 1 erhebt die oder der Hessische Datenschutzbeauftragte Kosten (Gebühren und Auslagen) nach Maßgabe des Hessischen Verwaltungskostengesetzes in der Fassung der Bekanntmachung vom 12. Januar 2004 (GVBl. I S. 36), zuletzt geändert durch Gesetz vom 13. Dezember 2012 (GVBl. S. 622), und § 88 Abs. 1 in Verbindung mit der Anlage zu diesem Gesetz.

(10) Die Erfüllung der Aufgaben der oder des Hessischen Datenschutzbeauftragten ist für die betroffene Person verwaltungskostenfrei. Bei offenkundig unbegründeten oder, insbesondere im Fall von häufiger Wiederholung, exzessiven Anfragen kann die oder der Hessische Datenschutzbeauftragte eine Gebühr auf der Grundlage der Anlage zu diesem Gesetz verlangen oder sich weigern, aufgrund der Anfrage tätig zu werden. In diesem Fall trägt die oder der Hessische Datenschutzbeauftragte die Beweislast für den offenkundig unbegründeten oder exzessiven Charakter der Anfrage.

(11) Die Landesregierung wird ermächtigt, nach Anhörung der oder des Hessischen Datenschutzbeauftragten die Anlage zu diesem Gesetz durch Rechtsverordnung nach Maßgabe des Hessischen Verwaltungskostengesetzes zu ändern.

§ 14
Befugnisse

(1) Die oder der Hessische Datenschutzbeauftragte nimmt im Anwendungsbereich der Verordnung (EU) Nr. 2016/679 die Befugnisse nach Art. 58 der Verordnung (EU) Nr. 2016/679 wahr. Kommt die oder der Hessische Datenschutzbeauftragte zu dem Ergebnis, dass Verstöße gegen die Vorschriften über den Datenschutz oder sonstige Mängel bei der Verarbeitung personenbezogener Daten vorliegen, teilt sie oder er dies der öffentlichen Stelle mit und gibt dieser vor der Ausübung der Befugnisse des Art. 58 Abs. 2 Buchst. b bis g, i und j der Verordnung (EU) Nr. 2016/679 Gelegenheit zur Stellungnahme innerhalb einer angemessenen Frist. Von der Einräumung der Gelegenheit zur Stellungnahme kann abgesehen werden, wenn eine sofortige Entscheidung wegen Gefahr im Verzug oder im öffentlichen Interesse notwendig erscheint oder ihr ein zwingendes öffentliches Interesse entgegensteht. Die Stellungnahme soll auch eine Darstellung der Maßnahmen enthalten, die aufgrund der Mitteilung der oder des Hessischen Datenschutzbeauftragten getroffen worden sind. Die Ausübung der Befugnisse nach Art. 58 Abs. 2 Buchst. b bis g, i und j der Verordnung (EU) Nr. 2016/679 teilt die oder der Hessische Datenschutzbeauftragte der jeweils zuständigen Rechts- und Fachaufsichtsbehörde mit.

(2) Stellt die oder der Hessische Datenschutzbeauftragte bei Datenverarbeitungen zu Zwecken außerhalb des Anwendungsbereichs der Verordnung (EU) Nr. 2016/679 Verstöße gegen die Vorschriften dieses Gesetzes oder gegen andere Vorschriften über den Datenschutz oder sonstige Mängel bei der Verarbeitung oder Nutzung personenbezogener Daten fest, so beanstandet sie oder er dies im Fall einer öffentlichen Stelle

1. des Landes gegenüber der zuständigen obersten Landesbehörde,
2. einer Gemeinde oder eines Landkreises gegenüber dem jeweiligen vertretungsberechtigten Organ

und fordert diese zur Stellungnahme innerhalb einer von ihr oder ihm zu bestimmenden Frist auf. In den Fällen des Satzes 1 Nr. 2 unterrichtet die oder der Hessische Datenschutzbeauftragte gleichzeitig die zuständige Aufsichtsbehörde. Die Stellungnahme soll auch eine Darstellung der Maßnahmen enthalten, die aufgrund der Beanstandung der oder des Hessischen Datenschutzbeauftragten getroffen worden sind. Die oder der Hessische Datenschutzbeauftragte kann von

einer Beanstandung absehen oder auf eine Stellungnahme verzichten, insbesondere wenn es sich um unerhebliche oder inzwischen beseitigte Mängel handelt. Die oder der Hessische Datenschutzbeauftragte kann den Verantwortlichen auch davor warnen, dass beabsichtigte Verarbeitungsvorgänge voraussichtlich gegen in diesem Gesetz enthaltene und andere auf die jeweilige Datenverarbeitung anzuwendende Vorschriften über den Datenschutz verstoßen.

(3) Die oder der Hessische Datenschutzbeauftragte kann bei Verstößen nach Abs. 2 Satz 1 darüber hinaus anordnen,

1. Verarbeitungsvorgänge, gegebenenfalls auf bestimmte Weise oder innerhalb eines bestimmten Zeitraums, mit den Vorschriften dieses Gesetzes oder anderen Vorschriften über den Datenschutz in Einklang zu bringen,
2. personenbezogene Daten zu berichtigen,
3. personenbezogene Daten in der Verarbeitung einzuschränken,
4. personenbezogene Daten zu löschen,

wenn dies zur Beseitigung eines erheblichen Verstoßes gegen datenschutzrechtliche Vorschriften erforderlich ist.

(4) Die öffentlichen Stellen sind verpflichtet, die Hessische Datenschutzbeauftragte oder den Hessischen Datenschutzbeauftragten bei der Erfüllung ihrer oder seiner Aufgaben zu unterstützen. Ihr oder ihm ist insbesondere

1. Auskunft zu allen Fragen zu erteilen und alle Dokumente vorzulegen, die im Zusammenhang mit der Verarbeitung personenbezogener Daten stehen,
2. Zugang zu allen personenbezogenen Daten, die verarbeitet werden, zu gewähren,
3. Zugang zu den Grundstücken und Diensträumen einschließlich aller Datenverarbeitungsanlagen und -geräte zu gewähren,

soweit dies zur Erfüllung ihrer oder seiner Aufgaben erforderlich ist.

(5) Wenn eine oberste Landesbehörde im Einzelfall feststellt, dass die Sicherheit des Bundes oder eines Landes dies gebietet, dürfen die Rechte nach Abs. 3 nur von der oder dem Hessischen Datenschutzbeauftragten persönlich ausgeübt werden. In diesem Fall dürfen personenbezogene Daten einer betroffenen Person, der von dem Verantwortlichen Vertraulichkeit besonders zugesichert worden ist, auch der oder dem Hessischen Datenschutzbeauftragten gegenüber nicht offenbart werden.

§ 15
Gutachten und Untersuchungen, Tätigkeitsbericht

(1) Der Landtag und die Landesregierung können die Hessische Datenschutzbeauftragte oder den Hessischen Datenschutzbeauftragten mit der Erstattung von Gutachten und der Durchführung von Untersuchungen in Datenschutzfragen und Fragen des freien Zugangs zu Informationen betrauen.

(2) Der Landtag, die Präsidentin oder der Präsident des Landtags und die in § 29 Abs. 3 genannten Vertretungsorgane können verlangen, dass die oder der Hessische Datenschutzbeauftragte untersucht, aus welchen Gründen Auskunftsersuchen nicht oder nicht ausreichend beantwortet wurden.

(3) Zum 31. Dezember jedes Jahres hat die oder der Hessische Datenschutzbeauftragte dem Landtag und der Landesregierung einen Bericht über das Ergebnis ihrer oder seiner Tätigkeit vorzulegen und regt Verbesserungen des Datenschutzes an. Die oder der Hessische Datenschutzbeauftragte macht diesen Bericht der Öffentlichkeit, der Europäischen Kommission und dem Europäischen Datenschutzausschuss zugänglich. Zwischenberichte zur Vorlage bei dem Landtag und der Landesregierung sind zulässig.

(4) Die Landesregierung legt ihre Stellungnahme zu einem Bericht nach Abs. 3 Satz 1 oder 3, soweit dessen Gegenstand die Verarbeitung personenbezogener Daten durch öffentliche Stellen ist, dem Landtag vor.

§ 16
Informationspflichten

(1) Die oder der Hessische Datenschutzbeauftragte ist über Verfahrensentwicklungen im Zusammenhang mit der automatisierten Verarbeitung personenbezogener Daten rechtzeitig und umfassend zu unterrichten.

(2) Wird die oder der Hessische Datenschutzbeauftragte aufgrund einer Rechtsvorschrift gehört, soll sie oder er unverzüglich mitteilen, ob und innerhalb welcher Frist eine Stellungnahme abgegeben wird.

§ 17
Benachteiligungsverbot bei Anrufung der oder des Hessischen Datenschutzbeauftragten

Unbeschadet des Art. 77 der Verordnung (EU) Nr. 2016/679 sowie § 55 darf keiner Person ein Nachteil daraus erwachsen, dass sie sich aufgrund tatsächlicher Anhaltspunkte für einen Verstoß gegen Vorschriften dieses Gesetzes oder anderer Vorschriften über den Datenschutz an die Hessische Datenschutzbeauftragte oder den Hessischen Datenschutzbeauftragten wendet. Beschäftigte öffentlicher Stellen können sich ohne Einhaltung des Dienstwegs an die Hessische Datenschutzbeauftragte oder den Hessischen Datenschutzbeauftragten wenden. Die dienstrechtlichen Pflichten der Beschäftigten bleiben im Übrigen unberührt.

§ 18
Personal- und Sachausstattung

(1) Der oder dem Hessischen Datenschutzbeauftragten ist die für die Erfüllung ihrer oder seiner Aufgaben notwendige Personal- und Sachausstattung zur Verfügung zu stellen. Sie ist im Einzelplan des Landtags in einem eigenen Kapitel auszuweisen. Die Präsidentin oder der Präsident des Landtags nimmt die Personal- und Sachausstattung nach Auswahl der oder des Hessischen Datenschutzbeauftragten vor.

(2) Die Beamtinnen und Beamten werden von der oder dem Hessischen Datenschutzbeauftragten ausgewählt und auf deren oder dessen Vorschlag durch die Präsidentin oder den Präsidenten des Landtags ernannt. Ihre Dienstvorgesetzte oder ihr Dienstvorgesetzter ist die oder der Hessische Datenschutzbeauftragte, an deren oder dessen Weisungen sie ausschließlich gebunden sind. Die oder der Hessische Datenschutzbeauftragte übt für die bei ihr oder ihm tätigen Beamtinnen und Beamten die Aufgaben der obersten Dienstbehörde nach dem Hessischen Disziplinargesetz aus. Für sonstige Beschäftigte gelten Satz 1 und 2 entsprechend.

Fünfter Abschnitt
Rechtsbehelfe

§ 19
Gerichtlicher Rechtsschutz

(1) Für Streitigkeiten zwischen einer natürlichen oder einer juristischen Person und der oder dem Hessischen Datenschutzbeauftragten über Rechte nach Art. 78 Abs. 1 und 2 der Verordnung (EU) Nr. 2016/679 sowie § 56 ist der Verwaltungsrechtsweg gegeben. Satz 1 gilt nicht für Bußgeldverfahren.

(2) Für Verfahren nach Abs. 1 Satz 1 findet § 20 Abs. 2, 3, 5 und 7 des Bundesdatenschutzgesetzes entsprechende Anwendung.

(3) In Verfahren nach Abs. 1 Satz 1 ist die oder der Hessische Datenschutzbeauftragte beteiligungsfähig.

(4) Für Klagen betroffener Personen gegen einen Verantwortlichen oder einen Auftragsverarbeiter wegen eines Verstoßes gegen datenschutzrechtliche Bestimmungen im Anwendungsbereich der Verordnung (EU) Nr. 2016/679 oder der darin enthaltenen Rechte der betroffenen Person findet § 44 des Bundesdatenschutzgesetzes entsprechende Anwendung.

(5) Behörden und sonstige öffentliche Stellen des Landes können unbeschadet anderer Rechtsbehelfe gerichtlich gegen sie betreffende verbindliche Entscheidungen der oder des Hessischen Datenschutzbeauftragten vorgehen. Geht die Behörde oder sonstige öffentliche Stelle des Landes nicht innerhalb eines Monats nach Bekanntgabe der verbindlichen Entscheidung der oder des Hessischen Datenschutzbeauftragten gerichtlich gegen diese vor, kann die oder der Hessische Datenschutzbeauftragte die gerichtliche Feststellung der Rechtmäßigkeit der getroffenen verbindlichen Entscheidung beantragen.

(6) Die Klage einer Behörde oder sonstigen öffentlichen Stelle des Landes gegen eine verbindliche Entscheidung der oder des Hessischen Datenschutzbeauftragten nach Art. 58 Abs. 2 Buchst. g der Verordnung (EU) Nr. 2016/679 oder § 14 Abs. 3 Nr. 4 hat aufschiebende Wirkung.

ZWEITER TEIL
Durchführungsbestimmungen für Verarbeitungen zu Zwecken nach Artikel 2 der Verordnung (EU) Nr. 2016/679

Erster Abschnitt
Rechtsgrundlagen der Verarbeitung personenbezogener Daten

Erster Titel
Verarbeitung personenbezogener Daten und Verarbeitung zu anderen Zwecken

§ 20
Verarbeitung besonderer Kategorien personenbezogener Daten

(1) Abweichend von Art. 9 Abs. 1 der Verordnung (EU) Nr. 2016/679 ist die Verarbeitung besonderer Kategorien personenbezogener Daten im Sinne des Art. 9 Abs. 1 der Verordnung (EU) Nr. 2016/679 durch öffentliche Stellen zulässig, wenn sie

1. erforderlich ist, um die aus dem Recht der sozialen Sicherheit und des Sozialschutzes erwachsenden Rechte auszuüben und den diesbezüglichen Pflichten nachzukommen,
2. zum Zweck der Gesundheitsvorsorge, für die Beurteilung der Arbeitsfähigkeit der Beschäftigten, für die medizinische Diagnostik, die Versorgung oder Behandlung im Gesundheits- oder Sozialbereich oder für die Verwaltung von Systemen und Diensten im Gesundheits- und Sozialbereich oder aufgrund eines Vertrags der betroffenen Person mit einem Angehörigen eines Gesundheitsberufs erforderlich ist, und diese Daten von ärztlichem Personal oder durch sonstige Personen, die einer entsprechenden Geheimhaltungspflicht unterliegen, oder unter deren Verantwortung verarbeitet werden, oder
3. aus Gründen des öffentlichen Interesses im Bereich der öffentlichen Gesundheit, wie dem Schutz vor schwerwiegenden grenzüberschreitenden Gesundheitsgefahren oder zur Gewährleistung hoher Qualitäts- und Sicherheitsstandards bei der Gesundheitsversorgung und bei Arzneimitteln und Medizinprodukten erforderlich ist; ergänzend zu den in Abs. 2 genannten Maßnahmen sind insbesondere die berufsrechtlichen und strafrechtlichen Vorgaben zur Wahrung des Berufsgeheimnisses einzuhalten,
4. a) aus Gründen eines erheblichen öffentlichen Interesses unbedingt erforderlich ist,
   b) zur Abwehr einer erheblichen Gefahr für die öffentliche Sicherheit erforderlich ist oder
   c) aus zwingenden Gründen der Verteidigung oder für humanitäre Maßnahmen erforderlich ist

und soweit die Interessen des Verantwortlichen an der Datenverarbeitung die Interessen der betroffenen Person überwiegen.

(2) In den Fällen des Abs. 1 sind angemessene und spezifische Maßnahmen zur Wahrung der Interessen der betroffenen Person vorzusehen. Unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere der mit der Verarbeitung verbundenen Risiken für die Rechte und Freiheiten natürlicher Personen können dazu insbesondere gehören:

1. technische und organisatorische Maßnahmen, um sicherzustellen, dass die Verarbeitung nach der Verordnung (EU) Nr. 2016/679 erfolgt,
2. Maßnahmen, die gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten eingegeben, verändert oder entfernt worden sind,
3. Sensibilisierung der an Verarbeitungsvorgängen Beteiligten,
4. Benennung einer oder eines Datenschutzbeauftragten,
5. Beschränkung des Zugangs zu den personenbezogenen Daten innerhalb der verantwortlichen Stelle und von Auftragsverarbeitern,
6. Pseudonymisierung personenbezogener Daten,
7. Verschlüsselung personenbezogener Daten,
8. Sicherstellung der Fähigkeit, Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung personenbezogener Daten, einschließlich der Fähigkeit, die Verfügbarkeit und den Zugang bei einem physischen oder technischen Zwischenfall rasch wiederherzustellen,

9. zur Gewährleistung der Sicherheit der Verarbeitung die Einrichtung eines Verfahrens zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen oder
10. spezifische Verfahrensregelungen, die im Fall einer Übermittlung oder Verarbeitung für andere Zwecke die Einhaltung der Vorgaben dieses Gesetzes sowie der Verordnung (EU) Nr. 2016/679 sicherstellen.

(3) Werden personenbezogene Daten nicht automatisiert verarbeitet, sind insbesondere Maßnahmen zu treffen, um den Zugriff Unbefugter bei der Bearbeitung, der Aufbewahrung, dem Transport und der Vernichtung zu verhindern.

§ 21
Verarbeitung zu anderen Zwecken

(1) Die Verarbeitung personenbezogener Daten zu einem anderen Zweck als zu demjenigen, zu dem die Daten erhoben wurden, durch öffentliche Stellen im Rahmen ihrer Aufgabenerfüllung ist zulässig, wenn

1. offensichtlich ist, dass sie im Interesse der betroffenen Person liegt und kein Grund zu der Annahme besteht, dass sie in Kenntnis des anderen Zwecks ihre Einwilligung verweigern würde,
2. Angaben der betroffenen Person überprüft werden müssen, weil tatsächliche Anhaltspunkte für deren Unrichtigkeit bestehen,
3. sie zur Abwehr erheblicher Nachteile für das Gemeinwohl oder einer Gefahr für die öffentliche Sicherheit oder Ordnung, die Verteidigung oder die nationale Sicherheit, zur Wahrung erheblicher Belange des Gemeinwohls oder zur Sicherung des Steuer- oder Zollaufkommens erforderlich ist,
4. sie zur Verfolgung von Straftaten oder Ordnungswidrigkeiten, zur Vollstreckung oder zum Vollzug von Strafen oder Maßnahmen im Sinne des § 11 Abs. 1 Nr. 8 des Strafgesetzbuchs oder von Erziehungsmaßregeln oder Zuchtmitteln im Sinne des Jugendgerichtsgesetzes oder zur Vollstreckung von Geldbußen erforderlich ist,
5. sie zur Abwehr einer schwerwiegenden Beeinträchtigung der Rechte und Freiheiten einer anderen Person erforderlich ist oder
6. sie der Wahrnehmung von Aufsichts- und Kontrollbefugnissen, der Rechnungsprüfung oder der Durchführung von Organisationsuntersuchungen des Verantwortlichen dient; dies gilt auch für die Verarbeitung zu Ausbildungs- und Prüfungszwecken durch den Verantwortlichen, soweit schutzwürdige Interessen der betroffenen Person dem nicht entgegenstehen.

(2) Die Verarbeitung besonderer Kategorien personenbezogener Daten im Sinne des Art. 9 Abs. 1 der Verordnung (EU) Nr. 2016/679 zu einem anderen Zweck als zu demjenigen, zu dem die Daten erhoben wurden, ist zulässig, wenn die Voraussetzungen des Abs. 1 und ein Ausnahmetatbestand nach Art. 9 Abs. 2 der Verordnung (EU) Nr. 2016/679 oder nach § 20 Abs. 1 vorliegen.

(3) Personenbezogene Daten, die ausschließlich zu Zwecken der Datenschutzkontrolle, der Datensicherung oder zur Sicherstellung des ordnungsgemäßen Betriebs einer Datenverarbeitungsanlage verarbeitet werden, dürfen nicht für andere Zwecke verarbeitet werden.

§ 22
Datenübermittlungen durch öffentliche Stellen

(1) Die Übermittlung personenbezogener Daten durch öffentliche Stellen an öffentliche Stellen ist zulässig, wenn sie zur Erfüllung der in der Zuständigkeit der übermittelnden Stelle oder des Dritten, an den die Daten übermittelt werden, liegenden Aufgaben erforderlich ist und die Voraussetzungen vorliegen, die eine Verarbeitung nach § 21 zulassen würden. Der Dritte, an den die Daten übermittelt werden, darf diese nur für den Zweck verarbeiten, zu dessen Erfüllung sie ihm übermittelt werden. Eine Verarbeitung für andere Zwecke ist unter den Voraussetzungen des § 21 zulässig.

(2) Die Übermittlung personenbezogener Daten durch öffentliche Stellen an nicht öffentliche Stellen ist zulässig, wenn

1. sie zur Erfüllung der in der Zuständigkeit der übermittelnden Stelle liegenden Aufgaben erforderlich ist und die Voraussetzungen vorliegen, die eine Verarbeitung nach § 21 zulassen würden,

2. der Dritte, an den die Daten übermittelt werden, ein berechtigtes Interesse an der Kenntnis der zu übermittelnden Daten glaubhaft darlegt und die betroffene Person kein schutzwürdiges Interesse an dem Ausschluss der Übermittlung hat oder

3. es zur Geltendmachung, Ausübung oder Verteidigung rechtlicher Ansprüche erforderlich ist

und der Dritte sich gegenüber der übermittelnden öffentlichen Stelle verpflichtet hat, die Daten nur für den Zweck zu verarbeiten, zu dessen Erfüllung sie ihm übermittelt werden. Eine Verarbeitung für andere Zwecke ist zulässig, wenn eine Übermittlung nach Satz 1 zulässig wäre und die übermittelnde Stelle zugestimmt hat.

(3) Die Übermittlung besonderer Kategorien personenbezogener Daten im Sinne des Art. 9 Abs. 1 der Verordnung (EU) Nr. 2016/679 ist zulässig, wenn die Voraussetzungen des Abs. 1 oder 2 und ein Ausnahmetatbestand nach Art. 9 Abs. 2 der Verordnung (EU) Nr. 2016/679 oder nach § 20 Abs. 1 vorliegen.

(4) Die Verantwortung für die Zulässigkeit der Übermittlung trägt die übermittelnde Stelle. Ist die Übermittlung zur Erfüllung von Aufgaben eines in § 2 Abs. 1 und 3 genannten Empfängers erforderlich, so trägt auch dieser hierfür die Verantwortung und hat sicherzustellen, dass die Erforderlichkeit nachträglich überprüft werden kann. Die übermittelnde Stelle hat in diesem Fall die Zuständigkeit des Empfängers und die Schlüssigkeit der Anfrage zu überprüfen. Bestehen im Einzelfall Zweifel an der Schlüssigkeit, so hat sie darüber hinaus die Erforderlichkeit zu überprüfen. Der Empfänger hat der übermittelnden Stelle die für ihre Prüfung erforderlichen Angaben zu machen.

Zweiter Titel
Besondere Verarbeitungssituationen

§ 23
Datenverarbeitung für Zwecke des Beschäftigungsverhältnisses

(1) Personenbezogene Daten von Beschäftigten dürfen für Zwecke des Beschäftigungsverhältnisses verarbeitet werden, wenn dies für die Entscheidung über die Begründung eines Beschäftigungsverhältnisses oder nach Begründung des Beschäftigungsverhältnisses für dessen Durchführung, Beendigung oder Abwicklung sowie zur Durchführung innerdienstlicher planerischer, organisatorischer, sozialer und personeller Maßnahmen erforderlich ist. Dies gilt auch zur Ausübung oder Erfüllung der sich aus einem Gesetz oder einem Tarifvertrag, einer Betriebs- oder Dienstvereinbarung (Kollektivvereinbarung) ergebenden Rechte und Pflichten der Interessenvertretung der Beschäftigten. Zur Aufdeckung von Straftaten dürfen personenbezogene Daten von Beschäftigten nur dann verarbeitet werden, wenn zu dokumentierende tatsächliche Anhaltspunkte den Verdacht begründen, dass die betroffene Person im Beschäftigungsverhältnis eine Straftat begangen hat, die Verarbeitung zur Aufdeckung erforderlich ist und das schutzwürdige Interesse der oder des Beschäftigten an dem Ausschluss der Verarbeitung nicht überwiegt, insbesondere Art und Ausmaß im Hinblick auf den Anlass nicht unverhältnismäßig sind.

(2) Erfolgt die Verarbeitung personenbezogener Daten von Beschäftigten auf der Grundlage einer Einwilligung, so sind für die Beurteilung der Freiwilligkeit der Einwilligung insbesondere die im Beschäftigungsverhältnis bestehende Abhängigkeit der beschäftigten Person sowie die Umstände, unter denen die Einwilligung erteilt worden ist, zu berücksichtigen. Freiwilligkeit kann insbesondere vorliegen, wenn für die beschäftigte Person ein rechtlicher oder wirtschaftlicher Vorteil erreicht wird oder Dienstherr oder Arbeitgeber und beschäftigte Person gleichgelagerte Interessen verfolgen. Die Einwilligung bedarf der Schriftform, soweit nicht wegen besonderer Umstände eine andere Form angemessen ist. Der Dienstherr oder Arbeitgeber hat die beschäftigte Person über den Zweck der Datenverarbeitung und über ihr Widerrufsrecht nach Art. 7 Abs. 3 der Verordnung (EU) Nr. 2016/679 in Textform aufzuklären.

(3) Abweichend von Art. 9 Abs. 1 der Verordnung (EU) Nr. 2016/679 ist die Verarbeitung besonderer Kategorien personenbezogener Daten im Sinne des Art. 9 Abs. 1 der Verordnung (EU) Nr. 2016/679 für Zwecke des Beschäftigungsverhältnisses zulässig, wenn sie zur Ausübung von Rechten oder zur Erfüllung rechtlicher Pflichten aus dem Arbeitsrecht, dem Recht der sozialen Sicherheit und des Sozialschutzes erforderlich ist und kein Grund zu der Annahme besteht, dass das schutzwürdige Interesse der betroffenen Person an dem Ausschluss der Verarbeitung überwiegt. Abs. 2 gilt auch für die Einwilligung in die Verarbeitung besonderer Kategorien personenbezogener Daten; die Einwilligung muss sich dabei ausdrücklich auf diese Daten beziehen. § 20 Abs. 2 gilt entsprechend.

(4) Die Verarbeitung personenbezogener Daten einschließlich besonderer Kategorien personenbezogener Daten von Beschäftigten für Zwecke des Beschäftigungsverhältnisses ist auf der Grundlage von Kollektivvereinbarungen zulässig. Dabei haben die Verhandlungspartner Art. 88 Abs. 2 der Verordnung (EU) Nr. 2016/679 zu beachten.

(5) Der Verantwortliche muss geeignete Maßnahmen ergreifen um sicherzustellen, dass insbesondere die in Art. 5 der Verordnung (EU) Nr. 2016/679 dargelegten Grundsätze für die Verarbeitung personenbezogener Daten eingehalten werden.

(6) Die Beteiligungsrechte der Interessenvertretungen der Beschäftigten bleiben unberührt.

(7) Die Abs. 1 bis 6 sind auch anzuwenden, wenn personenbezogene Daten, einschließlich besonderer Kategorien personenbezogener Daten, von Beschäftigten verarbeitet werden, ohne dass sie in einem Dateisystem gespeichert sind oder gespeichert werden sollen. Die für das Personalaktenrecht geltenden Vorschriften des Hessischen Beamtengesetzes sind, soweit tarifvertraglich nichts Abweichendes geregelt ist, auf Arbeitnehmerinnen und Arbeitnehmer im öffentlichen Dienst entsprechend anzuwenden.

(8) Beschäftigte im Sinne dieses Gesetzes sind:

1. Arbeitnehmerinnen und Arbeitnehmer, einschließlich der Leiharbeitnehmerinnen und Leiharbeitnehmer im Verhältnis zum Entleiher,
2. zu ihrer Berufsausbildung Beschäftigte,
3. Teilnehmerinnen und Teilnehmer an Leistungen zur Teilhabe am Arbeitsleben sowie an Abklärungen der beruflichen Eignung oder Arbeitserprobung (Rehabilitandinnen und Rehabilitanden),
4. in anerkannten Werkstätten für behinderte Menschen Beschäftigte,
5. Freiwillige, die einen Dienst nach dem Jugendfreiwilligendienstegesetz vom 16. Mai 2008 (BGBl. I S. 842), geändert durch Gesetz vom 20. Dezember 2011 (BGBl. I S. 2854), oder dem Bundesfreiwilligendienstgesetz vom 28. April 2011 (BGBl. I S. 687), zuletzt geändert durch Gesetz vom 20. Oktober 2015 (BGBl. I S. 1722), leisten,
6. Personen, die wegen ihrer wirtschaftlichen Unselbständigkeit als arbeitnehmerähnliche Personen anzusehen sind; zu diesen gehören auch die in Heimarbeit Beschäftigten und die ihnen Gleichgestellten,
7. Beamtinnen und Beamte im Geltungsbereich des Hessischen Beamtengesetzes, Richterinnen und Richter des Landes sowie Zivildienstleistende.

Bewerberinnen und Bewerber für ein Beschäftigungsverhältnis sowie Personen, deren Beschäftigungsverhältnis beendet ist, gelten als Beschäftigte.

§ 24
Datenverarbeitung zu wissenschaftlichen oder historischen Forschungszwecken und zu statistischen Zwecken

(1) Abweichend von Art. 9 Abs. 1 der Verordnung (EU) Nr. 2016/679 ist die Verarbeitung besonderer Kategorien personenbezogener Daten im Sinne des Art. 9 Abs. 1 der Verordnung (EU) Nr. 2016/679 auch ohne Einwilligung für wissenschaftliche oder historische Forschungszwecke oder für statistische Zwecke zulässig, wenn die Verarbeitung zu diesen Zwecken erforderlich ist und die Interessen des Verantwortlichen an der Verarbeitung die Interessen der betroffenen Person an einem Ausschluss der Verarbeitung überwiegen. Der Verantwortliche sieht angemessene und spezifische Maßnahmen zur Wahrung der Interessen der betroffenen Person nach § 20 Abs. 2 Satz 2 vor.

(2) Die in den Art. 15, 16, 18 und 21 der Verordnung (EU) Nr. 2016/679 vorgesehenen Rechte der betroffenen Person sind insoweit beschränkt, als diese Rechte voraussichtlich die Verwirklichung der Forschungs- oder Statistikzwecke unmöglich machen oder ernsthaft beeinträchtigen und die Beschränkung für die Erfüllung der Forschungs- oder Statistikzwecke notwendig ist. Das Recht auf Auskunft nach Art. 15 der Verordnung (EU) Nr. 2016/679 besteht darüber hinaus nicht, wenn die Daten für Zwecke der wissenschaftlichen Forschung erforderlich sind und die Auskunftserteilung einen unverhältnismäßigen Aufwand erfordern würde.

(3) Ergänzend zu den in § 20 Abs. 2 genannten Maßnahmen sind zu wissenschaftlichen oder historischen Forschungszwecken oder zu statistischen Zwecken verarbeitete besondere Kategorien personenbezogener Daten im Sinne des Art. 9 Abs. 1 der Verordnung (EU) Nr. 2016/679 zu anonymisieren, sobald dies nach dem Forschungs- oder Statistikzweck möglich ist, es sei denn, berechtigte Interessen der betroffenen Person stehen dem entgegen. Sobald der Forschungs- oder Statistikzweck dies erlaubt, sind die Merkmale, mit deren Hilfe ein Personenbezug hergestellt werden kann, gesondert zu speichern; die Merkmale sind zu löschen, sobald der Forschungs- oder Statistikzweck dies zulässt.

(4) Der Verantwortliche darf personenbezogene Daten zu wissenschaftlichen oder historischen Forschungszwecken nur veröffentlichen, wenn die betroffene Person eingewilligt hat oder dies

für die Darstellung von Forschungsergebnissen über Ereignisse der Zeitgeschichte unerlässlich ist.

§ 25
Datenverarbeitung zu im öffentlichen Interesse liegenden Archivzwecken

(1) Abweichend von Art. 9 Abs. 1 der Verordnung (EU) Nr. 2016/679 ist die Verarbeitung besonderer Kategorien personenbezogener Daten im Sinne des Art. 9 Abs. 1 der Verordnung (EU) Nr. 2016/679 zulässig, wenn sie für im öffentlichen Interesse liegende Archivzwecke erforderlich ist. Der Verantwortliche sieht angemessene und spezifische Maßnahmen zur Wahrung der Interessen der betroffenen Person nach § 20 Abs. 2 Satz 2 vor.

(2) Das Recht auf Auskunft der betroffenen Person nach Art. 15 der Verordnung (EU) Nr. 2016/679 besteht nicht, wenn das Archivgut nicht durch den Namen der Person erschlossen ist oder keine Angaben gemacht werden, die das Auffinden des betreffenden Archivguts mit vertretbarem Verwaltungsaufwand ermöglichen.

(3) Das Recht auf Berichtigung der betroffenen Person nach Art. 16 der Verordnung (EU) Nr. 2016/679 besteht nicht, wenn die personenbezogenen Daten zu Archivzwecken im öffentlichen Interesse verarbeitet werden. Bestreitet die betroffene Person die Richtigkeit der personenbezogenen Daten, ist ihr die Möglichkeit einer Gegendarstellung einzuräumen. Das zuständige Archiv ist verpflichtet, die Gegendarstellung den Unterlagen hinzuzufügen.

(4) Die in Art. 18 Abs. 1 Buchst. a, b und d, Art. 20 und 21 der Verordnung (EU) Nr. 2016/679 vorgesehenen Rechte bestehen nicht, soweit diese Rechte voraussichtlich die Verwirklichung der im öffentlichen Interesse liegenden Archivzwecke unmöglich machen oder ernsthaft beeinträchtigen und die Ausnahmen für die Erfüllung dieser Zwecke erforderlich sind.

§ 26
Rechte der betroffenen Person und aufsichtsbehördliche Untersuchungen im Fall von Geheimhaltungspflichten

(1) Die Pflicht zur Information der betroffenen Person nach Art. 14 Abs. 1 bis 4 der Verordnung (EU) Nr. 2016/679 besteht ergänzend zu den in Art. 14 Abs. 5 der Verordnung (EU) Nr. 2016/679 genannten Ausnahmen nicht, soweit durch ihre Erfüllung Informationen offenbart würden, die ihrem Wesen nach, insbesondere wegen der überwiegenden berechtigten Interessen eines Dritten, geheim gehalten werden müssen.

(2) Das Recht auf Auskunft der betroffenen Person nach Art. 15 der Verordnung Nr. 2016/679 besteht nicht, soweit durch die Auskunft Informationen offenbart würden, die nach einer Rechtsvorschrift oder ihrem Wesen nach, insbesondere wegen der überwiegenden berechtigten Interessen eines Dritten, geheim gehalten werden müssen.

(3) Die Pflicht zur Benachrichtigung nach Art. 34 der Verordnung (EU) Nr. 2016/679 besteht ergänzend zu der in Art. 34 Abs. 3 der Verordnung (EU) Nr. 2016/679 genannten Ausnahme nicht, soweit durch die Benachrichtigung Informationen offenbart würden, die nach einer Rechtsvorschrift oder ihrem Wesen nach, insbesondere wegen der überwiegenden berechtigten Interessen eines Dritten, geheim gehalten werden müssen. Abweichend von der Ausnahme nach Satz 1 ist die betroffene Person nach Art. 34 der Verordnung (EU) Nr. 2016/679 zu benachrichtigen, wenn die Interessen der betroffenen Person, insbesondere unter Berücksichtigung drohender Schäden, gegenüber dem Geheimhaltungsinteresse überwiegen.

(4) Werden Daten Dritter im Zuge der Aufnahme oder im Rahmen eines Mandatsverhältnisses an einen Berufsgeheimnisträger übermittelt, so besteht die Pflicht der übermittelnden Stelle zur Information der betroffenen Person nach Art. 13 Abs. 3 der Verordnung (EU) Nr. 2016/679 nicht, sofern nicht das Interesse der betroffenen Person an der Informationserteilung überwiegt.

(5) Erlangt die oder der Hessische Datenschutzbeauftragte oder ihre oder seine Beschäftigten im Rahmen einer Untersuchung Kenntnis von Daten, die nach einer Rechtsvorschrift oder ihrem Wesen nach einer Geheimhaltungspflicht unterliegen, gilt diese auch für sie.

§ 27
Datenübermittlung an öffentlich-rechtliche Religionsgemeinschaften

Die Übermittlung personenbezogener Daten an Stellen der öffentlich-rechtlichen Religionsgemeinschaften ist in entsprechender Anwendung der Vorschriften über die Übermittlung an öffentliche Stellen nur zulässig, sofern auf Grundlage geeigneter Garantien sichergestellt ist, dass bei der empfangenden Stelle eine Datenverarbeitung im Einklang mit der Verordnung (EU) Nr. 2016/679 erfolgt.

§ 28
Datenverarbeitung des Hessischen Rundfunks zu journalistischen Zwecken

(1) Führt die journalistische Verarbeitung personenbezogener Daten zur Veröffentlichung von Gegendarstellungen der betroffenen Personen, so sind diese Gegendarstellungen zu den gespeicherten Daten zu nehmen und für dieselbe Zeitdauer aufzubewahren wie die Daten selbst.

(2) Der Rundfunkrat bestellt eine Beauftragte oder einen Beauftragten für den Datenschutz, die oder der die Ausführung von Abs. 1 sowie anderer Vorschriften über den Datenschutz im journalistischen Bereich frei von Weisungen überwacht. An sie oder ihn kann sich jede Person wenden, wenn sie annimmt, bei der Verarbeitung personenbezogener Daten zu journalistischen Zwecken in ihren Rechten verletzt worden zu sein. Beanstandungen richtet die oder der Beauftragte für den Datenschutz an die Intendantin oder den Intendanten und unterrichtet gleichzeitig den Rundfunkrat. Die Dienstaufsicht obliegt dem Verwaltungsrat.

(3) Der oder dem nach Abs. 2 zu bestellenden Beauftragten für den Datenschutz können auch die Aufgaben nach § 7 zugewiesen werden.

Dritter Titel
Rechte des Landtags und der kommunalen Vertretungsorgane

§ 29
Auskunftsrecht des Landtags und der kommunalen Vertretungsorgane

(1) Die Hessische Zentrale für Datenverarbeitung, die Kommunalen Gebietsrechenzentren und die öffentlichen Stellen des Landes, die Datenverarbeitungsanlagen und -geräte betreiben, sind verpflichtet, dem Landtag, der Präsidentin oder dem Präsidenten des Landtags und den Fraktionen des Landtags die von diesen im Rahmen ihrer Zuständigkeit verlangten Auskünfte aufgrund der gespeicherten Daten zu geben, soweit Programme zur Auswertung vorhanden sind. Die Auskünfte dürfen keine personenbezogenen Daten enthalten. Den Auskünften darf ein gesetzliches Verbot oder ein öffentliches Interesse nicht entgegenstehen. Dem Auskunftsrecht des Landtags steht ein öffentliches Interesse in der Regel nicht entgegen. Der Landtag hat Zugriff auf die Daten, soweit durch technische Maßnahmen sichergestellt ist, dass die Grenzen von Satz 1 bis 3 eingehalten werden.

(2) Der Landtag kann von der Landesregierung Auskünfte über die bestehenden Verfahren verlangen, die für Auskünfte oder den Zugriff nach Abs. 1 geeignet sind. Das Auskunftsverlangen kann sich erstrecken auf

1. den Namen des Verfahrens mit kurzer Funktionsbeschreibung,
2. die vorhandenen Verfahren,
3. den Aufbau der Datensätze mit Angaben über den Inhalt und die Ordnungskriterien,
4. die vorhandenen Auswertungsprogramme,
5. die zuständige Behörde.

(3) Das Auskunftsrecht nach Abs. 1 steht im Rahmen ihrer Zuständigkeiten den Gemeindevertretungen und den Kreistagen sowie deren Fraktionen und den entsprechenden Organen der anderen in § 2 Abs. 1 genannten öffentlichen Stellen gegenüber der Hessischen Zentrale für Datenverarbeitung, dem zuständigen Kommunalen Gebietsrechenzentrum und den Behörden der Gemeinden und Landkreise zu, die Datenverarbeitungsanlagen und -geräte betreiben. Anträge der Fraktionen sind in den Gemeinden über den Gemeindevorstand, in den Kreisen über den Kreisausschuss zu leiten.

§ 30
Verarbeitung personenbezogener Daten durch den Landtag
und die kommunalen Vertretungsorgane

(1) Mit Ausnahme der §§ 15 und 29 gelten die Vorschriften dieses Gesetzes für den Landtag nur, soweit er in Verwaltungsangelegenheiten tätig wird, insbesondere wenn es sich um die wirtschaftlichen Angelegenheiten des Landtags, die Personalverwaltung oder die Ausführung von gesetzlichen Vorschriften, deren Vollzug der Präsidentin oder dem Präsidenten des Landtags zugewiesen ist, handelt. Im Übrigen gibt sich der Landtag eine seiner verfassungsrechtlichen Stellung entsprechende Datenschutzordnung. Sie findet auf die für die Fraktionen und Abgeordneten tätigen Personen entsprechende Anwendung.

(2) Die Landesregierung darf personenbezogene Daten, die für andere Zwecke erhoben worden sind, zur Beantwortung parlamentarischer Anfragen sowie zur Vorlage von Unterlagen und Berichten im Rahmen der Geschäftsordnung des Landtags in dem dafür erforderlichen Umfang

verwenden. Dies gilt nicht, wenn die Übermittlung der Daten wegen ihres streng persönlichen Charakters für die Betroffenen unzumutbar ist. Besondere gesetzliche Übermittlungsverbote bleiben unberührt.

(3) Von der Landesregierung übermittelte personenbezogene Daten dürfen nicht in Landtagsdrucksachen aufgenommen oder in sonstiger Weise allgemein zugänglich gemacht werden. Dies gilt nicht, wenn keine Anhaltspunkte dafür bestehen, dass schutzwürdige Belange der Betroffenen beeinträchtigt werden.

(4) Abs. 2 gilt entsprechend für die Verwaltungsbehörden der Gemeinden und Landkreise im Rahmen ihrer jeweiligen Auskunftspflichten nach der Hessischen Gemeindeordnung und der Hessischen Landkreisordnung.

Zweiter Abschnitt
Rechte der betroffenen Person

§ 31
Informationspflicht bei Erhebung von personenbezogenen Daten bei der betroffenen Person

(1) Die Pflicht zur Information der betroffenen Person nach Art. 13 Abs. 3 der Verordnung (EU) Nr. 2016/679 besteht ergänzend zu der in Art. 13 Abs. 4 der Verordnung (EU) Nr. 2016/679 genannten Ausnahme dann nicht, wenn die Erteilung der Information über die beabsichtigte Weiterverarbeitung

1. eine Weiterverarbeitung analog gespeicherter Daten betrifft, bei der sich der Verantwortliche durch die Weiterverarbeitung unmittelbar an die betroffene Person wendet, der Zweck mit dem Erhebungszweck nach der Verordnung (EU) Nr. 2016/679 vereinbar ist, die Kommunikation mit der betroffenen Person nicht in digitaler Form erfolgt und das Interesse der betroffenen Person an der Informationserteilung nach den Umständen des Einzelfalls, insbesondere mit Blick auf den Zusammenhang, in dem die Daten erhoben wurden, als gering anzusehen ist,
2. a) die ordnungsgemäße Erfüllung der in der Zuständigkeit des Verantwortlichen liegenden Aufgaben im Sinne des Art. 23 Abs. 1 Buchst. a bis e der Verordnung (EU) Nr. 2016/679 gefährden,
   b) die öffentliche Sicherheit oder Ordnung gefährden,
   c) die Rechte oder Freiheiten Dritter gefährden,
   d) die Geltendmachung, Ausübung oder Verteidigung rechtlicher Ansprüche beeinträchtigen oder
   e) sonst dem Wohle des Bundes oder eines Landes Nachteile bereiten

   würde und das Interesse des Verantwortlichen an der Nichterteilung der Information das Informationsinteresse der betroffenen Person überwiegt oder
3. eine vertrauliche Übermittlung von Daten an öffentliche Stellen gefährden würde.

Die Entscheidung trifft die Leitung der öffentlichen Stelle oder eine von ihr bestimmte, bei der öffentlichen Stelle beschäftigte Person.

(2) Unterbleibt eine Information der betroffenen Person nach Maßgabe des Abs. 1, ergreift der Verantwortliche geeignete Maßnahmen zum Schutz der berechtigten Interessen der betroffenen Person, einschließlich der Bereitstellung der in Art. 13 Abs. 1 und 2 der Verordnung (EU) Nr. 2016/679 genannten Informationen für die Öffentlichkeit in präziser, transparenter, verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache. Der Verantwortliche hält schriftlich fest, aus welchen Gründen er von einer Information abgesehen hat. Satz 1 und 2 finden in den Fällen des Abs. 1 Satz 1 Nr. 2 Buchst. d und Nr. 3 keine Anwendung.

(3) Unterbleibt eine Information der betroffenen Person nach Maßgabe des Abs. 1 wegen eines vorübergehenden Hinderungsgrundes, kommt der Verantwortliche der Informationspflicht unter Berücksichtigung der spezifischen Umstände der Verarbeitung innerhalb einer angemessenen Frist nach Fortfall des Hinderungsgrundes, spätestens jedoch innerhalb von zwei Wochen, nach.

§ 32
Informationspflicht, wenn die personenbezogenen Daten nicht bei der betroffenen Person erhoben wurden

(1) Die Pflicht zur Information der betroffenen Person nach Art. 14 Abs. 1, 2 und 4 der Verordnung (EU) Nr. 2016/679 besteht ergänzend zu den in Art. 14 Abs. 5 der Verordnung (EU) Nr. 2016/679 und § 26 Abs. 1 genannten Ausnahmen nicht, wenn die Erteilung der Information

1. die ordnungsgemäße Erfüllung der in der Zuständigkeit des Verantwortlichen liegenden Aufgaben im Sinne des Art. 23 Abs. 1 Buchst. a bis e der Verordnung (EU) Nr. 2016/679 gefährden,
2. die öffentliche Sicherheit oder Ordnung gefährden,
3. die Rechte oder Freiheiten Dritter gefährden oder
4. sonst dem Wohle des Bundes oder eines Landes Nachteile bereiten

würde und das Interesse des Verantwortlichen an der Nichterteilung der Information das Informationsinteresse der betroffenen Person überwiegt. Die Entscheidung trifft die Leitung der öffentlichen Stelle oder eine von ihr bestimmte, bei der öffentlichen Stelle beschäftigte Person.

(2) Unterbleibt eine Information der betroffenen Person nach Maßgabe des Abs. 1, ergreift der Verantwortliche geeignete Maßnahmen zum Schutz der berechtigten Interessen der betroffenen Person, einschließlich der Bereitstellung der in Art. 14 Abs. 1 und 2 der Verordnung (EU) Nr. 2016/679 genannten Informationen für die Öffentlichkeit in präziser, transparenter, verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache. Der Verantwortliche hält schriftlich fest, aus welchen Gründen er von einer Information abgesehen hat.

(3) Bezieht sich die Informationserteilung auf die Übermittlung personenbezogener Daten durch öffentliche Stellen an Verfassungsschutzbehörden, den Bundesnachrichtendienst, den Militärischen Abschirmdienst und, soweit die Sicherheit des Bundes berührt wird, andere Behörden des Bundesministeriums der Verteidigung, ist sie nur mit Zustimmung dieser Stellen zulässig.

§ 33
Auskunftsrecht der betroffenen Person

(1) Das Recht auf Auskunft der betroffenen Person nach Art. 15 der Verordnung (EU) Nr. 2016/679 besteht ergänzend zu den in § 24 Abs. 2, § 25 Abs. 2 und § 26 Abs. 2 genannten Ausnahmen nicht, wenn

1. die betroffene Person nach § 32 Abs. 1 oder 3 nicht zu informieren ist, oder
2. die Daten
   a) nur deshalb gespeichert sind, weil sie aufgrund gesetzlicher oder satzungsmäßiger Aufbewahrungsvorschriften nicht gelöscht werden dürfen, oder
   b) ausschließlich Zwecken der Datensicherung, der Datenschutzkontrolle oder der Sicherstellung des ordnungsgemäßen Betriebs einer Datenverarbeitungsanlage dienen.

(2) Die Gründe der Auskunftsverweigerung sind zu dokumentieren. Die Ablehnung der Auskunftserteilung ist gegenüber der betroffenen Person zu begründen, soweit nicht durch die Mitteilung der tatsächlichen und rechtlichen Gründe, auf die die Entscheidung gestützt wird, der mit der Auskunftsverweigerung verfolgte Zweck gefährdet würde. Die zum Zweck der Auskunftserteilung an die betroffene Person und zu deren Vorbereitung gespeicherten Daten dürfen nur für diesen Zweck sowie für Zwecke der Datenschutzkontrolle verarbeitet werden; für andere Zwecke ist die Verarbeitung nach Maßgabe des Art. 18 der Verordnung (EU) Nr. 2016/679 einzuschränken.

(3) Wird der betroffenen Person keine Auskunft erteilt, kann sie ihr Auskunftsrecht auch über die Hessische Datenschutzbeauftragte oder den Hessischen Datenschutzbeauftragten ausüben. Der Verantwortliche hat die betroffene Person über diese Möglichkeit sowie darüber zu unterrichten, dass sie nach Art. 77 der Verordnung (EU) Nr. 2016/679 die oder den Hessischen Datenschutzbeauftragten anrufen oder gerichtlichen Rechtsschutz suchen kann. Die oder der Hessische Datenschutzbeauftragte hat die betroffene Person darüber zu unterrichten, dass alle erforderlichen Prüfungen erfolgt sind oder eine Überprüfung durch sie oder ihn stattgefunden hat. Die Mitteilung der oder des Hessischen Datenschutzbeauftragten an die betroffene Person darf keine Rückschlüsse auf den Erkenntnisstand des Verantwortlichen zulassen, sofern dieser keiner weitergehenden Auskunft zustimmt. Die oder der Hessische Datenschutzbeauftragte hat zudem die betroffene Person über ihr Recht auf gerichtlichen Rechtsschutz zu unterrichten.

(4) Das Recht der betroffenen Person auf Auskunft über personenbezogene Daten, die weder automatisiert verarbeitet noch nicht automatisiert verarbeitet und in einem Dateisystem gespeichert werden, besteht nur, soweit die betroffene Person Angaben macht, die das Auffinden der Daten ermöglichen, und der für die Erteilung der Auskunft erforderliche Aufwand nicht außer Verhältnis zu dem von der betroffenen Person geltend gemachten Informationsinteresse steht. Statt einer Auskunft über personenbezogene Daten kann der betroffenen Person Akteneinsicht gewährt werden.

§ 34
Recht auf Löschung ("Recht auf Vergessenwerden")

(1) Ist eine Löschung im Fall nicht automatisierter Datenverarbeitung wegen der besonderen Art der Speicherung nicht oder nur mit unverhältnismäßig hohem Aufwand möglich und ist das Interesse der betroffenen Person an der Löschung als gering anzusehen, besteht das Recht der betroffenen Person auf und die Pflicht des Verantwortlichen zur Löschung personenbezogener Daten nach Art. 17 Abs. 1 der Verordnung (EU) Nr. 2016/679 ergänzend zu den in Art. 17 Abs. 3 der Verordnung (EU) Nr. 2016/679 genannten Ausnahmen nicht. In diesem Fall tritt an die Stelle einer Löschung die Einschränkung der Verarbeitung nach Art. 18 der Verordnung (EU) Nr. 2016/679. Satz 1 und 2 finden keine Anwendung, wenn die personenbezogenen Daten unrechtmäßig verarbeitet wurden.

(2) Ergänzend zu Art. 18 Abs. 1 Buchst. b und c der Verordnung (EU) Nr. 2016/679 gilt Abs. 1 Satz 1 und 2 entsprechend im Fall des Art. 17 Abs. 1 Buchst. a und d der Verordnung (EU) Nr. 2016/679, solange und soweit der Verantwortliche Grund zu der Annahme hat, dass durch eine Löschung schutzwürdige Interessen der betroffenen Person beeinträchtigt würden. Der Verantwortliche unterrichtet die betroffene Person über die Einschränkung der Verarbeitung, sofern sich die Unterrichtung nicht als unmöglich erweist oder einen unverhältnismäßigen Aufwand erfordern würde.

(3) Ergänzend zu Art. 17 Abs. 3 Buchst. b der Verordnung (EU) Nr. 2016/679 gilt Abs. 1 entsprechend im Fall des Art. 17 Abs. 1 Buchst. a der Verordnung (EU) Nr. 2016/679, wenn einer Löschung satzungsmäßige Aufbewahrungsfristen entgegenstehen.

§ 35
Widerspruchsrecht

Das Recht auf Widerspruch nach Art. 21 Abs. 1 der Verordnung (EU) Nr. 2016/679 besteht nicht, soweit an der Verarbeitung ein zwingendes öffentliches Interesse besteht, das die Interessen der betroffenen Person überwiegt, oder eine Rechtsvorschrift zur Verarbeitung verpflichtet.

Dritter Abschnitt
Sanktionen

§ 36
Anwendung der Vorschriften über das Bußgeld- und Strafverfahren
bei Verstößen nach Artikel 83 der Verordnung (EU) Nr. 2016/679

(1) Für Verstöße nach Art. 83 Abs. 4 bis 6 der Verordnung (EU) Nr. 2016/679 gilt, soweit dieses Gesetz nichts anderes bestimmt, § 41 des Bundesdatenschutzgesetzes entsprechend.

(2) Wegen eines Verstoßes gegen Art. 83 Abs. 4 bis 6 der Verordnung (EU) Nr. 2016/679 werden gegen Behörden und sonstige öffentliche Stellen nach § 2 Abs. 1 Satz 1 keine Geldbußen verhängt.

(3) Eine Meldung nach Art. 33 der Verordnung (EU) Nr. 2016/679 oder eine Benachrichtigung nach Art. 34 Abs. 1 der Verordnung (EU) Nr. 2016/679 darf in einem Verfahren nach dem Gesetz über Ordnungswidrigkeiten gegen die meldepflichtige oder benachrichtigende Person oder ihre in § 52 Abs. 1 der Strafprozessordnung bezeichneten Angehörigen nur mit Zustimmung der meldepflichtigen oder benachrichtigenden Person verwendet werden.

§ 37
Strafvorschriften

(1) Mit Freiheitsstrafe bis zu zwei Jahren oder mit Geldstrafe wird bestraft, wer personenbezogene Daten, die nicht allgemein zugänglich sind,

1. ohne hierzu berechtigt zu sein, verarbeitet oder
2. durch unrichtige Angaben erschleicht,

und hierbei gegen Entgelt oder in der Absicht handelt, sich oder einen anderen zu bereichern oder einen anderen zu schädigen.

(2) Abs. 1 findet nur Anwendung, soweit die Tat nicht in anderen Vorschriften mit einer schwereren Strafe bedroht ist.

(3) Die Tat wird nur auf Antrag verfolgt. Antragsberechtigt sind die betroffene Person, der Verantwortliche und die oder der Hessische Datenschutzbeauftragte.

(4) Eine Meldung nach Art. 33 der Verordnung (EU) Nr. 2016/679 oder eine Benachrichtigung nach Art. 34 Abs. 1 der Verordnung (EU) Nr. 2016/679 darf in einem Strafverfahren gegen die meldepflichtige oder benachrichtigende Person oder ihre in § 52 Abs. 1 der Strafprozessordnung bezeichneten Angehörigen nur mit Zustimmung der meldepflichtigen oder benachrichtigenden Person verwendet werden.

§ 38
Bußgeldvorschriften

(1) Ordnungswidrig handelt, wer vorsätzlich oder fahrlässig entgegen § 22 Abs. 2 Satz 2 personenbezogene Daten für andere Zwecke verarbeitet, als für die sie übermittelt wurden.

(2) Die Ordnungswidrigkeit nach Abs. 1 kann mit einer Geldbuße von bis zu fünfzigtausend Euro geahndet werden.

Vierter Abschnitt
Gemeinsame Verfahren, Gemeinsam Verantwortliche

§ 39
Gemeinsame Verfahren, Gemeinsam Verantwortliche

(1) Die Einrichtung eines Verfahrens, das mehreren Verantwortlichen als gemeinsam Verantwortliche im Sinne von Art. 26 der Verordnung (EU) Nr. 2016/679 die Verarbeitung personenbezogener Daten ermöglicht, ist nur zulässig, wenn dies unter Berücksichtigung der schutzwürdigen Belange der betroffenen Personen und der Aufgaben der beteiligten Stellen angemessen ist.

(2) Über die in Art. 26 der Verordnung (EU) Nr. 2016/679 genannten Festlegungen hinaus bestimmen die gemeinsam Verantwortlichen eine Stelle, der die Planung, Einrichtung und Durchführung des gemeinsamen Verfahrens obliegt.

(3) Abs. 1 und 2 gelten entsprechend, wenn innerhalb einer öffentlichen Stelle ein gemeinsames Verfahren zur Verarbeitung personenbezogener Daten für verschiedene Zwecke eingerichtet wird.

DRITTER TEIL
Bestimmungen für Verarbeitungen zu Zwecken nach
Artikel 1 Absatz 1 der Richtlinie (EU) Nr. 2016/680

Erster Abschnitt
Anwendungsbereich, Begriffsbestimmungen und allgemeine Grundsätze
für die Verarbeitung personenbezogener Daten

§ 40
Anwendungsbereich

(1) Die Vorschriften dieses Teils gelten für die Verarbeitung personenbezogener Daten durch die für die Verhütung, Ermittlung, Aufdeckung, Verfolgung oder Ahndung von Straftaten oder Ordnungswidrigkeiten, einschließlich des Schutzes vor und der Abwehr von Gefahren für die öffentliche Sicherheit, zuständigen öffentlichen Stellen. Dies gilt, soweit die öffentlichen Stellen zum Zwecke der Erfüllung dieser Aufgaben personenbezogene Daten verarbeiten. Die öffentlichen Stellen gelten dabei als Verantwortliche.

(2) Abs. 1 findet auch Anwendung auf diejenigen öffentlichen Stellen, die für die Vollstreckung und den Vollzug von Strafen, von Maßnahmen im Sinne des § 11 Abs. 1 Nr. 8 des Strafgesetzbuchs, von Erziehungsmaßregeln oder Zuchtmitteln im Sinne des Jugendgerichtsgesetzes und von Geldbußen zuständig sind.

(3) Soweit dieser Teil Vorschriften für Auftragsverarbeiter enthält, gilt er auch für diese.

§ 41
Begriffsbestimmungen

Im Sinne des Dritten Teils

1. sind personenbezogene Daten alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person (betroffene Person) beziehen; als identifizierbar wird eine natürliche Person angesehen, die direkt oder indirekt, insbesondere mittels Zuordnung zu einer Kennung wie einem Namen, zu einer Kennnummer, zu Standortdaten, zu einer Online-Kennung oder zu einem oder mehreren besonderen Merkmalen, die Aus-

druck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser Person sind, identifiziert werden kann;

2. ist Verarbeitung jeder mit oder ohne Hilfe automatisierter Verfahren ausgeführte Vorgang oder jede solche Vorgangsreihe im Zusammenhang mit personenbezogenen Daten wie das Erheben, das Erfassen, die Organisation, das Ordnen, die Speicherung, die Anpassung, die Veränderung, das Auslesen, das Abfragen, die Verwendung, die Offenlegung durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung, den Abgleich, die Verknüpfung, die Einschränkung, das Löschen oder die Vernichtung;

3. ist Einschränkung der Verarbeitung die Markierung gespeicherter personenbezogener Daten mit dem Ziel, ihre künftige Verarbeitung einzuschränken;

4. ist Profiling jede Art der automatisierten Verarbeitung personenbezogener Daten, die darin besteht, dass diese personenbezogenen Daten verwendet werden, um bestimmte persönliche Aspekte, die sich auf eine natürliche Person beziehen, zu bewerten, insbesondere um Aspekte bezüglich Arbeitsleistung, wirtschaftliche Lage, Gesundheit, persönliche Vorlieben, Interessen, Zuverlässigkeit, Verhalten, Aufenthaltsort oder Ortswechsel dieser natürlichen Person zu analysieren oder vorherzusagen;

5. ist Pseudonymisierung die Verarbeitung personenbezogener Daten in einer Weise, dass die personenbezogenen Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden können, sofern diese zusätzlichen Informationen gesondert aufbewahrt werden und technischen und organisatorischen Maßnahmen unterliegen, die gewährleisten, dass die personenbezogenen Daten nicht einer identifizierten oder identifizierbaren natürlichen Person zugewiesen werden;

6. ist Dateisystem jede strukturierte Sammlung personenbezogener Daten, die nach bestimmten Kriterien zugänglich sind, unabhängig davon, ob diese Sammlung zentral, dezentral oder nach funktionalen oder geografischen Gesichtspunkten geordnet geführt wird;

7. ist zuständige Behörde

   a) eine staatliche Stelle, die für die Aufgaben nach § 40 zuständig ist, oder

   b) eine andere staatliche Stelle oder Einrichtung, der durch Rechtsvorschrift die Ausübung öffentlicher Gewalt und hoheitlicher Befugnisse zur Erfüllung der Aufgaben nach § 40 übertragen wurde;

8. ist Verantwortlicher die zuständige Behörde, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet; sind die Zwecke und Mittel dieser Verarbeitung durch das Unionsrecht oder das Recht der Mitgliedstaaten vorgegeben, so kann der Verantwortliche beziehungsweise können die bestimmten Kriterien seiner Benennung nach dem Unionsrecht oder dem Recht der Mitgliedstaaten vorgesehen werden;

9. ist Auftragsverarbeiter eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die personenbezogene Daten im Auftrag des Verantwortlichen verarbeitet;

10. ist Empfänger eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, der personenbezogene Daten offengelegt werden, unabhängig davon, ob es sich bei ihr um einen Dritten handelt oder nicht. Behörden, die im Rahmen eines bestimmten Untersuchungsauftrags nach dem Recht der Mitgliedstaaten möglicherweise personenbezogene Daten erhalten, gelten jedoch nicht als Empfänger; die Verarbeitung dieser Daten durch die genannten Behörden erfolgt im Einklang mit den geltenden Datenschutzvorschriften nach den Zwecken der Verarbeitung;

11. ist Verletzung des Schutzes personenbezogener Daten eine Verletzung der Sicherheit, die zur Vernichtung, zum Verlust oder zur Veränderung, ob unbeabsichtigt oder unrechtmäßig, oder zur unbefugten Offenlegung von beziehungsweise zum unbefugten Zugang zu personenbezogenen Daten führt, die übermittelt, gespeichert oder auf sonstige Weise verarbeitet wurden;

12. sind genetische Daten personenbezogene Daten zu den ererbten oder erworbenen genetischen Eigenschaften einer natürlichen Person, die eindeutige Informationen über die Physiologie oder die Gesundheit dieser Person liefern und insbesondere aus der Analyse einer biologischen Probe der Person gewonnen wurden;

13. sind biometrische Daten mit speziellen technischen Verfahren gewonnene personenbezogene Daten zu den physischen, physiologischen oder verhaltenstypischen Merkmalen einer natürlichen Person, die die eindeutige Identifizierung dieser natürlichen Person ermöglichen oder bestätigen, wie Gesichtsbilder oder daktyloskopische Daten;

14. sind Gesundheitsdaten personenbezogene Daten, die sich auf die körperliche oder geistige Gesundheit einer natürlichen Person, einschließlich der Erbringung von Gesundheitsdienstleistungen, beziehen und aus denen Informationen über deren Gesundheitszustand hervorgehen;

15. sind besondere Kategorien personenbezogener Daten

    a) Daten, aus denen die rassische oder ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen oder die Gewerkschaftszugehörigkeit hervorgehen,

    b) genetische Daten,

    c) biometrische Daten zur eindeutigen Identifizierung einer natürlichen Person,

    d) Gesundheitsdaten und

    e) Daten zum Sexualleben oder zur sexuellen Orientierung;

16. ist Aufsichtsbehörde eine von einem Mitgliedstaat nach Art. 41 der Richtlinie (EU) Nr. 2016/680 eingerichtete unabhängige staatliche Stelle;

17. ist internationale Organisation eine völkerrechtliche Organisation und ihre nachgeordneten Stellen oder jede sonstige Einrichtung, die durch eine von zwei oder mehr Ländern geschlossene Übereinkunft oder auf der Grundlage einer solchen Übereinkunft geschaffen wurde;

18. ist Einwilligung jede freiwillig für den bestimmten Fall, in informierter Weise und unmissverständlich abgegebene Willensbekundung in Form einer Erklärung oder einer sonstigen eindeutigen bestätigenden Handlung, mit der die betroffene Person zu verstehen gibt, dass sie mit der Verarbeitung der sie betreffenden personenbezogenen Daten einverstanden ist.

§ 42
Allgemeine Grundsätze für die Verarbeitung personenbezogener Daten

Personenbezogene Daten müssen

1. auf rechtmäßige Weise und nach Treu und Glauben verarbeitet werden,

2. für festgelegte, eindeutige und rechtmäßige Zwecke erhoben und nicht in einer mit diesen Zwecken nicht zu vereinbarenden Weise verarbeitet werden,

3. dem Verarbeitungszweck entsprechen, für das Erreichen des Verarbeitungszwecks erforderlich sein und ihre Verarbeitung nicht außer Verhältnis zu diesem Zweck stehen,

4. sachlich richtig und erforderlichenfalls auf dem neuesten Stand sein; dabei sind alle angemessenen Maßnahmen zu treffen, damit personenbezogene Daten, die im Hinblick auf die Zwecke ihrer Verarbeitung unrichtig sind, unverzüglich gelöscht oder berichtigt werden,

5. nicht länger als es für die Zwecke, für die sie verarbeitet werden, erforderlich ist, in einer Form gespeichert werden, die die Identifizierung der betroffenen Personen ermöglicht, und

6. in einer Weise verarbeitet werden, die eine angemessene Sicherheit der personenbezogenen Daten gewährleistet; hierzu gehört auch ein durch geeignete technische und organisatorische Maßnahmen zu gewährleistender Schutz vor unbefugter oder unrechtmäßiger Verarbeitung, unbeabsichtigtem Verlust, unbeabsichtigter Zerstörung oder unbeabsichtigter Schädigung.

Zweiter Abschnitt
Rechtsgrundlagen für die Verarbeitung personenbezogener Daten

§ 43
Verarbeitung besonderer Kategorien personenbezogener Daten

(1) Die Verarbeitung besonderer Kategorien personenbezogener Daten ist nur zulässig, wenn sie zur Aufgabenerfüllung unbedingt erforderlich ist.

(2) Werden besondere Kategorien personenbezogener Daten verarbeitet, sind geeignete Garantien für die Rechte und Freiheiten der betroffenen Personen vorzusehen. Geeignete Garantien können insbesondere sein

1. spezifische Anforderungen an die Datensicherheit oder die Datenschutzkontrolle,

2. die Festlegung von besonderen Aussonderungsprüffristen,

3. die Sensibilisierung der an Verarbeitungsvorgängen Beteiligten,

4. die Beschränkung des Zugangs zu den personenbezogenen Daten innerhalb der verantwortlichen Stelle,

5. die von anderen Daten getrennte Verarbeitung,
6. die Pseudonymisierung personenbezogener Daten,
7. die Verschlüsselung personenbezogener Daten oder
8. spezifische Verfahrensregelungen, die im Fall einer Übermittlung oder Verarbeitung für andere Zwecke die Rechtmäßigkeit der Verarbeitung sicherstellen.

§ 44
Verarbeitung zu anderen Zwecken

Eine Verarbeitung personenbezogener Daten zu einem anderen Zweck als zu demjenigen, zu dem sie erhoben wurden, ist zulässig, wenn es sich bei dem anderen Zweck um einen der in § 40 genannten Zwecke handelt, der Verantwortliche befugt ist, Daten zu diesem Zweck zu verarbeiten und die Verarbeitung zu diesem Zweck erforderlich und verhältnismäßig ist. Die Verarbeitung personenbezogener Daten zu einem anderen, in § 40 nicht genannten Zweck ist zulässig, wenn sie in einer Rechtsvorschrift vorgesehen ist.

§ 45
Verarbeitung zu wissenschaftlichen oder historischen Forschungszwecken, archivarischen oder statistischen Zwecken

(1) Personenbezogene Daten dürfen im Rahmen der in § 40 genannten Zwecke zu wissenschaftlichen oder historischen Forschungszwecken, archivarischen oder statistischen Zwecken verarbeitet werden, wenn

1. die betroffene Person nach § 46 eingewilligt hat oder
2. hieran ein öffentliches Interesse besteht und geeignete Garantien für die Rechte und Freiheiten der betroffenen Personen vorgesehen werden. Solche Garantien können in einer so zeitnah wie möglich erfolgenden Anonymisierung der personenbezogenen Daten, in Vorkehrungen gegen ihre unbefugte Kenntnisnahme durch Dritte oder in ihrer räumlich und organisatorisch von den sonstigen Fachaufgaben getrennten Verarbeitung bestehen.

(2) Die Verarbeitung besonderer Kategorien personenbezogener Daten im Fall des Abs. 1 Satz 1 Nr. 2 muss darüber hinaus zu wissenschaftlichen oder historischen Forschungszwecken, archivarischen oder statistischen Zwecken unbedingt erforderlich sein und die Interessen des Verantwortlichen an der Verarbeitung die Interessen der betroffenen Person an einem Ausschluss der Verarbeitung überwiegen.

(3) Der Verantwortliche sieht im Fall des Abs. 2 angemessene und spezifische Maßnahmen zur Wahrung der Interessen der betroffenen Personen nach § 43 Abs. 2 vor. Ergänzend zu den in § 43 Abs. 2 genannten Maßnahmen sind zu wissenschaftlichen oder historischen Forschungszwecken oder zu statistischen Zwecken verarbeitete besondere Kategorien personenbezogener Daten zu anonymisieren, sobald dies nach dem Forschungs- oder Statistikzweck möglich ist, es sei denn, berechtigte Interessen der betroffenen Person stehen dem entgegen. Sobald der Forschungs- oder Statistikzweck dies erlaubt, sind die Merkmale, mit deren Hilfe ein Personenbezug hergestellt werden kann, gesondert zu speichern; die Merkmale sind zu löschen, sobald der Forschungs- oder Statistikzweck dies zulässt.

(4) Die in den §§ 50 bis 53 vorgesehenen Rechte sind insoweit beschränkt, als diese Rechte voraussichtlich die Verwirklichung der Forschungs- oder Statistikzwecke unmöglich machen oder ernsthaft beeinträchtigen und die Beschränkung für die Erfüllung der Forschungs- oder Statistikzwecke notwendig ist. Das Recht auf Auskunft besteht darüber hinaus nicht, wenn die Daten für Zwecke der wissenschaftlichen Forschung erforderlich sind und die Auskunftserteilung einen unverhältnismäßigen Aufwand erfordern würde.

(5) Das Recht auf Auskunft nach § 52 besteht nicht, wenn das Archivgut nicht durch den Namen der Person erschlossen ist oder keine Angaben gemacht werden, die das Auffinden des betreffenden Archivguts mit vertretbarem Verwaltungsaufwand ermöglichen. Das Recht auf Berichtigung der betroffenen Person nach § 53 besteht nicht, wenn die personenbezogenen Daten zu Archivzwecken im öffentlichen Interesse verarbeitet werden. Bestreitet die betroffene Person die Richtigkeit der personenbezogenen Daten, ist ihr die Möglichkeit einer Gegendarstellung einzuräumen. Das zuständige Archiv ist verpflichtet, die Gegendarstellung den Unterlagen hinzuzufügen. Das Recht auf Einschränkung der Verarbeitung nach § 53 besteht nicht, soweit dieses Recht voraussichtlich die Verwirklichung der im öffentlichen Interesse liegenden Archivzwecke unmöglich machen oder ernsthaft beeinträchtigen und die Ausnahmen für die Erfüllung dieser Zwecke erforderlich sind.

(6) Der Verantwortliche darf personenbezogene Daten zu wissenschaftlichen oder historischen Forschungszwecken nur veröffentlichen, wenn die betroffene Person eingewilligt hat oder dies für die Darstellung von Forschungsergebnissen über Ereignisse der Zeitgeschichte unerlässlich ist.

§ 46
Einwilligung

(1) Soweit die Verarbeitung personenbezogener Daten nach einer Rechtsvorschrift auf der Grundlage einer Einwilligung erfolgen kann, muss der Verantwortliche die Einwilligung der betroffenen Person nachweisen können.

(2) Erfolgt die Einwilligung der betroffenen Person durch eine schriftliche Erklärung, die noch andere Sachverhalte betrifft, muss das Ersuchen um Einwilligung in verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache so erfolgen, dass es von den anderen Sachverhalten klar zu unterscheiden ist.

(3) Die betroffene Person hat das Recht, ihre Einwilligung jederzeit zu widerrufen. Durch den Widerruf der Einwilligung wird die Rechtmäßigkeit der aufgrund der Einwilligung bis zum Widerruf erfolgten Verarbeitung nicht berührt. Die betroffene Person ist vor Abgabe der Einwilligung hiervon in Kenntnis zu setzen. Der Widerruf der Einwilligung muss so einfach wie die Erteilung der Einwilligung sein.

(4) Die Einwilligung ist nur wirksam, wenn sie auf der freien Entscheidung der betroffenen Person beruht. Bei der Beurteilung, ob die Einwilligung freiwillig erteilt wurde, müssen die Umstände der Erteilung berücksichtigt werden. Die betroffene Person ist auf den vorgesehenen Zweck der Verarbeitung hinzuweisen. Ist dies nach den Umständen des Einzelfalles erforderlich oder verlangt die betroffene Person dies, ist sie auch über die Folgen der Verweigerung der Einwilligung zu belehren.

(5) Soweit besondere Kategorien personenbezogener Daten verarbeitet werden, muss sich die Einwilligung ausdrücklich auf diese Daten beziehen.

§ 47
Verarbeitung auf Weisung des Verantwortlichen

Der Auftragsverarbeiter und jede einem Verantwortlichen oder dem Auftragsverarbeiter unterstellte Person, die Zugang zu personenbezogenen Daten hat, darf diese Daten ausschließlich auf Weisung des Verantwortlichen verarbeiten, es sei denn, dass sie nach einer Rechtsvorschrift zur Verarbeitung verpflichtet sind.

§ 48
Datengeheimnis

Mit Datenverarbeitung befasste Personen dürfen personenbezogene Daten nicht unbefugt verarbeiten (Datengeheimnis). Das Datengeheimnis besteht auch nach der Beendigung ihrer Tätigkeit fort. Die Personen sind über die bei ihrer Tätigkeit zu beachtenden Vorschriften über den Datenschutz zu unterrichten.

§ 49
Automatisierte Einzelentscheidung

(1) Eine ausschließlich auf einer automatischen Verarbeitung beruhende Entscheidung, die mit einer nachteiligen Rechtsfolge für die betroffene Person verbunden ist oder sie erheblich beeinträchtigt, ist nur zulässig, wenn sie in einer Rechtsvorschrift vorgesehen ist.

(2) Entscheidungen nach Abs. 1 dürfen nicht auf besonderen Kategorien personenbezogener Daten beruhen, sofern nicht geeignete Maßnahmen zum Schutz der Rechte und Freiheiten sowie der berechtigten Interessen der betroffenen Personen getroffen wurden.

(3) Profiling, das zur Folge hat, dass betroffene Personen auf der Grundlage von besonderen Kategorien personenbezogener Daten diskriminiert werden, ist verboten.

Dritter Abschnitt
Rechte der betroffenen Person

§ 50
Allgemeine Informationen zu Datenverarbeitungen

Der Verantwortliche hat in allgemeiner Form und für jedermann zugänglich Informationen zur Verfügung zu stellen über

1. die Zwecke der von ihm vorgenommenen Verarbeitungen,
2. die im Hinblick auf die Verarbeitung ihrer personenbezogenen Daten bestehenden Rechte der betroffenen Personen auf Auskunft, Berichtigung, Löschung und Einschränkung der Verarbeitung,
3. den Namen und die Kontaktdaten des Verantwortlichen und die Kontaktdaten der oder des Datenschutzbeauftragten,
4. das Recht, die oder den Hessischen Datenschutzbeauftragten anzurufen, und
5. die Erreichbarkeit der oder des Hessischen Datenschutzbeauftragten.

§ 51
Benachrichtigung betroffener Personen

(1) Ist die Benachrichtigung betroffener Personen über die Verarbeitung sie betreffender personenbezogener Daten in speziellen Rechtsvorschriften, insbesondere bei verdeckten Maßnahmen, vorgesehen oder angeordnet, so hat diese Benachrichtigung zumindest die folgenden Angaben zu enthalten:

1. die in § 50 genannten Angaben,
2. die Rechtsgrundlage der Verarbeitung,
3. die für die Daten geltende Speicherdauer oder, falls dies nicht möglich ist, die Kriterien für die Festlegung dieser Dauer,
4. gegebenenfalls die Kategorien von Empfängern der personenbezogenen Daten, auch der Empfänger in Drittländern oder in internationalen Organisationen, sowie
5. erforderlichenfalls weitere Informationen, insbesondere, wenn die personenbezogenen Daten ohne Wissen der betroffenen Person erhoben wurden.

(2) In den Fällen des Abs. 1 kann der Verantwortliche die Benachrichtigung insoweit und solange aufschieben, einschränken oder unterlassen, wie andernfalls

1. die
   a) Erfüllung der in § 40 genannten Aufgaben,
   b) öffentliche Sicherheit oder
   c) Rechte oder Freiheiten Dritter

   gefährdet würden oder
2. dem Wohle des Bundes oder eines Landes Nachteile bereitet würden

und wenn das Interesse des Verantwortlichen an der Nichterteilung der Information das Informationsinteresse der betroffenen Person überwiegt. Die Entscheidung trifft die Leitung der öffentlichen Stelle oder eine von ihr bestimmte, bei der öffentlichen Stelle beschäftigte Person.

(3) Bezieht sich die Benachrichtigung auf die Übermittlung personenbezogener Daten an Verfassungsschutzbehörden, den Bundesnachrichtendienst, den Militärischen Abschirmdienst und, soweit die Sicherheit des Bundes berührt wird, andere Behörden des Bundesministeriums der Verteidigung, ist sie nur mit Zustimmung dieser Stellen zulässig.

(4) Im Fall der Einschränkung nach Abs. 2 gilt § 52 Abs. 7 entsprechend.

§ 52
Auskunftsrecht

(1) Der Verantwortliche hat betroffenen Personen auf Antrag Auskunft darüber zu erteilen, ob er sie betreffende Daten verarbeitet. Betroffene Personen haben darüber hinaus das Recht, Informationen zu erhalten über

1. die personenbezogenen Daten, die Gegenstand der Verarbeitung sind, und die Kategorie, zu der sie gehören,
2. die verfügbaren Informationen über die Herkunft der Daten,
3. die Zwecke der Verarbeitung und deren Rechtsgrundlage,
4. die Empfänger oder die Kategorien von Empfängern, gegenüber denen die Daten offengelegt worden sind, insbesondere bei Empfängern in Drittländern oder bei internationalen Organisationen,

5. die für die Daten geltende Speicherdauer oder, falls dies nicht möglich ist, die Kriterien für die Festlegung dieser Dauer,
6. das Bestehen eines Rechts auf Berichtigung, Löschung oder Einschränkung der Verarbeitung der Daten durch den Verantwortlichen,
7. das Recht nach § 55, die Hessische Datenschutzbeauftragte oder den Hessischen Datenschutzbeauftragten anzurufen, sowie
8. Angaben zur Erreichbarkeit der oder des Hessischen Datenschutzbeauftragten.

(2) Abs. 1 gilt nicht für personenbezogene Daten, die nur deshalb verarbeitet werden, weil sie aufgrund gesetzlicher Aufbewahrungsvorschriften nicht gelöscht werden dürfen, oder die ausschließlich Zwecken der Datensicherung, der Datenschutzkontrolle oder der Sicherstellung des ordnungsgemäßen Betriebs einer Datenverarbeitungsanlage dienen.

(3) Das Recht der betroffenen Person auf Auskunft über personenbezogene Daten, die weder automatisiert verarbeitet noch nicht automatisiert verarbeitet und in einem Dateisystem gespeichert werden, besteht nur, soweit die betroffene Person Angaben macht, die das Auffinden der Daten ermöglichen, und der für die Erteilung der Auskunft erforderliche Aufwand nicht außer Verhältnis zu dem von der betroffenen Person geltend gemachten Informationsinteresse steht. Statt einer Auskunft über personenbezogene Daten kann der betroffenen Person Akteneinsicht gewährt werden.

(4) Der Verantwortliche kann unter den Voraussetzungen des § 51 Abs. 2 von der Auskunft nach Abs. 1 Satz 1 absehen oder die Auskunftserteilung nach Abs. 1 Satz 2 teilweise oder vollständig einschränken.

(5) Bezieht sich die Auskunftserteilung auf die Übermittlung personenbezogener Daten an Verfassungsschutzbehörden, den Bundesnachrichtendienst, den Militärischen Abschirmdienst und, soweit die Sicherheit des Bundes berührt wird, andere Behörden des Bundesministeriums der Verteidigung, ist sie nur mit Zustimmung dieser Stellen zulässig.

(6) Der Verantwortliche hat die betroffene Person über das Absehen von oder die Einschränkung einer Auskunft unverzüglich schriftlich zu unterrichten. Dies gilt nicht, wenn bereits die Erteilung dieser Informationen eine Gefährdung im Sinne des § 51 Abs. 2 mit sich bringen würde. Die Unterrichtung nach Satz 1 ist zu begründen, es sei denn, dass die Mitteilung der Gründe den mit dem Absehen von oder der Einschränkung der Auskunft verfolgten Zweck gefährden würde.

(7) Wird die betroffene Person nach Abs. 6 über das Absehen von oder die Einschränkung der Auskunft unterrichtet, kann sie ihr Auskunftsrecht auch über die Hessische Datenschutzbeauftragte oder den Hessischen Datenschutzbeauftragten ausüben. Der Verantwortliche hat die betroffene Person über diese Möglichkeit sowie darüber zu unterrichten, dass sie nach § 55 die Hessische Datenschutzbeauftragte oder den Hessischen Datenschutzbeauftragten anrufen oder gerichtlichen Rechtsschutz suchen kann. Die oder der Hessische Datenschutzbeauftragte hat die betroffene Person darüber zu unterrichten, dass alle erforderlichen Prüfungen erfolgt sind oder eine Überprüfung durch sie oder ihn stattgefunden hat. Die Mitteilung der oder des Hessischen Datenschutzbeauftragten an die betroffene Person darf keine Rückschlüsse auf den Erkenntnisstand des Verantwortlichen zulassen, sofern dieser keiner weitergehenden Auskunft zustimmt. Die oder der Hessische Datenschutzbeauftragte hat zudem die betroffene Person über ihr Recht auf gerichtlichen Rechtsschutz zu unterrichten.

(8) Der Verantwortliche hat die sachlichen oder rechtlichen Gründe für die Entscheidung zu dokumentieren.

§ 53
Rechte auf Berichtigung und Löschung sowie Einschränkung der Verarbeitung

(1) Die betroffene Person hat das Recht, von dem Verantwortlichen unverzüglich die Berichtigung sie betreffender unrichtiger Daten zu verlangen. Insbesondere im Fall von Aussagen oder Bewertungen betrifft die Frage der Richtigkeit nicht den Inhalt der Aussage oder der Bewertung. Wenn die Richtigkeit oder Unrichtigkeit der Daten nicht festgestellt werden kann, tritt an die Stelle der Berichtigung eine Einschränkung der Verarbeitung. In diesem Fall hat der Verantwortliche die betroffene Person zu unterrichten, bevor er die Einschränkung wieder aufhebt. Die betroffene Person kann zudem die Vervollständigung unvollständiger personenbezogener Daten verlangen, wenn dies unter Berücksichtigung der Verarbeitungszwecke angemessen ist.

(2) Die betroffene Person hat das Recht, von dem Verantwortlichen unverzüglich die Löschung sie betreffender Daten zu verlangen, wenn deren Verarbeitung unzulässig ist, deren Kenntnis

für die Aufgabenerfüllung nicht mehr erforderlich ist oder diese zur Erfüllung einer rechtlichen Verpflichtung gelöscht werden müssen.

(3) Anstatt die personenbezogenen Daten zu löschen, kann der Verantwortliche deren Verarbeitung einschränken, wenn

1. Grund zu der Annahme besteht, dass eine Löschung schutzwürdige Interessen einer betroffenen Person beeinträchtigen würde,
2. die Daten zu Beweiszwecken weiter aufbewahrt werden müssen oder
3. eine Löschung wegen der besonderen Art der Speicherung nicht oder nur mit unverhältnismäßig hohem Aufwand möglich ist.

In ihrer Verarbeitung nach Satz 1 eingeschränkte Daten dürfen nur zu dem Zweck, der ihrer Löschung entgegenstand, oder sonst mit Einwilligung der betroffenen Person verarbeitet werden.

(4) Bei automatisierten Dateisystemen ist technisch sicherzustellen, dass eine Einschränkung der Verarbeitung eindeutig erkennbar ist und eine Verarbeitung für andere Zwecke nicht ohne weitere Prüfung möglich ist.

(5) Hat der Verantwortliche eine Berichtigung vorgenommen, hat er der Stelle, die ihm die personenbezogenen Daten zuvor übermittelt hat, die Berichtigung mitzuteilen. In Fällen der Berichtigung, Löschung oder Einschränkung der Verarbeitung nach Abs. 1 bis 3 hat der Verantwortliche Empfängern, denen die Daten übermittelt wurden, diese Maßnahmen mitzuteilen. Der Empfänger hat die Daten zu berichtigen, zu löschen oder ihre Verarbeitung einzuschränken.

(6) Der Verantwortliche hat die betroffene Person über ein Absehen von der Berichtigung oder Löschung personenbezogener Daten oder über die an deren Stelle tretende Einschränkung der Verarbeitung schriftlich zu unterrichten. Dies gilt nicht, soweit bereits die Erteilung dieser Informationen eine Gefährdung im Sinne des § 51 Abs. 2 mit sich bringen würde. Die Unterrichtung nach Satz 1 ist zu begründen, es sei denn, dass die Mitteilung der Gründe den mit dem Absehen von der Unterrichtung verfolgten Zweck gefährden würde.

(7) § 52 Abs. 7 und 8 findet entsprechende Anwendung.

§ 54
Verfahren für die Ausübung der Rechte der betroffenen Person

(1) Der Verantwortliche hat mit betroffenen Personen unter Verwendung einer klaren und einfachen Sprache in präziser, verständlicher und leicht zugänglicher Form zu kommunizieren. Unbeschadet besonderer Formvorschriften soll er bei der Beantwortung von Anträgen die für den Antrag gewählte Form verwenden.

(2) Bei Anträgen hat der Verantwortliche die betroffene Person unbeschadet des § 52 Abs. 6 und des § 53 Abs. 6 unverzüglich schriftlich darüber in Kenntnis zu setzen, wie mit diesen Anträgen verfahren wurde.

(3) Die Erteilung von Informationen nach § 50, die Benachrichtigungen nach den §§ 51 und 61 und die Bearbeitung von Anträgen nach den §§ 52 und 53 erfolgen verwaltungskostenfrei. Bei offenkundig unbegründeten oder exzessiven Anträgen nach den §§ 52 und 53 kann der Verantwortliche entweder eine angemessene Gebühr auf der Grundlage des Verwaltungsaufwands verlangen oder sich weigern, aufgrund des Antrags tätig zu werden. In diesem Fall muss der Verantwortliche den offenkundig unbegründeten oder exzessiven Charakter des Antrags belegen können.

(4) Hat der Verantwortliche begründete Zweifel an der Identität einer betroffenen Person, die einen Antrag nach den §§ 52 oder 53 gestellt hat, kann er von ihr zusätzliche Informationen anfordern, die zur Bestätigung ihrer Identität erforderlich sind.

§ 55
Anrufung der oder des Hessischen Datenschutzbeauftragten

(1) Jede betroffene Person kann sich unbeschadet anderweitiger Rechtsbehelfe mit einer Beschwerde an die Hessische Datenschutzbeauftragte oder den Hessischen Datenschutzbeauftragten wenden, wenn sie der Auffassung ist, bei der Verarbeitung ihrer personenbezogenen Daten durch öffentliche Stellen zu den in § 40 genannten Zwecken in ihren Rechten verletzt worden zu sein. Dies gilt nicht für die Verarbeitung von personenbezogenen Daten durch Gerichte, soweit diese die Daten im Rahmen ihrer justiziellen Tätigkeit verarbeitet haben. Die oder der Hessische Datenschutzbeauftragte hat die betroffene Person über den Stand und das Ergebnis der Be-

schwerde zu unterrichten und sie hierbei auf die Möglichkeit gerichtlichen Rechtsschutzes nach § 56 hinzuweisen.

(2) Die oder der Hessische Datenschutzbeauftragte hat eine bei ihr oder ihm eingelegte Beschwerde über eine Verarbeitung, die in die Zuständigkeit einer anderen Aufsichtsbehörde fällt, unverzüglich an diese weiterzuleiten. Sie oder er hat in diesem Fall die betroffene Person über die Weiterleitung zu unterrichten und ihr auf deren Ersuchen weitere Unterstützung zu leisten.

§ 56
Rechtsschutz gegen Entscheidungen der oder des Hessischen Datenschutzbeauftragten oder bei deren oder dessen Untätigkeit

(1) Jede natürliche oder juristische Person kann unbeschadet anderer Rechtsbehelfe gerichtlich gegen eine sie betreffende verbindliche Entscheidung der oder des Hessischen Datenschutzbeauftragten vorgehen.

(2) Abs. 1 gilt entsprechend zugunsten betroffener Personen, wenn sich die oder der Hessische Datenschutzbeauftragte mit einer Beschwerde nach § 55 nicht befasst oder die betroffene Person nicht innerhalb von drei Monaten nach Einlegung der Beschwerde über den Stand oder das Ergebnis der Beschwerde in Kenntnis gesetzt hat.

Vierter Abschnitt
Pflichten der Verantwortlichen und Auftragsverarbeiter

§ 57
Auftragsverarbeitung

(1) Werden personenbezogene Daten im Auftrag eines Verantwortlichen durch andere Personen oder Stellen verarbeitet, hat der Verantwortliche für die Einhaltung der Vorschriften dieses Gesetzes und anderer Vorschriften über den Datenschutz zu sorgen. Die Rechte der betroffenen Personen auf Auskunft, Berichtigung, Löschung, Einschränkung der Verarbeitung und Schadensersatz sind in diesem Fall gegenüber dem Verantwortlichen geltend zu machen.

(2) Ein Verantwortlicher darf nur solche Auftragsverarbeiter mit der Verarbeitung personenbezogener Daten beauftragen, die mit geeigneten technischen und organisatorischen Maßnahmen sicherstellen, dass die Verarbeitung im Einklang mit den gesetzlichen Anforderungen erfolgt und der Schutz der Rechte der betroffenen Personen gewährleistet wird.

(3) Auftragsverarbeiter dürfen ohne vorherige schriftliche Genehmigung des Verantwortlichen keine weiteren Auftragsverarbeiter hinzuziehen. Hat der Verantwortliche dem Auftragsverarbeiter eine allgemeine Genehmigung zur Hinzuziehung weiterer Auftragsverarbeiter erteilt, hat der Auftragsverarbeiter den Verantwortlichen über jede beabsichtigte Hinzuziehung oder Ersetzung zu informieren. Der Verantwortliche kann in diesem Fall die Hinzuziehung oder Ersetzung untersagen.

(4) Zieht ein Auftragsverarbeiter einen weiteren Auftragsverarbeiter hinzu, so hat er diesem dieselben Verpflichtungen aus seinem Vertrag mit dem Verantwortlichen nach Abs. 5 aufzuerlegen, die auch für ihn gelten, soweit diese Pflichten für den weiteren Auftragsverarbeiter nicht schon aufgrund anderer Vorschriften verbindlich sind. Erfüllt ein weiterer Auftragsverarbeiter diese Verpflichtungen nicht, so haftet der ihn beauftragende Auftragsverarbeiter gegenüber dem Verantwortlichen für die Einhaltung der Pflichten des weiteren Auftragsverarbeiters.

(5) Die Verarbeitung durch einen Auftragsverarbeiter hat auf der Grundlage eines Vertrags oder eines anderen Rechtsinstruments zu erfolgen, der oder das den Auftragsverarbeiter an den Verantwortlichen bindet und der oder das den Gegenstand, die Dauer, die Art und den Zweck der Verarbeitung, die Art der personenbezogenen Daten, die Kategorien betroffener Personen und die Rechte und Pflichten des Verantwortlichen festlegt. Der Vertrag oder das andere Rechtsinstrument haben insbesondere vorzusehen, dass der Auftragsverarbeiter

1. nur auf dokumentierte Weisung des Verantwortlichen handelt; ist der Auftragsverarbeiter der Auffassung, dass eine Weisung rechtswidrig ist, hat er den Verantwortlichen unverzüglich zu informieren;
2. gewährleistet, dass die zur Verarbeitung der personenbezogenen Daten befugten Personen zur Vertraulichkeit verpflichtet werden, soweit sie keiner angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen;
3. den Verantwortlichen mit geeigneten Mitteln dabei unterstützt, die Einhaltung der Bestimmungen über die Rechte der betroffenen Person zu gewährleisten;

4. alle personenbezogenen Daten nach Abschluss der Erbringung der Verarbeitungsleistungen nach Wahl des Verantwortlichen zurückgibt oder löscht und bestehende Kopien vernichtet, wenn nicht nach einer Rechtsvorschrift eine Verpflichtung zur Speicherung der Daten besteht;
5. dem Verantwortlichen alle erforderlichen Informationen, insbesondere die nach § 71 erstellten Protokolle, zum Nachweis der Einhaltung seiner Pflichten zur Verfügung stellt;
6. Überprüfungen, die von dem Verantwortlichen oder einem von diesem beauftragten Prüfer durchgeführt werden, ermöglicht und dazu beiträgt;
7. die in den Abs. 3 und 4 aufgeführten Bedingungen für die Inanspruchnahme der Dienste eines weiteren Auftragsverarbeiters einhält;
8. alle nach § 59 erforderlichen Maßnahmen ergreift und
9. unter Berücksichtigung der Art der Verarbeitung und der ihm zur Verfügung stehenden Informationen den Verantwortlichen bei der Einhaltung der in den §§ 59 bis 62 und 64 genannten Pflichten unterstützt.

(6) Der Vertrag im Sinne des Abs. 5 ist schriftlich oder elektronisch abzufassen.

(7) Ein Auftragsverarbeiter, der die Zwecke und Mittel der Verarbeitung unter Verstoß gegen diese Vorschrift bestimmt, gilt in Bezug auf diese Verarbeitung als Verantwortlicher.

§ 58
Gemeinsame Verfahren, Gemeinsam Verantwortliche

(1) Die Einrichtung eines Verfahrens, das mehreren Verantwortlichen als gemeinsam Verantwortliche die Verarbeitung personenbezogener Daten ermöglicht, ist nur zulässig, wenn dies unter Berücksichtigung der schutzwürdigen Belange der betroffenen Personen und der Aufgaben der beteiligten Stellen angemessen ist.

(2) Legen zwei oder mehr Verantwortliche gemeinsam die Zwecke und die Mittel der Verarbeitung fest, gelten sie als gemeinsam Verantwortliche.

(3) Gemeinsam Verantwortliche haben eine Stelle zu bestimmen, der die Planung, Einrichtung und Durchführung des gemeinsamen Verfahrens obliegt, und ihre jeweiligen Aufgaben sowie datenschutzrechtlichen Verantwortlichkeiten in transparenter Form in einer Vereinbarung festzulegen, soweit diese nicht bereits in Rechtsvorschriften festgelegt sind. Aus der Vereinbarung muss insbesondere hervorgehen, wer welchen Informationspflichten nachzukommen hat und wie und gegenüber wem betroffene Personen ihre Rechte wahrnehmen können. Eine entsprechende Vereinbarung hindert die betroffene Person nicht, ihre Rechte gegenüber jedem der gemeinsam Verantwortlichen geltend zu machen.

(4) Abs. 1 bis 3 gelten entsprechend, wenn innerhalb einer öffentlichen Stelle ein gemeinsames Verfahren zur Verarbeitung personenbezogener Daten für verschiedene Zwecke eingerichtet wird.

§ 59
Anforderungen an die Sicherheit der Datenverarbeitung

(1) Der Verantwortliche und der Auftragsverarbeiter haben unter Berücksichtigung des Stands der Technik, der Implementierungskosten, der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der Eintrittswahrscheinlichkeit und der Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen geeignete technische und organisatorische Maßnahmen zu treffen, um bei der Verarbeitung personenbezogener Daten ein dem Risiko angemessenes Schutzniveau zu gewährleisten, insbesondere im Hinblick auf die Verarbeitung besonderer Kategorien personenbezogener Daten. Eintrittswahrscheinlichkeit und Schwere der Verletzung sollen nach der Art, dem Umfang, den Umständen und den Zwecken der Verarbeitung bestimmt und anhand einer objektiven Beurteilung die Höhe des Risikos festgestellt werden.

(2) Die in Abs. 1 genannten Maßnahmen können unter anderem die Pseudonymisierung und Verschlüsselung personenbezogener Daten umfassen, soweit solche Mittel in Anbetracht der Verarbeitungszwecke möglich sind. Die Maßnahmen nach Abs. 1 sollen dazu führen, dass

1. die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung auf Dauer sichergestellt werden und
2. die Verfügbarkeit der personenbezogenen Daten und der Zugang zu ihnen bei einem physischen oder technischen Zwischenfall rasch wiederhergestellt werden können.

(3) Im Fall einer automatisierten Verarbeitung haben der Verantwortliche und der Auftragsverarbeiter nach einer Risikobewertung Maßnahmen zu ergreifen, die Folgendes bezwecken:

1. Verwehrung des Zugangs zu Verarbeitungsanlagen, mit denen die Verarbeitung durchgeführt wird, für Unbefugte (Zugangskontrolle),
2. Verhinderung des unbefugten Lesens, Kopierens, Veränderns oder Löschens von Datenträgern (Datenträgerkontrolle),
3. Verhinderung der unbefugten Eingabe von personenbezogenen Daten sowie der unbefugten Kenntnisnahme, Veränderung und Löschung von gespeicherten personenbezogenen Daten (Speicherkontrolle),
4. Verhinderung der Nutzung automatisierter Verarbeitungssysteme mithilfe von Einrichtungen zur Datenübertragung durch Unbefugte (Benutzerkontrolle),
5. Gewährleistung, dass die zur Benutzung eines automatisierten Verarbeitungssystems Berechtigten ausschließlich zu den von ihrer Zugangsberechtigung umfassten personenbezogenen Daten Zugang haben (Zugriffskontrolle),
6. Gewährleistung, dass überprüft und festgestellt werden kann, an welche Stellen personenbezogene Daten mithilfe von Einrichtungen zur Datenübertragung übermittelt oder zur Verfügung gestellt wurden oder werden können (Übertragungskontrolle),
7. Gewährleistung, dass nachträglich überprüft und festgestellt werden kann, welche personenbezogenen Daten zu welcher Zeit und von wem in automatisierte Verarbeitungssysteme eingegeben oder verändert worden sind (Eingabekontrolle),
8. Gewährleistung, dass bei der Übermittlung personenbezogener Daten sowie beim Transport von Datenträgern die Vertraulichkeit und Integrität der Daten geschützt werden (Transportkontrolle),
9. Gewährleistung, dass eingesetzte Systeme im Störungsfall wiederhergestellt werden können (Wiederherstellbarkeit),
10. Gewährleistung, dass alle Funktionen des Systems zur Verfügung stehen und auftretende Fehlfunktionen gemeldet werden (Zuverlässigkeit),
11. Gewährleistung, dass gespeicherte personenbezogene Daten nicht durch Fehlfunktionen des Systems beschädigt werden können (Datenintegrität),
12. Gewährleistung, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können (Auftragskontrolle),
13. Gewährleistung, dass personenbezogene Daten gegen Zerstörung oder Verlust geschützt sind (Verfügbarkeitskontrolle),
14. Gewährleistung, dass zu unterschiedlichen Zwecken erhobene personenbezogene Daten getrennt verarbeitet werden können (Trennbarkeit).

Ein Zweck nach Satz 1 Nr. 2 bis 5 kann insbesondere durch die Verwendung von dem Stand der Technik entsprechenden Verschlüsselungsverfahren erreicht werden.

(4) Werden personenbezogene Daten nicht automatisiert verarbeitet, sind insbesondere Maßnahmen zu treffen, um den Zugriff Unbefugter bei der Bearbeitung, der Aufbewahrung, dem Transport und der Vernichtung zu verhindern.

§ 60
Meldung von Verletzungen des Schutzes personenbezogener Daten an die Hessische Datenschutzbeauftragte oder den Hessischen Datenschutzbeauftragten

(1) Der Verantwortliche hat eine Verletzung des Schutzes personenbezogener Daten unverzüglich und möglichst binnen 72 Stunden, nachdem sie ihm bekannt geworden ist, der oder dem Hessischen Datenschutzbeauftragten zu melden, es sei denn, dass die Verletzung voraussichtlich nicht zu einem Risiko für die Rechte und Freiheiten natürlicher Personen führt. Erfolgt die Meldung an die Hessische Datenschutzbeauftragte oder den Hessischen Datenschutzbeauftragten nicht binnen 72 Stunden, so ist ihr eine Begründung für die Verzögerung beizufügen. § 59 Abs. 1 Satz 2 gilt entsprechend.

(2) Wird dem Auftragsverarbeiter eine Verletzung des Schutzes personenbezogener Daten bekannt, meldet er diese dem Verantwortlichen unverzüglich.

(3) Die Meldung nach Abs. 1 hat zumindest folgende Informationen zu enthalten:

1. eine Beschreibung der Art der Verletzung des Schutzes personenbezogener Daten, die, soweit möglich, Angaben zu den Kategorien und der ungefähren Anzahl der betroffenen Personen, zu den betroffenen Kategorien personenbezogener Daten und zu der ungefähren Anzahl der betroffenen personenbezogenen Datensätze zu enthalten hat,
2. den Namen und die Kontaktdaten der oder des Datenschutzbeauftragten oder einer sonstigen Anlaufstelle für weitere Informationen,
3. eine Beschreibung der wahrscheinlichen Folgen der Verletzung des Schutzes personenbezogener Daten und
4. eine Beschreibung der von dem Verantwortlichen ergriffenen oder vorgeschlagenen Maßnahmen zur Behandlung der Verletzung des Schutzes personenbezogener Daten und gegebenenfalls der Maßnahmen zur Abmilderung ihrer möglichen nachteiligen Auswirkungen.

(4) Wenn und soweit die Informationen nach Abs. 3 nicht zur gleichen Zeit bereitgestellt werden können, hat der Verantwortliche diese Informationen ohne unangemessene weitere Verzögerung schrittweise zur Verfügung stellen.

(5) Der Verantwortliche hat Verletzungen des Schutzes personenbezogener Daten zu dokumentieren. Die Dokumentation hat alle mit den Vorfällen zusammenhängenden Tatsachen, deren Auswirkungen und die ergriffenen Abhilfemaßnahmen zu umfassen.

(6) Soweit von einer Verletzung des Schutzes personenbezogener Daten personenbezogene Daten betroffen sind, die von einem oder an einen Verantwortlichen in einem anderen Mitgliedstaat der Europäischen Union übermittelt wurden, sind die in Abs. 3 genannten Informationen dem dortigen Verantwortlichen unverzüglich zu übermitteln.

(7) § 37 Abs. 4 findet entsprechende Anwendung.

(8) Weitere Pflichten des Verantwortlichen zu Benachrichtigungen über Verletzungen des Schutzes personenbezogener Daten bleiben unberührt.

§ 61
Benachrichtigung betroffener Personen bei Verletzungen des Schutzes personenbezogener Daten

(1) Hat eine Verletzung des Schutzes personenbezogener Daten voraussichtlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen zur Folge, so hat der Verantwortliche die betroffenen Personen unverzüglich von der Verletzung zu benachrichtigen. § 59 Abs. 1 Satz 2 gilt entsprechend.

(2) Die Benachrichtigung nach Abs. 1 hat in klarer und einfacher Sprache die Art der Verletzung des Schutzes personenbezogener Daten zu beschreiben und zumindest die in § 60 Abs. 3 Nr. 2 bis 4 genannten Informationen und Maßnahmen zu enthalten.

(3) Die Benachrichtigung der betroffenen Person nach Abs. 1 ist nicht erforderlich, wenn

1. der Verantwortliche geeignete technische und organisatorische Sicherheitsvorkehrungen getroffen hat und diese Vorkehrungen auf die von der Verletzung des Schutzes personenbezogener Daten betroffenen Daten angewandt wurden; dies gilt insbesondere für Vorkehrungen wie Verschlüsselungen, durch die die Daten für unbefugte Personen unzugänglich gemacht werden;
2. der Verantwortliche durch im Anschluss an die Verletzung getroffene Maßnahmen sichergestellt hat, dass aller Wahrscheinlichkeit nach das hohe Risiko für die Rechte und Freiheiten der betroffenen Personen im Sinne des Abs. 1 nicht mehr besteht, oder
3. dies mit einem unverhältnismäßigen Aufwand verbunden wäre; in diesem Fall hat stattdessen eine öffentliche Bekanntmachung oder eine ähnliche Maßnahme zu erfolgen, durch die die betroffenen Personen vergleichbar wirksam informiert werden.

(4) Wenn der Verantwortliche die betroffenen Personen über eine Verletzung des Schutzes personenbezogener Daten nicht benachrichtigt hat, kann die oder der Hessische Datenschutzbeauftragte verlangen, dies nachzuholen oder verbindlich feststellen, dass bestimmte der in Abs. 3 genannten Voraussetzungen erfüllt sind. Hierbei hat sie oder er die Wahrscheinlichkeit zu berücksichtigen, mit der die Verletzung des Schutzes personenbezogener Daten zu einem hohen Risiko im Sinne des Abs. 1 führt.

(5) Die Benachrichtigung der betroffenen Personen nach Abs. 1 kann unter den in § 51 Abs. 2 genannten Voraussetzungen aufgeschoben, eingeschränkt oder unterlassen werden, soweit nicht

die Interessen der betroffenen Person aufgrund des von der Verletzung ausgehenden hohen Risikos im Sinne des Abs. 1 überwiegen.

(6) § 37 Abs. 4 findet entsprechende Anwendung.

§ 62
Durchführung einer Datenschutz-Folgenabschätzung

(1) Hat eine Form der Verarbeitung, insbesondere bei Verwendung neuer Technologien, aufgrund der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung voraussichtlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen zur Folge, so hat der Verantwortliche vorab eine Abschätzung der Folgen der vorgesehenen Verarbeitungsvorgänge für den Schutz personenbezogener Daten durchzuführen. § 59 Abs. 1 Satz 2 gilt entsprechend.

(2) Für die Untersuchung mehrerer ähnlicher Verarbeitungsvorgänge mit ähnlich hohen Risiken kann eine gemeinsame Datenschutz-Folgenabschätzung vorgenommen werden.

(3) Der Verantwortliche hat die Datenschutzbeauftragte oder den Datenschutzbeauftragten an der Durchführung der Folgenabschätzung zu beteiligen.

(4) Die Folgenabschätzung hat den Rechten und den berechtigten Interessen der von der Verarbeitung betroffenen Personen und sonstiger Betroffener Rechnung zu tragen und zumindest Folgendes zu enthalten:

1. eine systematische Beschreibung der geplanten Verarbeitungsvorgänge und der Zwecke der Verarbeitung,
2. eine Bewertung der Notwendigkeit und Verhältnismäßigkeit der Verarbeitungsvorgänge in Bezug auf deren Zweck,
3. eine Bewertung der Risiken für die Rechte und Freiheiten der betroffenen Personen und
4. die zur Bewältigung der Risiken geplanten Abhilfemaßnahmen, einschließlich der Garantien, der Sicherheitsvorkehrungen und der Verfahren, durch die der Schutz personenbezogener Daten sichergestellt und die Einhaltung der gesetzlichen Vorgaben nachgewiesen werden sollen.

(5) Soweit erforderlich, hat der Verantwortliche eine Überprüfung durchzuführen, ob die Verarbeitung den Maßgaben folgt, die sich aus der Folgenabschätzung ergeben haben.

§ 63
Zusammenarbeit mit der oder dem Hessischen Datenschutzbeauftragten

Der Verantwortliche und der Auftragsverarbeiter haben mit der oder dem Hessischen Datenschutzbeauftragten bei der Erfüllung ihrer oder seiner Aufgaben zusammenzuarbeiten.

§ 64
Vorherige Konsultation der oder des Hessischen Datenschutzbeauftragten

(1) Der Verantwortliche hat vor der Inbetriebnahme von neu anzulegenden Dateisystemen die Hessische Datenschutzbeauftragte oder den Hessischen Datenschutzbeauftragten zu konsultieren, wenn

1. aus einer Datenschutz-Folgenabschätzung nach § 62 hervorgeht, dass die Verarbeitung ein hohes Risiko für die Rechte und Freiheiten der betroffenen Personen zur Folge hätte, sofern der Verantwortliche keine Maßnahmen zur Eindämmung des Risikos trifft, oder
2. die Form der Verarbeitung, insbesondere bei der Verwendung neuer Technologien, Mechanismen oder Verfahren, ein hohes Risiko für die Rechte und Freiheiten der betroffenen Personen zur Folge hat.

Die oder der Hessische Datenschutzbeauftragte kann eine Liste der Verarbeitungsvorgänge erstellen, die der Pflicht zur vorherigen Konsultation nach Satz 1 unterliegen. § 59 Abs. 1 Satz 2 gilt entsprechend.

(2) Der oder dem Hessischen Datenschutzbeauftragten sind im Fall des Abs. 1 vorzulegen:

1. die nach § 62 durchgeführte Datenschutz-Folgenabschätzung,
2. gegebenenfalls Angaben zu den jeweiligen Zuständigkeiten des Verantwortlichen, der gemeinsam Verantwortlichen und der an der Verarbeitung beteiligten Auftragsverarbeiter,
3. Angaben zu den Zwecken und Mitteln der beabsichtigten Verarbeitung,

4. Angaben zu den zum Schutz der Rechte und Freiheiten der betroffenen Personen vorgesehenen Maßnahmen und Garantien und

5. die Kontaktdaten der oder des Datenschutzbeauftragten.

Auf Anfrage sind der oder dem Hessischen Datenschutzbeauftragten alle sonstigen Informationen zu übermitteln, die sie oder er benötigt, um die Rechtmäßigkeit der Verarbeitung sowie insbesondere die in Bezug auf den Schutz der personenbezogenen Daten der betroffenen Personen bestehenden Risiken und die diesbezüglichen Garantien bewerten zu können.

(3) Falls die oder der Hessische Datenschutzbeauftragte der Auffassung ist, dass die geplante Verarbeitung gegen gesetzliche Vorgaben verstoßen würde, insbesondere weil der Verantwortliche das Risiko nicht ausreichend ermittelt oder nicht ausreichend eingedämmt hat, kann sie oder er dem Verantwortlichen und gegebenenfalls dem Auftragsverarbeiter innerhalb eines Zeitraums von bis zu sechs Wochen nach Erhalt des Ersuchens um Konsultation schriftliche Empfehlungen unterbreiten, welche Maßnahmen noch ergriffen werden sollten. Die oder der Hessische Datenschutzbeauftragte kann diese Frist um einen Monat verlängern, wenn die geplante Verarbeitung besonders komplex ist. Sie oder er hat in diesem Fall innerhalb eines Monats nach Eingang des Antrags auf Konsultation den Verantwortlichen und gegebenenfalls den Auftragsverarbeiter über die Fristverlängerung zusammen mit den Gründen für die Verzögerung zu informieren.

(4) Hat die beabsichtigte Verarbeitung erhebliche Bedeutung für die Aufgabenerfüllung des Verantwortlichen und ist sie daher besonders dringlich, kann er mit der Verarbeitung nach Beginn der vorherigen Konsultation, aber vor Ablauf der in Abs. 3 genannten Frist beginnen. In diesem Fall sind die Empfehlungen der oder des Hessischen Datenschutzbeauftragten im Nachhinein zu berücksichtigen und sind die Art und Weise der Verarbeitung daraufhin gegebenenfalls anzupassen.

(5) Die oder der Hessische Datenschutzbeauftragte ist bei der Ausarbeitung eines Vorschlags für eine vom Landtag zu erlassende Gesetzgebungsmaßnahme oder von auf solchen Gesetzgebungsmaßnahmen basierenden Regelungsmaßnahmen, die die Verarbeitung personenbezogener Daten betreffen, zu konsultieren.

§ 65
Verzeichnis von Verarbeitungstätigkeiten

(1) Der Verantwortliche hat ein Verzeichnis aller Kategorien von Verarbeitungstätigkeiten zu führen, die seiner Zuständigkeit unterliegen. Dieses Verzeichnis hat die folgenden Angaben zu enthalten:

1. den Namen und die Kontaktdaten des Verantwortlichen und gegebenenfalls des gemeinsam mit ihm Verantwortlichen sowie der oder des Datenschutzbeauftragten,

2. die Zwecke der Verarbeitung,

3. die Kategorien von Empfängern, gegenüber denen die personenbezogenen Daten offengelegt worden sind oder noch offengelegt werden sollen, einschließlich Empfängern in Drittländern oder internationalen Organisationen,

4. eine Beschreibung der Kategorien betroffener Personen und der Kategorien personenbezogener Daten,

5. gegebenenfalls die Verwendung von Profiling,

6. gegebenenfalls die Kategorien von Übermittlungen personenbezogener Daten an ein Drittland oder an eine internationale Organisation,

7. Angaben über die Rechtsgrundlage der Verarbeitung, einschließlich der Übermittlungen, für die die personenbezogenen Daten bestimmt sind,

8. wenn möglich, die vorgesehenen Fristen für die Löschung oder die Überprüfung der Erforderlichkeit der Speicherung der verschiedenen Kategorien personenbezogener Daten und

9. wenn möglich, eine allgemeine Beschreibung der technischen und organisatorischen Maßnahmen nach § 59.

(2) Der Auftragsverarbeiter hat ein Verzeichnis aller Kategorien von Verarbeitungen zu führen, die er im Auftrag eines Verantwortlichen durchführt, das Folgendes zu enthalten hat:

1. den Namen und die Kontaktdaten des Auftragsverarbeiters, jedes Verantwortlichen, in dessen Auftrag der Auftragsverarbeiter tätig ist, sowie gegebenenfalls die Kontaktdaten der oder des Datenschutzbeauftragten,

2. die Kategorien von Verarbeitungen, die im Auftrag jedes Verantwortlichen durchgeführt werden,

3. gegebenenfalls Übermittlungen von personenbezogenen Daten an ein Drittland oder an eine internationale Organisation, wenn vom Verantwortlichen entsprechend angewiesen, unter Angabe des betreffenden Drittlands oder der betreffenden internationalen Organisation und
4. wenn möglich, eine allgemeine Beschreibung der technischen und organisatorischen Maßnahmen nach § 59.

(3) Die in den Abs. 1 und 2 genannten Verzeichnisse sind schriftlich oder elektronisch zu führen.

(4) Verantwortliche und Auftragsverarbeiter haben auf Anfrage ihre Verzeichnisse der oder dem Hessischen Datenschutzbeauftragten zur Verfügung zu stellen.

§ 66
Datenschutz durch Technikgestaltung und datenschutzfreundliche Voreinstellungen

(1) Der Verantwortliche hat sowohl zum Zeitpunkt der Festlegung der Mittel für die Verarbeitung als auch zum Zeitpunkt der Verarbeitung selbst angemessene technische und organisatorische Maßnahmen zu treffen, die geeignet sind, die Datenschutzgrundsätze wie etwa die Datensparsamkeit wirksam umzusetzen, und notwendige Garantien in die Verarbeitung aufzunehmen, um den gesetzlichen Anforderungen zu genügen und die Rechte der betroffenen Personen zu schützen. Er hat hierbei den Stand der Technik, die Implementierungskosten und die Art, den Umfang, die Umstände und die Zwecke der Verarbeitung sowie die unterschiedliche Eintrittswahrscheinlichkeit und Schwere der mit der Verarbeitung verbundenen Risiken für die Rechte und Freiheiten natürlicher Personen zu berücksichtigen. Insbesondere sind die Verarbeitung personenbezogener Daten und die Auswahl und Gestaltung von Datenverarbeitungssystemen an dem Ziel auszurichten, so wenig personenbezogene Daten wie möglich zu verarbeiten. Personenbezogene Daten sind zum frühestmöglichen Zeitpunkt zu anonymisieren oder zu pseudonymisieren, soweit dies nach dem Verarbeitungszweck möglich ist.

(2) Der Verantwortliche hat geeignete technische und organisatorische Maßnahmen zu treffen, die sicherstellen, dass durch Voreinstellungen grundsätzlich nur solche personenbezogenen Daten verarbeitet werden, deren Verarbeitung für den jeweiligen bestimmten Verarbeitungszweck erforderlich ist. Dies betrifft die Menge der erhobenen personenbezogenen Daten, den Umfang ihrer Verarbeitung, ihre Speicherfrist und ihre Zugänglichkeit. Die Maßnahmen müssen insbesondere sicherstellen, dass die personenbezogenen Daten durch Voreinstellungen nicht ohne Eingreifen einer Person einer unbestimmten Anzahl von natürlichen Personen zugänglich gemacht werden.

§ 67
Unterscheidung zwischen verschiedenen Kategorien betroffener Personen

Der Verantwortliche hat bei der Verarbeitung personenbezogener Daten so weit wie möglich zwischen den verschiedenen Kategorien betroffener Personen zu unterscheiden. Dies betrifft insbesondere folgende Kategorien:

1. Personen, gegen die ein begründeter Verdacht besteht, dass sie eine Straftat begangen haben,
2. Personen, gegen die ein begründeter Verdacht besteht, dass sie in naher Zukunft eine Straftat begehen werden,
3. verurteilte Straftäter,
4. Opfer einer Straftat oder Personen, bei denen bestimmte Tatsachen darauf hindeuten, dass sie Opfer einer Straftat sein könnten, und
5. andere Personen wie insbesondere Zeuginnen und Zeugen, Hinweisgeberinnen und Hinweisgeber oder Personen, die mit den in den Nr. 1 bis 4 genannten Personen in Kontakt oder Verbindung stehen.

§ 68
Unterscheidung zwischen Tatsachen und persönlichen Einschätzungen

Der Verantwortliche hat bei der Verarbeitung so weit wie möglich danach zu unterscheiden, ob personenbezogene Daten auf Tatsachen oder auf persönlichen Einschätzungen beruhen. Zu diesem Zweck soll er, soweit dies im Rahmen der jeweiligen Verarbeitung möglich und angemessen ist, Bewertungen, die auf persönlichen Einschätzungen beruhen, als solche kenntlich machen. Es muss außerdem feststellbar sein, welche Stelle die Unterlagen führt, die der auf einer persönlichen Einschätzung beruhenden Bewertung zugrunde liegen.

§ 69
Qualitätssicherung personenbezogener Daten vor deren Übermittlung

(1) Der Verantwortliche hat angemessene Maßnahmen zu ergreifen, um zu gewährleisten, dass unrichtige sowie ohne sachlichen Grund unvollständige oder nicht mehr aktuelle personenbezogene Daten nicht übermittelt oder sonst bereitgestellt werden. Zu diesem Zweck hat er, soweit dies mit angemessenem Aufwand möglich ist, die Qualität der personenbezogenen Daten vor ihrer Übermittlung oder Bereitstellung zu überprüfen. Bei jeder Übermittlung personenbezogener Daten hat er, soweit dies möglich und angemessen ist, Informationen beizufügen, die es dem Empfänger gestatten, die Richtigkeit, die Vollständigkeit und die Zuverlässigkeit der Daten sowie deren Aktualität zu beurteilen.

(2) Gelten für die Verarbeitung von personenbezogenen Daten besondere Bedingungen, so hat bei Datenübermittlungen die übermittelnde Stelle den Empfänger darauf hinzuweisen, dass diese Bedingungen gelten und einzuhalten sind. Die Hinweispflicht kann dadurch erfüllt werden, dass die Daten entsprechend markiert werden.

(3) Die übermittelnde Stelle darf auf Empfänger in anderen Mitgliedstaaten der Europäischen Union oder auf Einrichtungen und sonstige Stellen, die nach den Kapiteln 4 und 5 des Titels V des Dritten Teils des Vertrags über die Arbeitsweise der Europäischen Union errichtet wurden, keine Bedingungen anwenden, die nicht auch für entsprechende innerstaatliche Datenübermittlungen gelten.

§ 70
Berichtigung und Löschung personenbezogener Daten
sowie Einschränkung der Verarbeitung

(1) Der Verantwortliche hat personenbezogene Daten zu berichtigen, wenn sie unrichtig sind. § 53 Abs. 1 Satz 2 und 3 ist entsprechend anzuwenden.

(2) Der Verantwortliche hat personenbezogene Daten unverzüglich zu löschen, wenn ihre Verarbeitung unzulässig ist, ihre Kenntnis für seine Aufgabenerfüllung nicht mehr erforderlich ist oder sie zur Erfüllung einer rechtlichen Verpflichtung gelöscht werden müssen.

(3) § 53 Abs. 3 bis 5 ist entsprechend anzuwenden. Sind unrichtige personenbezogene Daten oder personenbezogene Daten unrechtmäßig übermittelt worden, ist auch dies dem Empfänger mitzuteilen.

(4) Unbeschadet in Rechtsvorschriften festgesetzter Höchstspeicher- oder Löschfristen hat der Verantwortliche für die Löschung von personenbezogenen Daten oder eine regelmäßige Überprüfung der Notwendigkeit ihrer Speicherung angemessene Fristen vorzusehen und durch verfahrensrechtliche Vorkehrungen sicherzustellen, dass diese Fristen eingehalten werden.

§ 71
Protokollierung

(1) In automatisierten Verarbeitungssystemen haben Verantwortliche und Auftragsverarbeiter mindestens die folgenden Verarbeitungsvorgänge zu protokollieren:

1. Erhebung,
2. Veränderung,
3. Abfrage,
4. Offenlegung einschließlich Übermittlung,
5. Kombination und
6. Löschung.

(2) Die Protokolle über Abfragen und Offenlegungen müssen es ermöglichen, die Begründung, das Datum und die Uhrzeit dieser Vorgänge und so weit wie möglich die Identität der Person, die die personenbezogenen Daten abgefragt oder offengelegt hat, und die Identität des Empfängers der Daten festzustellen.

(3) Die Protokolle dürfen ausschließlich zur Überprüfung der Rechtmäßigkeit der Datenverarbeitung durch die Datenschutzbeauftragte oder den Datenschutzbeauftragten und die Hessische Datenschutzbeauftragte oder den Hessischen Datenschutzbeauftragten sowie zur Eigenüberwachung, der Sicherstellung der Integrität und Sicherheit der personenbezogenen Daten und für Strafverfahren verwendet werden.

(4) Der Verantwortliche und der Auftragsverarbeiter haben die Protokolle der oder dem Hessischen Datenschutzbeauftragten auf Anforderung zur Verfügung zu stellen.

§ 72
Vertrauliche Meldung von Verstößen

Der Verantwortliche hat zu ermöglichen, dass ihm vertrauliche Meldungen über in seinem Verantwortungsbereich erfolgende Verstöße gegen Datenschutzvorschriften zugeleitet werden können.

Fünfter Abschnitt
Datenübermittlungen an Drittländer und an internationale Organisationen

§ 73
Allgemeine Voraussetzungen

(1) Die Übermittlung personenbezogener Daten an Stellen in Drittländern oder an internationale Organisationen ist bei Vorliegen der übrigen für Datenübermittlungen geltenden Voraussetzungen zulässig, wenn

1. die Stelle oder internationale Organisation für die in § 40 genannten Zwecke zuständig ist und
2. die Europäische Kommission nach Art. 36 Abs. 3 der Richtlinie (EU) Nr. 2016/680 einen Angemessenheitsbeschluss gefasst hat.

(2) Die Übermittlung personenbezogener Daten hat trotz des Vorliegens eines Angemessenheitsbeschlusses im Sinne des Abs. 1 Nr. 2 und des zu berücksichtigenden öffentlichen Interesses an der Datenübermittlung zu unterbleiben, wenn im Einzelfall ein datenschutzrechtlich angemessener und die elementaren Menschenrechte wahrender Umgang mit den Daten beim Empfänger nicht hinreichend gesichert ist oder sonst überwiegende schutzwürdige Interessen einer betroffenen Person entgegenstehen. Bei seiner Beurteilung hat der Verantwortliche maßgeblich zu berücksichtigen, ob der Empfänger im Einzelfall einen angemessenen Schutz der übermittelten Daten garantiert.

(3) Wenn personenbezogene Daten, die aus einem anderen Mitgliedstaat der Europäischen Union übermittelt oder zur Verfügung gestellt wurden, nach Abs. 1 übermittelt werden sollen, muss diese Übermittlung zuvor von der zuständigen Stelle des anderen Mitgliedstaats genehmigt werden. Übermittlungen ohne vorherige Genehmigung sind nur dann zulässig, wenn die Übermittlung erforderlich ist, um eine unmittelbare und ernsthafte Gefahr für die öffentliche Sicherheit eines Mitgliedstaats oder eines Drittlandes oder für die wesentlichen Interessen eines Mitgliedstaats abzuwehren, und die vorherige Genehmigung nicht rechtzeitig eingeholt werden kann. Im Fall des Satz 2 ist die Stelle des anderen Mitgliedstaats, die für die Erteilung der Genehmigung zuständig gewesen wäre, unverzüglich über die Übermittlung zu unterrichten.

(4) Der Verantwortliche, der Daten nach Abs. 1 übermittelt, hat durch geeignete Maßnahmen sicherzustellen, dass der Empfänger die übermittelten Daten nur dann an Stellen in anderen Drittländern oder andere internationale Organisationen weiterübermittelt, wenn der Verantwortliche diese Übermittlung zuvor genehmigt hat. Bei der Entscheidung über die Erteilung der Genehmigung hat der Verantwortliche alle maßgeblichen Faktoren zu berücksichtigen, insbesondere die Schwere der Straftat, den Zweck der ursprünglichen Übermittlung und das in dem Drittland oder der internationalen Organisation, an das oder an die die Daten weiterübermittelt werden sollen, bestehende Schutzniveau für personenbezogene Daten. Eine Genehmigung darf nur dann erfolgen, wenn auch eine direkte Übermittlung an die Stelle im anderen Drittland oder die andere internationale Organisation zulässig wäre. Die Zuständigkeit für die Erteilung der Genehmigung kann auch abweichend geregelt werden.

§ 74
Datenübermittlung bei geeigneten Garantien

(1) Liegt entgegen § 73 Abs. 1 Nr. 2 kein Beschluss nach Art. 36 Abs. 3 der Richtlinie (EU) Nr. 2016/680 vor, ist eine Übermittlung bei Vorliegen der übrigen Voraussetzungen des § 73 auch dann zulässig, wenn

1. in einem rechtsverbindlichen Instrument geeignete Garantien für den Schutz personenbezogener Daten vorgesehen sind oder
2. der Verantwortliche nach Beurteilung aller Umstände, die bei der Übermittlung eine Rolle spielen, zu der Auffassung gelangt ist, dass geeignete Garantien für den Schutz personenbezogener Daten bestehen.

(2) Der Verantwortliche hat Übermittlungen nach Abs. 1 Nr. 2 zu dokumentieren. Die Dokumentation hat den Zeitpunkt der Übermittlung, Informationen über die empfangende zuständige Behörde, die Begründung der Übermittlung und die übermittelten personenbezogenen Daten zu enthalten. Sie ist der oder dem Hessischen Datenschutzbeauftragten auf Anforderung zur Verfügung zu stellen.

(3) Der Verantwortliche hat die Hessische Datenschutzbeauftragte oder den Hessischen Datenschutzbeauftragten zumindest jährlich über Übermittlungen zu unterrichten, die aufgrund einer Beurteilung nach Abs. 1 Nr. 2 erfolgt sind. In der Unterrichtung kann er die Empfänger und die Übermittlungszwecke angemessen kategorisieren.

§ 75
Ausnahmen für eine Datenübermittlung ohne geeignete Garantien

(1) Liegt entgegen § 73 Abs. 1 Nr. 2 kein Beschluss nach Art. 36 Abs. 3 der Richtlinie (EU) Nr. 2016/680 vor und liegen auch keine geeigneten Garantien im Sinne des § 74 Abs. 1 vor, ist eine Übermittlung bei Vorliegen der übrigen Voraussetzungen des § 73 auch dann zulässig, wenn die Übermittlung erforderlich ist

1. zum Schutz lebenswichtiger Interessen einer natürlichen Person,
2. zur Wahrung berechtigter Interessen der betroffenen Person,
3. zur Abwehr einer gegenwärtigen und erheblichen Gefahr für die öffentliche Sicherheit eines Staates,
4. im Einzelfall für die in § 40 genannten Zwecke oder
5. im Einzelfall zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen im Zusammenhang mit den in § 40 genannten Zwecken.

(2) Der Verantwortliche hat von einer Übermittlung nach Abs. 1 abzusehen, wenn die Grundrechte der betroffenen Person das öffentliche Interesse an der Übermittlung überwiegen.

(3) Für Übermittlungen nach Abs. 1 gilt § 74 Abs. 2 und 3 entsprechend.

§ 76
Sonstige Datenübermittlung an Empfänger in Drittländern

(1) Verantwortliche können bei Vorliegen der übrigen für die Datenübermittlung in Drittländer geltenden Voraussetzungen im besonderen Einzelfall personenbezogene Daten unmittelbar an nicht in § 73 Abs. 1 Nr. 1 genannte Stellen in Drittländern übermitteln, wenn die Übermittlung zur Erfüllung ihrer Aufgaben für die in § 40 genannten Zwecke unbedingt erforderlich ist und

1. im konkreten Fall keine Grundrechte der betroffenen Person das öffentliche Interesse an einer Übermittlung überwiegen,
2. die Übermittlung an die in § 73 Abs. 1 Nr. 1 genannten Stellen wirkungslos oder ungeeignet wäre, insbesondere weil sie nicht rechtzeitig durchgeführt werden kann, und
3. der Verantwortliche dem Empfänger die Zwecke der Verarbeitung mitteilt und ihn darauf hinweist, dass die übermittelten Daten nur in dem Umfang verarbeitet werden dürfen, in dem ihre Verarbeitung für diese Zwecke erforderlich ist.

(2) Im Fall des Abs. 1 hat der Verantwortliche die in § 73 Abs. 1 Nr. 1 genannten Stellen unverzüglich über die Übermittlung zu unterrichten, sofern dies nicht wirkungslos oder ungeeignet ist.

(3) Für Übermittlungen nach Abs. 1 gilt § 74 Abs. 2 und 3 entsprechend.

(4) Bei Übermittlungen nach Abs. 1 hat der Verantwortliche den Empfänger zu verpflichten, die übermittelten personenbezogenen Daten ohne seine Zustimmung nur für den Zweck zu verarbeiten, für den sie übermittelt worden sind.

(5) Abkommen im Bereich der justiziellen Zusammenarbeit in Strafsachen und der polizeilichen Zusammenarbeit bleiben unberührt.

Sechster Abschnitt
Zusammenarbeit der Aufsichtsbehörden

§ 77
Gegenseitige Amtshilfe

(1) Die oder der Hessische Datenschutzbeauftragte hat den Datenschutzaufsichtsbehörden in anderen Mitgliedstaaten der Europäischen Union Informationen zu übermitteln und Amtshilfe zu

leisten, soweit dies für eine einheitliche Umsetzung und Anwendung der Richtlinie (EU) Nr. 2016/680 erforderlich ist. Die Amtshilfe betrifft insbesondere Auskunftsersuchen und aufsichtsbezogene Maßnahmen, beispielsweise Ersuchen um Konsultation oder um Vornahme von Nachprüfungen und Untersuchungen.

(2) Die oder der Hessische Datenschutzbeauftragte hat alle geeigneten Maßnahmen zu ergreifen, um Amtshilfeersuchen unverzüglich und spätestens innerhalb eines Monats nach deren Eingang nachzukommen.

(3) Die oder der Hessische Datenschutzbeauftragte darf Amtshilfeersuchen nur ablehnen, wenn

1. sie oder er für den Gegenstand des Ersuchens oder für die Maßnahmen, die sie oder er durchführen soll, nicht zuständig ist oder
2. ein Eingehen auf das Ersuchen gegen Rechtsvorschriften verstoßen würde.

(4) Die oder der Hessische Datenschutzbeauftragte hat die ersuchende Aufsichtsbehörde des anderen Staates über die Ergebnisse oder gegebenenfalls über den Fortgang der Maßnahmen zu informieren, die getroffen wurden, um dem Amtshilfeersuchen nachzukommen. Sie oder er hat im Fall des Abs. 3 die Gründe für die Ablehnung des Ersuchens zu erläutern.

(5) Die oder der Hessische Datenschutzbeauftragte hat die Informationen, um die sie oder er von der Aufsichtsbehörde des anderen Staates ersucht wurde, in der Regel elektronisch und in einem standardisierten Format zu übermitteln.

(6) Die oder der Hessische Datenschutzbeauftragte hat Amtshilfeersuchen kostenfrei zu erledigen, soweit sie oder er nicht im Einzelfall mit der Aufsichtsbehörde des anderen Staates die Erstattung entstandener Ausgaben vereinbart hat.

(7) Ein Amtshilfeersuchen der oder des Hessischen Datenschutzbeauftragten hat alle erforderlichen Informationen zu enthalten; hierzu gehören insbesondere der Zweck und die Begründung des Ersuchens. Die auf das Ersuchen übermittelten Informationen dürfen ausschließlich zu dem Zweck verwendet werden, zu dem sie angefordert wurden.

Siebter Abschnitt
Haftung und Sanktionen

§ 78
Schadensersatz und Entschädigung

(1) Hat ein Verantwortlicher einer betroffenen Person durch eine Verarbeitung personenbezogener Daten, die nach diesem Gesetz oder nach anderen auf ihre Verarbeitung anwendbaren Vorschriften rechtswidrig war, einen Schaden zugefügt, ist er oder sein Rechtsträger der betroffenen Person zum Schadensersatz verpflichtet. Die Ersatzpflicht entfällt, soweit bei einer nicht automatisierten Verarbeitung der Schaden nicht auf ein Verschulden des Verantwortlichen zurückzuführen ist.

(2) Wegen eines Schadens, der nicht Vermögensschaden ist, kann die betroffene Person eine angemessene Entschädigung in Geld verlangen.

(3) Lässt sich bei einer automatisierten Verarbeitung personenbezogener Daten nicht ermitteln, welche von mehreren beteiligten Verantwortlichen den Schaden verursacht hat, so haftet jeder Verantwortliche beziehungsweise sein Rechtsträger.

(4) Bei einem Mitverschulden der betroffenen Person ist § 254 des Bürgerlichen Gesetzbuchs entsprechend anzuwenden.

(5) Auf die Verjährung finden die für unerlaubte Handlungen geltenden Verjährungsvorschriften des Bürgerlichen Gesetzbuchs entsprechende Anwendung.

(6) Weitergehende sonstige Schadensersatzansprüche bleiben unberührt.

(7) Der Rechtsweg zu den ordentlichen Gerichten steht offen.

§ 79
Strafvorschriften

Für Verarbeitungen personenbezogener Daten durch öffentliche Stellen im Rahmen von Tätigkeiten nach § 40 findet § 37 entsprechende Anwendung.

VIERTER TEIL
Anspruch auf Informationszugang

§ 80
Anspruch auf Informationszugang

(1) Jeder hat nach Maßgabe des Vierten Teils dieses Gesetzes gegenüber öffentlichen Stellen Anspruch auf Zugang zu amtlichen Informationen.

(2) Soweit besondere Rechtsvorschriften die Auskunftserteilung regeln, gehen sie den Vorschriften des Vierten Teils dieses Gesetzes vor.

§ 81
Anwendungsbereich

(1) Nach Maßgabe des § 2 Abs. 1 bis 3 gelten die Vorschriften über den Zugang zu Informationen auch für

1. den Landtag, nur soweit er öffentlich-rechtliche Verwaltungsaufgaben wahrnimmt und auszuschließen ist, dass durch die Informationsweitergabe die Freiheit des Mandats, der Bereich der Abgeordneten- und Fraktionsangelegenheiten sowie die Nicht öffentlichkeit von Landtagsberatungen beeinträchtigt wird,
2. den Hessischen Rechnungshof und die oder den Hessischen Datenschutzbeauftragten, nur soweit deren Aufgabenstellung nicht beeinträchtigt wird,
3. die Gerichte, Strafverfolgungs- und Strafvollstreckungsbehörden sowie Disziplinarbehörden jeweils nur, soweit sie öffentlich-rechtliche Verwaltungsaufgaben wahrnehmen,
4. Finanzbehörden, nur soweit sie nicht in Verfahren nach der Abgabenordnung tätig werden,
5. Universitätskliniken, Forschungseinrichtungen, Hochschulen, Schulen sowie sonstige öffentliche Stellen, soweit sie nicht in den Bereichen Forschung und Lehre, Leistungsbeurteilungen und Prüfungen tätig werden,
6. die Behörden und sonstigen öffentlichen Stellen der Gemeinden und Landkreise sowie deren Vereinigungen ungeachtet ihrer Rechtsform, soweit die Anwendung des Vierten Teils dieses Gesetzes durch Satzung ausdrücklich bestimmt wird.

(2) Die Vorschriften des Vierten Teils dieses Gesetzes gelten nicht für

1. die Polizeibehörden und das Landesamt für Verfassungsschutz,
2. die Landeskartellbehörde und die Regulierungskammer Hessen,
3. die Industrie- und Handelskammern und die Handwerkskammern,
4. Notare.

(3) Von der Auskunft nach § 80 Abs. 1 sind Datei- und Aktenbestandteile von Stellen nach Abs. 2 vollständig und von Stellen nach Abs. 1, soweit sie sich auf vom Anwendungsbereich der Vorschriften über den Zugang zu Informationen ausgenommene Tätigkeitsfelder beziehen, auch dann ausgenommen, wenn sie sich in Dateien oder Akten anderer öffentlicher Stellen befinden.

§ 82
Schutz besonderer öffentlicher und privater Belange

Ein Anspruch auf Auskunft nach § 80 Abs. 1 besteht nicht

1. bei Verschlusssachen nach § 2 Abs. 1 des Hessischen Sicherheitsüberprüfungsgesetzes vom 19. Dezember 2014 (GVBl. S. 364),
2. bei Informationen, deren Bekanntwerden nachteilige Auswirkungen haben kann auf
   a) die inter- und supranationalen Beziehungen, die Beziehung zum Bund oder zu einem anderen Land,
   b) Belange der äußeren oder öffentlichen Sicherheit,
   c) die Kontroll-, Vollzugs- oder Aufsichtsaufgaben der Finanz-, Regulierungs-, Sparkassen, Versicherungs- und Wettbewerbsaufsichtsbehörden oder
   d) den Erfolg eines strafrechtlichen Ermittlungs- oder Strafvollstreckungsverfahrens oder den Verfahrensablauf eines Gerichts-, Ordnungswidrigkeiten- oder Disziplinarverfahrens,
3. bei einem Berufs- oder besonderen Amtsgeheimnis unterliegenden Datei- oder Akteninhalten,

4. bei zum persönlichen Lebensbereich gehörenden Geheimnissen oder Betriebs- oder Geschäftsgeheimnissen, sofern die betroffene Person nicht eingewilligt hat oder

5. soweit ein rein wirtschaftliches Interesse an den Informationen besteht.

§ 83
Schutz personenbezogener Daten

Der Zugang zu personenbezogenen Daten ist nur dann zu gewähren, wenn eine Übermittlung personenbezogener Daten an eine nicht öffentliche Stelle zulässig ist.

§ 84
Schutz behördlicher Entscheidungsprozesse

(1) Der Antrag auf Informationszugang kann abgelehnt werden für Entwürfe zu Entscheidungen sowie für Arbeiten und Beschlüsse zu ihrer unmittelbaren Vorbereitung, soweit und solange durch die vorzeitige Bekanntgabe der Informationen der Erfolg der Entscheidung oder bevorstehender behördlicher Maßnahme vereitelt würde. Nicht der unmittelbaren Entscheidungsvorbereitung nach Satz 1 dienen regelmäßig Ergebnisse der Beweiserhebung und Gutachten oder Stellungnahmen Dritter.

(2) Der Antrag ist abzulehnen, wenn das Bekanntwerden der Informationen den Kernbereich der Willens- und Entscheidungsbildung der Landesregierung betrifft.

(3) Der Antrag auf Informationszugang zu Protokollen vertraulicher Beratungen ist abzulehnen.

(4) Die Ablehnungsgründe nach Abs. 1 und 2 entfallen nach Abschluss des jeweiligen Entscheidungsprozesses. Hinsichtlich Abs. 2 gilt dies nur für Ergebnisprotokolle.

§ 85
Antrag

(1) Der Zugang zu Informationen wird auf Antrag gewährt. Der Antrag kann schriftlich, mündlich, zur Niederschrift oder in elektronischer Form gestellt werden.

(2) Im Antrag sollen die begehrten Informationen möglichst genau umschrieben werden. Ein Antrag, der auf allgemeines Behördenhandeln gerichtet ist und sich auf Informationen bezieht, die aus einer Vielzahl von Aktenvorgängen oder Informationsträgern zusammengetragen werden müssen, ist unzulässig. Sofern der antragstellenden Person Angaben zur Umschreibung der begehrten Informationen fehlen, ist die angerufene informationspflichtige Stelle zur Beratung verpflichtet.

(3) Betrifft der Antrag Daten Dritter im Sinne der §§ 82 und 83, muss er begründet werden.

(4) Der Antrag soll bei der informationspflichtigen Stelle gestellt werden, welche über die begehrten Informationen verfügt. Ist die angerufene Stelle nicht die informationspflichtige Stelle, so hat die angerufene Stelle die zuständige Stelle der antragstellenden Person zu benennen.

§ 86
Verfahren bei Beteiligung einer betroffenen Person

(1) Die informationspflichtige Stelle gibt einem Dritten, dessen Belange durch den Antrag auf Informationszugang berührt sind, schriftlich Gelegenheit zur Stellungnahme innerhalb eines Monats, sofern Anhaltspunkte dafür vorliegen, dass er ein schutzwürdiges Interesse am Ausschluss des Informationszugangs haben kann. Die Einwilligung des Dritten zum Informationszugang der antragstellenden Person gilt als verweigert, wenn sie nicht innerhalb eines Monats nach Anfrage durch die zuständige Stelle vorliegt.

(2) Die Entscheidung über den Antrag auf Informationszugang ist auch dem Dritten bekannt zu geben. Der Informationszugang darf erst erfolgen, wenn die Entscheidung dem Dritten gegenüber bestandskräftig ist oder die sofortige Vollziehung angeordnet wurde und seit der Bekanntgabe der Anordnung an den Dritten zwei Wochen verstrichen sind.

§ 87
Entscheidung

(1) Die informationspflichtige Stelle macht die begehrten Informationen unverzüglich, spätestens aber innerhalb eines Monats nach Eingang des hinreichend bestimmten Antrags bei der Stelle zugänglich. Die Frist beträgt drei Monate bei der Beteiligung Dritter.

(2) Die Ablehnung eines Antrages oder die Beschränkung des begehrten Zugangs zu Informationen ist innerhalb der in Abs. 1 genannten Frist schriftlich bekannt zu geben und zu begrün-

den. Soweit die informationspflichtige Stelle den Antrag ganz oder teilweise ablehnt, hat sie mitzuteilen, ob und wann der Informationszugang ganz oder teilweise zu einem späteren Zeitpunkt voraussichtlich möglich ist.

(3) Können die gewünschten Informationen nicht oder nicht vollständig innerhalb eines Monats zugänglich gemacht werden oder erfordern Umfang oder Komplexität eine intensive Prüfung, so kann die auskunftspflichtige Stelle die Frist um einen Monat verlängern. Die antragstellende Person ist über die Fristverlängerung unter Angabe der maßgeblichen Gründe schriftlich zu informieren.

§ 88
Kosten

(1) Die Erteilung mündlicher und einfacher schriftlicher Auskünfte sowie die Einsichtnahme in Dateien und Akten vor Ort nach dem Vierten Teil dieses Gesetzes sind kostenfrei. Für sonstige Amtshandlungen nach diesem Teil werden Kosten (Gebühren und Auslagen) nach Maßgabe des Hessischen Verwaltungskostengesetzes erhoben. Von § 9 des Hessischen Verwaltungskostengesetzes gelten nur Abs. 1 Satz 1 Nr. 6, insoweit mit der Maßgabe, dass Auslagen für Ausfertigungen, Abschriften und Kopien 0,10 Euro je Seite nicht überschreiten dürfen, und Abs. 5. Die Gebühren sind auch unter Berücksichtigung des Verwaltungsaufwandes so zu bemessen, dass die antragstellenden Personen dadurch nicht von der Geltendmachung ihres Informationsanspruchs nach § 80 Abs. 1 abgehalten werden.

(2) Im Fall des § 81 Satz 1 Nr. 6 werden Kosten nach Maßgabe der Satzung erhoben.

§ 89
Die oder der Hessische Informationsfreiheitsbeauftragte

(1) Jeder, der sich in seinem Recht auf Informationszugang nach den Vorschriften des Vierten Teils dieses Gesetzes verletzt sieht, kann unbeschadet anderweitiger Rechtsbehelfe die Hessische Informationsfreiheitsbeauftragte oder den Hessischen Informationsfreiheitsbeauftragten anrufen.

(2) Die Aufgabe der oder des Hessischen Informationsfreiheitsbeauftragten wird von der oder dem Hessischen Datenschutzbeauftragten wahrgenommen.

(3) Die auskunftspflichtigen Stellen sind verpflichtet, die Hessische Informationsfreiheitsbeauftragte oder den Hessischen Informationsfreiheitsbeauftragten und ihre oder seine Beauftragten in der Erfüllung ihrer Aufgaben zu unterstützen. Der oder dem Hessischen Informationsfreiheitsbeauftragten ist dabei insbesondere

1. Auskunft zu ihren oder seinen Fragen zu erteilen sowie Einsicht in alle Dateien und Akten zu verschaffen, die im Zusammenhang mit dem Informationsanliegen stehen und
2. Zutritt zu den Diensträumen zu gewähren.

Stellt die oder der Hessische Informationsfreiheitsbeauftragte Verstöße gegen die Vorschriften des Vierten Teils dieses Gesetzes fest, kann sie oder er ihre Behebung in angemessener Frist fordern. Darüber ist die zuständige Aufsichtsbehörde zu unterrichten.

(4) Zum 31. Dezember jedes Jahres hat die oder der Hessische Informationsfreiheitsbeauftragte dem Landtag und der Landesregierung einen Bericht über ihre oder seine Tätigkeit vorzulegen. Die Landesregierung legt ihre Stellungnahme zu dem Bericht dem Landtag vor.

FÜNFTER TEIL
Übergangs- und Schlussvorschriften

§ 90
Übergangsvorschriften

(1) Vor dem 6. Mai 2016 eingerichtete automatisierte Verarbeitungssysteme sind zeitnah, in Ausnahmefällen, in denen dies mit einem unverhältnismäßigen Aufwand verbunden ist, jedoch spätestens bis zum 6. Mai 2023, mit § 71 Abs. 1 und 2 in Einklang zu bringen.

(2) Für die Person, die am 24. Mai 2018 das Amt der oder des Hessischen Datenschutzbeauftragten innehat, gilt bis zur ersten Wahl der oder des Hessischen Datenschutzbeauftragten nach dem 25. Mai 2018 § 21 Abs. 4 Satz 1 in der bis zum 24. Mai 2018 geltenden Fassung fort.

§ 91
Inkrafttreten

Dieses Gesetz tritt am 25. Mai 2018 in Kraft.

Anlage zu § 13 Abs. 9 HDSG – Verwaltungskostenverzeichnis

Nr.	Gegenstand	Bemessungsgrundlage	Gebühr EUR
1	2	3	4
1	**Gebühren**		
11	**Auskünfte, Akteneinsicht**		
110	schriftliche Auskünfte Einfache schriftliche Auskünfte sind kostenfrei, soweit sich nicht aus Registern oder Dateien erteilt werden.		30 bis 600
111	Gewährung von Einsicht in amtliche Akten, Karteien, Datenträger usw. für Personen, die nicht am Verfahren beteiligt sind oder deren Verfahren abgeschlossen ist und die nicht betroffene Person im Sinne der Verordnung (EU) Nr. 2016/679 sind		10 bis 600
112	Zuschlag zu Nr. 111 für das Versenden von Akten oder Kopien aus Akten, auch von Bußgeldakten außerhalb eines Bußgeldverfahrens Die Auslagen sind mit der Gebühr abgegolten.	je Sendung	12
113	Gewährung von Einsicht in amtliche Akten usw. für Personen, die am Verfahren beteiligt sind, aber nicht betroffene Personen im Sinne der Verordnung (EU) Nr. 2016/679 sind, durch Versenden; dies gilt auch für das Versenden von Kopien aus Akten Die Auslagen sind mit der Gebühr abgegolten.	je Sendung	12
12	**Missbrauchsgebühr**		
121	Missbrauchsgebühr nach Art. 57 Abs. 4 der Verordnung (EU) Nr. 2016/679 oder § 13 Abs. 10		100 bis 1 000
13	**Überprüfungen der Datenverarbeitungen nach der Verordnung (EU) Nr. 2016/679**		
131	Überprüfung der Datenverarbeitung nach Art. 57 Abs. 1 Buchst. a mit besonderem Verwaltungsaufwand Die Gebühr wird nur erhoben, wenn ein Verstoß festgestellt und eine Maßnahme nach Art. 58 Abs. 2 Buchst. b bis g getroffen wird.		500 bis 15 000
132	Aussetzung einer Übermittlung von Daten an einen Empfänger in einem Drittland oder an eine internationale Organisation nach Art. 58 Abs. 2 Buchst. j		500 bis 5 000

14	**Stellungnahmen und Genehmigungen nach der Verordnung (EU) Nr. 2016/679**		
141	Beratung im Rahmen einer Datenschutz-Folgenabschätzung nach Art. 58 Abs. 3 Buchst. a einschließlich einer Genehmigung nach Art. 36 Abs. 5		500 bis 5 000
142	Stellungnahme zu und Billigung von Verhaltensregeln nach Art. 58 Abs. 3 Buchst. d in Verbindung mit Art. 40 Abs. 5		500 bis 5 000
143	Erteilung einer Zertifizierung oder Billigung von Kriterien für eine Zertifizierung nach Art. 58 Abs. 3 Buchst. f in Verbindung mit Art. 42 Abs. 5		1 000 bis 30 000
144	Genehmigung von Vertragsklauseln nach Art. 58 Abs. 3 Buchst. h in Verbindung mit Art. 46 Abs. 3 Buchst. a		500 bis 15 000
145	Genehmigung von verbindlichen internen Vorschriften nach Art. 58 Abs. 3 Buchst. j in Verbindung mit Art. 47		500 bis 15 000
2	**Auslagen**		
21	Anfertigung von Kopien unabhängig von der Art der Herstellung bis DIN A 3 - die vom Kostenschuldner besonders beantragt oder - die aus vom Kostenschuldner zu vertretenden Gründen notwendig wurden		

Artikel 2
Änderung des Hessischen Jugendstrafvollzugsgesetzes

Das Hessische Jugendstrafvollzugsgesetz vom 19. November 2007 (GVBl. I S. 758), zuletzt geändert durch Gesetz vom 30. November 2015 (GVBl. S. 498), wird wie folgt geändert:

1. Die Inhaltsübersicht wird wie folgt geändert:

   a) Die Angabe zu § 59 wird wie folgt gefasst:

   "§ 59 Auslesen von Datenspeichern"

   b) Die Angabe zu den §§ 64 und 65 wird wie folgt gefasst:

   "§ 64 Information und Auskunft an die Betroffenen, Akteneinsicht

   § 65 Berichtigung, Einschränkung der Verarbeitung und Löschung"

2. § 24 Abs. 8 wird wie folgt gefasst:

   "(8) Bei schwerer Erkrankung oder Tod von Gefangenen werden die der Anstalt bekannten nächsten Angehörigen, insbesondere die Personensorgeberechtigten, unverzüglich benachrichtigt, im Falle der schweren Erkrankung nur, wenn die Gefangenen hierin eingewilligt haben. Dem Wunsch der Gefangenen, auch andere Personen zu benachrichtigen, soll nach Möglichkeit entsprochen werden. Die Gefangenen sind bei Aufnahme über die Möglichkeit einer Einwilligung zu belehren."

3. § 33 wird folgt geändert:

   a) Abs. 4 Satz 1 und 2 wird wie folgt gefasst:

   "Abgesehen von den Fällen des § 32 Abs. 3 und 4 dürfen Besuche aus erzieherischen Gründen oder aus Gründen der Sicherheit oder Ordnung der Anstalt offen überwacht werden; die Überwachung erstreckt sich hierbei sowohl auf die Gefangenen wie deren Besuch. Die Unterhaltung darf nur überwacht werden, soweit dies im Einzelfall aus den in Satz 1 genannten Gründen erforderlich ist, und, soweit sie besondere Kategorien personenbezogener Daten nach § 41 Nr. 15 des Hessischen Datenschutz- und Informationsfreiheitsgesetzes vom ... [*einsetzen: Ausfertigungsdatum und Fundstelle dieses Gesetzes, ggf. Fundstelle von Art. 1*] zum Gegenstand hat, unbedingt erforderlich ist."

   b) In Abs. 5 werden Satz 1 und 2 durch die folgenden Sätze ersetzt:

   "Die optische Überwachung eines Besuchs kann auch durch technische Hilfsmittel erfolgen, insbesondere durch optisch-elektronische Einrichtungen (Videoüberwachung). Die Aufzeichnung und Speicherung von nach Satz 1 erhobenen Daten sind zulässig, wenn sie zum Erreichen des verfolgten Zwecks unbedingt erforderlich sind."

   c) In Abs. 5 Satz 5 wird die Angabe "§ 47" durch "§ 46" ersetzt.

4. In § 34 Abs. 2 Satz 1 werden die Wörter "erforderlich ist" durch "unbedingt erforderlich ist; Gefangene sind auf entsprechende Maßnahmen bei Aufnahme hinzuweisen" ersetzt.

5. § 44 Abs. 2 Satz 2 wird wie folgt gefasst:

   "Soweit es zur Gewährleistung von Sicherheit oder Ordnung der Anstalt unbedingt erforderlich ist, erfolgt eine offene optische Überwachung der Gefangenen außerhalb der Hafträume mit technischen Hilfsmitteln, insbesondere Videoüberwachung."

6. § 49 wird wie folgt geändert:

   a) Dem Abs. 2 Nr. 2 wird die Angabe "insbesondere Videoüberwachung, soweit dies unbedingt erforderlich ist," angefügt.

   b) In Abs. 6 Satz 2 wird vor dem Wort "erforderlich" das Wort "unbedingt" eingefügt.

7. Die §§ 58 bis 61 werden wie folgt gefasst:

"§ 58
Zulässigkeit der Verarbeitung personenbezogener Daten

(1) Die Anstalt und die Aufsichtsbehörde dürfen personenbezogene Daten nur verarbeiten, wenn eine Rechtsvorschrift dies vorsieht oder zwingend voraussetzt oder soweit dies für den Vollzug der Jugendstrafe erforderlich ist und im Falle der Verarbeitung besonderer Kategorien personenbezogener Daten nach § 41 Nr. 15 des Hessischen Datenschutz- und Informationsfreiheitsgesetzes unbedingt erforderlich ist. Soweit in den folgenden Vorschriften nichts Abweichendes geregelt ist, findet das Hessische Datenschutz- und Informationsfreiheitsgesetz Anwendung; dabei finden insbesondere die Vorschriften von

Teil 3 des Hessischen Datenschutz- und Informationsfreiheitsgesetzes auf die Datenverarbeitung durch die Anstalt oder Aufsichtsbehörde Anwendung, soweit die Datenverarbeitung zu den in § 40 des Hessischen Datenschutz- und Informationsfreiheitsgesetzes genannten Zwecken erfolgt. Bei der Verarbeitung personenbezogener Daten sind schutzwürdige Interessen der Betroffenen in jedem Fall der Verarbeitung zu berücksichtigen; sofern der Kernbereich privater Lebensgestaltung betroffen ist, darf keine Verarbeitung erfolgen.

(2) Zur Sicherung von Ziel und Aufgaben des Vollzugs der Jugendstrafe nach § 2, insbesondere zur Aufrechterhaltung der Sicherheit oder Ordnung der Anstalt, zur Identitätsfeststellung oder zur Aufrechterhaltung der medizinischen Versorgung und Gesundheitsfürsorge unbedingt erforderlich ist, soweit hierfür unbedingt erforderlich, die Verarbeitung folgender Daten von Gefangenen mit deren Kenntnis zulässig:

1. biometrische Daten von Fingern und Händen,
2. Lichtbilder,
3. Feststellungen äußerlicher körperlicher Merkmale,
4. Körpermessungen und
5. Gesundheitsdaten.

(3) Alle zur Person der Gefangenen erhobenen und für den Vollzug der Jugendstrafe erforderlichen Daten einschließlich derjenigen, die nach Abs. 2 Nr. 1 bis 4 erhoben worden sind, sind in eine Gefangenenpersonalakte aufzunehmen, die auch elektronisch geführt werden kann. Gesundheitsdaten und die sonstigen in § 61 Abs. 2 und 3 aufgeführten personenbezogenen Daten sind getrennt von der Gefangenenpersonalakte zu führen.

(4) Die einzelnen Vollzugsbediensteten sowie die in § 61 Abs. 3, § 72 Abs. 1 Satz 2 und 3, § 73 Abs. 1 und § 77 genannten Personen dürfen von personenbezogenen Daten nur Kenntnis erhalten, soweit dies zur Erfüllung der ihnen obliegenden Aufgabe oder für die Zusammenarbeit nach § 72 Abs. 5 erforderlich ist. Bei personenbezogenen Daten im Sinne von Abs. 2 ist über Satz 1 hinaus erforderlich, dass dies zur Erfüllung der ihnen obliegenden Aufgabe oder für die Zusammenarbeit nach § 72 Abs. 5 unbedingt erforderlich ist.

(5) Die Anstalt ist befugt, zur Aufrechterhaltung der Sicherheit oder Ordnung der Anstalt die Identität aller Personen festzustellen, die Zugang zur Anstalt begehren. Sofern unbedingt erforderlich, nimmt die Anstalt den Abgleich biometrischer Daten vor.

(6) Soweit dies zur Aufrechterhaltung von Sicherheit oder Ordnung der Anstalt erforderlich ist, werden Außenbereiche der Anstalt mit technischen Hilfsmitteln, insbesondere Videoüberwachung, offen überwacht, sofern keine Anhaltspunkte dafür bestehen, dass schutzwürdige Interessen der Betroffenen überwiegen. Der Umstand der Überwachung und der Name und die Kontaktdaten des Verantwortlichen sind den Betroffenen durch geeignete Maßnahmen zum frühestmöglichen Zeitpunkt kenntlich zu machen. § 33 Abs. 5 Satz 2 gilt entsprechend; darüber hinaus ist eine Speicherung nur zulässig, wenn keine Anhaltspunkte dafür bestehen, dass schutzwürdige Interessen der Betroffenen überwiegen.

§ 58a
Überprüfung anstaltsfremder Personen

(1) Personen, die in der Anstalt tätig werden sollen und die zur Anstalt oder Aufsichtsbehörde nicht in einem Dienst- oder Arbeitsverhältnis stehen und nicht im Auftrag einer anderen Behörde Zugang begehren, können zu diesen Tätigkeiten nur zugelassen werden, wenn keine Sicherheitsbedenken bestehen. Die Anstalt nimmt zur Aufrechterhaltung der Sicherheit oder Ordnung der Anstalt mit Einwilligung der betroffenen Person eine Zuverlässigkeitsüberprüfung vor. Sie darf dazu

1. eine Auskunft nach § 41 Abs. 1 Nr. 1 des Bundeszentralregistergesetzes in der Fassung der Bekanntmachung vom 21. September 1984 (BGBl. I S. 1229, 1985 I S. 195), zuletzt geändert durch Gesetz vom 18. Juli 2017 (BGBl. I S. 2732), einholen,
2. Erkenntnisse der Polizeibehörden und, soweit im Einzelfall erforderlich, des Landesamts für Verfassungsschutz abfragen.

Ist eine Überprüfung in Eilfällen, beispielsweise bei kurzfristig notwendigen Reparaturarbeiten, nicht möglich, hat eine entsprechende Beaufsichtigung der Person bei der Tätigkeit in der Anstalt zu erfolgen. Die Vorschriften des Hessischen Sicherheitsüberprüfungsgesetzes vom 19. Dezember 2014 (GVBl. S. 364) in seiner jeweils geltenden Fassung bleiben unberührt.

(2) Abgesehen von den Fällen des § 32 Abs. 3 und 4 darf die Anstalt auch bei Personen, die die Zulassung zum Gefangenenbesuch oder zum Besuch der Anstalt begehren, zur

Aufrechterhaltung der Sicherheit oder Ordnung der Anstalt hierfür mit ihrer Einwilligung eine Zuverlässigkeitsüberprüfung vornehmen. Abs. 1 Satz 3 gilt entsprechend; hierbei teilt die Anstalt den in Abs. 1 Satz 3 Nr. 2 genannten Behörden auch mit, dass und für welche Gefangenen die Person die Zulassung zum Gefangenenbesuch begehrt.

(3) Werden der Anstalt sicherheitsrelevante Erkenntnisse bekannt, wird die betroffene Person nicht oder nur unter Beschränkungen zu der Tätigkeit oder dem Besuch zugelassen. Gleiches gilt, wenn die betroffene Person eine Einwilligung in eine Zuverlässigkeitsüberprüfung verweigert.

(4) Personen nach Abs. 1 und 2 sind über die Benachrichtigung nach § 51 des Hessischen Datenschutz- und Informationsfreiheitsgesetzes hinaus über den Anlass der Zuverlässigkeitsprüfung, ihren möglichen Umfang nach Abs. 1 und 2 und über die Rechtsfolgen nach Abs. 3 mit der Einwilligungsanfrage zu belehren.

(5) Im Rahmen der Überprüfung bekannt gewordene Daten dürfen, soweit nicht aufgrund einer anderen gesetzlichen Vorschrift ihre Übermittlung gestattet oder vorgeschrieben ist, mit Ausnahme des für die Überprüfung einer Entscheidung nach Abs. 3 zuständigen Gerichts nicht an Dritte übermittelt werden.

(6) Die Zuverlässigkeitsüberprüfung ist in der Regel nach Ablauf einer Frist von fünf Jahren zu wiederholen, sofern ihre Erforderlichkeit nach Abs. 1 Satz 1 weiter besteht. Sie kann zudem wiederholt werden, wenn neue sicherheitsrelevante Erkenntnisse dies nahelegen.

§ 59
Auslesen von Datenspeichern

Elektronische Datenspeicher sowie elektronische Geräte mit Datenspeicher, die ohne Erlaubnis in die Anstalt eingebracht wurden, dürfen auf schriftliche Anordnung der Anstaltsleitung ausgelesen werden, soweit konkrete Anhaltspunkte die Annahme rechtfertigen, dass dies für die Erfüllung von Ziel und Aufgabe des Vollzugs der Jugendstrafe nach § 2, insbesondere zur Aufrechterhaltung der Sicherheit oder Ordnung der Anstalt, unbedingt erforderlich ist. Die Gründe sind in der Anordnung festzuhalten. Sind die Betroffenen bekannt, sind ihnen die Gründe vor dem Auslesen mitzuteilen. Die Gefangenen sind bei der Aufnahme über die Möglichkeit des Auslesens von nicht gestatteten Datenspeichern zu belehren.

§ 60
Zweckbindung und Übermittlung

(1) Personenbezogene Daten dürfen zu Zwecken, für die sie nicht erhoben oder gespeichert worden sind, nur verarbeitet, insbesondere übermittelt werden, wenn ein Fall der §§ 20 bis 27 und 44 bis 45 des Hessischen Datenschutz- und Informationsfreiheitsgesetzes vorliegt, insbesondere soweit dies

1. zu den in § 40 des Hessischen Datenschutz- und Informationsfreiheitsgesetzes genannten Zwecken,
2. in gerichtlichen Verfahren wegen Maßnahmen nach diesem Gesetz,
3. für Maßnahmen der Gerichtshilfe, Jugendgerichtshilfe, Bewährungshilfe oder Führungsaufsicht,
4. zur Vorbereitung und Durchführung von Maßnahmen der Entlassungsvorbereitung und Nachsorge,
5. für Entscheidungen in Gnadensachen,
6. für sozialrechtliche Maßnahmen,
7. für die Einleitung von Hilfsmaßnahmen für Angehörige der Gefangenen (§ 11 Abs. 1 Nr. 1 des Strafgesetzbuchs),
8. für dienstliche Maßnahmen der Bundeswehr im Zusammenhang mit der Aufnahme und Entlassung von Soldaten,
9. für ausländerrechtliche Maßnahmen,
10. für die Durchführung der Besteuerung,
11. zur Ausübung von Aufsichts- und Kontrollbefugnissen sowie zu Ausbildungs- und Prüfungszwecken oder
12. für gesetzlich angeordnete Statistiken der Rechtspflege

erforderlich und bei besonderen Kategorien personenbezogener Daten nach § 41 Nr. 15 des Hessischen Datenschutz- und Informationsfreiheitsgesetzes unbedingt erforderlich ist.

(2) Bei der Überwachung der Besuche, der Telekommunikation oder des Schriftwechsels sowie bei der Überwachung des Inhalts von Paketen und dem Auslesen von Datenspeichern bekannt gewordene personenbezogene Daten dürfen über ihre Erhebung oder Speicherung hinaus nur verarbeitet, insbesondere übermittelt werden, wenn dies

1. nach Abs. 1 Nr. 1 oder 2 zulässig ist,
2. eine Rechtsvorschrift vorsieht, zwingend voraussetzt oder
3. die Wahrung der Sicherheit oder Ordnung der Anstalt oder die Erreichung des Vollzugsziels gebietet

und es unbedingt erforderlich ist. Daten nach Satz 1 sind hinsichtlich des Ursprungs ihrer Erhebung und Speicherung eindeutig zu kennzeichnen. § 4 Abs. 3 Satz 2 des Hessischen Datenschutz- und Informationsfreiheitsgesetzes bleibt unberührt.

(3) Die Anstalt oder Aufsichtsbehörde kann auf Antrag mitteilen, ob sich jemand in Haft befindet sowie ob und wann die Entlassung voraussichtlich ansteht, soweit dies nach Abs. 1 zulässig ist. Weiterhin können unter den Voraussetzungen des Satzes 1 auf schriftlichen Antrag Auskünfte auch über die Vermögensverhältnisse der Gefangenen oder ihre Entlassungsadresse erteilt werden, wenn dies zur Feststellung oder Durchsetzung von Rechtsansprüchen im Zusammenhang mit der Straftat erforderlich ist. Unter den Voraussetzungen von § 406d Abs. 2 und 3 der Strafprozessordnung können Mitteilungen über die erstmalige Gewährung von vollzugsöffnenden Maßnahmen (§ 13) auch durch die Anstalt erfolgen. Die Gefangenen werden vor Mitteilungen nach Satz 1 bis 3 gehört, es sei denn, es ist zu besorgen, dass dadurch die Verfolgung des Interesses der Antragsteller vereitelt oder wesentlich erschwert werden würde. Ist die Anhörung unterblieben, werden die betroffenen Gefangenen über die Mitteilung der Anstalt oder Aufsichtsbehörde nachträglich unterrichtet.

(4) Akten mit personenbezogenen Daten dürfen nur anderen Anstalten, Aufsichtsbehörden, den für Strafvollzugs-, strafvollstreckungs- und strafrechtliche Entscheidungen zuständigen Gerichten sowie den Strafvollstreckungs- und Strafverfolgungsbehörden überlassen werden; die Überlassung an andere öffentliche Stellen ist zulässig, soweit die Erteilung einer Auskunft einen unvertretbaren Aufwand erfordert oder nach Darlegung der die Akteneinsicht begehrenden Stellen für die Erfüllung der Aufgabe nicht ausreicht. Entsprechendes gilt für die Überlassung von Akten an die von der Vollzugsbehörde mit Gutachten beauftragten Personen oder Stellen.

(5) Von der Anstalt oder der Aufsichtsbehörde übermittelte personenbezogene Daten dürfen nur zu dem Zweck verarbeitet werden, zu dessen Erfüllung sie übermittelt worden sind. Der Empfänger darf die Daten für andere Zwecke nur verarbeiten, soweit sie ihm auch für diese Zwecke hätten übermittelt werden dürfen und wenn im Falle einer Übermittlung an nicht öffentliche Stellen die übermittelnde Vollzugsbehörde eingewilligt hat. Die Anstalt oder Aufsichtsbehörde hat den Empfänger auf die Zweckbindung nach Satz 1 hinzuweisen und für den Fall, dass die übermittelten Daten besondere Kategorien personenbezogener Daten nach § 41 Nr. 15 des Hessischen Datenschutz- und Informationsfreiheitsgesetzes enthalten, auf diese Einstufung.

(6) Die Übermittlung von personenbezogenen Daten unterbleibt, soweit die in § 61 Abs. 2 und § 65 Abs. 4 und 6 geregelten Einschränkungen oder besondere gesetzliche Verwendungsregelungen entgegenstehen. Dies gilt nicht, wenn ein nach Abs. 1 Nr. 1 bis 3 zuständiges Gericht diese Daten anfordert oder dies zur Erfüllung der Aufgaben einer in § 119 Abs. 4 Nr. 13 der Strafprozessordnung genannten Stelle im Rahmen eines Besuchs der Anstalt erforderlich ist.

(7) Die Verantwortung für Zulässigkeit der Übermittlung trägt die übermittelnde Anstalt oder Aufsichtsbehörde. Erfolgt die Übermittlung auf Ersuchen einer öffentlichen Stelle, trägt diese die Verantwortung. In diesem Fall prüft die übermittelnde Anstalt oder Aufsichtsbehörde nur, ob das Übermittlungsersuchen im Rahmen der Aufgaben des Empfängers liegt und die Abs. 2 und 6 der Übermittlung nicht entgegenstehen, es sei denn, dass besonderer Anlass zur Prüfung der Zulässigkeit der Übermittlung besteht.

§ 61
Schutz besonderer Daten

(1) Besondere Kategorien personenbezogener Daten nach § 41 Nr. 15 des Hessischen Datenschutz- und Informationsfreiheitsgesetzes, insbesondere das religiöse oder weltanschauliche Bekenntnis von Gefangenen und personenbezogene Daten, die anlässlich ärztlicher Untersuchungen erhoben worden sind, dürfen in der Anstalt nicht allgemein kenntlich gemacht werden. Andere personenbezogene Daten über die Gefangenen dürfen innerhalb der Anstalt allgemein kenntlich gemacht werden, soweit dies für ein geordnetes Zusammenleben in der Anstalt erforderlich ist.

(2) Personenbezogene Daten, die in der Anstalt tätigen Personen im Sinne von § 203 Abs. 1 Nr. 1, 2 und 5 des Strafgesetzbuchs von Gefangenen als Geheimnis anvertraut oder über Gefangene als Geheimnis sonst bekannt geworden sind, unterliegen auch gegenüber der Anstalt und der Aufsichtsbehörde der Schweigepflicht. Die in Satz 1 genannten Personen sind befugt und verpflichtet, diese Daten gegenüber der Anstaltsleitung zu offenbaren, soweit dies für die Sicherheit der Anstalt oder zur Abwehr von erheblichen Gefahren für Leben oder Gesundheit von Gefangenen oder Dritten unbedingt erforderlich ist. Eine Befugnis zur Offenbarung besteht auch, soweit es die Feststellung betrifft, ob Gefangene fähig sind, an bestimmten vollzuglichen Maßnahmen teilzunehmen oder ob sie an Behandlungsmaßnahmen teilnehmen und daran mitwirken.

(3) In Abs. 2 gelten Satz 2 und 3 entsprechend für die in § 203 Abs. 1 Nr. 1, 2, 4 und 5 des Strafgesetzbuchs genannten Personen außerhalb des Vollzugs, die mit der Untersuchung, Behandlung oder Betreuung von Gefangenen beauftragt wurden, mit der Maßgabe, dass die vorgenannten Personen lediglich zu einer Offenbarung befugt sind.

(4) Die Gefangenen sind bei der Aufnahme über die nach Abs. 2 Satz 2 und Abs. 3 bestehenden Offenbarungsbefugnisse und Offenbarungspflichten zu unterrichten.

(5) Die nach Abs. 2 und 3 offenbarten Daten dürfen nur für den Zweck, für den sie offenbart wurden oder für den eine Offenbarung zulässig gewesen wäre, und in dem hierfür unbedingt erforderlichen Umfang verarbeitet werden."

8. In § 62 Abs. 3 wird die Angabe "§ 15" durch "§ 58" ersetzt.

9. Die §§ 63 bis 65 werden wie folgt gefasst:

"§ 63
Datensicherung

(1) Mit der Datenverarbeitung befasste Personen dürfen personenbezogene Daten nicht unbefugt verarbeiten. Sie sind über die bei ihrer Tätigkeit zu beachtenden Vorschriften über den Datenschutz zu unterrichten. Auf die besonderen Anforderungen bei der Verarbeitung von Daten, die aus Videoüberwachung oder aus Maßnahmen nach § 60 Abs. 2 und § 61 Abs. 1 und 2 stammen oder besondere Kategorien personenbezogener Daten nach § 41 Nr. 15 des Hessischen Datenschutz- und Informationsfreiheitsgesetzes oder den Kernbereich privater Lebensgestaltung betreffen, sind sie gesondert hinzuweisen. Das Datengeheimnis besteht auch nach der Beendigung der Tätigkeit fort.

(2) Akten und Dateien mit personenbezogenen Daten sind nach Maßgabe des § 59 des Hessischen Datenschutz- und Informationsfreiheitsgesetzes durch technische und organisatorische Maßnahmen gegen unbefugten Zugriff zu schützen. Gefangenenpersonalakten, Gesundheitsakten, Krankenblätter und sonstige in § 61 Abs. 2 und 3 aufgeführte personenbezogene Daten sind getrennt von anderen Unterlagen zu führen und besonders zu sichern.

§ 64
Information und Auskunft an die Betroffenen, Akteneinsicht

Die Betroffenen erhalten Auskunft und Information hinsichtlich der zu ihrer Person verarbeiteten Daten nach Maßgabe der §§ 50 bis 52 des Hessischen Datenschutz- und Informationsfreiheitsgesetzes, soweit die Datenverarbeitung zu den in § 40 des Hessischen Datenschutz- und Informationsfreiheitsgesetzes genannten Zwecken erfolgt; im Übrigen nach Maßgabe der §§ 31 bis 33 des Hessischen Datenschutz- und Informationsfreiheitsgesetzes. Soweit dies zur Wahrnehmung rechtlicher Interessen erforderlich ist, wird dem Betroffenen Akteneinsicht gewährt.

§ 65
Berichtigung, Einschränkung der Verarbeitung und Löschung

(1) Personenbezogene Daten sind nach Maßgabe der §§ 53 und 70 des Hessischen Datenschutz- und Informationsfreiheitsgesetzes zu berichtigen, zu löschen oder in der Verarbeitung einzuschränken, soweit sie zu den in § 40 des Hessischen Datenschutz- und Informationsfreiheitsgesetzes genannten Zwecken verarbeitet wurden und in den nachfolgenden Absätzen keine besonderen Regelungen getroffen sind; im Übrigen gilt § 34 des Hessischen Datenschutz- und Informationsfreiheitsgesetzes.

(2) Personenbezogene Daten, die durch den Einsatz eines elektronischen Überwachungssystems erhoben wurden oder hierbei angefallen sind, sind nach Beendigung der Maßnahme unverzüglich, Videoaufnahmen oder Ergebnisse von Maßnahmen nach § 59 spätestens 72 Stunden nach Ende des Kalendertages, an dem sie angefallen sind, zu löschen, soweit nicht zum Zeitpunkt der Entscheidung über die Löschung die weitere Aufbewahrung bei Einschränkung der Verarbeitung zu konkreten Beweiszwecken unbedingt erforderlich ist. Sind personenbezogene Daten entgegen § 58 Abs. 1 Satz 3 verarbeitet worden, sind diese unverzüglich, spätestens 24 Stunden nach Ende des Kalendertages, an

dem sie angefallen sind, zu löschen. Die Tatsache der Löschung nach Satz 1 und 2 ist zu dokumentieren; die Dokumentation darf ausschließlich zu Zwecken der Datenschutzkontrolle verwendet werden und ist zu löschen, wenn sie für diese Zwecke nicht mehr erforderlich ist, spätestens jedoch am Ende des Kalenderjahres, das dem Jahr der Dokumentation folgt.

(3) Personenbezogene Daten, die in der Gefangenenpersonalakte oder in anderen zur Person der Gefangenen geführten Dateien und Akten gespeichert sind, sind spätestens drei Jahre nach der Entlassung oder der Verlegung der Gefangenen in eine andere Anstalt zu löschen. Sonstige personenbezogene Daten, die in anderen Dateien und Akten gespeichert sind, sind, sofern ihre Speicherung nicht mehr erforderlich ist, unverzüglich, spätestens nach Ablauf von fünf Jahren ab ihrer Erhebung zu löschen.

(4) Eine Löschung personenbezogener Daten unterbleibt, soweit ihre Speicherung bei Einschränkung ihrer Verarbeitung nach

1. § 53 des Hessischen Datenschutz- und Informationsfreiheitsgesetzes, insbesondere aufgrund ärztlicher Dokumentationspflichten, oder
2. § 34 des Hessischen Datenschutz- und Informationsfreiheitsgesetzes

erfolgt. In ihrer Verarbeitung eingeschränkte Daten sind besonders zu kennzeichnen und dürfen außer bei Einwilligung der Betroffenen nur zu dem Zweck verarbeitet, insbesondere übermittelt werden, der ihrer Löschung entgegenstand. Die Einschränkung der Verarbeitung endet, wenn Gefangene erneut zum Vollzug einer Freiheitsentziehung aufgenommen werden oder die Betroffenen eingewilligt haben. Bei den in der Verarbeitung eingeschränkten personenbezogenen Daten können bis zum Ablauf der Aufbewahrungsfrist für die Gefangenenpersonalakte oder anderer zur Person der Gefangenen geführten Dateien oder Akten die Angaben über Familienname, Vorname, Geburtsname, Geburtstag, Geburtsort, Eintritts- und Austrittsdatum gespeichert werden, soweit dies für das Auffinden dieser Dateien oder Akten erforderlich ist.

(5) Die Erforderlichkeit der Löschung, auch bei in der Verarbeitung eingeschränkten personenbezogenen Daten, ist jährlich zu kontrollieren. Die Frist zur Kontrolle personenbezogener Daten, die in der Gefangenenpersonalakte oder in anderen zur Person der Gefangenen geführten Dateien und Akten gespeichert sind, beginnt mit der Entlassung oder Verlegung der Gefangenen in eine andere Anstalt, in sonstigen Fällen mit Erhebung der personenbezogenen Daten.

(6) Folgende Aufbewahrungsfristen von Dateien und Akten, soweit diese in der Verarbeitung eingeschränkt sind, dürfen nicht überschritten werden:

1. 20 Jahre bei Daten aus Gefangenenpersonalakten, Gesundheitsakten und Krankenblättern,
2. 30 Jahre bei Daten aus Gefangenenbüchern.

Dies gilt nicht, wenn konkrete Anhaltspunkte dafür vorliegen, dass die Aufbewahrung für die in Abs. 4 genannten Zwecke weiterhin erforderlich ist. Die Aufbewahrungsfrist beginnt mit dem auf das Jahr der Weglegung folgenden Kalenderjahr. Die Vorschriften des Hessischen Archivgesetzes vom 26. November 2012 (GVBl. S. 458) in seiner jeweils geltenden Fassung bleiben unberührt."

10. § 66 wird wie folgt geändert:

a) Dem Abs. 2 wird folgender Satz angefügt:

"Die Ergebnisse dienen dem öffentlichen Interesse und sind für die Fortentwicklung des Vollzugs nutzbar zu machen."

b) Abs. 5 wird wie folgt gefasst:

"(5) Für die Übermittlung personenbezogener Daten gilt § 476 der Strafprozessordnung mit der Maßgabe entsprechend, dass

1. auch elektronisch gespeicherte personenbezogene Daten übermittelt werden können und
2. besondere Kategorien personenbezogener Daten nach § 41 Nr. 15 des Hessischen Datenschutz- und Informationsfreiheitsgesetzes nur übermittelt werden, soweit dies für den Zweck nach § 476 Abs. 1 Nr. 1 der Strafprozessordnung unbedingt erforderlich ist."

Artikel 3
Änderung des Hessischen Strafvollzugsgesetzes

Das Hessische Strafvollzugsgesetz vom 28. Juni 2010 (GVBl. I S. 185), zuletzt geändert durch Gesetz vom 30. November 2015 (GVBl. S. 498), wird wie folgt geändert:

1. Die Inhaltsübersicht wird wie folgt geändert:

   a) Die Angabe zu § 59 wird wie folgt gefasst:

   "§ 59 Auslesen von Datenspeichern"

   b) Die Angabe zu den §§ 64 und 65 wird wie folgt gefasst:

   "§ 64 Information und Auskunft an die Betroffenen, Akteneinsicht

   § 65 Berichtigung, Einschränkung der Verarbeitung und Löschung"

2. § 24 Abs. 8 wird wie folgt gefasst:

   "(8) Bei schwerer Erkrankung oder Tod von Gefangenen werden die der Anstalt bekannten nächsten Angehörigen unverzüglich benachrichtigt, im Falle der schweren Erkrankung nur, wenn die Gefangenen hierin eingewilligt haben. Dem Wunsch der Gefangenen, auch andere Personen zu benachrichtigen, soll nach Möglichkeit entsprochen werden. Die Gefangenen sind bei Aufnahme über die Möglichkeit einer Einwilligung zu belehren."

3. § 34 wird wie folgt geändert:

   a) Abs. 4 Satz 1 und 2 wird wie folgt gefasst:

   "Abgesehen von den Fällen des § 33 Abs. 3 und 4 dürfen Besuche aus Gründen der Sicherheit oder Ordnung der Anstalt oder aus Gründen der Behandlung offen überwacht werden; die Überwachung erstreckt sich hierbei sowohl auf die Gefangenen wie deren Besuch. Die Unterhaltung darf nur überwacht werden, soweit dies im Einzelfall aus den in Satz 1 genannten Gründen erforderlich ist, und, soweit sie besondere Kategorien personenbezogener Daten nach § 41 Nr. 15 des Hessischen Datenschutz- und Informationsfreiheitsgesetzes vom … [*einsetzen: Ausfertigungsdatum und Fundstelle dieses Gesetzes, ggf. Fundstelle von Art. 1*] zum Gegenstand hat, unbedingt erforderlich ist."

   b) Abs. 5 Satz 1 und 2 wird wie folgt gefasst:

   "Die optische Überwachung eines Besuchs kann auch durch technische Hilfsmittel erfolgen, insbesondere durch optisch-elektronische Einrichtungen (Videoüberwachung). Die Aufzeichnung und Speicherung von nach Satz 1 erhobenen Daten sind zulässig, wenn sie zum Erreichen des verfolgten Zwecks unbedingt erforderlich sind."

4. § 35 Abs. 2 Satz 1 wird wie folgt gefasst:

   "Abgesehen von den Fällen des § 33 Abs. 3 und 4 darf der Schriftwechsel überwacht werden, soweit es zur Erfüllung von Ziel und Aufgaben des Vollzugs der Freiheitsstrafe nach § 2, insbesondere aus Gründen der Sicherheit oder Ordnung der Anstalt oder aus Gründen der Behandlung unbedingt erforderlich ist; Gefangene sind auf entsprechende Maßnahmen bei Aufnahme hinzuweisen."

5. § 45 Abs. 2 Satz 2 wird wie folgt gefasst:

   "Soweit es zur Gewährleistung von Sicherheit oder Ordnung der Anstalt unbedingt erforderlich ist, erfolgt eine offene optische Überwachung der Gefangenen außerhalb der Hafträume mit technischen Hilfsmitteln, insbesondere Videoüberwachung."

6. § 50 wird wie folgt geändert:

   a) Dem Abs. 2 Nr. 2 werden die Wörter "insbesondere Videoüberwachung, soweit dies unbedingt erforderlich ist," angefügt.

   b) In Abs. 6 Satz 2 wird vor dem Wort "erforderlich" das Wort "unbedingt" eingefügt.

7. Die §§ 58 bis 61 werden wie folgt gefasst:

"§ 58
Zulässigkeit der Verarbeitung personenbezogener Daten

(1) Die Anstalt und die Aufsichtsbehörde dürfen personenbezogene Daten nur verarbeiten, wenn eine Rechtsvorschrift dies vorsieht oder zwingend voraussetzt oder soweit dies für den Vollzug der Freiheitsstrafe erforderlich und im Falle der Verarbeitung besonde-

rer Kategorien personenbezogener Daten nach § 41 Nr. 15 des Hessischen Datenschutz- und Informationsfreiheitsgesetzes unbedingt erforderlich ist. Soweit in den folgenden Vorschriften nichts Abweichendes geregelt ist, findet das Hessische Datenschutz- und Informationsfreiheitsgesetz Anwendung; dabei finden insbesondere die Vorschriften von Teil 3 des Hessischen Datenschutz- und Informationsfreiheitsgesetzes auf die Datenverarbeitung durch die Anstalt oder Aufsichtsbehörde Anwendung, soweit die Datenverarbeitung zu den in § 40 des Hessischen Datenschutz- und Informationsfreiheitsgesetzes genannten Zwecken erfolgt. Bei der Verarbeitung personenbezogener Daten sind schutzwürdige Interessen der Betroffenen in jedem Fall der Verarbeitung zu berücksichtigen; sofern der Kernbereich privater Lebensgestaltung betroffen ist, darf keine Verarbeitung erfolgen.

(2) Zur Sicherung von Ziel und Aufgabe des Vollzugs der Freiheitsstrafe nach § 2, insbesondere zur Aufrechterhaltung der Sicherheit oder Ordnung der Anstalt, zur Identitätsfeststellung oder zur Aufrechterhaltung der medizinischen Versorgung und Gesundheitsfürsorge ist, soweit hierfür unbedingt erforderlich, die Verarbeitung folgender Daten von Gefangenen mit deren Kenntnis zulässig:

1. biometrische Daten von Fingern und Händen,
2. Lichtbilder,
3. Feststellungen äußerlicher körperlicher Merkmale,
4. Körpermessungen und
5. Gesundheitsdaten.

(3) Alle zur Person der Gefangenen erhobenen und für den Vollzug der Freiheitsstrafe erforderlichen Daten einschließlich derjenigen, die nach Abs. 2 Nr. 1 bis 4 erhoben worden sind, sind in eine Gefangenenpersonalakte aufzunehmen, die auch elektronisch geführt werden kann. Gesundheitsdaten und die sonstigen in § 61 Abs. 2 und 3 aufgeführten personenbezogenen Daten sind getrennt von der Gefangenenpersonalakte zu führen.

(4) Die einzelnen Vollzugsbediensteten sowie die in § 61 Abs. 3, § 76 Abs. 1 Satz 2 und 3, § 77 Abs. 1 und § 81 genannten Personen dürfen von personenbezogenen Daten nur Kenntnis erhalten, soweit dies zur Erfüllung der ihnen obliegenden Aufgabe oder für die Zusammenarbeit nach § 76 Abs. 4 erforderlich ist. Bei personenbezogenen Daten im Sinne von Abs. 2 ist über Satz 1 hinaus erforderlich, dass dies zur Erfüllung der ihnen obliegenden Aufgabe oder für die Zusammenarbeit nach § 76 Abs. 4 unbedingt erforderlich ist.

(5) Die Anstalt ist befugt, zur Aufrechterhaltung der Sicherheit oder Ordnung der Anstalt die Identität aller Personen, die Zugang zur Anstalt begehren, festzustellen. Sofern unbedingt erforderlich, ist die Anstalt berechtigt, hierzu den Abgleich biometrischer Daten vorzunehmen.

(6) Soweit dies zur Aufrechterhaltung von Sicherheit oder Ordnung der Anstalt erforderlich ist, werden Außenbereiche der Anstalt mit technischen Hilfsmitteln, insbesondere Videoüberwachung, offen überwacht, sofern keine Anhaltspunkte dafür bestehen, dass schutzwürdige Interessen der Betroffenen überwiegen. Der Umstand der Überwachung und der Name und die Kontaktdaten der Verantwortlichen sind den Betroffenen durch geeignete Maßnahmen zum frühestmöglichen Zeitpunkt kenntlich zu machen. § 34 Abs. 5 Satz 2 gilt entsprechend; darüber hinaus ist eine Speicherung nur zulässig, wenn keine Anhaltspunkte dafür bestehen, dass schutzwürdige Interessen der Betroffenen überwiegen.

§ 58a
Überprüfung anstaltsfremder Personen

(1) Personen, die in der Anstalt tätig werden sollen und die zur Anstalt oder Aufsichtsbehörde nicht in einem Dienst- oder Arbeitsverhältnis stehen und nicht im Auftrag einer anderen Behörde Zugang begehren, können zu diesen Tätigkeiten nur zugelassen werden, wenn keine Sicherheitsbedenken bestehen. Die Anstalt nimmt zur Aufrechterhaltung der Sicherheit oder Ordnung der Anstalt und zur Abwendung von Gefahren hierfür mit Einwilligung der betroffenen Person eine Zuverlässigkeitsüberprüfung vor. Sie darf dazu

1. eine Auskunft nach § 41 Abs. 1 Nr. 1 des Bundeszentralregistergesetzes in der Fassung der Bekanntmachung vom 21. September 1984 (BGBl. I S. 1229, 1985 I S. 195), zuletzt geändert durch Gesetz vom 18. Juli 2017 (BGBl. I S. 2732), einholen,
2. Erkenntnisse der Polizeibehörden und, soweit im Einzelfall erforderlich, des Landesamts für Verfassungsschutz abfragen.

Ist eine Überprüfung in Eilfällen, beispielsweise bei kurzfristig notwendigen Reparaturarbeiten, nicht möglich, hat eine entsprechende Beaufsichtigung der Person bei der Tätigkeit in der Anstalt zu erfolgen. Die Vorschriften des Hessischen Sicherheitsüberprü-

fungsgesetzes vom 19. Dezember 2014 (GVBl. S. 364) in seiner jeweils geltenden Fassung bleiben unberührt.

(2) Abgesehen von den Fällen des § 33 Abs. 3 und 4 darf die Anstalt auch bei Personen, die die Zulassung zum Gefangenenbesuch oder zum Besuch der Anstalt begehren, zur Aufrechterhaltung der Sicherheit oder Ordnung der Anstalt mit ihrer Einwilligung eine Zuverlässigkeitsüberprüfung vornehmen. Abs. 1 Satz 3 gilt entsprechend; hierbei teilt die Anstalt den in Abs. 1 Satz 3 Nr. 2 genannten Behörden auch mit, dass und für welche Gefangenen die Person die Zulassung zum Gefangenenbesuch begehrt.

(3) Werden der Anstalt sicherheitsrelevante Erkenntnisse bekannt, wird die betroffene Person nicht oder nur unter Beschränkungen zu der Tätigkeit oder dem Besuch zugelassen. Gleiches gilt, wenn die betroffene Person eine Einwilligung in eine Zuverlässigkeitsüberprüfung verweigert.

(4) Personen nach Abs. 1 und 2 sind über die Benachrichtigung nach § 51 des Hessischen Datenschutz- und Informationsfreiheitsgesetzes hinaus über den Anlass der Zuverlässigkeitsprüfung, ihren möglichen Umfang nach Abs. 1 und 2 und über die Rechtsfolgen nach Abs. 3 mit der Einwilligungsanfrage zu belehren.

(5) Im Rahmen der Überprüfung bekannt gewordene Daten dürfen, soweit nicht aufgrund einer anderen gesetzlichen Vorschrift ihre Übermittlung gestattet oder vorgeschrieben ist, mit Ausnahme des für die Überprüfung einer Entscheidung nach Abs. 3 zuständigen Gerichts nicht an Dritte übermittelt werden.

(6) Die Zuverlässigkeitsüberprüfung ist in der Regel nach Ablauf einer Frist von fünf Jahren zu wiederholen, sofern ihre Erforderlichkeit nach Abs. 1 Satz 1 weiter besteht. Sie kann zudem wiederholt werden, wenn neue sicherheitsrelevante Erkenntnisse dies nahelegen.

§ 59
Auslesen von Datenspeichern

Elektronische Datenspeicher sowie elektronische Geräte mit Datenspeicher, die ohne Erlaubnis in die Anstalt eingebracht wurden, dürfen auf schriftliche Anordnung der Anstaltsleitung ausgelesen werden, soweit konkrete Anhaltspunkte die Annahme rechtfertigen, dass dies für die Erfüllung von Ziel und Aufgabe des Vollzugs der Freiheitsstrafe nach § 2, insbesondere zur Aufrechterhaltung der Sicherheit oder Ordnung der Anstalt, unbedingt erforderlich ist. Die Gründe sind in der Anordnung festzuhalten. Sind die Betroffenen bekannt, sind ihnen die Gründe vor dem Auslesen mitzuteilen. Die Gefangenen sind bei der Aufnahme über die Möglichkeit des Auslesens von nicht gestatteten Datenspeichern zu belehren.

§ 60
Zweckbindung und Übermittlung

(1) Personenbezogene Daten dürfen zu Zwecken, für die sie nicht erhoben oder gespeichert worden sind, nur verarbeitet, insbesondere übermittelt werden, wenn ein Fall der §§ 20 bis 27 und 44 bis 45 des Hessischen Datenschutz- und Informationsfreiheitsgesetzes vorliegt, insbesondere soweit dies

1. zu den in § 40 des Hessischen Datenschutz- und Informationsfreiheitsgesetzes genannten Zwecken,
2. in gerichtlichen Verfahren wegen Maßnahmen nach diesem Gesetz,
3. für Maßnahmen der Gerichtshilfe, Bewährungshilfe oder Führungsaufsicht,
4. zur Vorbereitung und Durchführung von Maßnahmen der Entlassungsvorbereitung und Nachsorge,
5. für Entscheidungen in Gnadensachen,
6. für sozialrechtliche Maßnahmen,
7. für die Einleitung von Hilfsmaßnahmen für Angehörige der Gefangenen (§ 11 Abs. 1 Nr. 1 des Strafgesetzbuchs),
8. für dienstliche Maßnahmen der Bundeswehr im Zusammenhang mit der Aufnahme und Entlassung von Soldaten,
9. für ausländerrechtliche Maßnahmen,
10. für die Durchführung der Besteuerung,
11. zur Ausübung von Aufsichts- und Kontrollbefugnissen sowie zu Ausbildungs- und Prüfungszwecken oder
12. für gesetzlich angeordnete Statistiken der Rechtspflege

erforderlich und bei besonderen Kategorien personenbezogener Daten nach § 41 Nr. 15 des Hessischen Datenschutz- und Informationsfreiheitsgesetzes unbedingt erforderlich ist.

(2) Bei der Überwachung der Besuche, der Telekommunikation oder des Schriftwechsels sowie bei der Überwachung des Inhalts von Paketen und dem Auslesen von Datenspeichern bekannt gewordene personenbezogene Daten dürfen über ihre Erhebung oder Speicherung hinaus nur verarbeitet, insbesondere übermittelt werden, wenn dies

1. nach Abs. 1 Nr. 1 oder 2 zulässig ist,
2. eine Rechtsvorschrift vorsieht, zwingend voraussetzt oder
3. die Wahrung der Sicherheit oder Ordnung der Anstalt oder die Erfüllung des Eingliederungsauftrags gebietet

und es unbedingt erforderlich ist. Daten nach Satz 1 sind hinsichtlich des Ursprungs ihrer Erhebung und Speicherung eindeutig zu kennzeichnen. § 4 Abs. 3 Satz 2 des Hessischen Datenschutz- und Informationsfreiheitsgesetzes bleibt unberührt.

(3) Die Anstalt oder Aufsichtsbehörde kann auf Antrag mitteilen, ob sich jemand in Haft befindet sowie ob und wann die Entlassung voraussichtlich ansteht, soweit dies nach Abs. 1 zulässig ist. Weiterhin können unter den Voraussetzungen des Satzes 1 auf schriftlichen Antrag Auskünfte auch über die Vermögensverhältnisse der Gefangenen oder ihre Entlassungsadresse erteilt werden, wenn dies zur Feststellung oder Durchsetzung von Rechtsansprüchen im Zusammenhang mit der Straftat erforderlich ist. Unter den Voraussetzungen von § 406d Abs. 2 und 3 der Strafprozessordnung können Mitteilungen über die erstmalige Gewährung von vollzugsöffnenden Maßnahmen (§ 13) auch durch die Anstalt erfolgen. Die Gefangenen werden vor Mitteilungen nach Satz 1 bis 3 gehört, es sei denn, es ist zu besorgen, dass dadurch die Verfolgung des Interesses der Antragsteller vereitelt oder wesentlich erschwert werden würde. Ist die Anhörung unterblieben, werden die betroffenen Gefangenen über die Mitteilung der Anstalt oder Aufsichtsbehörde nachträglich unterrichtet.

(4) Akten mit personenbezogenen Daten dürfen nur anderen Anstalten, Aufsichtsbehörden, den für Strafvollzugs-, strafvollstreckungs- und strafrechtliche Entscheidungen zuständigen Gerichten sowie den Strafvollstreckungs- und Strafverfolgungsbehörden überlassen werden; die Überlassung an andere öffentliche Stellen ist zulässig, soweit die Erteilung einer Auskunft einen unvertretbaren Aufwand erfordert oder nach Darlegung der die Akteneinsicht begehrenden Stellen für die Erfüllung der Aufgabe nicht ausreicht. Entsprechendes gilt für die Überlassung von Akten an die von der Vollzugsbehörde mit Gutachten beauftragten Personen oder Stellen.

(5) Von der Anstalt oder der Aufsichtsbehörde übermittelte personenbezogene Daten dürfen nur zu dem Zweck verarbeitet werden, zu dessen Erfüllung sie übermittelt worden sind. Der Empfänger darf die Daten für andere Zwecke nur verarbeiten, soweit sie ihm auch für diese Zwecke hätten übermittelt werden dürfen und wenn im Falle einer Übermittlung an nicht öffentliche Stellen die übermittelnde Vollzugsbehörde eingewilligt hat. Die Anstalt oder Aufsichtsbehörde hat den Empfänger auf die Zweckbindung nach Satz 1 hinzuweisen und für den Fall, dass die übermittelten Daten besondere Kategorien personenbezogener Daten nach § 41 Nr. 15 des Hessischen Datenschutz- und Informationsfreiheitsgesetzes enthalten, auf diese Einstufung.

(6) Die Übermittlung von personenbezogenen Daten unterbleibt, soweit die in § 61 Abs. 2 und § 65 Abs. 4 und 6 geregelten Einschränkungen oder besondere gesetzliche Verwendungsregelungen entgegenstehen. Dies gilt nicht, wenn ein nach Abs. 1 Nr. 1 bis 3 zuständiges Gericht diese Daten anfordert oder dies zur Erfüllung der Aufgaben einer in § 119 Abs. 4 Nr. 13 der Strafprozessordnung genannten Stelle im Rahmen eines Besuchs der Anstalt erforderlich ist.

(7) Die Verantwortung für die Zulässigkeit der Übermittlung trägt die übermittelnde Anstalt oder Aufsichtsbehörde. Erfolgt die Übermittlung auf Ersuchen einer öffentlichen Stelle, trägt diese die Verantwortung. In diesem Fall prüft die übermittelnde Anstalt oder Aufsichtsbehörde nur, ob das Übermittlungsersuchen im Rahmen der Aufgaben des Empfängers liegt und die Abs. 2 und 6 der Übermittlung nicht entgegenstehen, es sei denn, dass besonderer Anlass zur Prüfung der Zulässigkeit der Übermittlung besteht.

§ 61
Schutz besonderer Daten

(1) Besondere Kategorien personenbezogener Daten nach § 41 Nr. 15 des Hessischen Datenschutz- und Informationsfreiheitsgesetzes, insbesondere das religiöse oder weltanschauliche Bekenntnis von Gefangenen und personenbezogene Daten, die anlässlich ärztlicher Untersuchungen erhoben worden sind, dürfen in der Anstalt nicht allgemein kenntlich gemacht werden. Andere personenbezogene Daten über die Gefangenen dürfen in-

nerhalb der Anstalt allgemein kenntlich gemacht werden, soweit dies für ein geordnetes Zusammenleben in der Anstalt erforderlich ist.

(2) Personenbezogene Daten, die in der Anstalt tätigen Personen im Sinne von § 203 Abs. 1 Nr. 1, 2 und 5 des Strafgesetzbuchs von Gefangenen als Geheimnis anvertraut oder über Gefangene als Geheimnis sonst bekannt geworden sind, unterliegen auch gegenüber der Anstalt und der Aufsichtsbehörde der Schweigepflicht. Die in Satz 1 genannten Personen sind befugt und verpflichtet, diese Daten gegenüber der Anstaltsleitung zu offenbaren, soweit dies für die Sicherheit der Anstalt oder zur Abwehr von erheblichen Gefahren für Leben oder Gesundheit von Gefangenen oder Dritten unbedingt erforderlich ist. Eine Befugnis zur Offenbarung besteht auch, soweit es die Feststellung betrifft, ob Gefangene fähig sind, an bestimmten vollzuglichen Maßnahmen teilzunehmen oder ob sie an Behandlungsmaßnahmen teilnehmen und daran mitwirken.

(3) In Abs. 2 gelten Satz 2 und 3 entsprechend für die in § 203 Abs. 1 Nr. 1, 2, 4 und 5 des Strafgesetzbuchs genannten Personen außerhalb des Vollzugs, die mit der Untersuchung, Behandlung oder Betreuung von Gefangenen beauftragt wurden, mit der Maßgabe, dass die vorgenannten Personen lediglich zu einer Offenbarung befugt sind.

(4) Die Gefangenen sind bei der Aufnahme über die nach Abs. 2 Satz 2 und Abs. 3 bestehenden Offenbarungsbefugnisse und Offenbarungspflichten zu unterrichten.

(5) Die nach Abs. 2 und 3 offenbarten Daten dürfen nur für den Zweck, für den sie offenbart wurden oder für den eine Offenbarung zulässig gewesen wäre, und in dem hierfür unbedingt erforderlichen Umfang verarbeitet werden."

8. In § 62 Abs. 3 wird die Angabe "§ 15" durch "§ 58" ersetzt.

9. Die §§ 63 bis 65 werden wie folgt gefasst:

"§ 63
Datensicherung

(1) Mit der Datenverarbeitung befasste Personen dürfen personenbezogene Daten nicht unbefugt verarbeiten. Sie sind auf die bei ihrer Tätigkeit zu beachtenden Vorschriften über den Datenschutz zu unterrichten. Auf die besonderen Anforderungen bei von Verarbeitung von Daten, die aus Videoüberwachung oder aus Maßnahmen nach § 60 Abs. 2 und § 61 Abs. 1 und 2 stammen oder besondere Kategorien personenbezogener Daten nach § 41 Nr. 15 des Hessischen Datenschutz- und Informationsfreiheitsgesetzes oder den Kernbereich privater Lebensgestaltung betreffen, sind sie gesondert hinzuweisen. Das Datengeheimnis besteht auch nach der Beendigung der Tätigkeit fort.

(2) Akten und Dateien mit personenbezogenen Daten sind nach Maßgabe des § 59 des Hessischen Datenschutz- und Informationsfreiheitsgesetzes durch technische und organisatorische Maßnahmen gegen unbefugten Zugriff zu schützen. Gefangenenpersonalakten, Gesundheitsakten, Krankenblätter und sonstige in § 61 Abs. 2 und 3 aufgeführte personenbezogene Daten sind getrennt von anderen Unterlagen zu führen und besonders zu sichern.

§ 64
Information und Auskunft an die Betroffenen, Akteneinsicht

Die Betroffenen erhalten Auskunft und Information hinsichtlich der zu ihrer Person verarbeiteten Daten nach Maßgabe der §§ 50 bis 52 des Hessischen Datenschutz- und Informationsfreiheitsgesetzes, soweit die Datenverarbeitung zu den in § 40 des Hessischen Datenschutz- und Informationsfreiheitsgesetzes genannten Zwecken erfolgt; im Übrigen nach Maßgabe der §§ 31 bis 33 des Hessischen Datenschutz- und Informationsfreiheitsgesetzes. Soweit dies zur Wahrnehmung rechtlicher Interessen erforderlich ist, wird dem Betroffenen Akteneinsicht gewährt.

§ 65
Berichtigung, Einschränkung der Verarbeitung und Löschung

(1) Personenbezogene Daten sind nach Maßgabe der §§ 53 und 70 des Hessischen Datenschutz- und Informationsfreiheitsgesetzes zu berichtigen, zu löschen oder in der Verarbeitung einzuschränken, soweit sie zu den in § 40 des Hessischen Datenschutz- und Informationsfreiheitsgesetzes genannten Zwecken verarbeitet wurden und in den nachfolgenden Absätzen keine besonderen Regelungen getroffen sind; im Übrigen gilt § 34 des Hessischen Datenschutz- und Informationsfreiheitsgesetzes.

(2) Personenbezogene Daten, die durch den Einsatz eines elektronischen Überwachungssystems erhoben wurden oder hierbei angefallen sind, sind nach Beendigung der Maßnahme unverzüglich, Videoaufnahmen oder Ergebnisse von Maßnahmen nach § 59 spätestens 72 Stunden nach Ende des Kalendertages, an dem sie angefallen sind, zu löschen, soweit nicht zum Zeitpunkt der Entscheidung über die Löschung die weitere Aufbewah-

rung bei Einschränkung der Verarbeitung zu konkreten Beweiszwecken unbedingt erforderlich ist. Sind personenbezogene Daten entgegen § 58 Abs. 1 Satz 3 verarbeitet worden, sind diese unverzüglich, spätestens 24 Stunden nach Ende des Kalendertages, an dem sie angefallen sind, zu löschen. Die Tatsache der Löschung nach Satz 1 und 2 ist zu dokumentieren; die Dokumentation darf ausschließlich zu Zwecken der Datenschutzkontrolle verwendet werden und ist zu löschen, wenn sie für diese Zwecke nicht mehr erforderlich ist, spätestens jedoch am Ende des Kalenderjahres, das dem Jahr der Dokumentation folgt.

(3) Personenbezogene Daten, die in der Gefangenenpersonalakte oder in anderen zur Person der Gefangenen geführten Dateien und Akten gespeichert sind, sind spätestens fünf Jahre nach der Entlassung oder der Verlegung der Gefangenen in eine andere Anstalt zu löschen. Sonstige personenbezogene Daten, die in anderen Dateien und Akten gespeichert sind, sind, sofern ihre Speicherung nicht mehr erforderlich ist, unverzüglich, spätestens nach Ablauf von fünf Jahren ab ihrer Erhebung zu löschen.

(4) Eine Löschung personenbezogener Daten unterbleibt, soweit ihre Speicherung bei Einschränkung ihrer Verarbeitung nach

1. § 53 des Hessischen Datenschutz- und Informationsfreiheitsgesetzes, insbesondere aufgrund ärztlichen Dokumentationspflichten, oder
2. § 34 des Hessischen Datenschutz- und Informationsfreiheitsgesetzes

erfolgt. In ihrer Verarbeitung eingeschränkte Daten sind besonders zu kennzeichnen und dürfen außer bei Einwilligung der Betroffenen nur zu dem Zweck verarbeitet, insbesondere übermittelt werden, der ihrer Löschung entgegenstand. Die Einschränkung der Verarbeitung endet, wenn Gefangene erneut zum Vollzug einer Freiheitsentziehung aufgenommen werden oder die Betroffenen eingewilligt haben. Bei den in der Verarbeitung eingeschränkten personenbezogenen Daten können bis zum Ablauf der Aufbewahrungsfrist für die Gefangenenpersonalakte oder anderer zur Person der Gefangenen geführten Dateien oder Akten die Angaben über Familienname, Vorname, Geburtsname, Geburtstag, Geburtsort, Eintritts- und Austrittsdatum gespeichert werden, soweit dies für das Auffinden dieser Dateien oder Akten erforderlich ist.

(5) Die Erforderlichkeit der Löschung, auch bei in der Verarbeitung eingeschränkten personenbezogenen Daten, ist jährlich zu kontrollieren. Die Frist zur Kontrolle personenbezogener Daten, die in der Gefangenenpersonalakte oder in anderen zur Person der Gefangenen geführten Dateien und Akten gespeichert sind, beginnt mit der Entlassung oder Verlegung der Gefangenen in eine andere Anstalt, in sonstigen Fällen mit Erhebung der personenbezogenen Daten.

(6) Folgende Aufbewahrungsfristen von Dateien und Akten, soweit diese in der Verarbeitung eingeschränkt sind, dürfen nicht überschritten werden:

1. 20 Jahre bei Daten aus Gefangenenpersonalakten, Gesundheitsakten und Krankenblättern,
2. 30 Jahre bei Daten aus Gefangenenbüchern.

Dies gilt nicht, wenn konkrete Anhaltspunkte dafür vorliegen, dass die Aufbewahrung für die in Abs. 4 genannten Zwecke weiterhin erforderlich ist. Die Aufbewahrungsfrist beginnt mit dem auf das Jahr der Weglegung folgenden Kalenderjahr. Die Vorschriften des Hessischen Archivgesetzes vom 26. November 2012 (GVBl. S. 458) in seiner jeweils geltenden Fassung bleiben unberührt."

10. § 69 wird wie folgt geändert:

a) In Abs. 1 Satz 2 werden nach dem Wort "Ergebnisse" die Wörter "dienen dem öffentlichen Interesse und" eingefügt.

b) Abs. 3 wird wie folgt gefasst:

"(3) Für die Übermittlung personenbezogener Daten gilt § 476 der Strafprozessordnung mit der Maßgabe entsprechend, dass

1. auch elektronisch gespeicherte personenbezogene Daten übermittelt werden können und
2. besondere Kategorien personenbezogener Daten nach § 41 Nr. 15 des Hessischen Datenschutz- und Informationsfreiheitsgesetzes nur übermittelt werden, soweit dies für den Zweck nach § 476 Abs. 1 Nr. 1 der Strafprozessordnung unbedingt erforderlich ist."

Artikel 4
Änderung des Hessischen Untersuchungshaftvollzugsgesetzes

Das Hessische Untersuchungshaftvollzugsgesetz vom 28. Juni 2010 (GVBl. I S. 185, 208), zuletzt geändert durch Gesetz vom 5. Oktober 2017 (GVBl. S. 294), wird wie folgt geändert:

1. Die Inhaltsübersicht wird wie folgt geändert:

   a) Die Angabe zu § 55 wird wie folgt gefasst:

   "§ 55 Auslesen von Datenspeichern"

   b) Die Angabe zu den §§ 60 und 61 wird wie folgt gefasst:

   "§ 60 Information und Auskunft an die Betroffenen, Akteneinsicht

   § 61 Berichtigung, Einschränkung der Verarbeitung und Löschung"

2. § 17 Abs. 7 wird wie folgt gefasst:

   "(7) Bei schwerer Erkrankung oder Tod von Untersuchungsgefangenen werden die der Anstalt bekannten nächsten Angehörigen unverzüglich benachrichtigt, im Falle der schweren Erkrankung nur, wenn die Untersuchungsgefangenen hierin eingewilligt haben. Dem Wunsch der Untersuchungsgefangenen, auch andere Personen zu benachrichtigen, soll nach Möglichkeit entsprochen werden. Die Untersuchungsgefangenen sind bei Aufnahme über die Möglichkeit einer Einwilligung zu belehren."

3. § 26 wird folgt geändert:

   a) Abs. 4 Satz 1 und 2 wird wie folgt gefasst:

   "Abgesehen von den Fällen des § 25 Abs. 3 und 4 dürfen Besuche aus Gründen der Sicherheit oder Ordnung der Anstalt oder bei Vorliegen einer entsprechenden verfahrenssichernden Anordnung offen überwacht werden; die Überwachung erstreckt sich hierbei sowohl auf die Untersuchungsgefangenen wie deren Besuch. Die Unterhaltung darf nur überwacht werden, soweit dies im Einzelfall aus den in Satz 1 genannten Gründen erforderlich ist, und, soweit und solange sie besondere Kategorien personenbezogener Daten nach § 41 Nr. 15 des Hessischen Datenschutz- und Informationsfreiheitsgesetzes zum Gegenstand hat, unbedingt erforderlich ist."

   b) Abs. 5 Satz 1 und 2 wird wie folgt gefasst:

   "Die optische Überwachung eines Besuchs kann auch durch technische Hilfsmittel erfolgen, insbesondere durch optisch-elektronische Einrichtungen (Videoüberwachung). Die Aufzeichnung und Speicherung von nach Satz 1 erhobenen Daten ist zulässig, wenn sie zum Erreichen des verfolgten Zwecks unbedingt erforderlich ist."

4. § 27 Abs. 2 Satz 2 wird wie folgt gefasst:

   "Im Übrigen darf der Schriftwechsel von der Anstalt nach Maßgabe der Abs. 3 und 4 kontrolliert werden, soweit es wegen eines in § 25 Abs. 2 genannten Grundes unbedingt erforderlich ist; die Untersuchungsgefangenen sind auf entsprechende Maßnahmen bei Aufnahme hinzuweisen."

5. § 30 Abs. 2 Satz 2 wird wie folgt gefasst:

   "Soweit es zur Gewährleistung von Sicherheit oder Ordnung der Anstalt unbedingt erforderlich ist, erfolgt eine offene optische Überwachung der Untersuchungsgefangenen außerhalb der Hafträume mit technischen Hilfsmitteln, insbesondere Videoüberwachung."

6. § 35 wird wie folgt geändert:

   a) Dem Abs. 2 Nr. 2 werden die Wörter "insbesondere Videoüberwachung, soweit dies unbedingt erforderlich ist," angefügt.

   b) In Abs. 6 Satz 2 wird vor dem Wort "erforderlich" das Wort "unbedingt" eingefügt.

7. In § 46 Abs. 5 wird die Angabe "abweichend von § 55 Abs. 1" gestrichen.

8. Die §§ 54 bis 57 werden wie folgt gefasst:

"§ 54
Zulässigkeit der Verarbeitung personenbezogener Daten

(1) Die Anstalt und die Aufsichtsbehörde dürfen personenbezogene Daten nur verarbeiten, wenn eine Rechtsvorschrift dies vorsieht oder zwingend voraussetzt oder soweit dies

für den Vollzug der Untersuchungshaft erforderlich und im Falle der Verarbeitung besonderer Kategorien personenbezogener Daten nach § 41 Nr. 15 des Hessischen Datenschutz- und Informationsfreiheitsgesetzes unbedingt erforderlich ist. Soweit in den folgenden Vorschriften nichts Abweichendes geregelt ist, findet das Hessische Datenschutz- und Informationsfreiheitsgesetz Anwendung; dabei finden insbesondere die Vorschriften von Teil 3 des Hessischen Datenschutz- und Informationsfreiheitsgesetzes auf die Datenverarbeitung durch die Anstalt oder Aufsichtsbehörde Anwendung, soweit die Datenverarbeitung zu den in § 40 des Hessischen Datenschutz- und Informationsfreiheitsgesetzes genannten Zwecken erfolgt. Bei der Verarbeitung personenbezogener Daten sind schutzwürdige Interessen der Betroffenen in jedem Fall der Verarbeitung zu berücksichtigen; sofern der Kernbereich privater Lebensgestaltung betroffen ist, darf keine Verarbeitung erfolgen.

(2) Zur Sicherung des Vollzugs, zur Aufrechterhaltung der Sicherheit oder Ordnung der Anstalt, zur Identitätsfeststellung oder zur Aufrechterhaltung der medizinischen Versorgung und Gesundheitsfürsorge ist, soweit hierfür unbedingt erforderlich, die Verarbeitung folgender Daten von Untersuchungsgefangenen mit deren Kenntnis zulässig:

1. biometrische Daten von Fingern und Händen,
2. Lichtbilder,
3. Feststellungen äußerlicher körperlicher Merkmale,
4. Körpermessungen und
5. Gesundheitsdaten.

(3) Alle zur Person der Untersuchungsgefangenen erhobenen und für den Vollzug der Freiheitsstrafe erforderlichen Daten einschließlich derjenigen, die nach Abs. 2 Nr. 1 bis 4 erhoben worden sind, sind in eine Gefangenenpersonalakte aufzunehmen, die auch elektronisch geführt werden kann. Gesundheitsdaten und die sonstigen in § 57 Abs. 2 und 3 aufgeführten personenbezogenen Daten sind getrennt von der Gefangenenpersonalakte zu führen.

(4) Die einzelnen Vollzugsbediensteten sowie die in § 57 Abs. 3, § 67 Abs. 1 Satz 2 und 3, § 68 Abs. 1 und § 72 genannten Personen dürfen von personenbezogenen Daten nur Kenntnis erhalten, soweit dies zur Erfüllung der ihnen obliegenden Aufgabe oder für die Zusammenarbeit nach § 67 Abs. 3 erforderlich ist. Bei personenbezogenen Daten im Sinne von Abs. 2 ist über Satz 1 hinaus erforderlich, dass dies zur Erfüllung der ihnen obliegenden Aufgabe oder für die Zusammenarbeit nach § 67 Abs. 3 unbedingt erforderlich ist.

(5) Die Anstalt ist befugt, zur Aufrechterhaltung der Sicherheit oder Ordnung der Anstalt hierfür die Identität aller Personen festzustellen, die Zugang zur Anstalt begehren. Sofern unbedingt erforderlich, nimmt die Anstalt den Abgleich biometrischer Daten vor.

(6) Soweit dies zur Aufrechterhaltung von Sicherheit oder Ordnung der Anstalt hierfür erforderlich ist, werden Außenbereiche der Anstalt mit technischen Hilfsmitteln, insbesondere Videoüberwachung, offen überwacht, sofern keine Anhaltspunkte dafür bestehen, dass schutzwürdige Interessen der Betroffenen überwiegen. Der Umstand der Überwachung und der Name und die Kontaktdaten der Verantwortlichen sind den Betroffenen durch geeignete Maßnahmen zum frühestmöglichen Zeitpunkt kenntlich zu machen. § 26 Abs. 5 Satz 2 gilt entsprechend; darüber hinaus ist eine Speicherung nur zulässig, wenn keine Anhaltspunkte dafür bestehen, dass schutzwürdige Interessen der Betroffenen überwiegen.

§ 54a
Überprüfung anstaltsfremder Personen

(1) Personen, die in der Anstalt tätig werden sollen und die zur Anstalt oder Aufsichtsbehörde nicht in einem Dienst- oder Arbeitsverhältnis stehen und nicht im Auftrag einer anderen Behörde Zugang begehren, können zu diesen Tätigkeiten nur zugelassen werden, wenn keine Sicherheitsbedenken bestehen. Die Anstalt nimmt zur Aufrechterhaltung der Sicherheit oder Ordnung der Anstalt mit Einwilligung der betroffenen Person eine Zuverlässigkeitsüberprüfung vor. Sie darf dazu

1. eine Auskunft nach § 41 Abs. 1 Nr. 1 des Bundeszentralregistergesetzes in der Fassung der Bekanntmachung vom 21. September 1984 (BGBl. I S. 1229, 1985 I S. 195), zuletzt geändert durch Gesetz vom 18. Juli 2017 (BGBl. I S. 2732), einholen,
2. Erkenntnisse der Polizeibehörden und, soweit im Einzelfall erforderlich, des Landesamts für Verfassungsschutz abfragen.

Ist eine Überprüfung in Eilfällen, beispielsweise bei kurzfristig notwendigen Reparaturarbeiten, nicht möglich, hat eine entsprechende Beaufsichtigung der Person bei der Tätigkeit in der Anstalt zu erfolgen. Die Vorschriften des Hessischen Sicherheitsüberprü-

fungsgesetzes vom 19. Dezember 2014 (GVBl. S. 364) in seiner jeweils geltenden Fassung bleiben unberührt.

(2) Abgesehen von den Fällen des § 25 Abs. 3 und 4 darf die Anstalt auch bei Personen, die die Zulassung zum Besuch von Untersuchungsgefangenen oder zum Besuch der Anstalt begehren, zur Aufrechterhaltung der Sicherheit oder Ordnung der Anstalt mit ihrer Einwilligung eine Zuverlässigkeitsüberprüfung vornehmen. Abs. 1 Satz 3 gilt entsprechend; hierbei teilt die Anstalt den in Abs. 1 Satz 3 Nr. 2 genannten Behörden auch mit, dass und für welche Untersuchungsgefangenen die Person die Zulassung zum Besuch begehrt.

(3) Werden der Anstalt sicherheitsrelevante Erkenntnisse bekannt, wird die betroffene Person nicht oder nur unter Beschränkungen zu der Tätigkeit oder dem Besuch zugelassen. Gleiches gilt, wenn die betroffene Person eine Einwilligung in eine Zuverlässigkeitsüberprüfung verweigert.

(4) Personen nach Abs. 1 und 2 sind über die Benachrichtigung nach § 51 des Hessischen Datenschutz- und Informationsfreiheitsgesetzes hinaus über den Anlass der Zuverlässigkeitsprüfung, ihren möglichen Umfang nach Abs. 1 und 2 und über die Rechtsfolgen nach Abs. 3 mit der Einwilligungsanfrage zu belehren.

(5) Im Rahmen der Überprüfung bekannt gewordene Daten dürfen, soweit nicht aufgrund einer anderen gesetzlichen Vorschrift ihre Übermittlung gestattet oder vorgeschrieben ist, mit Ausnahme des für die Überprüfung einer Entscheidung nach Abs. 3 zuständigen Gerichts nicht an Dritte übermittelt werden.

(6) Die Zuverlässigkeitsüberprüfung ist in der Regel nach Ablauf einer Frist von fünf Jahren zu wiederholen, sofern ihre Erforderlichkeit nach Abs. 1 Satz 1 weiter besteht. Sie kann zudem wiederholt werden, wenn neue sicherheitsrelevante Erkenntnisse dies nahelegen.

§ 55
Auslesen von Datenspeichern

Elektronische Datenspeicher sowie elektronische Geräte mit Datenspeicher, die ohne Erlaubnis in die Anstalt eingebracht wurden, dürfen auf schriftliche Anordnung der Anstaltsleitung ausgelesen werden, soweit konkrete Anhaltspunkte die Annahme rechtfertigen, dass dies für die Erfüllung von Ziel und Aufgabe des Vollzugs der Untersuchungshaft, insbesondere zur Aufrechterhaltung der Sicherheit oder Ordnung der Anstalt, unbedingt erforderlich ist. Die Gründe sind in der Anordnung festzuhalten. Sind die Betroffenen bekannt, sind ihnen die Gründe vor dem Auslesen mitzuteilen. Die Untersuchungsgefangenen sind bei der Aufnahme über die Möglichkeit des Auslesens von nicht gestatteten Datenspeichern zu belehren.

§ 56
Zweckbindung und Übermittlung

(1) Personenbezogene Daten dürfen zu Zwecken, für die sie nicht erhoben oder gespeichert worden sind, nur verarbeitet, insbesondere übermittelt werden, wenn ein Fall der §§ 20 bis 27 und 44 bis 45 des Hessischen Datenschutz- und Informationsfreiheitsgesetzes vorliegt, insbesondere soweit dies

1. zu den in § 40 des Hessischen Datenschutz- und Informationsfreiheitsgesetzes genannten Zwecken,
2. in gerichtlichen Verfahren wegen Maßnahmen nach diesem Gesetz,
3. für Maßnahmen der Gerichtshilfe, Bewährungshilfe oder Führungsaufsicht,
4. zur Vorbereitung und Durchführung von Maßnahmen der Entlassungsvorbereitung und Nachsorge,
5. für Entscheidungen in Gnadensachen,
6. für sozialrechtliche Maßnahmen,
7. für die Einleitung von Hilfsmaßnahmen für Angehörige der Untersuchungsgefangenen (§ 11 Abs. 1 Nr. 1 des Strafgesetzbuchs),
8. für dienstliche Maßnahmen der Bundeswehr im Zusammenhang mit der Aufnahme und Entlassung von Soldaten,
9. für ausländerrechtliche Maßnahmen,
10. für die Durchführung der Besteuerung,
11. zur Ausübung von Aufsichts- und Kontrollbefugnissen sowie zu Ausbildungs- und Prüfungszwecken oder

12. für gesetzlich angeordnete Statistiken der Rechtspflege

erforderlich und bei besonderen Kategorien personenbezogener Daten nach § 41 Nr. 15 des Hessischen Datenschutz- und Informationsfreiheitsgesetzes unbedingt erforderlich ist.

(2) Bei der Überwachung der Besuche, der Telekommunikation oder des Schriftwechsels sowie bei der Überwachung des Inhalts von Paketen und dem Auslesen von Datenspeichern bekannt gewordene personenbezogene Daten dürfen über ihre Erhebung oder Speicherung hinaus nur verarbeitet, insbesondere übermittelt werden, wenn dies

1. nach Abs. 1 Nr. 1 oder 2 zulässig ist,
2. eine Rechtsvorschrift vorsieht, zwingend voraussetzt oder
3. die Wahrung der Sicherheit oder Ordnung der Anstalt, die Sicherung des Vollzugs der Untersuchungshaft oder die Umsetzung einer verfahrenssichernden Anordnung gebietet

und es unbedingt erforderlich ist. Daten nach Satz 1 sind hinsichtlich des Ursprungs ihrer Erhebung und Speicherung eindeutig zu kennzeichnen. § 4 Abs. 3 Satz 2 des Hessischen Datenschutz- und Informationsfreiheitsgesetzes bleibt unberührt.

(3) Die Anstalt oder Aufsichtsbehörde kann auf Antrag mitteilen, ob sich jemand in Untersuchungshaft befindet sowie ob und wann die Entlassung voraussichtlich ansteht, soweit dies nach Abs. 1 zulässig ist. Die Untersuchungsgefangenen werden vor der Mitteilung gehört, es sei denn, es ist zu besorgen, dass dadurch die Verfolgung des Interesses der Antragsteller vereitelt oder wesentlich erschwert werden würde. Ist die Anhörung unterblieben, werden die betroffenen Untersuchungsgefangenen über die Mitteilung der Anstalt oder Aufsichtsbehörde nachträglich unterrichtet. Bei einer nicht nur vorläufigen Einstellung des Verfahrens, einer unanfechtbaren Ablehnung der Eröffnung des Hauptverfahrens oder einem rechtskräftigen Freispruch sind auf Antrag der betroffenen Untersuchungsgefangenen die Stellen, die eine Mitteilung nach Satz 1 erhalten haben, in Kenntnis zu setzen. Die betroffenen Untersuchungsgefangenen sind bei der Anhörung nach Satz 2 auf ihr Antragsrecht hinzuweisen.

(4) Akten mit personenbezogenen Daten dürfen nur anderen Anstalten, Aufsichtsbehörden, den für strafvollzugs-, strafvollstreckungs- und strafrechtliche Entscheidungen zuständigen Gerichten sowie den Strafvollstreckungs- und Strafverfolgungsbehörden überlassen werden; die Überlassung an andere öffentliche Stellen ist zulässig, soweit die Erteilung einer Auskunft einen unvertretbaren Aufwand erfordert oder nach Darlegung der die Akteneinsicht begehrenden Stellen für die Erfüllung der Aufgabe nicht ausreicht. Entsprechendes gilt für die Überlassung von Akten an die von der Vollzugsbehörde mit Gutachten beauftragten Personen oder Stellen.

(5) Von der Anstalt oder der Aufsichtsbehörde übermittelte personenbezogene Daten dürfen nur zu dem Zweck verarbeitet werden, zu dessen Erfüllung sie übermittelt worden sind. Der Empfänger darf die Daten für andere Zwecke nur verarbeiten, soweit sie ihm auch für diese Zwecke hätten übermittelt werden dürfen und wenn im Falle einer Übermittlung an nicht öffentliche Stellen die übermittelnde Vollzugsbehörde eingewilligt hat. Die Anstalt oder Aufsichtsbehörde hat den Empfänger auf die Zweckbindung nach Satz 1 hinzuweisen und für den Fall, dass die übermittelten Daten besondere Kategorien personenbezogener Daten nach § 41 Nr. 15 des Hessischen Datenschutz-Informationsfreiheitsgesetzes enthalten, auf diese Einstufung.

(6) Die Übermittlung von personenbezogenen Daten unterbleibt, soweit die in § 57 Abs. 2 und § 61 Abs.4 und 7 geregelten Einschränkungen oder besondere gesetzliche Verwendungsregelungen entgegenstehen. Dies gilt nicht, wenn ein nach Abs. 1 Nr. 1 bis 3 zuständiges Gericht diese Daten anfordert oder dies zur Erfüllung der Aufgaben einer in § 119 Abs. 4 Nr. 13 der Strafprozessordnung genannten Stelle im Rahmen eines Besuchs der Anstalt erforderlich ist.

(7) Die Verantwortung für die Zulässigkeit der Übermittlung trägt die übermittelnde Anstalt oder Aufsichtsbehörde. Erfolgt die Übermittlung auf Ersuchen einer öffentlichen Stelle, trägt diese die Verantwortung. In diesem Fall prüft die übermittelnde Anstalt oder Aufsichtsbehörde nur, ob das Übermittlungsersuchen im Rahmen der Aufgaben des Empfängers liegt und die Abs. 2 und 6 der Übermittlung nicht entgegenstehen, es sei denn, dass besonderer Anlass zur Prüfung der Zulässigkeit der Übermittlung besteht.

§ 57
Schutz besonderer Daten

(1) Besondere Kategorien personenbezogener Daten nach § 41 Nr. 15 des Hessischen Datenschutz- und Informationsfreiheitsgesetzes, insbesondere das religiöse oder weltanschauliche Bekenntnis von Untersuchungsgefangenen und personenbezogene Daten, die anlässlich ärztlicher Untersuchungen erhoben worden sind, dürfen in der Anstalt nicht allgemein kenntlich gemacht werden. Andere personenbezogene Daten über die Gefan-

genen dürfen innerhalb der Anstalt allgemein kenntlich gemacht werden, soweit dies für ein geordnetes Zusammenleben in der Anstalt erforderlich ist.

(2) Personenbezogene Daten, die in der Anstalt tätigen Personen im Sinne von § 203 Abs. 1 Nr. 1, 2 und 5 des Strafgesetzbuchs von Untersuchungsgefangenen als Geheimnis anvertraut oder über Untersuchungsgefangene als Geheimnis sonst bekannt geworden sind, unterliegen auch gegenüber der Anstalt und der Aufsichtsbehörde der Schweigepflicht. Die in Satz 1 genannten Personen sind befugt und verpflichtet, diese Daten gegenüber der Anstaltsleitung zu offenbaren, soweit dies für die Sicherheit der Anstalt oder zur Abwehr von erheblichen Gefahren für Leben oder Gesundheit von Untersuchungsgefangenen oder Dritten unbedingt erforderlich ist. Eine Befugnis zur Offenbarung besteht auch, soweit es die Feststellung betrifft, ob Untersuchungsgefangene fähig sind, an bestimmten vollzuglichen Maßnahmen teilzunehmen.

(3) In Abs. 2 gelten Satz 2 und 3 entsprechend für die in § 203 Abs. 1 Nr. 1, 2, 4 und 5 des Strafgesetzbuchs genannten Personen außerhalb des Vollzugs, die mit der Untersuchung, Behandlung oder Betreuung von Untersuchungsgefangenen beauftragt wurden, mit der Maßgabe, dass die vorgenannten Personen lediglich zu einer Offenbarung befugt sind.

(4) Die Untersuchungsgefangenen sind bei der Aufnahme über die nach Abs. 2 Satz 2 und Abs. 3 bestehenden Offenbarungsbefugnisse und Offenbarungspflichten zu unterrichten.

(5) Die nach Abs. 2 und 3 offenbarten Daten dürfen nur für den Zweck, für den sie offenbart wurden oder für den eine Offenbarung zulässig gewesen wäre, und in dem hierfür unbedingt erforderlichen Umfang verarbeitet werden."

9. In § 58 Abs. 3 wird die Angabe "§ 15" durch "§ 58" ersetzt.

10. Die §§ 59 bis 61 werden wie folgt gefasst:

"§ 59
Datensicherung

(1) Mit der Datenverarbeitung befasste Personen dürfen personenbezogene Daten nicht unbefugt verarbeiten. Sie sind über die bei ihrer Tätigkeit zu beachtenden Vorschriften über den Datenschutz zu unterrichten. Auf die besonderen Anforderungen bei der Verarbeitung von Daten, die aus Videoüberwachung oder aus Maßnahmen im Sinne von § 56 Abs. 2, § 57 Abs. 1 und 2 stammen oder besondere Kategorien personenbezogener Daten nach § 41 Nr. 15 des Hessischen Datenschutz- und Informationsfreiheitsgesetzes oder den Kernbereich privater Lebensgestaltung betreffen, sind sie gesondert hinzuweisen. Das Datengeheimnis besteht auch nach der Beendigung der Tätigkeit fort.

(2) Akten und Dateien mit personenbezogenen Daten sind nach Maßgabe des § 59 des Hessischen Datenschutz- und Informationsfreiheitsgesetzes durch technische und organisatorische Maßnahmen gegen unbefugten Zugriff zu schützen. Gefangenenpersonalakten, Gesundheitsakten, Krankenblätter und sonstige in § 57 Abs. 2 und 3 aufgeführte personenbezogene Daten sind getrennt von anderen Unterlagen zu führen und besonders zu sichern.

§ 60
Information und Auskunft an die Betroffenen, Akteneinsicht

Die Betroffenen erhalten Auskunft und Information hinsichtlich der zu ihrer Person verarbeiteten Daten nach Maßgabe der §§ 50 bis 52 des Hessischen Datenschutz- und Informationsfreiheitsgesetzes, soweit die Datenverarbeitung zu den in § 40 des Hessischen Datenschutz- und Informationsfreiheitsgesetzes genannten Zwecken erfolgt; im Übrigen nach Maßgabe der §§ 31 bis 33 des Hessischen Datenschutz- und Informationsfreiheitsgesetzes. Soweit dies zur Wahrnehmung rechtlicher Interessen erforderlich ist, wird dem Betroffenen Akteneinsicht gewährt.

§ 61
Berichtigung, Einschränkung der Verarbeitung und Löschung

(1) Personenbezogene Daten sind nach Maßgabe der §§ 53 und 70 des Hessischen Datenschutz- und Informationsfreiheitsgesetzes zu berichtigen, zu löschen oder in der Verarbeitung einzuschränken, soweit sie zu den in § 40 des Hessischen Datenschutz- und Informationsfreiheitsgesetzes genannten Zwecken verarbeitet wurden und in den nachfolgenden Absätzen keine besonderen Regelungen getroffen sind; im Übrigen gilt § 34 des Hessischen Datenschutz- und Informationsfreiheitsgesetzes.

(2) Personenbezogene Daten, die durch den Einsatz eines elektronischen Überwachungssystems erhoben wurden oder hierbei angefallen sind, sind nach Beendigung der Maßnahme unverzüglich, Videoaufnahmen oder Ergebnisse von Maßnahmen nach § 55 spätestens 72 Stunden nach Ende des Kalendertages, an dem sie angefallen sind, zu löschen,

soweit nicht zum Zeitpunkt der Entscheidung über die Löschung die weitere Aufbewahrung bei Einschränkung der Verarbeitung zu konkreten Beweiszwecken unbedingt erforderlich ist. Sind personenbezogene Daten entgegen § 54 Abs. 1 Satz 3 verarbeitet worden, sind diese unverzüglich, spätestens 24 Stunden nach Ende des Kalendertages, an dem sie angefallen sind, zu löschen. Die Tatsache der Löschung nach Satz 1 und 2 ist zu dokumentieren; die Dokumentation darf ausschließlich zu Zwecken der Datenschutzkontrolle verwendet werden und ist zu löschen, wenn sie für diese Zwecke nicht mehr erforderlich ist, spätestens jedoch am Ende des Kalenderjahres, das dem Jahr der Dokumentation folgt.

(3) Personenbezogene Daten, die in der Gefangenenpersonalakte oder in anderen zur Person der Untersuchungsgefangenen geführten Dateien und Akten gespeichert sind, sind spätestens zwei Jahre nach der Entlassung oder der Verlegung in eine andere Anstalt zu löschen. Sonstige personenbezogene Daten, die in anderen Dateien und Akten gespeichert sind, sind, sofern ihre Speicherung nicht mehr erforderlich ist, unverzüglich, spätestens nach Ablauf von fünf Jahren ab ihrer Erhebung zu löschen.

(4) Eine Löschung personenbezogener Daten unterbleibt, soweit und solange ihre Speicherung bei Einschränkung ihrer Verarbeitung nach

1. § 53 des Hessischen Datenschutz- und Informationsfreiheitsgesetzes, insbesondere aufgrund ärztlicher Dokumentationspflichten, oder
2. § 34 des Hessischen Datenschutz- und Informationsfreiheitsgesetzes

erfolgt. In ihrer Verarbeitung eingeschränkte Daten sind besonders zu kennzeichnen und dürfen außer bei Einwilligung der Betroffenen nur zu dem Zweck verarbeitet, insbesondere übermittelt werden, der ihrer Löschung entgegenstand. Die Einschränkung der Verarbeitung endet, wenn Untersuchungsgefangene erneut zum Vollzug einer Freiheitsentziehung aufgenommen werden oder die Betroffenen eingewilligt haben. Bei den in der Verarbeitung eingeschränkten personenbezogenen Daten können bis zum Ablauf der Aufbewahrungsfrist für die Gefangenenpersonalakten oder anderer zur Person der Untersuchungsgefangenen geführten Dateien oder Akten die Angaben über Familienname, Vorname, Geburtsname, Geburtstag, Geburtsort, Eintritts- und Austrittsdatum gespeichert werden, soweit dies für das Auffinden dieser Dateien oder Akten erforderlich ist.

(5) Die Erforderlichkeit der Löschung, auch bei in der Verarbeitung eingeschränkten personenbezogenen Daten, ist jährlich zu kontrollieren. Die Frist zur Kontrolle personenbezogener Daten, die in der Gefangenenpersonalakte oder in anderen zur Person der Gefangenen geführten Dateien und Akten gespeichert sind, beginnt mit der Entlassung oder Verlegung des Gefangenen in eine andere Anstalt, in sonstigen Fällen mit Erhebung der personenbezogenen Daten.

(6) Erhält die Anstalt von einer nicht nur vorläufigen Einstellung des Verfahrens, einer unanfechtbaren Ablehnung der Eröffnung des Hauptverfahrens oder einem rechtskräftigen Freispruch Kenntnis, so tritt an die Stelle der in Abs. 3 Satz 1 und der in Abs. 5 Satz 2 genannten Fristen zur Kontrolle personenbezogener Daten, die in der Gefangenenpersonalakte oder in anderen zur Person der Gefangenen geführten Dateien und Akten gespeichert sind, eine Frist von einem Monat ab Kenntniserlangung.

(7) Folgende Aufbewahrungsfristen von Dateien und Akten, soweit diese in der Verarbeitung eingeschränkt sind, dürfen nicht überschritten werden:

1. 20 Jahre bei Daten aus Gefangenenpersonalakten, Gesundheitsakten und Krankenblättern,
2. 30 Jahre bei Daten aus Gefangenenbüchern.

Dies gilt nicht, wenn konkrete Anhaltspunkte dafür vorliegen, dass die Aufbewahrung für die in Abs. 4 genannten Zwecke weiterhin erforderlich ist. Die Aufbewahrungsfrist beginnt mit dem auf das Jahr der Weglegung folgenden Kalenderjahr. Die Vorschriften des Hessischen Archivgesetzes vom 26. November 2012 (GVBl. S. 458) in seiner jeweils geltenden Fassung bleiben unberührt."

Artikel 5
Änderung des Hessischen Sicherungsverwahrungsvollzugsgesetzes

Das Hessische Sicherungsverwahrungsvollzugsgesetz vom 5. März 2013 (GVBl. S. 46), zuletzt geändert durch Gesetz vom 5. Oktober 2017 (GVBl. S. 294), wird wie folgt geändert:

1. Die Inhaltsübersicht wird wie folgt geändert:
   a) Die Angabe zu § 59 wird wie folgt gefasst:
      "§ 59 Auslesen von Datenspeichern"

b) Die Angabe zu den §§ 64 und 65 wird wie folgt gefasst:

"§ 64 Information und Auskunft an die Betroffenen, Akteneinsicht

§ 65 Berichtigung, Einschränkung der Verarbeitung und Löschung"

2. § 24 Abs. 9 wird wie folgt gefasst:

"(9) Bei schwerer Erkrankung oder Tod von Untergebrachten werden die der Einrichtung bekannten nächsten Angehörigen unverzüglich benachrichtigt, im Falle der schweren Erkrankung nur, wenn die Untergebrachten hierin eingewilligt haben. Dem Wunsch der Untergebrachten, auch andere Personen zu benachrichtigen, soll nach Möglichkeit entsprochen werden. Die Untergebrachten sind bei Aufnahme über die Möglichkeit einer Einwilligung zu belehren."

3. § 34 wird folgt geändert:

a) Abs. 4 Satz 1 und 2 wird wie folgt gefasst:

"Abgesehen von den Fällen des § 33 Abs. 3 und 4 dürfen Besuche aus Gründen der Sicherheit oder Ordnung der Einrichtung oder aus Gründen der Behandlung offen überwacht werden; die Überwachung erstreckt sich hierbei sowohl auf die Untergebrachten wie deren Besuch. Die Unterhaltung darf nur überwacht werden, soweit dies im Einzelfall aus den in Satz 1 genannten Gründen erforderlich ist, und, soweit sie besondere Kategorien personenbezogener Daten nach § 41 Nr. 15 des Hessischen Datenschutz- und Informationsfreiheitsgesetzes vom ... [*einsetzen: Ausfertigungsdatum und Fundstelle dieses Gesetzes, ggf. Fundstelle von Art. 1*] zum Gegenstand hat, unbedingt erforderlich ist."

b) In Abs. 5 werden Satz 1 und 2 durch die folgenden Sätze ersetzt:

"Die optische Überwachung eines Besuchs kann auch durch technische Hilfsmittel erfolgen, insbesondere durch optisch-elektronische Einrichtungen (Videoüberwachung). Die Aufzeichnung und Speicherung von nach Satz 1 erhobenen Daten ist zulässig, wenn sie zum Erreichen des verfolgten Zwecks unbedingt erforderlich ist."

4. § 35 Abs. 2 Satz 1 wird wie folgt gefasst:

"Abgesehen von den Fällen des § 33 Abs. 3 und 4 darf der Schriftwechsel überwacht werden, soweit zur Erfüllung von Ziel und Aufgaben des Vollzugs der Sicherungsverwahrung nach § 2, insbesondere aus Gründen der Sicherheit oder Ordnung der Einrichtung oder aus Gründen der Behandlung unbedingt erforderlich ist; die Untergebrachten sind auf entsprechende Maßnahmen bei Aufnahme hinzuweisen."

5. § 45 Abs. 2 Satz 1 wird wie folgt gefasst:

"Soweit es zur Gewährleistung von Sicherheit oder Ordnung der Anstalt unbedingt erforderlich ist, erfolgt eine offene optische Überwachung der Gefangenen außerhalb der Hafträume mit technischen Hilfsmitteln, insbesondere Videoüberwachung."

6. § 50 wird wie folgt geändert:

a) Dem Abs. 2 Nr. 2 wird die Angabe "insbesondere Videoüberwachung, soweit dies unbedingt erforderlich ist," angefügt.

b) In Abs. 6 Satz 2 wird vor dem Wort "erforderlich" das Wort "unbedingt" eingefügt.

7. Die §§ 58 bis 61 werden wie folgt gefasst:

"§ 58
Zulässigkeit der Verarbeitung personenbezogener Daten

(1) Die Einrichtung und die Aufsichtsbehörde dürfen personenbezogene Daten nur verarbeiten, wenn eine Rechtsvorschrift dies vorsieht oder zwingend voraussetzt oder soweit dies für den Vollzug der Unterbringung erforderlich und im Falle der Verarbeitung besonderer Kategorien personenbezogener nach § 41 Nr. 15 des Hessischen Datenschutz- und Informationsfreiheitsgesetzes unbedingt erforderlich ist. Soweit in den folgenden Vorschriften nichts Abweichendes geregelt ist, findet das Hessische Datenschutzgesetz in der jeweils geltenden Fassung Anwendung; dabei finden insbesondere die Vorschriften von Teil 3 des Hessischen Datenschutz- und Informationsfreiheitsgesetzes auf die Datenverarbeitung durch die Anstalt oder Aufsichtsbehörde Anwendung, soweit die Datenverarbeitung zu den in § 40 des Hessischen Datenschutz- und Informationsfreiheitsgesetzes genannten Zwecken erfolgt. Bei der Verarbeitung personenbezogener Daten sind schutzwürdige Interessen der Betroffenen in jedem Fall der Verarbeitung zu berücksichtigen; sofern der Kernbereich privater Lebensgestaltung betroffen ist, darf keine Verarbeitung erfolgen.

(2) Zur Sicherung von Ziel und Aufgabe des Vollzugs der Sicherungsverwahrung nach § 2, insbesondere zur Aufrechterhaltung der Sicherheit oder Ordnung der Einrichtung, zur Identitätsfeststellung oder zur Aufrechterhaltung der medizinischen Versorgung und Gesundheitsfürsorge ist, soweit hierfür unbedingt erforderlich, die Verarbeitung folgender Daten von Gefangenen mit deren Kenntnis zulässig:

1. biometrische Daten von Fingern und Händen,
2. Lichtbilder,
3. Feststellungen äußerlicher körperlicher Merkmale,
4. Körpermessungen und
5. Gesundheitsdaten.

(3) Alle zur Person der Untergebrachten erhobenen und für den Vollzug der Unterbringung erforderlichen Daten einschließlich derjenigen, die nach Abs. 2 Nr. 1 bis 4 erhoben worden sind, sind in eine Untergebrachtenpersonalakte aufzunehmen, die auch elektronisch geführt werden kann. Gesundheitsdaten und die sonstigen in § 61 Abs. 2 und 3 aufgeführten personenbezogenen Daten sind getrennt von der Untergebrachtenpersonalakte zu führen.

(4) Die einzelnen Vollzugsbediensteten sowie die in § 61 Abs. 3, § 71 Abs. 1 Satz 2 und 3, § 72 Abs. 1 und § 76 genannten Personen dürfen von personenbezogenen Daten nur Kenntnis erhalten, soweit dies zur Erfüllung der ihnen obliegenden Aufgabe oder für die Zusammenarbeit nach § 4 Abs. 2 und § 71 Abs. 5 erforderlich ist. Bei personenbezogenen Daten im Sinne von Abs. 2 ist über Satz 1 hinaus erforderlich, dass dies zur Erfüllung der ihnen obliegenden Aufgabe oder für die Zusammenarbeit nach § nach § 4 Abs. 2 und § 71 Abs. 5 unbedingt erforderlich ist.

(5) Die Einrichtung ist befugt, zur Aufrechterhaltung der Sicherheit oder Ordnung der Einrichtung die Identität aller Personen festzustellen, die Zugang zur Einrichtung begehren. Sofern unbedingt erforderlich, nimmt die Einrichtung den Abgleich biometrischer Daten vor.

(6) Soweit dies zur Aufrechterhaltung von Sicherheit oder Ordnung der Einrichtung oder zur Abwendung von Gefahren hierfür erforderlich ist, werden Außenbereiche der Einrichtung mit technischen Hilfsmitteln, insbesondere Videoüberwachung, offen überwacht, sofern keine Anhaltspunkte dafür bestehen, dass schutzwürdige Interessen der Betroffenen überwiegen. Der Umstand der Überwachung und der Name und die Kontaktdaten der Verantwortlichen sind den Betroffenen durch geeignete Maßnahmen zum frühestmöglichen Zeitpunkt kenntlich zu machen. § 45 Abs. 5 Satz 2 gilt entsprechend; darüber hinaus ist eine Speicherung nur zulässig, wenn keine Anhaltspunkte dafür bestehen, dass schutzwürdige Interessen der Betroffenen überwiegen.

§ 58a
Überprüfung einrichtungsfremder Personen

(1) Personen, die in der Einrichtung tätig werden sollen und die zur Einrichtung oder Aufsichtsbehörde nicht in einem Dienst- oder Arbeitsverhältnis stehen und nicht im Auftrag einer anderen Behörde Zugang begehren, können zu diesen Tätigkeiten nur zugelassen werden, wenn keine Sicherheitsbedenken bestehen. Die Einrichtung nimmt zur Aufrechterhaltung der Sicherheit oder Ordnung der Einrichtung und zur Abwendung von Gefahren hierfür mit Einwilligung der betroffenen Person eine Zuverlässigkeitsüberprüfung vor. Sie darf dazu

1. eine Auskunft nach § 41 Abs. 1 Nr. 1 des Bundeszentralregistergesetzes in der Fassung der Bekanntmachung vom 21. September 1984 (BGBl. I S. 1229, 1985 I S. 195), zuletzt geändert durch Gesetz vom 18. Juli 2017 (BGBl. I S. 2732), einholen,
2. Erkenntnisse der Polizeibehörden und, soweit im Einzelfall erforderlich, des Landesamts für Verfassungsschutz abfragen.

Ist eine Überprüfung in Eilfällen, beispielsweise bei kurzfristig notwendigen Reparaturarbeiten, nicht möglich, hat eine entsprechende Beaufsichtigung der Person bei der Tätigkeit in der Einrichtung zu erfolgen. Die Vorschriften des Hessischen Sicherheitsüberprüfungsgesetzes vom 19. Dezember 2014 (GVBl. S. 364) in seiner jeweils geltenden Fassung bleiben unberührt.

(2) Abgesehen von den Fällen des § 33 Abs. 3 und 4 darf die Einrichtung auch bei Personen, die die Zulassung zum Untergebrachtenbesuch oder zum Besuch der Einrichtung begehren, zur Aufrechterhaltung der Sicherheit oder Ordnung der Einrichtung mit ihrer Einwilligung eine Zuverlässigkeitsüberprüfung vornehmen. Abs. 1 Satz 3 gilt entsprechend; hierbei teilt die Einrichtung den in Abs. 1 Satz 3 Nr. 2 genannten Behörden auch mit, dass und für welche Untergebrachten die Person die Zulassung zum Untergebrachtenbesuch begehrt.

(3) Werden der Einrichtung sicherheitsrelevante Erkenntnisse bekannt, wird die betroffene Person nicht oder nur unter Beschränkungen zu der Tätigkeit oder dem Besuch zugelassen. Gleiches gilt, wenn die betroffene Person eine Einwilligung in eine Zuverlässigkeitsüberprüfung verweigert.

(4) Personen nach Abs. 1 und 2 sind über die Benachrichtigung nach § 51 des Hessischen Datenschutz- und Informationsfreiheitsgesetzes hinaus über den Anlass der Zuverlässigkeitsprüfung, ihren möglichen Umfang nach Abs. 1 und 2 und über die Rechtsfolgen nach Abs. 3 mit der Einwilligungsanfrage zu belehren.

(5) Im Rahmen der Überprüfung bekannt gewordene Daten dürfen, soweit nicht aufgrund einer anderen gesetzlichen Vorschrift ihre Übermittlung gestattet oder vorgeschrieben ist, mit Ausnahme des für die Überprüfung einer Entscheidung nach Abs. 3 zuständigen Gerichts nicht an Dritte übermittelt werden.

(6) Die Zuverlässigkeitsüberprüfung ist in der Regel nach Ablauf einer Frist von fünf Jahren zu wiederholen, sofern ihre Erforderlichkeit nach Abs. 1 Satz 1 weiter besteht. Sie kann zudem wiederholt werden, wenn neue sicherheitsrelevante Erkenntnisse dies nahelegen.

§ 59
Auslesen von Datenspeichern

Elektronische Datenspeicher sowie elektronische Geräte mit Datenspeicher, die ohne Erlaubnis in die Einrichtung eingebracht wurden, dürfen auf schriftliche Anordnung der Einrichtungsleitung ausgelesen werden, soweit konkrete Anhaltspunkte die Annahme rechtfertigen, dass dies für die Erfüllung von Ziel und Aufgabe des Vollzugs der Sicherungsverwahrung nach § 2, insbesondere zur Aufrechterhaltung der Sicherheit oder Ordnung der Einrichtung, unbedingt erforderlich ist. Die Gründe sind in der Anordnung festzuhalten. Sind die Betroffenen bekannt, sind ihnen die Gründe vor dem Auslesen mitzuteilen. Die Untergebrachten sind bei der Aufnahme über die Möglichkeit des Auslesens von nicht gestatteten Datenspeichern zu belehren.

§ 60
Zweckbindung und Übermittlung

(1) Personenbezogene Daten dürfen zu Zwecken, für die sie nicht erhoben oder gespeichert worden sind, nur verarbeitet, insbesondere übermittelt werden, wenn ein Fall der §§ 20 bis 27 und 44 bis 45 des Hessischen Datenschutz- und Informationsfreiheitsgesetzes vorliegt, insbesondere soweit dies

1. zu den in § 40 des Hessischen Datenschutz- und Informationsfreiheitsgesetzes genannten Zwecken,
2. in gerichtlichen Verfahren wegen Maßnahmen nach diesem Gesetz,
3. für Maßnahmen der Gerichtshilfe, Bewährungshilfe oder Führungsaufsicht,
4. zur Vorbereitung und Durchführung von Maßnahmen der Entlassungsvorbereitung und Nachsorge,
5. für Entscheidungen in Gnadensachen,
6. für sozialrechtliche Maßnahmen,
7. für die Einleitung von Hilfsmaßnahmen für Angehörige der Untergebrachten (§ 11 Abs. 1 Nr. 1 des Strafgesetzbuchs),
9. für ausländerrechtliche Maßnahmen,
10. für die Durchführung der Besteuerung,
11. zur Ausübung von Aufsichts- und Kontrollbefugnissen sowie zu Ausbildungs- und Prüfungszwecken oder
12. für gesetzlich angeordnete Statistiken der Rechtspflege

erforderlich und bei besonderen Kategorien personenbezogener Daten nach § 41 Nr. 15 des Hessischen Datenschutz- und Informationsfreiheitsgesetzes unbedingt erforderlich ist.

(2) Bei der Überwachung der Besuche, der Telekommunikation oder des Schriftwechsels sowie bei der Überwachung des Inhalts von Paketen und dem Auslesen von Datenspeichern bekannt gewordene personenbezogene Daten dürfen über ihre Erhebung oder Speicherung hinaus nur verarbeitet, insbesondere übermittelt werden, wenn dies

1. nach Abs. 1 Nr. 1 oder 2 zulässig ist,
2. eine Rechtsvorschrift vorsieht, zwingend voraussetzt oder

3. die Wahrung der Sicherheit oder Ordnung der Einrichtung oder die Erreichung des Vollzugsziels gebietet

und es unbedingt erforderlich ist. Daten nach Satz 1 sind hinsichtlich des Ursprungs ihrer Erhebung und Speicherung eindeutig zu kennzeichnen. § 4 Abs. 3 Satz 2 des Hessischen Datenschutz- und Informationsfreiheitsgesetzes bleibt unberührt.

(3) Die Einrichtung oder Aufsichtsbehörde kann auf Antrag mitteilen, ob sich jemand in Sicherungsverwahrung befindet sowie ob und wann die Entlassung voraussichtlich ansteht, soweit dies nach Abs. 1 zulässig ist. Weiterhin können unter den Voraussetzungen des Satzes 1 auf schriftlichen Antrag Auskünfte auch über die Vermögensverhältnisse der Untergebrachten oder ihre Entlassungsadresse erteilt werden, wenn dies zur Feststellung oder Durchsetzung von Rechtsansprüchen im Zusammenhang mit der Straftat erforderlich ist. Unter den Voraussetzungen von § 406d Abs. 2 und 3 der Strafprozessordnung können Mitteilungen über die erstmalige Gewährung von vollzugsöffnenden Maßnahmen nach den §§ 13 und 16 Abs. 2 auch durch die Einrichtung erfolgen. Die Untergebrachten werden vor Mitteilungen nach Satz 1 bis 3 gehört, es sei denn, es ist zu besorgen, dass dadurch die Verfolgung des Interesses der Antragsteller vereitelt oder wesentlich erschwert werden würde. Ist die Anhörung unterblieben, werden die betroffenen Untergebrachten über die Mitteilung der Einrichtung oder Aufsichtsbehörde nachträglich unterrichtet.

(4) Akten mit personenbezogenen Daten dürfen nur anderen Einrichtungen, Aufsichtsbehörden, den für strafvollzugs-, strafvollstreckungs- und strafrechtliche Entscheidungen zuständigen Gerichten sowie den Strafvollstreckungs- und Strafverfolgungsbehörden überlassen werden; die Überlassung an andere öffentliche Stellen ist zulässig, soweit die Erteilung einer Auskunft einen unvertretbaren Aufwand erfordert oder nach Darlegung der die Akteneinsicht begehrenden Stellen für die Erfüllung der Aufgabe nicht ausreicht. Entsprechendes gilt für die Überlassung von Akten an die von der Vollzugsbehörde mit Gutachten beauftragten Personen oder Stellen.

(5) Von der Einrichtung oder der Aufsichtsbehörde übermittelte personenbezogene Daten dürfen nur zu dem Zweck verarbeitet werden, zu dessen Erfüllung sie übermittelt worden sind. Der Empfänger darf die Daten für andere Zwecke nur verarbeiten, soweit sie ihm auch für diese Zwecke hätten übermittelt werden dürfen und wenn im Falle einer Übermittlung an nicht öffentliche Stellen die übermittelnde Vollzugsbehörde eingewilligt hat. Die Einrichtung oder Aufsichtsbehörde hat den Empfänger auf die Zweckbindung nach Satz 1 hinzuweisen und für den Fall, dass die übermittelten Daten besondere Kategorien personenbezogener Daten nach § 41 Nr. 15 des Hessischen Datenschutz- und Informationsfreiheitsgesetzes enthalten, auf diese Einstufung.

(6) Die Übermittlung von personenbezogenen Daten unterbleibt, soweit die in § 61 Abs. 2 und § 65 Abs. 4 und 6 geregelten Einschränkungen oder besondere gesetzliche Verwendungsregelungen entgegenstehen. Dies gilt nicht, wenn ein nach Abs. 1 Nr. 1 bis 3 zuständiges Gericht diese Daten anfordert oder dies zur Erfüllung der Aufgaben einer in § 119 Abs. 4 Nr. 13 der Strafprozessordnung genannten Stelle im Rahmen eines Besuchs der Einrichtung erforderlich ist.

(7) Die Verantwortung für die Zulässigkeit der Übermittlung trägt die übermittelnde Einrichtung oder Aufsichtsbehörde. Erfolgt die Übermittlung auf Ersuchen einer öffentlichen Stelle, trägt diese die Verantwortung. In diesem Fall prüft die übermittelnde Einrichtung oder Aufsichtsbehörde nur, ob das Übermittlungsersuchen im Rahmen der Aufgaben des Empfängers liegt und die Abs. 2 und 6 der Übermittlung nicht entgegenstehen, es sei denn, dass besonderer Anlass zur Prüfung der Zulässigkeit der Übermittlung besteht.

(8) Für Daten, die im Rahmen einer Maßnahme nach § 14 Abs. 2 erhoben werden, gilt § 463a Abs. 4 der Strafprozessordnung entsprechend mit der Maßgabe, dass

1. diese Daten ohne Einwilligung der betroffenen Person nur verwendet werden, soweit dies erforderlich ist zur

   a) Feststellung oder Ahndung eines Verstoßes gegen eine Weisung nach § 14 Abs. 1 Nr. 1, 2 und 9,

   b) Wiederergreifung,

   c) Abwehr einer erheblichen gegenwärtigen Gefahr für das Leben, die körperliche Unversehrtheit, die persönliche Freiheit oder sexuelle Selbstbestimmung Dritter oder

   d) Verfolgung einer Straftat der in § 66 Abs. 3 Satz 1 des Strafgesetzbuchs genannten Art,

2. sich die Einrichtung zur Verarbeitung der Daten einer öffentlichen Stelle bedienen kann, zu deren Aufgaben die elektronische Überwachung von Weisungen nach § 68b Abs. 1 Nr. 12 des Strafgesetzbuchs gehört.

§ 61
Schutz besonderer Daten

(1) Besondere Kategorien personenbezogener Daten nach § 41 Nr. 15 des Hessischen Datenschutz- und Informationsfreiheitsgesetzes, insbesondere das religiöse oder weltanschauliche Bekenntnis von Untergebrachten und personenbezogene Daten, die anlässlich ärztlicher Untersuchungen erhoben worden sind, dürfen in der Einrichtung nicht allgemein kenntlich gemacht werden. Andere personenbezogene Daten über die Untergebrachten dürfen innerhalb der Einrichtung allgemein kenntlich gemacht werden, soweit dies für ein geordnetes Zusammenleben in der Einrichtung erforderlich ist.

(2) Personenbezogene Daten, die in der Einrichtung tätigen Personen im Sinne von § 203 Abs. 1 Nr. 1, 2 und 5 des Strafgesetzbuchs von Untergebrachten als Geheimnis anvertraut oder über Untergebrachte als Geheimnis sonst bekannt geworden sind, unterliegen auch gegenüber der Einrichtung und der Aufsichtsbehörde der Schweigepflicht. Die in Satz 1 genannten Personen sind befugt und verpflichtet, diese Daten gegenüber der Einrichtungsleitung zu offenbaren, soweit dies für die Sicherheit der Einrichtung oder zur Abwehr von erheblichen Gefahren für Leben oder Gesundheit von Untergebrachten oder Dritten unbedingt erforderlich ist. Eine Befugnis zur Offenbarung besteht auch, soweit es die Feststellung betrifft, ob die Untergebrachten fähig sind, an bestimmten vollzuglichen Maßnahmen teilzunehmen oder ob sie an Behandlungsmaßnahmen teilnehmen und daran mitwirken.

(3) In Abs. 2 gelten Satz 2 und 3 entsprechend für die in § 203 Abs. 1 Nr. 1, 2, 4 und 5 des Strafgesetzbuchs genannten Personen außerhalb des Vollzugs, die mit der Untersuchung, Behandlung oder Betreuung von Untergebrachten beauftragt wurden, mit der Maßgabe, dass die vorgenannten Personen lediglich zu einer Offenbarung befugt sind.

(4) Die Untergebrachten sind bei der Aufnahme über die nach Abs. 2 Satz 2 und Abs. 3 bestehenden Offenbarungsbefugnisse und Offenbarungspflichten zu unterrichten.

(5) Die nach Abs. 2 und 3 offenbarten Daten dürfen nur für den Zweck, für den sie offenbart wurden oder für den eine Offenbarung zulässig gewesen wäre, und in dem hierfür unbedingt erforderlichen Umfang verarbeitet werden."

8. In § 62 Abs. 3 wird die Angabe "§ 15" durch "§ 58" ersetzt.

9. Die §§ 63 bis 65 werden folgt gefasst:

"§ 63
Datensicherung

(1) Mit der Datenverarbeitung befasste Personen dürfen personenbezogene Daten nicht unbefugt verarbeiten. Sie sind über die bei ihrer Tätigkeit zu beachtenden Vorschriften über den Datenschutz zu unterrichten. Auf die besonderen Anforderungen bei der Verarbeitung von Daten, die aus Videoüberwachung oder aus Maßnahmen nach § 60 Abs. 2 und § 61 Abs. 1 und 2 stammen oder besondere Kategorien personenbezogener Daten nach § 41 Nr. 15 des Hessischen Datenschutz- und Informationsfreiheitsgesetzes oder den Kernbereich privater Lebensgestaltung betreffen, sind sie gesondert hinzuweisen. Das Datengeheimnis besteht auch nach der Beendigung der Tätigkeit fort.

(2) Akten und Dateien mit personenbezogenen Daten sind nach Maßgabe des § 59 des Hessischen Datenschutz- und Informationsfreiheitsgesetzes durch technische und organisatorische Maßnahmen gegen unbefugten Zugriff zu schützen. Untergebrachtenpersonalakten, Gesundheitsakten, Krankenblätter und sonstige in § 61 Abs. 2 und 3 aufgeführte personenbezogene Daten sind getrennt von anderen Unterlagen zu führen und besonders zu sichern.

§ 64
Information und Auskunft an die Betroffenen, Akteneinsicht

Die Betroffenen erhalten Auskunft und Information hinsichtlich der zu ihrer Person verarbeiteten Daten nach Maßgabe der §§ 50 bis 52 des Hessischen Datenschutz- und Informationsfreiheitsgesetzes, soweit die Datenverarbeitung zu den in § 40 des Hessischen Datenschutzgesetzes genannten Zwecken erfolgt; im Übrigen nach Maßgabe der §§ 31 bis 33 des Hessischen Datenschutz- und Informationsfreiheitsgesetzes. Soweit dies zur Wahrnehmung rechtlicher Interessen erforderlich ist, wird dem Betroffenen Akteneinsicht gewährt.

§ 65
Berichtigung, Einschränkung der Verarbeitung und Löschung

(1) Personenbezogene Daten sind nach Maßgabe der §§ 53 und 70 des Hessischen Datenschutz- und Informationsfreiheitsgesetzes zu berichtigen, zu löschen oder in der Verarbeitung einzuschränken, soweit sie zu den in § 40 des Hessischen Datenschutz- und Informationsfreiheitsgesetzes genannten Zwecken verarbeitet wurden und in den nachfolgenden Absätzen keine besonderen Regelungen getroffen sind; im Übrigen gilt § 34 des Hessischen Datenschutz- und Informationsfreiheitsgesetzes.

(2) Personenbezogene Daten, die durch den Einsatz eines elektronischen Überwachungssystems erhoben wurden oder hierbei angefallen sind, sind nach Beendigung der Maßnahme unverzüglich, Videoaufnahmen oder Ergebnisse von Maßnahmen nach § 59 spätestens 72 Stunden nach Ende des Kalendertages, an dem sie angefallen sind, zu löschen, soweit nicht zum Zeitpunkt der Entscheidung über die Löschung die weitere Aufbewahrung bei Einschränkung der Verarbeitung zu konkreten Beweiszwecken unbedingt erforderlich ist. Sind personenbezogene Daten entgegen § 58 Abs. 1 Satz 3 verarbeitet worden, sind diese unverzüglich, spätestens 24 Stunden nach Ende des Kalendertages, an dem sie angefallen sind, zu löschen. Die Tatsache der Löschung nach Satz 1 und 2 ist zu dokumentieren; die Dokumentation darf ausschließlich zu Zwecken der Datenschutzkontrolle verwendet werden und ist zu löschen, wenn sie für diese Zwecke nicht mehr erforderlich ist, spätestens jedoch am Ende des Kalenderjahres, das dem Jahr der Dokumentation folgt.

(3) Personenbezogene Daten, die in der Untergebrachtenpersonalakte oder in anderen zur Person der Untergebrachten geführten Dateien und Akten gespeichert sind, sind spätestens fünf Jahre nach der Entlassung oder der Verlegung der Untergebrachten in eine andere Anstalt zu löschen. Sonstige personenbezogene Daten, die in anderen Dateien und Akten gespeichert sind, sind, sofern ihre Speicherung nicht mehr erforderlich ist, unverzüglich, spätestens nach Ablauf von fünf Jahren ab ihrer Erhebung zu löschen.

(4) Eine Löschung personenbezogener Daten unterbleibt, soweit ihre Speicherung bei Einschränkung ihrer Verarbeitung nach

1. § 53 des Hessischen Datenschutz- und Informationsfreiheitsgesetzes, insbesondere aufgrund ärztlicher Dokumentationspflichten, oder
2. § 34 des Hessischen Datenschutz- und Informationsfreiheitsgesetzes

erfolgt. In ihrer Verarbeitung eingeschränkte Daten sind besonders zu kennzeichnen und dürfen außer bei Einwilligung der Betroffenen nur zu dem Zweck verarbeitet, insbesondere übermittelt werden, der ihrer Löschung entgegenstand. Die Einschränkung der Verarbeitung endet, wenn die Untergebrachten erneut zum Vollzug einer Freiheitsentziehung aufgenommen werden oder die Betroffenen eingewilligt haben. Bei den in der Verarbeitung eingeschränkten personenbezogenen Daten können bis zum Ablauf der Aufbewahrungsfrist für die Untergebrachtenpersonalakte oder anderer zur Person der Untergebrachten geführten Dateien oder Akten die Angaben über Familienname, Vorname, Geburtsname, Geburtstag, Geburtsort, Eintritts- und Austrittsdatum gespeichert werden, soweit dies für das Auffinden dieser Dateien oder Akten erforderlich ist.

(5) Die Erforderlichkeit der Löschung, auch bei in der Verarbeitung eingeschränkten personenbezogenen Daten, ist jährlich zu kontrollieren. Die Frist zur Kontrolle personenbezogener Daten, die in der Untergebrachtenpersonalakte oder in anderen zur Person der Untergebrachten geführten Dateien und Akten gespeichert sind, beginnt mit der Entlassung oder Verlegung der Untergebrachten in eine andere Anstalt, in sonstigen Fällen mit Erhebung der personenbezogenen Daten.

(6) Bei der Aufbewahrung von Dateien und Akten, soweit diese in der Verarbeitung eingeschränkt sind, dürfen folgende Fristen nicht überschritten werden:

1. 20 Jahre bei Daten aus Untergebrachtenpersonalakten, Gesundheitsakten und Krankenblättern,
2. 30 Jahre bei Daten aus Untergebrachtenbüchern.

Dies gilt nicht, wenn konkrete Anhaltspunkte dafür vorliegen, dass die Aufbewahrung für die in Abs. 4 genannten Zwecke weiterhin erforderlich ist. Die Aufbewahrungsfrist beginnt mit dem auf das Jahr der Weglegung folgenden Kalenderjahr. Die Vorschriften des Hessischen Archivgesetzes vom 26. November 2012 (GVBl. S. 458) in seiner jeweils geltenden Fassung bleiben unberührt."

10. § 66 wird wie folgt geändert:

a) Dem Abs. 2 wird folgender Satz angefügt:

"Die Ergebnisse dienen dem öffentlichen Interesse und sind für die Fortentwicklung des Vollzugs nutzbar zu machen."

b) Abs. 4 wird wie folgt gefasst:

"(4) Für die Übermittlung personenbezogener Daten gilt § 476 der Strafprozessordnung mit der Maßgabe entsprechend, dass

1. auch elektronisch gespeicherte personenbezogene Daten übermittelt werden können und
2. besondere Kategorien personenbezogener Daten nach § 41 Nr. 15 des Hessischen Datenschutz- und Informationsfreiheitsgesetzes nur übermittelt werden, soweit dies für den Zweck nach § 476 Abs. 1 Nr. 1 der Strafprozessordnung unbedingt erforderlich ist."

Artikel 6
Änderung des Hessischen Jugendarrestvollzugsgesetzes

Das Hessische Jugendarrestvollzugsgesetz vom 27. Mai 2015 (GVBl. S. 223) wird wie folgt geändert:

1. § 19 Abs. 2 wird wie folgt gefasst:

"(2) Aus Gründen der Sicherheit oder Ordnung der Einrichtung kann ein Besuch davon abhängig gemacht werden, dass sich die Besucherin oder der Besucher absuchen oder durchsuchen lässt. § 24 Abs. 1 gilt entsprechend. Abgesehen von den Fällen des Abs. 3 dürfen Besuche und Telefongespräche aus Gründen der Sicherheit oder Ordnung der Einrichtung oder aus Gründen der Behandlung offen optisch überwacht werden; die Überwachung erstreckt sich hierbei sowohl auf die Jugendlichen wie deren Besuch. Die Besuche und Telefongespräche dürfen nur überwacht werden, soweit dies im Einzelfall aus den in Satz 3 genannten Gründen erforderlich ist, und, soweit sie besondere Kategorien personenbezogener Daten nach § 41 Nr. 15 des Hessischen Datenschutz- und Informationsfreiheitsgesetzes vom … [*einsetzen: Ausfertigungsdatum und Fundstelle dieses Gesetzes, ggf. Fundstelle von Art. 1*] zum Gegenstand haben, unbedingt erforderlich ist. Ein Besuch oder ein Telefongespräch darf abgebrochen werden, wenn die Sicherheit oder Ordnung der Einrichtung gefährdet ist. Gegenstände dürfen beim Besuch nur mit Erlaubnis übergeben werden. Die optische Überwachung eines Besuchs kann auch durch technische Hilfsmittel erfolgen, insbesondere durch optisch-elektronische Einrichtungen (Videoüberwachung); die betroffenen Personen sind hierauf hinzuweisen."

2. § 26 wird wie folgt geändert:

a) Dem Abs. 2 Nr. 2 wird die Angabe "insbesondere Videoüberwachung, soweit dies für Zwecke nach Abs. 1 unbedingt erforderlich ist," angefügt.

b) In Abs. 6 Satz 1 wird vor dem Wort "erforderlich" das Wort "unbedingt" eingefügt.

3. In § 27 Abs. 1 Satz 1 wird die Angabe "5. März 2013 (GVBl. S. 46)" durch "… [*einsetzen: Ausfertigungsdatum und Fundstelle dieses Gesetzes*]" ersetzt.

4. Die §§ 37 und 38 werden wie folgt gefasst:

"§ 37
Kriminologische Forschung

"(1) Der Vollzug, insbesondere seine Gestaltung sowie die Maßnahmen und deren Wirkungen auf die Erreichung des Vollzugsziels, soll regelmäßig durch den kriminologischen Dienst in Zusammenarbeit mit Hochschulen oder anderen Stellen wissenschaftlich begleitet und erforscht werden. Die Ergebnisse dienen dem öffentlichen Interesse und sind für die Fortentwicklung des Vollzugs nutzbar zu machen.

(2) Für die Übermittlung personenbezogener Daten gilt § 476 der Strafprozessordnung mit der Maßgabe entsprechend, dass

1. auch elektronisch gespeicherte personenbezogene Daten übermittelt werden können und
2. besondere Kategorien personenbezogener Daten nach § 41 Nr. 15 des Hessischen Datenschutz- und Informationsfreiheitsgesetzes nur übermittelt werden, soweit dies für den Zweck nach § 476 Abs. 1 Nr. 1 der Strafprozessordnung unbedingt erforderlich ist.

§ 38
Datenschutz

Die §§ 58 bis 65 des Hessischen Jugendstrafvollzugsgesetzes in ihrer jeweils geltenden Fassung gelten entsprechend mit der Maßgabe, dass § 60 Abs. 3 Satz 2 und 3 keine Anwendung findet und die Frist nach § 65 Abs. 3 Satz 1 zwei Jahre beträgt."

Artikel 7
Änderung des Hessischen Justizkostengesetzes

§ 4 des Hessischen Justizkostengesetzes vom 15. Mai 1958 (GVBl. S. 60), zuletzt geändert durch Gesetz vom 24. Januar 2017 (GVBl. S. 12), wird wie folgt geändert:

1. Abs. 2 Nr. 1 wird wie folgt geändert:
   a) Dem Buchst. a wird das Wort "und" angefügt.
   b) In Buchst. b wird das Wort "und" gestrichen.
   c) Buchst. c wird aufgehoben.
2. In Abs. 4 Satz 2 Nr. 1 Buchst. c wird die Angabe "§ 13 Abs. 5 des Hessischen Datenschutzgesetzes in der Fassung vom 7. Januar 1999 (GVBl. I S. 98), geändert durch Gesetz vom 20. Mai 2011 (GVBl. I S. 208)," durch "§ 21 Abs. 3 des Hessischen Datenschutz- und Informationsfreiheitsgesetzes" ersetzt.
3. In Abs. 6 Satz 3 wird das Wort "Sperrung" durch die Wörter "Einschränkung der Verarbeitung" ersetzt.

Artikel 8
Änderung der Hessischen Landeshaushaltsordnung

In § 95 Abs. 3 der Hessischen Landeshaushaltsordnung in der Fassung der Bekanntmachung vom 15. März 1999 (GVBl. I S. 248), zuletzt geändert durch Gesetz vom 26. Juni 2013 (GVBl. S. 447), werden nach dem Wort "Daten" die Wörter "sowie deren automatisierten Abruf" eingefügt.

Artikel 9
Änderung des Gesetzes über die Hessische Steuerberaterversorgung

In § 11 Satz 2 Nr. 5 des Gesetzes über die Hessische Steuerberaterversorgung vom 13. Dezember 2001 (GVBl. I S. 578), geändert durch Gesetz vom 30. September 2008 (GVBl. I S. 874), wird die Angabe "§ 6 Abs. 3 und" gestrichen.

Artikel 10
Änderung des Hessischen Ingenieurgesetzes

§ 35 Abs. 2 Satz 1 des Hessischen Ingenieurgesetzes vom 30. November 2015 (GVBl. S. 457) wird wie folgt gefasst:

"Die Staatsaufsicht erstreckt sich auf die Beachtung dieses Gesetzes und des maßgeblichen Rechts der Europäischen Union und der zu ihrer Durchführung ergangenen Rechtsverordnungen, Richtlinien, Entscheidungen und Verwaltungsvorschriften sowie der Satzungen."

Artikel 11
Änderung des Hessischen Straßengesetzes

§ 33 Abs. 2 des Hessischen Straßengesetzes in der Fassung der Bekanntmachung vom 8. Juni 2003 (GVBl. I S. 166), zuletzt geändert durch Gesetz vom 26. Juni 2015 (GVBl. S. 254) [ggf. einsetzen*: Datum und Fundstelle des derzeit im Gesetzgebungsverfahren befindlichen Änderungsgesetzes zum HStrG*], wird wie folgt gefasst:

"(2) Der Plan besteht aus Zeichnungen und Erläuterungen, die das Vorhaben, seinen Anlass sowie die von dem Vorhaben betroffenen Grundstücke und Anlagen erkennen lassen."

Artikel 12
Änderung des Hessischen Gesetzes über den Bau und die Finanzierung öffentlicher Straßen durch Private

Das Hessische Gesetz über den Bau und die Finanzierung öffentlicher Straßen durch Private vom 27. November 2002 (GVBl. I S. 705), zuletzt geändert durch Gesetz vom 27. September 2012 (GVBl. S. 290), wird wie folgt geändert:

1. In § 9 Abs. 5 Satz 1 wird die Angabe "§ 4 des Hessischen Datenschutzgesetzes in der Fassung vom 7. Januar 1999 (GVBl. I S. 98), geändert durch Gesetz vom 20. Mai 2011 (GVBl. I S. 208)," durch "Art. 28 der Verordnung (EU) Nr. 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung) (ABl. EU Nr. L 119 S. 1, Nr. L 314 S. 72)" ersetzt.

2. § 13 Abs. 1 wird wie folgt gefasst:

   "(1) Ordnungswidrig handelt, wer vorsätzlich oder fahrlässig entgegen § 9 Abs. 1 in Verbindung mit der Rechtsverordnung nach § 6 Abs. 2 die Mautgebühr nicht oder nicht rechtzeitig entrichtet."

Artikel 13
Änderung des Hessischen Schulgesetzes

§ 83 Abs. 4 Satz 5 und § 84 Abs. 2 Satz 2 des Hessischen Schulgesetzes in der Fassung der Bekanntmachung vom 30. Juni 2017 (GVBl. S. 150) werden aufgehoben.

Artikel 14
Änderung des Hessischen Pressegesetzes

§ 10 des Hessischen Pressegesetzes in der Fassung der Bekanntmachung vom 12. Dezember 2003 (GVBl. 2004 I S. 2), zuletzt geändert durch Gesetz vom 13. Dezember 2012 (GVBl. S. 622), wird wie folgt gefasst:

"§ 10

Soweit Unternehmen und Hilfsunternehmen der Presse personenbezogene Daten zu journalistischen oder literarischen Zwecken verarbeiten, ist es den hiermit befassten Personen untersagt, diese personenbezogenen Daten zu anderen Zwecken zu verarbeiten (Datengeheimnis). Bei der Aufnahme ihrer Tätigkeit sind diese Personen auf das Datengeheimnis zu verpflichten. Das Datengeheimnis besteht auch nach Beendigung ihrer Tätigkeit fort. Im Übrigen finden für die Datenverarbeitung zu journalistischen oder literarischen Zwecken außer den Kapiteln I, X und XI nur Art. 5 Abs. 1 Buchst. f in Verbindung mit Abs. 2, Art. 24 Abs. 1 Satz 1 und Abs. 2, Art. 32 Abs. 1 Buchst. b bis d, Abs. 2 und 4 und Art. 82 der Verordnung (EU) Nr. 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (ABl. EU Nr. L 119 S. 1, Nr. L 314 S. 72) sowie § 83 des Bundesdatenschutzgesetzes vom 30. Juni 2017 (BGBl. I S. 2097) in der jeweils geltenden Fassung Anwendung. Art. 82 der Verordnung (EU) Nr. 2016/679 findet nur bei einem Verstoß gegen Art. 5 Abs. 1 Buchst. f, Art. 24 Abs. 1 Satz 1 und Abs. 2 sowie Art. 32 Abs. 1 Buchst. b bis d, Abs. 2 und 4 der Verordnung (EU) Nr. 2016/679 Anwendung. § 83 des Bundesdatenschutzgesetzes findet mit der Maßgabe Anwendung, dass nur für eine Verletzung des Datengeheimnisses nach Satz 1 bis 3 gehaftet wird."

Artikel 15
Änderung des Hessischen Ausführungsgesetzes zum Kreislaufwirtschaftsgesetz

§ 17 des Hessischen Ausführungsgesetzes zum Kreislaufwirtschaftsgesetz vom 6. März 2013 (GVBl. S. 80), geändert durch Gesetz vom 17. Dezember 2015 (GVBl. S. 636), wird wie folgt geändert:

1. Die Absatzbezeichnung "(1)" wird gestrichen.

2. In Abs. 1 Satz 4 werden die Wörter "auch ohne Vorliegen der Voraussetzungen des § 13 Abs. 2 des Hessischen Datenschutzgesetzes in der Fassung vom 7. Januar 1999 GVBl. I S. 98), geändert durch Gesetz vom 20. Mai 2011 (GVBl. I S. 208)," gestrichen.

3. Abs. 2 wird aufgehoben.

Artikel 16
Änderung des Hessischen Beamtengesetzes

Das Hessische Beamtengesetz vom 27. Mai 2013 (GVBl. S. 218, 508), zuletzt geändert durch Gesetz vom 5. Februar 2016 (GVBl. S. 30), wird wie folgt geändert:

1. Die Inhaltsübersicht wird wie folgt geändert:

   a) Die Angabe zu § 86 wird wie folgt gefasst:

   "§ 86 Personaldatenverarbeitung, Inhalt und Führung der Personalakte sowie Zugang zur Personalakte".

   b) Die Angabe zu § 89 wird wie folgt gefasst:

   "§ 89 Einsichts- und Auskunftsrecht".

   c) Die Angabe zu § 90 wird wie folgt gefasst:

   "§ 90 Übermittlung der Personalakte, Auskünfte an Dritte".

   d) Die Angabe zu § 93 wird wie folgt gefasst:

   "§ 93 Verarbeitung von Personalaktendaten in automatisierten Verfahren".

2. § 80 Abs. 6 wird wie folgt geändert:

   a) Satz 1 wird wie folgt gefasst:

   "Zur Erfüllung seiner Pflichten nach Abs. 1 kann sich der Dienstherr geeigneter Stellen auch außerhalb des öffentlichen Dienstes nach den Art. 28 und 29 der Verordnung (EU) Nr. 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Verkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung) (ABl. EU Nr. L 119 S. 1, Nr. L 314 S. 72) in der jeweils geltenden Fassung bedienen und diesen die zur Beihilfebearbeitung erforderlichen Daten übermitteln."

   b) Satz 3 wird wie folgt gefasst:

   "Die §§ 87 und 93 Abs. 2 gelten entsprechend."

3. § 86 wird wie folgt geändert:

   a) Die Überschrift wird wie folgt gefasst:

   "Personaldatenverarbeitung, Inhalt und Führung der Personalakte sowie Zugang zur Personalakte"

   b) Abs. 3 wird wie folgt geändert:

      aa) In Satz 1 werden die Wörter "Zugriff auf Personalaktendaten dürfen nur Beschäftigte haben" durch "Die Verarbeitung von Personalaktendaten erfolgt ausschließlich durch Beschäftigte" ersetzt.

      bb) In Satz 2 wird die Angabe "der Zugriff auf" durch "die Verarbeitung von" ersetzt.

      cc) Satz 4 wird wie folgt gefasst:

      "Die oberste Dienstbehörde kann abweichend von Satz 1 die Verarbeitung von personenbezogenen Daten nach den Art. 28 und 29 der Verordnung (EU) Nr. 2016/679 in der jeweils geltenden Fassung an einen Auftragsverarbeiter übertragen."

4. § 89 wird wie folgt geändert:

   a) Die Überschrift wird wie folgt gefasst:

   "Einsichts- und Auskunftsrecht"

   b) Dem Abs. 1 werden folgende Sätze angefügt:

   "Die personalaktenführende Behörde bestimmt, wo die Einsicht gewährt wird. Auskunft nach Art. 15 Abs. 1 der Verordnung (EU) Nr. 2016/679 über den Inhalt der Personalakte kann auch in Form der Einsichtnahme erteilt werden."

   c) Abs. 3 wird wie folgt gefasst:

   "(3) Kopien sowie Informationen in einem gängigen elektronischen Format werden nach Art. 15 Abs. 3 der Verordnung (EU) Nr. 2016/679 auf Verlangen zur Verfügung gestellt, soweit der Schutz wichtiger Ziele des allgemeinen öffentlichen Interesses oder der Rechte und Freiheiten anderer Personen nicht entgegenstehen."

5. § 90 wird wie folgt geändert:

   a) Die Überschrift wird wie folgt gefasst:

   "Übermittlung der Personalakte, Auskünfte an Dritte"

b) Abs. 1 wird wie folgt geändert:

aa) In Satz 1 wird das Wort "vorzulegen" durch die Wörter "zu übermitteln" ersetzt.

bb) In Satz 2 wird das Wort "die Vorlage" durch "die Übermittlung" ersetzt.

cc) In Satz 3 wird das Wort "vorgelegt" durch "übermittelt" ersetzt.

dd) In Satz 5 wird das Wort "Vorlage" durch "Übermittlung" ersetzt.

c) In Abs. 2 Satz 1 werden nach dem Wort "Auskünfte" die Wörter "über den Inhalt der Personalakte" eingefügt.

d) In Abs. 3 wird das Wort "Vorlage" durch "Übermittlung" ersetzt.

6. § 93 wird wie folgt geändert:

a) Die Überschrift wird wie folgt gefasst:

"Verarbeitung von Personalaktendaten in automatisierten Verfahren"

b) Abs. 1 wird wie folgt geändert:

aa) In Satz 1 werden die Wörter "und genutzt" gestrichen.

bb) In Satz 3 werden die Wörter "automatisierter Datenabruf" durch "Datenabruf in automatisierten Verfahren" ersetzt.

c) In Abs. 2 wird das Wort "automatisiert" durch die Wörter "in automatisierten Verfahren" ersetzt.

d) In Abs. 3 wird das Wort "automatisiert" durch die Wörter "in automatisierten Verfahren" ersetzt und werden die Wörter "oder genutzt" gestrichen.

e) Abs. 4 wird aufgehoben.

f) Der bisherige Abs. 5 wird Abs. 4 und in Satz 2 werden die Wörter "Verarbeitungs- und Nutzungsformen" durch das Wort "Verarbeitungsformen" und die Wörter "automatisierter Datenübermittlung" durch "der Datenübermittlung in automatisierten Verfahren" ersetzt.

g) Der bisherige Abs. 6 wird Abs. 5.

7. § 96 wird wie folgt geändert:

a) In Abs. 2 Satz 2 wird das Wort "automatisiert" durch die Wörter "in automatisierten Verfahren" ersetzt.

b) Abs. 3 wird wie folgt gefasst:

"(3) Das für das Dienstrecht zuständige Ministerium kann abweichend von Abs. 1 Nr. 3 die Verarbeitung von personenbezogenen Daten nach den Art. 28 und 29 der Verordnung (EU) Nr. 2016/679 in der jeweils geltenden Fassung an einen Auftragsverarbeiter übertragen."

Artikel 17
Änderung des Gesetzes über den Einheitlichen Ansprechpartner Hessen

§ 5 Abs. 3 Satz 1 des Gesetzes über den Einheitlichen Ansprechpartner Hessen vom 15. Dezember 2009 (GVBl. I S. 716), geändert durch Gesetz vom 28. September 2014 (GVBl. S. 218), wird wie folgt gefasst:

"Soweit der Dienstleistungserbringer den EAH zur Verfahrensabwicklung in Anspruch nimmt, kann er die Rechte nach der Verordnung (EU) Nr. 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Warenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung) (ABl. EU Nr. L 119 S. 1, Nr. L 314 S. 72) und nach sonstigen datenschutzrechtlichen Vorschriften, die ihm als betroffene Person gegenüber dem Verantwortlichen zustehen, auch gegenüber dem EAH geltend machen, unabhängig davon, wer im Einzelfall für die Verarbeitung der betroffenen Daten verantwortlich ist."

Artikel 18
Änderung des Hessischen Gesetzes über die öffentliche Sicherheit und Ordnung

Das Hessische Gesetz über die öffentliche Sicherheit und Ordnung in der Fassung der Bekanntmachung vom 14. Januar 2005 (GVBl. I S. 14), zuletzt geändert durch Gesetz vom ... [*einsetzen: Ausfertigungsdatum und Fundstelle des Gesetzes*], wird wie folgt geändert:

1. Die Übersicht wird wie folgt geändert:
   a) Nach der Angabe zu § 17 wird folgende Angabe eingefügt:
      "§ 17a Berichtspflichten gegenüber dem Parlament und der Öffentlichkeit"
   b) Die Angabe zu den §§ 20 bis 23 wird durch folgende Angabe ersetzt:
      "§ 20 Datenweiterverarbeitung, Zweckbindung, Grundsatz der hypothetischen Datenneuerhebung
      § 20a Kennzeichnung
      § 20b Weiterverarbeitung für die wissenschaftliche Forschung"
      § 21 Allgemeine Regeln der Datenübermittlung, Übermittlungsverbote und Verweigerungsgründe
      § 22 Datenübermittlung im innerstaatlichen Bereich und im Bereich der Europäischen Union und deren Mitgliedstaaten
      § 23 Datenübermittlung im internationalen Bereich"
   c) Die Angabe zu den §§ 27 bis 29 wird durch folgende Angabe ersetzt:
      "§ 27 Berichtigung, Löschung und Einschränkung der Verarbeitung von Daten zu den in § 40 des Hessischen Datenschutz- und Informationsfreiheitsgesetzes genannten Zwecken, Verwertungsverbot
      § 27a Berichtigung, Löschung und Einschränkung der Verarbeitung von Daten zu anderen als den in § 40 des Hessischen Datenschutz- und Informationsfreiheitsgesetzes genannten Zwecken, Verwertungsverbot
      § 28 Protokollierung bei verdeckten und eingriffsintensiven Maßnahmen, Verwendungsbeschränkung
      § 29 Information, Benachrichtigung, Auskunft
      § 29a Datenschutzkontrolle"
   d) Der Angabe zu § 115 werden ein Komma und das Wort "Außerkrafttreten" angefügt.

2. In § 1 Abs. 6 Satz 4 wird die Angabe "29" durch "29a" ersetzt.

3. Dem § 3 wird als Abs. 4 angefügt:
   "(4) Soweit dieses Gesetz keine abschließenden Regelungen enthält, ist auf die Verarbeitung personenbezogener Daten durch die Gefahrenabwehr- und die Polizeibehörden zur Erfüllung ihrer Aufgaben nach diesem Gesetz ergänzend das Hessische Datenschutz- und Informationsfreiheitsgesetz in der jeweils geltenden Fassung anzuwenden. Die Vorschriften dieses Gesetzes finden keine Anwendung, soweit das Recht der Europäischen Union, insbesondere die Verordnung (EU) Nr. 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung) (ABl. EU Nr. L 119 S. 1, Nr. L 314 S. 72) in der jeweils geltenden Fassung, unmittelbar gilt."

4. § 13 wird wie folgt geändert:
   a) Abs. 1 wird wie folgt geändert:
      aa) Nr. 1 wird wie folgt gefasst:
         "1. die Person in Kenntnis des Zwecks der Erhebung in diese nach Abs. 9 eingewilligt hat,"
      bb) In Nr. 2 werden nach dem Wort "können" die Wörter "oder die betroffene Person die Daten offensichtlich öffentlich gemacht hat" eingefügt.
   b) Abs. 2 wird wie folgt gefasst:
      "(2) Die Polizeibehörden können personenbezogene Daten ferner zu folgenden Kategorien betroffener Personen erheben:

1. wenn tatsächliche Anhaltspunkte die Annahme rechtfertigen, dass die Person Straftaten mit erheblicher Bedeutung begehen wird,
2. wenn tatsächliche Anhaltspunkte die Annahme rechtfertigen, dass die Person mit einer in Nr. 1 genannten Person nicht nur in einem flüchtigen oder zufälligen Kontakt, sondern in einer Weise in Verbindung steht oder treten wird, die die Erhebung ihrer personenbezogenen Daten zur Verhütung von Straftaten mit erheblicher Bedeutung erfordert, weil Tatsachen die Annahme rechtfertigen, dass
   a) die Person von der Planung oder Vorbereitung dieser Straftaten oder der Verwertung der Tatvorteile Kenntnis hat oder daran mitwirkt oder
   b) eine in Nr. 1 genannte Person sich dieser Person zur Begehung dieser Straftaten bedienen könnte oder wird,
3. wenn tatsächliche Anhaltspunkte die Annahme rechtfertigen, dass die Person als Zeugin oder Zeuge, Hinweisgeberin oder Hinweisgeber oder sonstige Auskunftsperson in Betracht kommt, die die Erhebung ihrer personenbezogenen Daten zur Verhütung von Straftaten mit erheblicher Bedeutung erfordert,
4. wenn tatsächliche Anhaltspunkte die Annahme rechtfertigen, dass die Person Opfer einer Straftat mit erheblicher Bedeutung werden könnte,
5. wenn die Person sich im räumlichen Umfeld einer Person aufhält, die in besonderem Maße als gefährdet erscheint, und tatsächliche Anhaltspunkte die Maßnahme zum Schutz der gefährdeten Person rechtfertigen, oder
6. wenn dies zur Leistung von Vollzugshilfe nach den §§ 44 bis 46 erforderlich ist."

c) Abs. 5 Satz 1 und 2 wird wie folgt gefasst:

"Die Erhebung nicht gefahren- oder tatbezogener persönlicher Merkmale ist nur insoweit zulässig, als dies für Identifizierungszwecke oder zum Schutz der Person oder der Bediensteten der Gefahrenabwehr- und der Polizeibehörden erforderlich ist. Soweit es sich bei der Erhebung nach Satz 1 um eine Erhebung besonderer Kategorien personenbezogener Daten im Sinne des § 41 Nr. 15 des Hessischen Datenschutz- und Informationsfreiheitsgesetzes handelt, muss dies unbedingt erforderlich sein."

d) Abs. 6 Satz 1 wird wie folgt gefasst:

"Im Anwendungsbereich des § 40 des Hessischen Datenschutz- und Informationsfreiheitsgesetzes sind personenbezogene Daten, ausgenommen in den Fällen des Abs. 1 Nr. 1 und 2, grundsätzlich bei der betroffenen Person zu erheben."

e) Abs. 8 wird wie folgt gefasst:

"(8) Werden die personenbezogenen Daten bei der betroffenen Person oder Dritten erhoben, sind diese auf die Freiwilligkeit der Auskunft oder auf eine bestehende Auskunftspflicht hinzuweisen. Der Hinweis kann im Einzelfall unterbleiben, wenn er die Erfüllung der gefahrenabwehrbehördlichen oder polizeilichen Aufgaben gefährden oder erheblich erschweren würde."

f) Als Abs. 9 wird angefügt:

"(9) Die Erhebung personenbezogener Daten nach Abs. 1 Nr. 1 ist unter Beachtung des § 46 des Hessischen Datenschutz- und Informationsfreiheitsgesetzes unbeschadet spezieller Rechtsvorschriften nur dann zulässig, wenn die betroffene Person eine echte Wahlfreiheit hat und nicht aufgefordert oder angewiesen wird, einer rechtlichen Verpflichtung nachzukommen; die betroffene Person ist auf die Freiwilligkeit hinzuweisen. Werden personenbezogene Daten nach Abs. 1 Nr. 1 für die Zwecke außerhalb des § 40 des Hessischen Datenschutz- und Informationsfreiheitsgesetzes nach den Voraussetzungen des Satz 1 erhoben, findet die Verordnung (EU) Nr. 2016/679, insbesondere Art. 6 Abs. 1 Buchst. a, Art. 7, Art. 9 Abs. 2 Buchst. a der Verordnung (EU) Nr. 2016/679, Anwendung."

5. § 13a wird wie folgt geändert:

a) In Abs. 2 Satz 3 wird die Angabe "§ 7 Abs. 2" durch "§ 46" ersetzt.

b) In Abs. 3 Satz 3 wird die Angabe "§ 15" durch "§ 58" ersetzt.

c) In Abs. 5 Satz 2 werden nach dem Wort "statt" die Wörter "oder wird die betroffene Person aus einem anderen Anlass erneut einer Zuverlässigkeitsüberprüfung unterzogen" eingefügt.

6. In § 13b Abs. 2 Satz 1 wird die Angabe "5 und" durch "4 bis" und die Angabe "§ 15" durch "§ 58" ersetzt.

7. § 14 wird wie folgt geändert:

   a) In Abs. 1 Satz 4 und Abs. 2 Satz 4 wird die Angabe "Abs. 7" jeweils durch "Abs. 8" ersetzt.

   b) In Abs. 3 Satz 4 wird die Angabe "sowie § 15 des Hessischen Datenschutzgesetzes" gestrichen und das Wort "gelten" durch "gilt" ersetzt.

   c) In Abs. 4 Satz 3 wird nach der Angabe "Abs. 1 Satz 2 und 3" das Komma durch das Wort "und" ersetzt und die Angabe "sowie § 15 des Hessischen Datenschutzgesetzes" gestrichen.

8. § 15 wird wie folgt geändert:

   a) In Abs. 2 Satz 1 Nr. 4 wird die Angabe "Nr. 3" durch "Nr. 5" ersetzt.

   b) In Abs. 6 werden Satz 3 und 4 durch folgenden Satz ersetzt:

   "Erlangte Erkenntnisse aufgrund von Anordnungen nach Satz 2 dürfen anderweitig nur zum Zwecke der Gefahrenabwehr und nur dann verwertet werden, wenn zuvor die Rechtmäßigkeit der Maßnahme richterlich festgestellt worden ist; bei Gefahr im Verzug ist die richterliche Entscheidung unverzüglich nachzuholen, § 39 Abs. 1 Satz 2 und 3 gilt entsprechend."

   c) Abs. 9 wird aufgehoben.

9. § 15a wird wie folgt geändert:

   a) Abs. 2 wird wie folgt geändert:

      aa) In Satz 1 wird die Angabe "20. Juni 2013 (BGBl. I S. 1602)" durch "27. Juni 2017 (BGBl. I S. 1963)" ersetzt.

      bb) In Satz 6 wird die Angabe "Abs. 6" durch "Abs. 5 bis 7" ersetzt.

   b) Abs. 5a wird Abs. 6.

   c) Der bisherige Abs. 6 wird aufgehoben.

   d) In Abs. 7 wird die Angabe "21. Dezember 2007 (BGBl. I S. 3198)" durch "17. August 2017 (BGBl. I S. 3202)" ersetzt.

10. In § 17 Abs. 2 wird nach dem Wort "zulässig," die Angabe "soweit eine Auskunftspflicht nach § 12 Abs. 2 besteht und" eingefügt.

11. Nach § 17 wird als § 17a eingefügt:

"§ 17a
Berichtspflichten gegenüber dem Parlament und der Öffentlichkeit

Die Landesregierung berichtet dem Landtag alle zwei Jahre über die nach den §§ 15 bis 16 getroffenen Maßnahmen sowie über Polizeiliche Beobachtungen nach § 17, soweit bei den genannten Maßnahmen eine richterliche Anordnung oder richterliche Bestätigung der Anordnung erforderlich ist, und über Übermittlungen nach § 23. Abweichend von Satz 1 ist dem Landtag über die nach § 15 Abs. 4 und 6 Satz 3 getroffenen Maßnahmen jährlich zu berichten. In diesen Berichten wird insbesondere dargestellt, in welchem Umfang, von welchen Befugnissen, aus Anlass welcher Art von Verdachtslagen Gebrauch gemacht wurde und inwieweit die betroffenen Personen hierüber benachrichtigt wurden. Die parlamentarische Kontrolle wird auf der Grundlage dieser Berichte von einer parlamentarischen Kontrollkommission ausgeübt. § 20 Abs. 2 bis 4, § 21 sowie § 22 Abs. 4 des Gesetzes über das Landesamt für Verfassungsschutz vom 19. Dezember 1990 (GVBl. I S. 753), zuletzt geändert durch Gesetz vom 27. Juni 2013 (GVBl. S. 444), in der jeweils geltenden Fassung gelten entsprechend. Der Landtag macht die Berichte in anonymisierter Form öffentlich."

12. Dem § 19 wird als Abs. 6 angefügt:

"(6) Soweit sich die Maßnahmen nach Abs. 1 bis 5 auf besondere Kategorien personenbezogener Daten beziehen, sind die §§ 20 und 43 des Hessischen Datenschutz- und Informationsfreiheitsgesetzes und Art. 9 der Verordnung (EU) Nr. 2016/679 zu beachten."

13. § 20 wird wie folgt gefasst:

"§ 20
Datenweiterverarbeitung, Zweckbindung,
Grundsatz der hypothetischen Datenneuerhebung

(1) Die Gefahrenabwehr- und die Polizeibehörden können personenbezogene Daten, die sie selbst erhoben haben, unter Berücksichtigung der jeweiligen Datenerhebungsvorschrift weiterverarbeiten

1. zur Erfüllung derselben Aufgabe und
2. zum Schutz derselben Rechtsgüter oder sonstigen Rechte oder zur Verhütung derselben Straftaten oder Ordnungswidrigkeiten.

Satz 1 gilt entsprechend für personenbezogene Daten, denen keine Erhebung vorausgegangen ist, mit der Maßgabe, dass für die Weiterverarbeitung der Zweck der Speicherung zu berücksichtigen ist. Für die Weiterverarbeitung von personenbezogenen Daten, die aus Maßnahmen nach § 15 Abs. 4 erlangt wurden, muss eine Gefahr im Sinne der Vorschrift vorliegen.

(2) Die Gefahrenabwehr- und die Polizeibehörden können zur Erfüllung ihrer Aufgaben personenbezogene Daten zu anderen Zwecken als denjenigen, zu denen sie erhoben worden sind, weiterverarbeiten, wenn unter Berücksichtigung der jeweiligen Datenerhebungsvorschrift

1. mindestens
   a) vergleichbar schwerwiegende Straftaten oder Ordnungswidrigkeiten verhütet oder
   b) vergleichbar bedeutsame Rechtsgüter oder sonstige Rechte geschützt

   werden sollen und
2. sich im Einzelfall konkrete Ermittlungsansätze
   a) zur Verhütung solcher Straftaten oder Ordnungswidrigkeiten ergeben oder
   b) zur Abwehr von in einem übersehbaren Zeitraum drohenden Gefahren für mindestens vergleichbar bedeutsame Rechtsgüter oder sonstige Rechte erkennen lassen.

Abweichend von Satz 1 können die vorhandenen zur Identifizierung dienenden Daten einer Person, wie insbesondere Namen, Geschlecht, Geburtsdatum, Geburtsort, Staatsangehörigkeit, Anschrift (Grunddaten), auch weiterverarbeitet werden, um diese Person zu identifizieren. Abs. 8 und 9, die §§ 24, 25 und 45 des Hessischen Datenschutz- und Informationsfreiheitsgesetzes sowie § 20b und besondere Vorschriften zur Weiterverarbeitung bleiben unberührt. Satz 1 bis 3 gelten entsprechend für personenbezogene Daten, denen keine Erhebung vorausgegangen ist, mit der Maßgabe, dass für die Weiterverarbeitung der Zweck der Speicherung zu berücksichtigen ist.

(3) Für die Weiterverarbeitung von personenbezogenen Daten, die durch einen verdeckten Einsatz technischer Mittel in oder aus Wohnungen oder verdeckten Eingriff in informationstechnische Systeme erlangt wurden, gilt Abs. 2 Satz 1 Nr. 2 Buchst. b mit der Maßgabe entsprechend, dass bei personenbezogenen Daten, die durch einen verdeckten Einsatz technischer Mittel in oder aus Wohnungen erlangt wurden, eine Gefahr im Sinne des § 15 Abs. 4 vorliegen muss. Personenbezogene Daten, die durch Herstellung von Lichtbildern oder Bildaufzeichnungen über eine Person im Wege eines verdeckten Einsatzes technischer Mittel in oder aus Wohnungen erlangt wurden, dürfen nicht zu Strafverfolgungszwecken weiterverarbeitet werden.

(4) Bei der Weiterverarbeitung von personenbezogenen Daten ist durch organisatorische und technische Vorkehrungen sicherzustellen, dass die Abs. 1 bis 3 beachtet werden.

(5) Die Gefahrenabwehr- und die Polizeibehörden können personenbezogene Daten nach Maßgabe der Abs. 1 bis 4 weiterverarbeiten, soweit dies zur Erfüllung ihrer Aufgaben erforderlich ist und soweit andere Rechtsvorschriften keine besonderen Voraussetzungen vorsehen.

(6) Die Polizeibehörden können, soweit Bestimmungen der Strafprozessordnung oder andere Rechtsvorschriften nicht entgegenstehen, personenbezogene Daten, die sie im Rahmen der Verfolgung von Straftaten gewonnen haben, zur Abwehr einer Gefahr oder zur vorbeugenden Bekämpfung von Straftaten weiterverarbeiten. Soweit es sich um Daten von Personen handelt, die verdächtig sind, eine Straftat begangen zu haben, sind die Daten zu löschen, sobald der Verdacht entfällt.

(7) Die Polizeibehörden können zur vorbeugenden Bekämpfung von Straftaten personenbezogene Daten über die in § 13 Abs. 2 Nr. 1 bis 5 genannten Personen weiterverarbeiten. Eine automatisierte Weiterverarbeitung personenbezogener Daten über die in § 13 Abs. 2 Nr. 2 bis 5 genannten Personen ist jedoch nur zulässig, soweit dies zur vorbeugenden Bekämpfung von Straftaten mit erheblicher Bedeutung erforderlich ist.

(8) Die Polizeibehörden und die Hessische Hochschule für Polizei und Verwaltung können gespeicherte personenbezogene Daten zur polizeilichen Aus- oder Fortbildung oder effektiven Wirksamkeitskontrolle oder zu statistischen Zwecken weiterverarbeiten. Die Daten sind zum frühestmöglichen Zeitpunkt zu anonymisieren. Die Abs. 1, 2, 4 bis 7 und § 68 des Hessischen Datenschutz- und Informationsfreiheitsgesetzes finden insoweit keine Anwendung. Eine Weiterverarbeitung von personenbezogenen Daten, die aus in Abs. 3 genannten Maßnahmen erlangt wurden, ist ausgeschlossen; dies gilt nicht, soweit die Weiterverarbeitung dieser Daten für die Zwecke nach Satz 1 unerlässlich ist.

(9) Die Gefahrenabwehr- und die Polizeibehörden können zur Vorgangsverwaltung oder zur befristeten Dokumentation behördlichen Handelns personenbezogene Daten speichern und ausschließlich zu diesem Zweck, zu den in den §§ 13a und 13b genannten Zwecken oder zu dem in Abs. 10 Satz 1 genannten Zweck weiterverarbeiten. Die Abs. 1 bis 7 finden insoweit keine Anwendung.

(10) Die Polizeibehörden können für die Planung von Maßnahmen der Kriminalitätsbekämpfung vorhandene personenbezogene Daten über Vermisstenfälle, auswertungsrelevante Straftaten und verdächtige Wahrnehmungen zur Erstellung eines Kriminalitätslagebildes weiterverarbeiten. Ein Kriminalitätslagebild darf Daten von Geschädigten, Zeuginnen und Zeugen sowie anderen nicht tatverdächtigen Personen nur enthalten, soweit dies zur Zweckerreichung erforderlich ist. Die automatisiert verarbeiteten personenbezogenen Daten sind spätestens am Ende des der Speicherung folgenden Jahres zu löschen.

(11) Die Polizeibehörden zeichnen Notrufe und Meldungen über sonstige Notrufeinrichtungen sowie den Funkverkehr ihrer Leitstellen auf. Gefahrenabwehr- und Polizeibehörden können sonstige Telekommunikation aufzeichnen, wenn dies für ihre Aufgabenerfüllung erforderlich ist; auf die Aufzeichnung soll hingewiesen werden, soweit dadurch die Aufgabenerfüllung nicht gefährdet wird. Soweit erforderlich, können die Aufzeichnungen

1. zur Abwehr einer Gefahr,
2. zur Strafverfolgung oder
3. zur Dokumentation behördlichen Handelns

weiterverarbeitet werden. Aufzeichnungen sind spätestens nach drei Monaten zu löschen, wenn sie nicht zu einem Zweck nach Satz 3 verarbeitet werden.

(12) § 13 Abs. 9 gilt bei der Weiterverarbeitung personenbezogener Daten entsprechend. Bei Bewertungen ist § 68 des Hessischen Datenschutz- und Informationsfreiheitsgesetzes zu beachten. In den Fällen, in denen bereits Daten zu einer Person vorhanden sind, können zu dieser Person auch personengebundene Hinweise, die zum Schutz dieser Person oder zum Schutz der Bediensteten der Gefahrenabwehr- und der Polizeibehörden erforderlich sind, und weitere Hinweise, die geeignet sind, dem Schutz Dritter oder der Gewinnung von Ermittlungsansätzen zu dienen, weiterverarbeitet werden."

14. Nach § 20 werden als §§ 20a und 20b eingefügt:

"§ 20a
Kennzeichnung

(1) Bei der Speicherung in polizeilichen Informationssystemen sind personenbezogene Daten wie folgt zu kennzeichnen:

1. Angabe des Mittels der Erhebung der Daten einschließlich der Angabe, ob die Daten offen oder verdeckt erhoben wurden,
2. Angabe der Kategorie betroffener Personen bei denjenigen Personen, zu denen der Identifizierung dienende Daten, wie insbesondere Namen, Geschlecht, Geburtsdatum, Geburtsort, Staatsangehörigkeit, Anschrift, angelegt wurden (Grunddaten),
3. Angabe der Rechtsgüter oder sonstiger Rechte, deren Schutz die Erhebung dient, oder der Straftaten oder Ordnungswidrigkeiten, deren Verfolgung oder Verhütung die Erhebung dient,
4. Angabe der Stelle, die die Daten erhoben hat.

Die Kennzeichnung nach Satz 1 Nr. 1 kann auch durch die Angabe der Rechtsgrundlage der jeweiligen Mittel der Datenerhebung ergänzt werden. Personenbezogene Daten, denen keine Erhebung vorausgegangen ist, sind, soweit möglich, nach Satz 1 zu kenn-

zeichnen; darüber hinaus sind die erste Daten verarbeitende Stelle sowie, soweit möglich, derjenige, von dem die Daten erlangt wurden, anzugeben.

(2) Personenbezogene Daten, die nicht entsprechend den Anforderungen des Abs. 1 gekennzeichnet sind, dürfen so lange nicht weiterverarbeitet oder übermittelt werden, bis eine Kennzeichnung entsprechend den Anforderungen des Abs. 1 erfolgt ist.

(3) Nach einer Übermittlung an eine andere Stelle ist die Kennzeichnung nach Abs. 1 durch diese Stelle aufrechtzuerhalten.

(4) Die Abs. 1 bis 3 gelten nicht, soweit eine Kennzeichnung tatsächlich nicht möglich ist. Die Abs. 1 bis 3 gelten ebenfalls nicht, solange eine Kennzeichnung technisch nicht möglich ist oder einen unverhältnismäßigen Aufwand erfordern würde.

§ 20b
Weiterverarbeitung für die wissenschaftliche Forschung

(1) Abweichend von den §§ 24 und 45 des Hessischen Datenschutz- und Informationsfreiheitsgesetzes ist eine Weiterverarbeitung oder Übermittlung von personenbezogenen Daten, die aus den in § 20 Abs. 3 genannten Maßnahmen erlangt wurden, ausgeschlossen. Dies gilt nicht, soweit die Weiterverarbeitung für die polizeiliche Eigenforschung und effektive Wirksamkeitskontrolle unerlässlich ist.

(2) Personenbezogene Daten dürfen nur an Amtsträger, für den öffentlichen Dienst besonders Verpflichtete oder Personen, die zur Geheimhaltung verpflichtet worden sind, übermittelt werden.

(3) Durch organisatorische und technische Maßnahmen hat die die wissenschaftliche Forschung betreibende Stelle zu gewährleisten, dass die Daten gegen unbefugte Kenntnisnahme geschützt sind."

15. § 21 wird wie folgt gefasst:

"§ 21
Allgemeine Regeln der Datenübermittlung,
Übermittlungsverbote und Verweigerungsgründe

(1) Die Gefahrenabwehr- und die Polizeibehörden können personenbezogene Daten unter Beachtung des § 20 Abs. 1 bis 3 sowie der nachstehenden Bestimmungen übermitteln. Die empfangende Stelle, Tag und wesentlicher Inhalt der Übermittlung sind festzuhalten; dies gilt nicht für das automatisierte Abrufverfahren (§ 24). Bewertungen dürfen anderen als Gefahrenabwehr- und Polizeibehörden nicht übermittelt werden. Dies gilt nicht, soweit Fahndungsaufrufe mit einer Warnung verbunden sind.

(2) Eine Übermittlung hat zu unterbleiben, wenn für die übermittelnde Gefahrenabwehr- oder Polizeibehörde erkennbar ist, dass unter Berücksichtigung der Art der Daten und ihrer Erhebung die schutzwürdigen Interessen der betroffenen Person das Allgemeininteresse an der Übermittlung überwiegen, oder besondere gesetzliche Verwendungsregelungen entgegenstehen. Die Verpflichtung zur Wahrung gesetzlicher Geheimhaltungspflichten oder von Berufs- oder besonderen Amtsgeheimnissen, die nicht auf Rechtsvorschriften beruhen, bleibt unberührt.

(3) Die Datenübermittlung nach § 22 Abs. 5 und § 23 hat darüber hinaus zu unterbleiben,

1. wenn hierdurch wesentliche Sicherheitsinteressen des Bundes oder der Länder beeinträchtigt würden,
2. wenn hierdurch der Erfolg laufender Ermittlungen oder Leib, Leben oder Freiheit einer Person gefährdet würde oder
3. soweit Grund zu der Annahme besteht, dass dadurch gegen den Zweck eines deutschen Gesetzes verstoßen würde, oder
4. wenn tatsächliche Anhaltspunkte dafür vorliegen, dass die Übermittlung der Daten zu den in der Charta der Grundrechte der Europäischen Union enthaltenen Grundsätzen, insbesondere dadurch, dass durch die Nutzung der übermittelten Daten im Empfängerstaat Verletzungen von elementaren rechtsstaatlichen Grundsätzen oder Menschenrechtsverletzungen drohen, in Widerspruch stünde.

(4) Die Übermittlung darf nicht zu einer Erweiterung des Kreises der Stellen nach den §§ 41 und 61 des Bundeszentralregistergesetzes in der Fassung der Bekanntmachung vom 21. September 1984 (BGBl. I S. 1229, 1985 I S. 195), zuletzt geändert durch Gesetz vom 18. Juli 2017 (BGBl. I S. 2732), führen, die von Eintragungen, die in ein Führungszeugnis nicht aufgenommen werden, Kenntnis erhalten, und muss das Verwertungsverbot im Bundeszentralregister getilgter oder zu tilgender Eintragungen nach den §§ 51, 52 und 63 des Bundeszentralregistergesetzes berücksichtigen.

(5) Die übermittelnde Gefahrenabwehr- oder Polizeibehörde prüft die Zulässigkeit der Übermittlung. Erfolgt die Übermittlung aufgrund eines Ersuchens der empfangenden Stelle, hat die übermittelnde Gefahrenabwehr- oder Polizeibehörde nur zu prüfen, ob das Übermittlungsersuchen im Rahmen der Aufgaben der empfangenden Stelle liegt. Die Zulässigkeit der Übermittlung im Übrigen prüft sie nur, wenn hierfür im Einzelfall besonderer Anlass besteht. Die empfangende Stelle hat der übermittelnden Gefahrenabwehr- oder Polizeibehörde die erforderlichen Angaben zu machen.

(6) Die empfangende Stelle darf die übermittelten personenbezogenen Daten, soweit gesetzlich nichts anderes bestimmt ist, nur zu dem Zweck verarbeiten, zu dem sie ihr übermittelt worden sind. Eine Verarbeitung für andere Zwecke ist unter Beachtung des § 20 Abs. 2 und 3 zulässig; im Falle des § 22 Abs. 3 gilt dies nur, soweit zusätzlich die übermittelnde Gefahrenabwehr- oder Polizeibehörde zustimmt. Bei Übermittlungen nach § 22 Abs. 3 und § 23 hat die übermittelnde Gefahrenabwehr- oder Polizeibehörde die empfangende Stelle darauf hinzuweisen.

(7) Sind mit personenbezogenen Daten, die übermittelt werden dürfen, weitere personenbezogene Daten der betroffenen Person oder eines Dritten in Akten so verbunden, dass eine Trennung nicht oder nur mit unvertretbarem Aufwand möglich ist, so ist die Übermittlung auch dieser Daten zulässig, soweit nicht berechtigte Interessen der betroffenen Person oder eines Dritten an der Geheimhaltung offensichtlich überwiegen; eine Verwendung dieser Daten ist unzulässig.

(8) Andere besondere Rechtsvorschriften über die Datenübermittlung bleiben unberührt."

16. § 22 wird wie folgt geändert:

a) In der Überschrift werden die Wörter "innerhalb des öffentlichen Bereichs" durch "im innerstaatlichen Bereich und im Bereich der Europäischen Union und deren Mitgliedstaaten" ersetzt.

b) Abs. 1 wird wie folgt geändert:

aa) In Satz 2 werden die Wörter "sowie der anderen Mitgliedstaaten der Europäischen Union und der am Schengen-Besitzstand teilhabenden assoziierten Staaten" gestrichen.

bb) Satz 4 und 5 werden aufgehoben.

c) Abs. 2 wird wie folgt geändert:

aa) In Satz 1 werden die Wörter "Im Übrigen" durch "Liegen die Voraussetzungen des Abs. 1 nicht vor," ersetzt.

bb) In Satz 2 wird das Wort "unterrichten" durch "benachrichtigen" ersetzt.

d) Abs. 3 wird wie folgt gefasst:

(3) Die Gefahrenabwehr- und die Polizeibehörden können in den Fällen des Abs. 2 Satz 1 Nr. 1, 2, 4 und 5 personenbezogene Daten auch an nicht öffentliche Stellen übermitteln. Abs. 2 Satz 2 gilt entsprechend. Über die Übermittlungen ist ein Nachweis zu führen, aus dem der Anlass, der Inhalt, die empfangende Stelle, der Tag der Übermittlung sowie die Aktenfundstelle hervorgehen. Er ist am Ende des Kalenderjahres, das dem Jahr seiner Erstellung folgt, zu löschen oder zu vernichten. Die Löschung oder Vernichtung unterbleibt, solange der Nachweis für Zwecke einer bereits eingeleiteten Datenschutzkontrolle oder zur Verhinderung oder Verfolgung einer Straftat mit erheblicher Bedeutung benötigt wird oder Grund zu der Annahme besteht, dass im Falle einer Löschung schutzwürdige Interessen der betroffenen Person beeinträchtigt würden. Besteht Grund zu der Annahme, dass durch die Übermittlung der der Erhebung der Daten zugrunde liegende Zweck gefährdet würde, ist vor der Übermittlung die Zustimmung der Stelle einzuholen, von der die Daten übermittelt wurden; die übermittelnde Stelle kann bestimmte von ihr übermittelte Daten so kennzeichnen oder mit einem Hinweis versehen, dass vor einer Übermittlung ihre Zustimmung einzuholen ist."

e) In Abs. 4 wird die Angabe "Satz 1 und Abs. 3 Satz 1" durch "Satz 3" ersetzt.

f) Als neuer Abs. 5 wird eingefügt:

"(5) Die Abs. 1 bis 4 gelten entsprechend für die Übermittlung von personenbezogenen Daten an

1. öffentliche und nicht öffentliche Stellen in Mitgliedstaaten der Europäischen Union sowie an über- und zwischenstaatliche Stellen der Europäischen Union oder deren Mitgliedstaaten,

2. Polizeibehörden oder sonstige für die Zwecke des § 40 des Hessischen Datenschutz- und Informationsfreiheitsgesetzes zuständige öffentliche Stellen der am Schengen-Besitzstand teilhabenden assoziierten Staaten."

g) Der bisherige Abs. 5 wird Abs. 6.

17. § 23 wird wie folgt gefasst:

"§ 23
Datenübermittlung im internationalen Bereich

(1) Die Gefahrenabwehr- und die Polizeibehörden können personenbezogene Daten zu Zwecken des § 40 des Hessischen Datenschutz- und Informationsfreiheitsgesetzes unter Beachtung der §§ 73 bis 75 des Hessischen Datenschutz- und Informationsfreiheitsgesetzes an für Zwecke des § 40 des Hessischen Datenschutz- und Informationsfreiheitsgesetzes zuständige

1. öffentliche Stellen in anderen als den in § 22 Abs. 5 genannten Staaten (Drittländer) und

2. andere über- und zwischenstaatliche Stellen, die in § 22 Abs. 5 nicht genannt sind,

übermitteln, soweit dies erforderlich ist zur Erfüllung einer Aufgabe der übermittelnden Gefahrenabwehr- oder Polizeibehörde oder zur Abwehr einer erheblichen Gefahr durch die empfangende Stelle. Entsprechendes gilt, wenn tatsächliche Anhaltspunkte dafür bestehen, dass Straftaten von erheblicher Bedeutung begangen werden sollen.

(2) Die Gefahrenabwehr- und die Polizeibehörden können zu Zwecken des § 40 des Hessischen Datenschutz- und Informationsfreiheitsgesetzes unter Beachtung des § 76 des Hessischen Datenschutz- und Informationsfreiheitsgesetzes auch an die dort genannten Stellen personenbezogene Daten übermitteln. Zusätzlich können personenbezogene Daten unter den Voraussetzungen des Satzes 1 an andere über- und zwischenstaatlichen Stellen als die in Abs. 1 genannten übermittelt werden, soweit ein Fall des Abs. 1 vorliegt.

(3) Abs. 1 gilt für die Übermittlung zu Zwecken außerhalb des § 40 des Hessischen Datenschutz- und Informationsfreiheitsgesetzes unter Beachtung der Art. 44 bis 49 der Verordnung (EU) Nr. 2016/679 an öffentliche Stellen in anderen als den in § 22 Abs. 5 genannten Staaten (Drittländer) und an andere über- und zwischenstaatliche Stellen als die in § 22 Abs. 5 genannten entsprechend.

(4) Zur Beurteilung der Zulässigkeit der Datenübermittlung ist eine fortlaufend aktualisierte Aufstellung über die Einhaltung der elementaren rechtsstaatlichen Grundsätze und Menschenrechtsstandards sowie das Datenschutzniveau in den jeweiligen Drittländern, die die speziellen Erfordernisse des polizeilichen Informationsaustauschs berücksichtigt, heranzuziehen. Hierbei sind insbesondere die jeweils aktuellen Erkenntnisse und maßgeblich zu berücksichtigen, ob ein Angemessenheitsbeschluss der Europäischen Kommission nach Art. 36 der Richtlinie (EU) Nr. 2016/680 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung sowie zum freien Datenverkehr und zur Aufhebung des Rahmenbeschlusses 2008/977/JI des Rates (ABl. EU Nr. L 119 S. 89) oder nach Art. 45 der Verordnung (EU) Nr. 2016/679 vorliegt."

18. § 24 wird wie folgt geändert:

a) Die Absatzbezeichnung "(1)" wird gestrichen.

b) Abs. 1 wird wie folgt geändert:

aa) Satz 2 wird wie folgt geändert:

aaa) In Nr. 2 wird das Wort "Verwaltungsfachhochschule" durch die Wörter "Hessische Hochschule für Polizei und Verwaltung" ersetzt.

bbb) In Nr. 4 werden nach dem Wort "Gefahrenabwehrbehörden" die Wörter "und sonstige öffentliche Stellen" eingefügt.

bb) Folgender Satz wird angefügt:

"Die speichernde Stelle hat in den Fällen des Satzes 2 Nr. 1 bis 6 zu gewährleisten, dass die Übermittlung festgestellt und überprüft werden kann, mindestens durch geeignete Stichprobenverfahren."

c) Die Abs. 2 und 3 werden aufgehoben.

19. § 26 wird wie folgt geändert:

a) Abs. 3 Satz 2 und 3 wird durch folgende Sätze ersetzt:

"Die getroffenen Maßnahmen sind zu dokumentieren. Diese Dokumentation ist gesondert aufzubewahren und durch technische und organisatorische Maßnahmen zu sichern. Sie ist sechs Monate nach der Benachrichtigung nach § 29 Abs. 5 oder nach dem endgültigen Zurückstellen der Benachrichtigung nach § 29 Abs. 6 zu löschen; ist die Datenschutzkontrolle nach § 29a noch nicht beendet, ist die Dokumentation bis zu deren Abschluss aufzubewahren."

b) Abs. 5 wird aufgehoben.

20. § 27 wird wie folgt gefasst:

"§ 27
Berichtigung, Löschung und Einschränkung der Verarbeitung von Daten zu den in § 40 des Hessischen Datenschutz- und Informationsfreiheitsgesetzes genannten Zwecken, Verwertungsverbot

(1) Personenbezogene Daten und die dazugehörigen Unterlagen sind nach Maßgabe der §§ 53 und 70 des Hessischen Datenschutz- und Informationsfreiheitsgesetzes zu berichtigen, zu löschen oder in der Verarbeitung einzuschränken, soweit sie zu den in § 40 des Hessischen Datenschutz- und Informationsfreiheitsgesetzes genannten Zwecken verarbeitet wurden und in Abs. 2 bis 6 keine besonderen Regelungen getroffen sind.

(2) Ergänzend zu § 53 Abs. 2 und § 70 Abs. 2 des Hessischen Datenschutz- und Informationsfreiheitsgesetzes sind personenbezogene Daten unverzüglich zu löschen und die dazugehörigen Unterlagen unverzüglich zu vernichten, wenn

1. bei der nach bestimmten Fristen vorzunehmenden Überprüfung oder aus Anlass einer Einzelfallbearbeitung festgestellt wird, dass ihre Kenntnis für die speichernde Stelle zur Erfüllung der in ihrer Zuständigkeit liegenden Aufgaben nicht mehr erforderlich ist, oder
2. die durch eine verdeckte Datenerhebung gewonnenen Daten für den der Anordnung zugrunde liegenden Zweck, zur Strafverfolgung oder zur Strafvollstreckung oder für eine etwaige gerichtliche Kontrolle nicht mehr erforderlich sind, soweit keine zulässige Weiterverarbeitung erfolgt; die Löschung bedarf der Zustimmung der Staatsanwaltschaft, wenn die Daten zur Strafverfolgung oder Strafvollstreckung verarbeitet worden sind.

Im Fall des Satzes 1 Nr. 2 gilt, dass anstatt die personenbezogenen Daten zu löschen und die dazugehörigen Unterlagen zu vernichten die Einschränkung der Verarbeitung erfolgt, wenn die betroffene Person über eine verdeckte Datenerhebung noch nicht unterrichtet worden ist, es sei denn, dass die Datenerhebung den Kernbereich privater Lebensgestaltung betroffen hat. Die Daten nach Satz 2 dürfen nur verwendet werden für die Zwecke der Benachrichtigung der betroffenen Person und um eine Prüfung zu ermöglichen, ob die Maßnahme rechtmäßig durchgeführt worden ist.

(3) Wird festgestellt, dass personenbezogene Daten in Akten unrichtig sind, ist die in § 53 Abs. 1, § 70 Abs. 1 des Hessischen Datenschutz- und Informationsfreiheitsgesetzes genannte Berichtigungspflicht dadurch zu erfüllen, dass dies in der Akte vermerkt oder auf sonstige Weise festgehalten wird. Bestreitet die betroffene Person die Richtigkeit sie betreffender personenbezogener Daten und lässt sich weder die Richtigkeit noch die Unrichtigkeit feststellen, sind die Daten entsprechend zu kennzeichnen, um eine Einschränkung der Verarbeitung nach § 53 Abs. 1 Satz 3 des Hessischen Datenschutz- und Informationsfreiheitsgesetzes zu ermöglichen. Die Verarbeitung personenbezogener Daten in Akten ist einzuschränken, wenn die Verarbeitung nach Abs. 2 Satz 1 Nr. 1, § 53 Abs. 2 oder § 70 Abs. 2 des Hessischen Datenschutz- und Informationsfreiheitsgesetzes zu löschen sind. Die Einschränkung der Verarbeitung personenbezogener Daten in Akten nach Satz 3 sowie § 53 Abs. 3 Satz 1 und § 70 Abs. 3 Satz 1 des Hessischen Datenschutz- und Informationsfreiheitsgesetzes ist durch Anbringung eines entsprechenden Vermerks vorzunehmen. Die Akten sind spätestens zu vernichten, wenn die gesamte Akte zur Erfüllung der in der Zuständigkeit der speichernden Stelle liegenden Aufgaben nicht mehr erforderlich ist. Personenbezogene Daten in Akten über eine verdeckte Datenerhebung sind nach Maßgabe des Abs. 2 Satz 1 Nr. 2 zu vernichten. Im Übrigen gilt Abs. 2 entsprechend.

(4) Die Ministerin oder der Minister des Innern wird ermächtigt, durch Rechtsverordnung die Fristen, nach deren Ablauf zu prüfen ist, ob die weitere Speicherung der Daten zur Aufgabenerfüllung erforderlich ist und gegebenenfalls nach deren Ablauf eine Löschung vorzusehen ist, zu bestimmen. Bei Daten, die nach § 20 Abs. 6 gespeichert sind, dürfen die Fristen für die Prüfung

1. bei Erwachsenen zehn Jahre,

2. bei Jugendlichen fünf Jahre und

3. bei Kindern zwei Jahre

nicht überschreiten, wobei nach Art und Zweck der Speicherung sowie Art und Bedeutung des Anlasses zu unterscheiden ist. Die Frist beginnt regelmäßig mit dem letzten Anlass der Speicherung, jedoch nicht vor Entlassung der betroffenen Person aus einer Justizvollzugsanstalt oder Beendigung einer mit Freiheitsentzug verbundenen Maßregel der Besserung und Sicherung. Werden innerhalb der Frist nach Satz 2 und 3 weitere personenbezogene Daten über dieselbe Person gespeichert, gilt für alle Speicherungen gemeinsam die Frist, die als letzte abläuft. Bei Daten, die nach § 20 Abs. 7 über die in § 13 Abs. 2 Nr. 2 bis 5 genannten Personen gespeichert sind, dürfen die Fristen für die Prüfung drei Jahre nicht überschreiten; die Entscheidung, dass eine weitere Speicherung erforderlich ist, trifft die Behördenleitung oder eine von dieser beauftragte Bedienstete oder ein von dieser beauftragter Bediensteter.

(5) Bei Daten aus dem Kernbereich privater Lebensgestaltung sowie im Falle der Unzulässigkeit der Speicherung und in sonstigen Fällen des Abs. 2 Satz 1 besteht ein Verwertungsverbot; § 53 Abs. 3 des Hessischen Datenschutz- und Informationsfreiheitsgesetzes findet insoweit keine Anwendung. Aufzeichnungen hierüber sind unverzüglich zu löschen. Die Tatsachen der Erfassung der Daten und der Löschung im Fall der Unzulässigkeit der Speicherung, einschließlich der Daten aus dem Kernbereich privater Lebensgestaltung, sind zu dokumentieren. Im Fall des Abs. 2 Satz 1 Nr. 2 ist die Tatsache der Löschung zu dokumentieren. Die Dokumentation darf ausschließlich für Zwecke der Datenschutzkontrolle verwendet werden. Sie ist sechs Monate nach der Benachrichtigung nach § 29 Abs. 5 oder nach dem endgültigen Zurückstellen der Benachrichtigung nach § 29 Abs. 6 zu löschen; ist die Datenschutzkontrolle nach § 29a noch nicht beendet, ist die Dokumentation bis zu ihrem Abschluss aufzubewahren. Satz 1 bis 6 gelten für personenbezogene Daten in Akten entsprechend.

(6) Anstelle der Löschung und Vernichtung nach Abs. 2 Satz 1 Nr. 1 oder Abs. 3 Satz 5 können die Datenträger an ein öffentliches Archiv abgegeben werden, soweit besondere archivrechtliche Regelungen dies vorsehen."

21. Nach § 27 wird als § 27a eingefügt:

"§ 27a
Berichtigung, Löschung und Einschränkung der Verarbeitung von Daten zu anderen als den in § 40 des Hessischen Datenschutz- und Informationsfreiheitsgesetzes genannten Zwecken, Verwertungsverbot

(1) Ergänzend zu Art. 18 Abs. 1 Buchst. a der Verordnung (EU) Nr. 2016/679 gilt für Datenverarbeitungen zu Zwecken außerhalb des § 40 des Hessischen Datenschutz- und Informationsfreiheitsgesetzes, dass insbesondere im Fall von Aussagen oder Bewertungen die Frage der Richtigkeit nicht den Inhalt der Aussage oder der Bewertung betrifft. Wenn die Richtigkeit oder Unrichtigkeit der Daten nicht festgestellt werden kann, tritt an die Stelle der Berichtigung nach Art. 16 der Verordnung (EU) 2016/679 eine Einschränkung der Verarbeitung nach Art. 18 der Verordnung (EU) 2016/679. Die oder der Verantwortliche hat die betroffene Person, die ihr Recht auf Berichtigung geltend gemacht hat, über die an die Stelle der Berichtigung tretende Einschränkung der Verarbeitung schriftlich zu unterrichten. Satz 3 gilt nicht, soweit bereits die Erteilung dieser Information eine Gefährdung im Sinne des § 32 Abs. 1 des Hessischen Datenschutz- und Informationsfreiheitsgesetzes mit sich bringen würde. Die Unterrichtung nach Satz 3 ist zu begründen, es sei denn, dass die Mitteilung der Gründe den mit dem Absehen von der Unterrichtung verfolgten Zweck gefährden würde. § 33 Abs. 3 des Hessischen Datenschutz- und Informationsfreiheitsgesetzes gilt entsprechend. Die oder der Verantwortliche hat die sachlichen oder rechtlichen Gründe für die Entscheidung zu dokumentieren.

(2) Wird festgestellt, dass personenbezogene Daten in Akten unrichtig sind, ist die in Art. 16 der Verordnung (EU) Nr. 2016/679 genannte Berichtigungspflicht dadurch zu erfüllen, dass dies in der Akte vermerkt oder auf sonstige Weise festgehalten wird. Bestreitet die betroffene Person die Richtigkeit sie betreffender personenbezogener Daten und lässt sich weder die Richtigkeit noch die Unrichtigkeit feststellen, sind die Daten entsprechend zu kennzeichnen, um eine Verarbeitungseinschränkung nach Abs. 1 Satz 2 zu ermöglichen.

(3) Ergänzend zu Art. 17 Abs. 1 der Verordnung (EU) Nr. 2016/679 gilt § 27 Abs. 2 Satz 1 und Abs. 5 im Fall der Löschung und Vernichtung personenbezogener Daten zu Zwecken außerhalb des § 40 des Hessischen Datenschutz- und Informationsfreiheitsgesetzes entsprechend. Bei personenbezogenen Daten in Akten gilt § 27 Abs. 3 Satz 3 bis 6 entsprechend; an die Stelle der Löschung nach Art. 17 Abs. 1 der Verordnung (EU) Nr. 2016/679 tritt die Einschränkung der Verarbeitung nach Art. 18 der Verordnung (EU) Nr. 2016/679.

(4) Abweichend von § 34 Abs. 1 und 2 des Hessischen Datenschutz- und Informationsfreiheitsgesetzes gilt für die Verarbeitung personenbezogener Daten zu Zwecken außerhalb des § 40 des Hessischen Datenschutz und Informationsfreiheitsgesetzes das Recht der betroffenen Person auf und die Pflicht der oder des Verantwortlichen zur Löschung personenbezogener Daten und zur Vernichtung der dazugehörigen Unterlagen nach Art. 17 Abs. 1 der Verordnung (EU) Nr. 2016/679 ergänzend zu Art. 17 Abs. 3 der Verordnung (EU) Nr. 2016/679 nicht, wenn

1. Grund zu der Annahme besteht, dass eine Löschung schutzwürdige Interessen einer betroffenen Person beeinträchtigen würde,
2. die Daten zu Beweiszwecken weiter aufbewahrt werden müssen,
3. eine Löschung wegen der besonderen Art der Speicherung nicht oder nur mit unverhältnismäßig hohem Aufwand möglich ist oder
4. im Fall des § 27 Abs. 2 Satz 1 Nr. 2 die betroffene Person über eine verdeckte Datenerhebung noch nicht unterrichtet worden ist, es sei denn, dass die Datenerhebung den Kernbereich privater Lebensgestaltung betroffen hat.

In den Fällen des Satzes 1 tritt an die Stelle einer Löschung oder Vernichtung die Einschränkung der Verarbeitung nach Art. 18 der Verordnung (EU) Nr. 2016/679. Bei personenbezogenen Daten in Akten gilt Satz 2 mit der Maßgabe, dass anstelle der Vernichtung die Verarbeitung personenbezogener Daten in Akten durch Anbringung eines entsprechenden Vermerks einzuschränken ist. In ihrer Verarbeitung nach Satz 1 Nr. 1 bis 3 eingeschränkte Daten dürfen nur zu dem Zweck, der ihrer Löschung entgegenstand, oder sonst mit Einwilligung der betroffenen Person verwendet werden. In ihrer Verarbeitung nach Satz 1 Nr. 4 eingeschränkte Daten dürfen nur verwendet werden für die Zwecke der Benachrichtigung der betroffenen Person und um eine Prüfung zu ermöglichen, ob die Maßnahme rechtmäßig durchgeführt worden ist.

(5) Die oder der Verantwortliche hat die betroffene Person über die Einschränkung der Verarbeitung nach Abs. 4 Satz 1 Nr. 1 bis 3 schriftlich zu unterrichten. Dies gilt nicht, soweit bereits die Erteilung dieser Information eine Gefährdung im Sinne des § 32 Abs. 1 des Hessischen Datenschutz- und Informationsfreiheitsgesetzes mit sich bringen würde. Die Unterrichtung nach Satz 1 ist zu begründen, es sei denn, dass die Mitteilung der Gründe den mit dem Absehen von der Unterrichtung verfolgten Zweck gefährden würde. § 33 Abs. 3 des Hessischen Datenschutz- und Informationsfreiheitsgesetzes gilt entsprechend. Die oder der Verantwortliche hat die sachlichen oder rechtlichen Gründe für die Entscheidung zu dokumentieren.

(6) Ergänzend zu Art. 17 und 18 der Verordnung (EU) Nr. 2016/679 gelten § 53 Abs. 4 und § 70 Abs. 4 des Hessischen Datenschutz- und Informationsfreiheitsgesetzes und § 27 Abs. 4 und 6 entsprechend."

22. Die §§ 28 und 29 werden wie folgt gefasst:

"§ 28
Protokollierung bei verdeckten und eingriffsintensiven Maßnahmen, Verwendungsbeschränkung

(1) Bei der Erhebung von Daten nach den §§ 15, 15a Abs. 1, 2 Satz 1 und Abs. 3 sowie den §§ 15b, 16, 17 und 26 sind zu protokollieren:

1. das zur Datenerhebung eingesetzte Mittel,
2. der Zeitpunkt des Einsatzes,
3. die Angaben, die die Feststellung der erhobenen Daten ermöglichen, sowie
4. die Organisationseinheit, die die Maßnahme durchführt.

(2) Zu protokollieren sind je nach Durchführung der konkreten Maßnahme auch bei

1. Maßnahmen nach § 15 Abs. 2 und 6, bei denen Vorgänge außerhalb von Wohnungen erfasst wurden, die Zielperson und die erheblich mitbetroffenen Personen,
2. Maßnahmen nach § 15 Abs. 4 die Person, gegen die sich die Maßnahme richtete, sonstige überwachte Personen und die Personen, die die überwachte Wohnung zur Zeit der Durchführung der Maßnahme innehatten oder bewohnten,
3. Maßnahmen nach § 15 Abs. 6, bei denen Vorgänge innerhalb von Wohnungen erfasst wurden, und nach § 16 die Zielperson, die erheblich mitbetroffenen Personen und die Personen, deren nicht allgemein zugängliche Wohnung betreten wurde,
4. Maßnahmen nach § 15a Abs. 1, 2 Satz 1 sowie Abs. 3 die Beteiligten der überwachten und betroffenen Telekommunikation sowie die Zielperson,

5. Maßnahmen nach § 15b die Beteiligten der überwachten Telekommunikation und die Angaben zur Identifizierung des informationstechnischen Systems und die daran vorgenommenen nicht nur flüchtigen Veränderungen,
6. Maßnahmen nach § 17 die Zielperson und die Personen, deren personenbezogene Daten gemeldet worden sind,
7. Maßnahmen nach § 26 die im Übermittlungsersuchen nach § 26 Abs. 2 enthaltenen Merkmale und die betroffenen Personen, gegen die nach Auswertung der Daten weitere Maßnahmen getroffen wurden.

(3) Nachforschungen zur Feststellung der Identität einer in Abs. 2 bezeichneten Person sind nur vorzunehmen, wenn dies unter Berücksichtigung der Eingriffsintensität der Maßnahme gegenüber dieser Person, des Aufwands für die Feststellung ihrer Identität sowie der daraus für diese oder andere Personen folgenden Beeinträchtigungen geboten ist. Die Zahl der Personen, deren Protokollierung unterblieben ist, ist im Protokoll anzugeben.

(4) Die Protokolldaten dürfen nur verwendet werden für die Zwecke der Benachrichtigung und um eine Prüfung zu ermöglichen, ob die Maßnahme rechtmäßig durchgeführt worden ist. Sie sind bis zum Ablauf der Datenschutzkontrolle nach § 29a aufzubewahren und sodann automatisiert zu löschen, es sei denn, dass sie für den in Satz 1 genannten Zweck noch erforderlich sind.

§ 29
Information, Benachrichtigung, Auskunft

(1) Die Betroffenen erhalten Information, Benachrichtigung oder Auskunft hinsichtlich der zu ihrer Person verarbeiteten Daten nach Maßgabe der §§ 50 bis 52 des Hessischen Datenschutz- und Informationsfreiheitsgesetzes, soweit die Datenverarbeitung zu den in § 40 des Hessischen Datenschutz- und Informationsfreiheitsgesetzes genannten Zwecken erfolgt, und im Übrigen nach Maßgabe der §§ 31 bis 33 des Hessischen Datenschutz- und Informationsfreiheitsgesetzes und der Art. 13 bis 15 der Verordnung (EU) Nr. 2016/679, soweit in den Abs. 2 bis 7 nichts Abweichendes geregelt ist.

(2) Abweichend von § 31 Abs. 1 des Hessischen Datenschutz- und Informationsfreiheitsgesetzes kann die oder der Verantwortliche die Information der betroffenen Person nach Art. 13 Abs. 1 bis 3 der Verordnung (EU) Nr. 2016/679 bei der Verarbeitung personenbezogener Daten zu Zwecken außerhalb des § 40 des Hessischen Datenschutz- und Informationsfreiheitsgesetzes insoweit und solange aufschieben, einschränken oder unterlassen, wie andernfalls die Erteilung der Information die Voraussetzungen des § 31 Abs. 1 des Hessischen Datenschutz- und Informationsfreiheitsgesetzes erfüllt. § 31 Abs. 3 des Hessischen Datenschutz- und Informationsfreiheitsgesetzes findet insoweit keine Anwendung. Abweichend von § 32 Abs. 1 des Hessischen Datenschutz- und Informationsfreiheitsgesetzes kann die oder der Verantwortliche die Information nach Art. 14 Abs. 1, 2 und 4 der Verordnung (EU) Nr. 2016/679 insoweit und solange aufschieben, einschränken oder unterlassen, wie andernfalls die Erteilung der Information die Voraussetzungen des § 32 Abs. 1 des Hessischen Datenschutz- und Informationsfreiheitsgesetzes erfüllt. Im Fall der Einschränkung gilt § 33 Abs. 3 des Hessischen Datenschutz- und Informationsfreiheitsgesetzes entsprechend.

(3) Ergänzend zu § 33 Abs. 1 des Hessischen Datenschutz- und Informationsfreiheitsgesetzes kann bei Datenverarbeitungen zu Zwecken außerhalb des § 40 des Hessischen Datenschutz- und Informationsfreiheitsgesetzes die Auskunftserteilung über die personenbezogenen Daten, die Gegenstand der Verarbeitung sind, und zu Informationen nach Art. 15 Abs. 1 Buchst. a bis h der Verordnung (EU) Nr. 2016/679 auch teilweise oder vollständig eingeschränkt werden. § 33 Abs. 2 des Hessischen Datenschutz- und Informationsfreiheitsgesetzes findet insoweit keine Anwendung. Die oder der Verantwortliche hat die betroffene Person über das Absehen von oder die Einschränkung einer Auskunft unverzüglich schriftlich zu unterrichten. Dies gilt nicht, soweit bereits die Erteilung dieser Informationen eine Gefährdung im Sinne des § 32 Abs. 1 des Hessischen Datenschutz- und Informationsfreiheitsgesetzes mit sich bringen würde. Die Unterrichtung nach Satz 3 ist zu begründen, es sei denn, dass die Mitteilung der Gründe den mit dem Absehen von oder der Einschränkung der Auskunft verfolgten Zweck gefährden würde. Die oder der Verantwortliche hat die sachlichen und rechtlichen Gründe für die Entscheidung zu dokumentieren. § 33 Abs. 3 des Hessischen Datenschutz- und Informationsfreiheitsgesetzes gilt ergänzend auch bei der Einschränkung der Auskunft.

(4) Werden personenbezogene Daten von Kindern, die ohne Kenntnis der Sorgeberechtigten erhoben worden sind, gespeichert, sind die Sorgeberechtigten zu benachrichtigen, sobald die Aufgabenerfüllung dadurch nicht mehr erheblich gefährdet wird. Von der Unterrichtung kann abgesehen werden, solange zu besorgen ist, dass sie zu erheblichen Nachteilen für das Kind führt.

(5) Wurden personenbezogene Daten durch eine Maßnahmen nach § 28 Abs. 2 erlangt, sind die dort jeweils bezeichneten betroffenen Personen hierüber nach Abschluss der Maßnahme zu benachrichtigen. Nachforschungen zur Feststellung der Identität oder zur Anschrift einer zu benachrichtigenden Person sind nur vorzunehmen, wenn dies unter Berücksichtigung der Eingriffsintensität der Maßnahme gegenüber dieser Person, des Aufwands für die Feststellung ihrer Identität sowie der daraus für diese oder anderes Personen folgenden Beeinträchtigungen geboten ist.

(6) Eine Benachrichtigung nach Abs. 5 ist zurückzustellen, solange sie

1. den Zweck der Maßnahme,
2. ein sich an den auslösenden Sachverhalt anschließendes strafrechtliches Ermittlungsverfahren,
3. den Bestand des Staates,
4. Leib, Leben oder Freiheit einer Person oder
5. Sachen von bedeutendem Wert, deren Erhaltung im öffentlichen Interesse geboten ist,

gefährden würde. Im Falle des Einsatzes einer V-Person oder VE-Person erfolgt die Benachrichtigung erst, sobald dies auch ohne Gefährdung der Möglichkeit der weiteren Verwendung der V-Person oder VE-Person möglich ist. Die Entscheidung über das Zurückstellen einer Benachrichtigung trifft die Behördenleitung oder eine von dieser beauftragte Bedienstete oder ein von dieser beauftragter Bediensteter. Wird die Benachrichtigung aus einem der vorgenannten Gründe zurückgestellt, ist dies zu dokumentieren. Über die Zurückstellung der Benachrichtigung ist die oder der Hessische Datenschutzbeauftragte spätestens sechs Monate nach Abschluss der Maßnahme und danach in halbjährlichen Abständen in Kenntnis zu setzen.

(7) Eine Benachrichtigung nach Abs. 5 unterbleibt, soweit dies im überwiegenden Interesse einer betroffenen Person liegt. Zudem kann die Benachrichtigung einer in § 28 Abs. 2 Nr. 4 und 5 bezeichneten Person, gegen die sich die Maßnahme nicht gerichtet hat, unterbleiben, wenn diese von der Maßnahme nur unerheblich betroffen ist und anzunehmen ist, dass sie kein Interesse an der Benachrichtigung hat. Die Entscheidung über das Unterbleiben einer Benachrichtung trifft die Behördenleitung oder eine von dieser beauftragte Bedienstete oder ein von dieser beauftragter Bediensteter.

(8) Sind die personenbezogenen Daten in ein anhängiges Strafverfahren eingeführt, so ist vor Erteilung der Auskunft an die betroffene Person oder vor der Benachrichtigung der betroffenen Person die Zustimmung der Staatsanwaltschaft herbeizuführen."

23. Nach § 29 wird als § 29a eingefügt:

"§ 29a
Datenschutzkontrolle

Die oder der Hessische Datenschutzbeauftragte führt unbeschadet ihrer oder seiner sonstigen Aufgaben und Kontrollen mindestens alle zwei Jahre zumindest stichprobenartig Kontrollen bezüglich der Datenverarbeitung bei nach § 28 Abs. 2 zu protokollierenden Maßnahmen und von Übermittlungen nach § 23 durch."

24. § 115 wird wie folgt geändert:

a) Der Überschrift werden ein Komma und das Wort "Außerkrafttreten" angefügt.

b) Folgender Satz wird angefügt:

"§ 20a Abs. 4 Satz 2 tritt mit Ablauf des 31. Dezember 2029 außer Kraft."

Artikel 19
Änderung des Hessischen Brand- und Katastrophenschutzgesetzes

§ 55 Abs. 1 des Hessischen Brand- und Katastrophenschutzgesetzes in der Fassung der Bekanntmachung vom 14. Januar 2014 (GVBl. S. 26) wird wie folgt gefasst:

"(1) Für die Verarbeitung personenbezogener Daten gelten die Bestimmungen der Verordnung (EU) Nr. 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung) (ABl. EU Nr. L 119 S. 1, Nr. L 314 S. 72) und des Hessischen Datenschutz- und Informationsfreiheitsgesetzes nach Maßgabe der folgenden Vorschriften."

Artikel 20
Änderung des Hessischen Spielhallengesetzes

In § 12 Abs. 1 Nr. 16 des Hessischen Spielhallengesetzes vom 28. Juni 2012 (GVBl. S. 213), geändert durch Gesetz vom … [einsetzen*: Datum und Fundstelle des derzeit im Gesetzgebungsverfahren befindlichen Änderungsgesetzes zum HessSpielhG*], werden die Wörter "und Löschung" gestrichen.

Artikel 21
Änderung des Hessischen Disziplinargesetzes

§ 33 des Hessischen Disziplinargesetzes vom 21. Juli 2006 (GVBl. I S. 394), zuletzt geändert durch Gesetz vom 27. Mai 2013 (GVBl. S. 218), wird wie folgt geändert:

1. In Abs. 1 wird das Wort "Vorlage" durch "Übermittlung" ersetzt und werden die Wörter "oder Nutzung" gestrichen.

2. In Abs. 2 wird das Wort "Vorlage" durch "Übermittlung" ersetzt.

Artikel 22
Änderung des Hessischen Personalvertretungsgesetzes

§ 62 Abs. 2 des Hessischen Personalvertretungsgesetzes vom 24. März 1988 (GVBl. I S. 103), zuletzt geändert durch Gesetz vom 16. Dezember 2015 (GVBl. S. 594), wird wie folgt geändert:

1. In Satz 2 wird das Wort "vorzulegen" durch die Wörter "zu übermitteln" ersetzt.

2. In Satz 4 wird das Wort "Zustimmung" durch "Einwilligung" ersetzt.

3. In Satz 5 werden die Wörter "zur Kenntnis zu bringen" durch "offen zu legen" ersetzt.

Artikel 23
Änderung des Heilberufsgesetzes

Das Heilberufsgesetz in der Fassung der Bekanntmachung vom 7. Februar 2003 (GVBl. I S. 66, 242), zuletzt geändert durch Gesetz vom 19. Dezember 2016 (GVBl. S. 329), wird wie folgt geändert:

1. § 2 Abs. 3 Satz 4 wird wie folgt gefasst:

   "Für die Kammern gelten die Bestimmungen der Verordnung (EU) Nr. 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung) (ABl. EU Nr. L 119 S. 1, Nr. L 314 S. 72) in der jeweils geltenden Fassung sowie des Hessischen Datenschutz- und Informationsfreiheitsgesetzes in der jeweils geltenden Fassung."

2. § 9 Satz 6 wird wie folgt gefasst:

   "Dabei sind die Rechtsvorschriften zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr im Sinne der Verordnung (EU) Nr. 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung) in der jeweils geltenden Fassung einzuhalten."

Artikel 24
Änderung des Hessischen Gesetzes über den öffentlichen Gesundheitsdienst

§ 18 Abs. 4 des Gesetzes über den öffentlichen Gesundheitsdienst vom 28. September 2007 (GVBl. I S. 659), zuletzt geändert durch Gesetz vom 15. Oktober 2014 (GVBl. S. 214), wird wie folgt gefasst:

"(4) Im Übrigen finden die Bestimmungen der Verordnung (EU) Nr. 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der

Richtlinie 95/46/EG (Datenschutz-Grundverordnung) (ABl. EU Nr. L 119 S. 1, Nr. L 314 S. 72) in der jeweils geltenden Fassung sowie des Hessischen Datenschutz- und Informationsfreiheitsgesetzes in der jeweils geltenden Fassung Anwendung."

Artikel 25
Änderung des Hessischen Krankenhausgesetzes 2011

§ 12 des Hessischen Krankenhausgesetzes 2011 vom 21. Dezember 2010, zuletzt geändert durch Gesetz vom 4. Mai 2017 (GVBl. S. 66), wird wie folgt geändert:

1. Abs. 1 wird wie folgt gefasst:

   "(1) Für Krankenhäuser gelten die Bestimmungen der Verordnung (EU) Nr. 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung) (ABl. EU Nr. L 119 S. 1, Nr. L 314 S. 72) in der jeweils geltenden Fassung sowie des Hessischen Datenschutz- und Informationsfreiheitsgesetzes in der jeweils geltenden Fassung abweichend von dessen § 2 Abs. 2 uneingeschränkt nach Maßgaben der Abs. 2 bis 5."

2. In Abs. 3 wird die Angabe "§ 33" durch "§ 24" ersetzt.

Artikel 26
Änderung des Patientenmobilitätsgesetzes

§ 5 Abs. 2 des Patientenmobilitätsgesetzes vom 20. November 2013 (GVBl. S. 638) wird wie folgt gefasst:

"(2) Die Bereitstellung der Informationen hat im Einklang mit den Kapiteln II und III der Richtlinie 2011/24/EU und der Verordnung (EU) Nr. 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung) (ABl. EU Nr. L 119 S. 1, Nr. L 314 S. 72) in der jeweils geltenden Fassung sowie dem Grundsatz der Unschuldsvermutung zu erfolgen."

Artikel 27
Änderung des Maßregelvollzugsgesetzes

Das Maßregelvollzugsgesetz vom 3. Dezember 1981 (GVBl. I S. 414), zuletzt geändert durch Gesetz vom 4. Mai 2017 (GVBl. S. 66), wird wie folgt geändert:

1. § 5a Satz 2 wird wie folgt geändert:

   a) Die Angabe "1. Juli 2014 (GVBl. S. 154)" wird durch "4. Mai 2017 (GVBl. S. 66)" ersetzt.

   b) In Nr. 3 werden nach dem Wort "Fassung" die Wörter "der Bekanntmachung" eingefügt und wird die Angabe "21. Juli 2014 (BGBl. I S. 1133)" durch "17. Juli 2017 (BGBl. I S. 2581)" ersetzt.

2. In § 7 Abs. 1 Satz 1 werden nach der Angabe "2088" ein Komma und die Angabe "1977 S. 436" eingefügt und wird die Angabe "25. April 2013 (BGBl. I S. 935)" durch "17. Juli 2017 (BGBl. I S. 2581)" ersetzt.

3. Dem § 19 Abs. 1 wird folgender Satz angefügt:

   "§ 34 Abs. 5 des Hessischen Strafvollzugsgesetzes vom 28. Juni 2010 (GVBl. I S. 185), zuletzt geändert durch Gesetz vom ... [*einsetzen: Ausfertigungsdatum und Fundstelle des Hessischen Gesetzes zur Anpassung des Hessischen Datenschutzrechts an die Verordnung (EU) Nr. 2016/679 und zur Umsetzung der Richtlinie (EU) Nr. 2016/680 und zur Informationsfreiheit*], ist entsprechend anwendbar."

4. § 31 Satz 4 wird aufgehoben.

5. In § 32 wird die Angabe "vom 28. Juni 2010 (GVBl. I S. 185), geändert durch Gesetz vom 5. März 2013 (GVBl. S. 46)," gestrichen.

6. § 36 Abs. 1 wird wie folgt gefasst:

"(1) § 58 Abs. 1 Satz 1 und 2, Abs. 2, 5 und 6, die §§ 59, 60 Abs. 1, 2, 3 Satz 1, 2, 4 und 5, Abs. 4 bis 7, die §§ 61, 62 Abs. 1, § 63 Abs. 2 Satz 1 und § 65 Abs. 1, 2, 4 bis 6 des Hessischen Strafvollzugsgesetzes gelten entsprechend mit der Maßgabe, dass

1. Daten über die untergebrachte Person bei ihr erhoben werden sollen und bei Dritten erhoben werden dürfen, soweit die Daten zur Beurteilung des Gesundheitszustands der untergebrachten Person oder zu ihrer Eingliederung erforderlich sind oder soweit eine Erhebung bei der untergebrachten Person nicht möglich ist,
2. zu den Daten über die untergebrachte Person auch die Angaben über gegenwärtige oder frühere Krankheiten, Körperschäden und Verhaltensauffälligkeiten der untergebrachten Person zählen,
3. die Übermittlung der Daten der untergebrachten Person an Personen und Stellen außerhalb der Einrichtung auch zulässig ist, soweit dies zur Weiterbehandlung der untergebrachten Person durch eine Einrichtung, in die sie im Rahmen des Maßregelvollzugs verlegt worden ist oder verlegt werden soll, oder durch eine forensisch-psychiatrische Ambulanz erforderlich ist,
4. Kenntnisse aus der Überwachung der Besuche, des Schriftwechsels, der Ferngespräche oder sonstiger Sendungen und der Überprüfung der Mobilfunkendgeräte und Datenträger auch verwertet werden dürfen, soweit dies aus Gründen der Behandlung geboten ist,
5. bei der Übersendung der Personalakte Daten, die dem § 203 des Strafgesetzbuchs unterliegen, nur übermittelt werden dürfen, soweit sie für den Zweck des Empfängers erforderlich sind,
6. der Aufsichtsbehörde Daten, die dem § 203 des Strafgesetzbuches unterliegen, nur übermittelt werden dürfen, soweit sie für die Zwecke der Fach- und Rechtsaufsicht nach § 3 erforderlich sind,
7. bei der Aufbewahrung von Daten aus der Personal- und Krankenakte eine Frist von 30 Jahren nicht überschritten werden darf."

Artikel 28
Änderung des Hessischen Ausführungsgesetzes zum Therapieunterbringungsgesetz

In § 7 Abs. 1 des Hessischen Ausführungsgesetzes zum Therapieunterbringungsgesetz vom 27. Juni 2013 (GVBl. S. 442) werden nach der Angabe "(GVBl. S. 46)" ein Komma und die Angabe "zuletzt geändert durch Gesetz vom … [*einsetzen: Ausfertigungsdatum und Fundstelle dieses Gesetzes]*, in der jeweils geltenden Fassung" und in § 7 Abs. 2 nach der Angabe "(GVBl. S. 290)" ein Komma und die Angabe "zuletzt geändert durch Gesetz vom … [*einsetzen: Ausfertigungsdatum und Fundstelle dieses Gesetzes*]," eingefügt.

Artikel 29
Änderung des Hessischen Vermessungs- und Geoinformationsgesetzes

§ 9 Abs. 5 des Hessischen Vermessungs- und Geoinformationsgesetzes vom 6. September 2007 (GVBl. I S. 548), zuletzt geändert durch Gesetz vom 27. September 2012 (GVBl. S. 290), wird wie folgt geändert:

1. Satz 4 wird wie folgt gefasst:

"Auf Eigentumsangaben, die nach Satz 1 in Übereinstimmung mit dem Grundbuch zu führen sind, finden die Art. 16, 18 und 21 der Verordnung (EU) Nr. 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung) (ABl. EU Nr. L 119 S. 1, Nr. L 314 S. 72) keine Anwendung."

2. Folgender Satz wird angefügt:

"Satz 4 gilt nicht, wenn die betroffene Person die fehlende Übereinstimmung der Eigentumsangaben mit dem Grundbuch geltend macht."

Artikel 30
Aufhebung bisherigen Rechts

Das Hessische Datenschutzgesetz in der Fassung der Bekanntmachung vom 7. Januar 1999 (GVBl. I S. 98), zuletzt geändert durch Gesetz vom 14. Juli 2016 (GVBl. S. 121), wird aufgehoben.

Artikel 31
Inkrafttreten

Dieses Gesetz tritt am 25. Mai 2018 in Kraft.

Begründung

Allgemeines

I. Veranlassung und Zielsetzung

Am 25. Mai 2018 wird die Verordnung (EU) Nr. 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung) (ABl. EU Nr. L 119 S. 1, Nr. L 314 S. 72) unmittelbar geltendes Recht in allen Mitgliedstaaten der Europäischen Union sein. Die Verordnung (EU) Nr. 2016/679 gilt nach Art. 2 Abs. 1 für die ganz oder teilweise automatisierte Verarbeitung personenbezogener Daten sowie für die nicht automatisierte Verarbeitung personenbezogener Daten, die in einem Dateisystem gespeichert sind oder gespeichert werden sollen. Die Verordnung enthält nach deren Art. 1 Abs. 1 Vorschriften zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten sowie zum freien Verkehr solcher Daten und schützt nach Art. 1 Abs. 2 die Grundrechte und Grundfreiheiten natürlicher Personen und insbesondere deren Recht auf Schutz personenbezogener Daten. Ziel ist ein gleichwertiges Schutzniveau für die Rechte und Freiheiten von natürlichen Personen bei der Verarbeitung von Daten in allen Mitgliedstaaten (Erwägungsgrund 10). Der Unionsgesetzgeber hat sich für die Handlungsform einer Verordnung entschieden, damit innerhalb der Europäischen Union ein gleichmäßiges Datenschutzniveau für natürliche Personen gewährleistet ist (Erwägungsgrund 13).

Nach Art. 288 Abs. 2 des Vertrags über die Arbeitsweise der Europäischen Union (AEUV) haben Verordnungen allgemeine Geltung, sind in allen ihren Teilen verbindlich und gelten unmittelbar in jedem Mitgliedstaat. Ihrem Charakter als Grundverordnung folgend sieht die Verordnung (EU) Nr. 2016/679 jedoch Öffnungsklauseln für den nationalen Gesetzgeber vor. Zugleich enthält die Verordnung (EU) Nr. 2016/679 konkrete, an die Mitgliedstaaten gerichtete Regelungsaufträge. Daraus ergibt sich in Bund und Ländern gesetzlicher Anpassungs- und Ausgestaltungsbedarf im nationalen Datenschutzrecht und im Landesdatenschutzrecht. Während der Bund in einem neugefassten Bundesdatenschutzgesetz (BDSG) Vorschriften für die Verarbeitung personenbezogener Daten durch die öffentlichen Stellen des Bundes und die nicht öffentlichen Stellen geschaffen hat, richtet sich der Auftrag an den Hessischen Landesgesetzgeber, das Hessische Datenschutzgesetz mit seinen Vorschriften über die Verarbeitung personenbezogener Daten durch die öffentlichen Stellen des Landes, der Gemeinden und Landkreise an die Vorgaben der Verordnung (EU) Nr. 2016/679 anzupassen.

Zeitgleich mit der Verordnung (EU) Nr. 2016/679 in Kraft getreten ist die Richtlinie (EU) Nr. 2016/680 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zweck der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung sowie zum freien Datenverkehr und zur Aufhebung des Rahmenbeschlusses 2008/977/JI des Rates (ABl. EU Nr. L 119 S. 89). Nach deren Art. 63 sind die der Richtlinie (EU) Nr. 2016/680 unterfallenden Staaten verpflichtet, bis zum 6. Mai 2018 die Rechts- und Verwaltungsvorschriften zu erlassen, die erforderlich sind, um dieser Richtlinie nachzukommen. Die Mitgliedstaaten haben nach Art. 1 Abs. 2 der Richtlinie (EU) Nr. 2016/680 die Grundrechte und Grundfreiheiten natürlicher Personen, insbesondere deren Recht auf Schutz personenbezogener Daten, zu schützen und sicherzustellen, dass der Austausch personenbezogener Daten zwischen den zuständigen Behörden in der Union - sofern er nach dem Unionsrecht oder dem Recht der Mitgliedstaaten vorgesehen ist - nicht aus Gründen, die mit dem Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten verbunden sind, eingeschränkt oder verboten wird. Nach Art. 2 Abs. 2 gilt die Richtlinie für die ganz oder teilweise automatisierte Verarbeitung personenbezogener Daten sowie für die nicht automatisierte Verarbeitung personenbezogener Daten, die in einem Dateisystem gespeichert sind oder gespeichert werden sollen.

Die beiden EU-Rechtsakte der Verordnung (EU) Nr. 2016/679 und der Richtlinie (EU) Nr. 2016/680 bilden die wesentlichen Elemente der EU-Datenschutzreform und grenzen sich ausgehend von Art. 2 Abs. 1 der Richtlinie (EU) Nr. 2016/680 insoweit voneinander ab, dass die Richtlinie Anwendung findet bei der Verarbeitung personenbezogener Daten zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung, einschließlich des Schutzes vor und der Abwehr von Gefahren für die öffentliche Sicherheit. Spiegelbildlich erklärt Art. 2 Buchst. d der Verordnung (EU) Nr. 2016/679 diese für die Verarbeitung personenbezogener Daten zu den vorgenannten Zwecken für nicht anwendbar.

Ziel des Gesetzentwurfs ist die Anpassung des Hessischen Datenschutzgesetzes und datenschutzrechtlicher Vorschriften in Landesgesetzen an die Vorgaben der Verordnung (EU) Nr. 2016/679 sowie die landesrechtliche Umsetzung der Richtlinie (EU) Nr. 2016/680.

Das Verwaltungshandeln soll zukünftig offener und transparenter gestaltet werden. Im Vierten Teil des Hessischen Datenschutz- und Informationsfreiheitsgesetzes werden deshalb erstmals Regelungen für ein Recht auf Informationszugang gegenüber den öffentlichen Stellen in Hessen geschaffen. Bürgerinnen und Bürger erhalten damit die Möglichkeit, unmittelbar Einblick in Vorgänge der öffentlichen Verwaltung zu nehmen. Entscheidungen der Verwaltung werden damit nachvollziehbar, deren Akzeptanz wird erhöht. Die Schaffung eines Anspruchs auf Informationszugang hat so eine wichtige demokratische und rechtstaatliche Funktion, denn der freie Zugang zu bei öffentlichen Stellen vorhandenen Informationen ist wesentlicher Bestandteil öffentlicher Partizipation und der Kontrolle staatlichen Handelns. Er fördert die demokratische Meinungs- und Willensbildung. Der effektive Schutz personenbezogener Daten bleibt dabei gewährleistet, entgegenstehende berechtigte öffentliche und private Interessen werden angemessen berücksichtigt.

Daneben ergibt sich durch die Verordnung (EU) Nr. 2016/679 und die Richtlinie (EU) Nr. 2016/680 weiterer Anpassungs- und Umsetzungsbedarf bei bereichsspezifischen datenschutzrechtlichen Vorschriften in Landesgesetzen.

II. Inhalt und Systematik des Gesetzentwurfs

Um ein reibungsloses Zusammenspiel von Verordnung (EU) Nr. 2016/679 und Richtlinie (EU) Nr. 2016/680 mit dem stark ausdifferenzierten Datenschutzrecht sicherzustellen, ist es erforderlich, das bisherige Hessische Datenschutzgesetz durch eine Neufassung abzulösen. Der vorliegende Gesetzentwurf, dessen Anwendungsbereich sich an die Verarbeitung personenbezogener Daten durch die öffentlichen Stellen des Landes, der Gemeinden und Landkreise richtet, lehnt sich soweit wie möglich und vorbehaltlich landesrechtlicher Besonderheiten in Aufbau und Regelungsinhalten an die Vorschriften des neugefassten Bundesdatenschutzgesetzes betreffend die Verarbeitung personenbezogener Daten durch die öffentlichen Stellen des Bundes an, um vor dem Hintergrund der umfassenden EU-Datenschutzreform eine möglichst einheitliche und parallele Rechtsentwicklung in Bundes- und Landesdatenschutzrecht zu erreichen.

Nicht übernommen werden Bestimmungen des Bundesdatenschutzgesetzes, welche die Verarbeitung personenbezogener Daten durch nicht öffentliche Stellen regeln. Im Interesse einer homogenen Entwicklung des allgemeinen Datenschutzrechts soll das neugefasste Hessische Datenschutz- und Informationsfreiheitsgesetz, soweit nicht dieses selbst oder bereichsspezifische Gesetze abweichende Regelungen treffen, auch für die Verarbeitung personenbezogener Daten im Rahmen von Tätigkeiten öffentlicher Stellen Anwendung finden, die nicht in den Anwendungsbereich des Unionsrechts und damit der beiden EU-Rechtsakte der Verordnung (EU) Nr. 2016/679 und der Richtlinie (EU) Nr. 2016/680 fallen, wie etwa die Datenverarbeitung durch das Landesamt für Verfassungsschutz.

Der Gesetzentwurf sieht im Einzelnen folgende Gesetzesänderungen vor:

1. Hessisches Datenschutz- und Informationsfreiheitsgesetz (HDSIG-E)

   In das neue Hessische Datenschutz- und Informationsfreiheitsgesetz (Artikel 1), welches für die Verarbeitung personenbezogener Daten durch die öffentlichen Stellen des Landes, der Gemeinden und Landkreise Anwendung findet, werden Regelungen mit folgendem Inhalt aufgenommen:

   a) Gemeinsame Bestimmungen mit folgenden Regelungsschwerpunkten (Erster Teil):

      - Anwendungsbereich und Begriffsbestimmungen (§§ 1, 2 HDSIG-E);
      - Schaffung allgemeiner Rechtsgrundlagen für die Datenverarbeitung durch öffentliche Stellen und für die Videoüberwachung (§§ 3, 4 HDSIG-E);
      - Regelungen zu Datenschutzbeauftragten öffentlicher Stellen (§§ 5 bis 7 HDSIG-E);
      - Ausgestaltung des Amtes, der Aufgaben und Befugnisse der oder des Hessischen Datenschutzbeauftragten (§§ 8 bis 18 HDSIG-E);
      - Rechtsbehelfe (§ 19 HDSIG-E).

      Die gemeinsamen Bestimmungen finden keine Anwendung, soweit das Recht der Europäischen Union unmittelbar gilt, insbesondere die Verordnung (EU) Nr. 2016/679. Sie gelten im Anwendungsbereich der Richtlinie (EU) Nr. 2016/680 sowie für die Bereiche, die außerhalb des Unionsrechts liegen.

   b) Bestimmungen zur Ausgestaltung der Verordnung (EU) Nr. 2016/679 mit folgenden Regelungsschwerpunkten (Zweiter Teil):

      - Schaffung einer Rechtsgrundlage für die Verarbeitung besonderer Kategorien personenbezogener Daten (§ 20 HDSIG-E);

- Festlegung der Zulässigkeitsvoraussetzungen für Verarbeitungen zu anderen Zwecken (§ 21 HDSIG-E) sowie für Datenübermittlungen durch öffentliche Stellen (§ 22 HDSIG-E);
- Regelungen weiterer besonderer Verarbeitungssituationen (§§ 23 bis 30 HDSIG-E);
- Regelungen zu den Betroffenenrechten (§§ 31 bis 35 HDSIG-E);
- Verhängung von Sanktionen bei Verstößen gegen die Verordnung (EU) Nr. 2016/679 (§§ 36 bis 38 HDSIG-E)
- Gemeinsame Verfahren, Gemeinsam Verantwortliche (§ 39 HDSIG-E).

c) Bestimmungen zur Umsetzung der Richtlinie EU Nr. 2016/680 mit folgenden Regelungsschwerpunkten (Dritter Teil):

- Anwendungsbereich und Begriffsbestimmungen (§§ 40, 41 HDSIG-E);
- Schaffung allgemeiner Rechtsgrundlagen zur Verarbeitung, Zweckbindung und Zweckänderung (§§ 42 bis 49 HDSIG-E);
- Ausformung der Betroffenenrechte (§§ 50 bis 56 HDSIG-E);
- Festlegung von Pflichten der Verantwortlichen und Auftragsverarbeiter, wie
  - Anforderungen an Auftragsverarbeitungsverhältnisse (§ 57 HDSIG-E) und gemeinsame Verfahren, gemeinsam Verantwortliche (§ 58 HDSIG-E);
  - Datensicherheit und Meldungen von Verletzungen des Schutzes personenbezogener Daten sowie vertrauliche Meldungen von Verstößen (§§ 59 bis 61 und § 72 HDSIG-E);
  - Weitere Vorgaben und Maßnahmen zur Berücksichtigung des Datenschutzes (§§ 62 bis 69 HDSIG-E, insbesondere Datenschutz-Folgenabschätzung, vorherige Konsultation der oder des Hessischen Datenschutzbeauftragten, Verzeichnis von Verarbeitungstätigkeiten);
  - Regelungen zu Berichtigungs- und Löschungspflichten (§ 70 HDSIG-E) sowie Protokollierung (§ 71 HDSIG-E);
- Datenübermittlungen an Stellen in Drittländern und an internationale Organisationen (§§ 73 bis 76 HDSIG-E);
- Zusammenarbeit der Aufsichtsbehörden (§ 77 HDSIG-E);
- Haftung und Sanktionen (§§ 78, 79 HDSIG-E).

d) Bestimmungen zum Recht auf Informationszugang gegenüber öffentlichen Stellen und Einführung einer oder eines Hessischen Informationsfreiheitsbeauftragten (Vierter Teil).

2. Folgeänderungen

In den weiteren Artikeln finden sich Anpassungen bereichsspezifischer datenschutzrechtlicher Vorschriften an die Verordnung (EU) Nr. 2016/679, zur Umsetzung der Richtlinie (EU) Nr. 2016/680 sowie an das neugefasste HDSIG-E.

Zu den einzelnen Vorschriften

Zu Art. 1 (Hessisches Datenschutz- und Informationsfreiheitsgesetz)

Zu § 1 (Anwendungsbereich)
Die Vorschrift bestimmt den Anwendungsbereich des Gesetzes.

Nach Abs. 1 gilt das Gesetz - wie auch das Hessische Datenschutzgesetz in der bisher geltenden Fassung - für jede Form der Verarbeitung personenbezogener Daten durch öffentliche Stellen des Landes, der Gemeinden und Landkreise. Umfasst werden hiernach sämtliche Phasen der Verarbeitung personenbezogener Daten (Erhebung, Speicherung, Veränderung und Nutzung). Welche Institutionen öffentliche Stellen des Landes, der Gemeinden und Landkreise sein können, definiert § 2 näher.

Soweit die Verarbeitung personenbezogener Daten im Rahmen von Tätigkeiten öffentlicher Stellen des Landes, der Gemeinden und Landkreise erfolgt, die weder vom Anwendungsbereich der Verordnung (EU) Nr. 2016/679 noch von der Richtlinie (EU) Nr. 2016/680 erfasst sind, richtet sich das anzuwendende Datenschutzrecht allein nach nationalen Regelungen. So besitzt die Europäische Union etwa nach Art. 4 Abs. 2 Satz 3 des Vertrags über die Europäische Union (EUV) keine Regelungskompetenz für den Bereich der nationalen Sicherheit. Dies betrifft beispielsweise die

Datenverarbeitung durch das Landesamt für Verfassungsschutz. Das neugefasste Hessische Datenschutz- und Informationsfreiheitsgesetz gibt für diese Bereiche außerhalb des Rechts der Europäischen Union allgemeine Regelungen vor. Soweit in bereichsspezifischen Gesetzen abweichende Regelungen getroffen werden, gehen sie gemäß § 1 Abs. 2 den Vorschriften des HDSIG-E vor.

Abs. 2 Satz 1 bestimmt das Verhältnis dieses Gesetzes zu spezifischen datenschutzrechtlichen Vorschriften. Dieses Gesetz hat den Charakter eines "Auffanggesetzes". Spezifische datenschutzrechtliche Vorschriften des Bundes und des Landes genießen gegenüber den Vorschriften des HDSIG-E Vorrang. Dies wird durch die Formulierung in Abs. 2 Satz 1 ausdrücklich klargestellt. Durch Abs. 2 Satz 2 wird zusätzlich klargestellt, dass die jeweilige bereichsspezifische Spezialregelung nur dann vorrangig ist, wenn eine Tatbestandskongruenz besteht. Sie beurteilt sich im Einzelfall nach den Tatbeständen des jeweiligen bereichsspezifischen Gesetzes (für einen Vergleich heranzuziehen sind danach etwa der Sachverhalt "Datenverarbeitung", ggf. in den jeweiligen Verarbeitungsphasen, oder bezogen auf sog. Individual- oder Betroffenenrechte der Sachverhalt "Informationspflicht", "Auskunftsrecht" oder "Widerspruchsrecht"). Dies gilt unabhängig davon, ob in der bereichsspezifischen Vorschrift eine im Vergleich zum HDSIG-E weitergehende oder restriktivere gesetzliche Regelung getroffen ist. Liegt allerdings keine bereichsspezifische Datenschutzregelung für einen vergleichbaren Sachverhalt vor, so übernimmt das HDSIG-E seine lückenfüllende Auffangfunktion. Auch eine nicht abschließende (teilweise) Regelung oder das Schweigen eines bereichsspezifischen Gesetzes führt dazu, dass subsidiär auf die Vorschriften des HDSIG-E zurückgegriffen werden kann. Dies gilt allerdings nicht, wenn spezifische Regelungen für einen bestimmten Bereich insgesamt umfassend und damit abschließend die Verarbeitung personenbezogener Daten regeln und damit für das HDSIG-E kein Anwendungsbereich verbleibt.

Abs. 3 entspricht der bisherigen Regelung des § 3 Abs. 2 HDSG.

Abs. 4 übernimmt die Regelung des § 3 Abs. 5 HDSG und erklärt von den Vorschriften dieses Gesetzes bei der Verarbeitung personenbezogener Daten durch den Hessischen Rundfunk zu journalistischen Zwecken lediglich die Vorschrift des § 28 für anwendbar. Sofern eine Verarbeitung personenbezogener Daten durch den Hessischen Rundfunk zu anderen als journalistischen Zwecken erfolgt, finden die Vorschriften des Hessischen Datenschutz- und Informationsfreiheitsgesetzes uneingeschränkt Anwendung. Dies wird durch § 1 Abs. 4 Satz 2 klargestellt.

Abs. 5 berücksichtigt, dass der Verordnung (EU) Nr. 2016/679 im Rahmen ihres Anwendungsbereichs unmittelbare Geltung im Sinne des Art. 288 Abs. 2 AEUV zukommt. Soweit in diesem Abschnitt punktuelle Wiederholungen sowie Verweise auf Bestimmungen der Verordnung (EU) Nr. 2016/679 erfolgen, so geschieht dies aus Gründen der Verständlichkeit und Kohärenz und lässt die unmittelbare Geltung der Verordnung (EU) Nr. 2016/679 unberührt. Dies wird hiermit an herausgehobener Stelle klargestellt. Die punktuellen Wiederholungen und Verweise im HDSIG-E sind dem rechtlichen Mehrebenensystem geschuldet, das sich aus dem Zusammenspiel zwischen der Verordnung (EU) Nr. 2016/679, der Richtlinie (EU) Nr. 2016/680 sowie dem nationalen allgemeinen und fachspezifischen Recht ergibt. Für den Bereich der Richtlinie (EU) Nr. 2016/680 sind nach deren Art. 1 Abs. 3 damit einhergehende strengere Vorgaben möglich. Dies stellt ausdrücklich Erwägungsgrund 15 klar, wonach die Mitgliedstaaten nicht daran gehindert werden, zum Schutz der Rechte und Freiheiten der betroffenen Person bei der Verarbeitung personenbezogener Daten durch die zuständigen Behörden Garantien festzulegen, die strenger sind als die Garantien dieser Richtlinie.

Abs. 6 und 7 dienen der Klarstellung, welche Staaten den Mitgliedstaaten der Europäischen Union gleichgestellt sind.

Abs. 8 bestimmt, dass für Verarbeitungen personenbezogener Daten im Rahmen der Tätigkeiten, die weder dem Anwendungsbereich der Verordnung (EU) Nr. 2016/679 noch dem der Richtlinie (EU) Nr. 2016/680 unterfallen, die Verordnung (EU) Nr. 2016/679 sowie der Erste und Zweite Teil des HDSIG-E Anwendung finden. Abs. 8 stellt sicher, dass auch für die nicht unter die beiden EU-Rechtsakte fallenden Bereiche entsprechend der bisherigen Regelungssystematik des HDSIG-E eine datenschutzrechtliche Vollregelung im Geltungsbereich des Grundgesetzes erfolgt.

Abs. 9 übernimmt die in Erwägungsgrund 26 der Verordnung (EU) Nr. 2016/679 zum Ausdruck gebrachte Absicht des Verordnungsgebers, dass die Grundsätze des Datenschutzes nicht für anonyme Informationen gelten sollen.

Zu § 2 (Begriffsbestimmungen)
Abs. 1 Satz 1 bestimmt, welche öffentlichen Stellen unter den Anwendungsbereich des § 1 Abs. 1 HDSIG-E fallen. Nach Abs. 1 Satz 2 gelten nicht öffentliche Stellen, soweit sie hoheitliche Aufgaben der öffentlichen Verwaltung wahrnehmen (Beliehene), als öffentliche Stellen im Sinne dieses Gesetzes.

Abs. 2 vollzieht den Regelungsgehalt des § 3 Abs. 6 HDSG nach, indem bestimmt wird, dass öffentliche Stellen des Landes, der Gemeinden und Landkreise dann als nicht öffentliche Stellen gelten, soweit sie als öffentlich-rechtliche Unternehmen am Wettbewerb teilnehmen.

Abs. 3 sieht eine Regelung zu Vereinigungen des privaten Rechts vor, an denen eine oder mehrere öffentliche Stellen im Sinne des Abs. 1 beteiligt sind.

Abs. 4 enthält eine Definition des Begriffs Anonymisierung und orientiert sich an den in Erwägungsgrund 26 der Verordnung Nr. 2016/679 sowie Erwägungsgrund 21 der Richtlinie Nr. 2016/680 zu findenden Wortlauten.

Zu § 3 (Verarbeitung personenbezogener Daten, Auftragsverarbeitung)
Die Vorschrift enthält eine allgemeine Rechtsgrundlage für die Verarbeitung personenbezogener Daten. Durch die Stellung im Ersten Teil "Gemeinsame Bestimmungen" können Verantwortliche - vorbehaltlich bereichsspezifischer Regelungen - auf die Bestimmung unabhängig davon zurückgreifen, zu welchen Zwecken die Datenverarbeitung erfolgt.

Soweit nicht öffentliche Stellen hoheitliche Aufgaben der öffentlichen Verwaltung wahrnehmen (sog. Beliehene), gelten sie nach § 2 Abs. 1 S. 2 HDSIG-E als öffentliche Stellen und können ihre Datenverarbeitung daher ebenfalls auf die Befugnis in § 3 Abs. 1 HDSIG-E stützen.

Soweit die Vorschrift für Datenverarbeitungen zu Zwecken nach Art. 2 der Verordnung (EU) Nr. 2016/679 zur Anwendung kommt, wird mit ihr eine Regelung auf der Grundlage von Art. 6 Abs. 1 Buchst. e i.V.m. Art. 6 Abs. 3 Satz 1 der Verordnung (EU) Nr. 2016/679 geschaffen. Dies ist rechtlich notwendig, da Art. 6 Abs. 1 Buchst. e der Verordnung (EU) Nr. 2016/679 selbst keine Rechtsgrundlage für die Verarbeitung von Daten schafft, was sich aus der Formulierung in Art. 6 Abs. 3 Satz 1 der Verordnung (EU) Nr. 2016/679 ergibt. Der Unions- oder der nationale Gesetzgeber hat eine eigenständige Rechtsgrundlage zu setzen. Diesem Regelungsauftrag kommt der hessische Gesetzgeber an dieser Stelle für die Verarbeitung personenbezogener Daten durch die öffentlichen Stellen des Landes, der Gemeinden und Landkreise nach.

Die Verarbeitung personenbezogener Daten durch öffentliche Stellen ist nach der Vorschrift des § 3 Abs. 1 zulässig, wenn sie für die Wahrnehmung einer im öffentlichen Interesse liegenden Aufgabe erforderlich ist oder wenn sie in Ausübung öffentlicher Gewalt erfolgt, die dem Verantwortlichen übertragen wurde. Beides kann sich sowohl aus nationalen Rechtsvorschriften als auch aus europarechtlichen Vorgaben ergeben. Die Verarbeitung personenbezogener Daten ist allerdings nicht nur auf dieser Rechtsgrundlage zulässig, sondern auch auf der Grundlage der weiteren in Art. 6 Abs. 1 der Verordnung (EU) Nr. 2016/679 aufgeführten Erlaubnistatbestände einschließlich der auf der Grundlage der Verordnung (EU) Nr. 2016/679 und der Richtlinie (EU) Nr. 2016/680 erlassenen bereichsspezifischen Regelungen.

Die Regelung unterscheidet nicht zwischen den Phasen der Erhebung, Speicherung, Veränderung und Nutzung, sondern verwendet, dem Grundgedanken der Verordnung (EU) Nr. 2016/679 und der Richtlinie (EU) Nr. 2016/680 folgend, allgemein den umfassenden Begriff der Verarbeitung.

Abs. 2 Satz 1 übernimmt Teile der Regelung des § 4 Abs. 3 Satz 1 HDSG, um sicherzustellen, dass der Schutz der Rechte betroffener Personen nicht durch ggf. abweichende gesetzliche Regelungen gemindert wird, wenn der Auftragsverarbeiter seinen Sitz außerhalb Hessens hat. Abs. 2 Satz 2 übernimmt die Regelung des bisherigen § 4 Abs. 4 HDSG.

Zu § 4 (Videoüberwachung öffentlich zugänglicher Räume)
Mit der Vorschrift des § 4 wird erstmalig eine Rechtsgrundlage in das HDSIG-E aufgenommen, welche die Beobachtung öffentlich zugänglicher Räume mittels optisch-elektronischer Einrichtungen (Videoüberwachung) gestattet. § 4 regelt die Voraussetzungen für die Videoüberwachung öffentlich zugänglicher Räume durch öffentliche Stellen des Landes, der Gemeinden oder Landkreise zum Zweck der Aufgabenerfüllung der jeweiligen öffentlichen Stelle, zur Wahrnehmung des öffentlichen Hausrechts oder zur Wahrnehmung berechtigter Interessen für konkret festgelegte Zwecke. Hierbei wird in einem Stufenverhältnis unterschieden zwischen der Beobachtung (Abs. 1) und der Speicherung oder Verwendung (Abs. 3) sowie den Kennzeichnungs-, Informations- und Löschungspflichten (Abs. 2 und 4).

Nach § 4 Abs. 1 muss die Beobachtung öffentlich zugänglicher Räume mit optisch-elektronischen Einrichtungen für die vorgenannten Zwecke erforderlich sein und es dürfen keine Anhaltspunkte dafür bestehen, dass schutzwürdige Interessen der betroffenen Personen überwiegen. Öffentlich zugängliche Räume sind alle Bereiche, innerhalb oder außerhalb von Gebäuden, die von einem unbestimmten oder nur nach allgemeinen Merkmalen bestimmten Personenkreis betreten werden können und ihrem Zweck nach auch dazu bestimmt sind.

Die Beobachtung stellt eine Erhebung personenbezogener Daten dar. Soweit die Vorschrift für Datenverarbeitungen zu Zwecken nach Art. 2 der Verordnung (EU) Nr. 2016/679 zur Anwendung kommt, wird mit ihr eine Regelung auf der Grundlage von Art. 6 Abs. 1 Buchst. f der Verordnung (EU) Nr. 2016/679 geschaffen. Nach Art. 6 Abs. 1 Buchst. f der Verordnung (EU) Nr. 2016/679 ist die Verarbeitung personenbezogener Daten zur Wahrung berechtigter Interessen des Verantwortlichen zulässig, sofern nicht schutzwürdige Interessen der betroffenen Person überwiegen.

Abs. 2 regelt das Erfordernis, dass der Umstand der Beobachtung und die verantwortliche Stelle erkennbar zu machen sind. Hierfür sind beispielsweise Hinweisschilder anzubringen, die hinreichend wahrnehmbar und verständlich sind.

Abs. 3 Satz 1 sieht die Zulässigkeit der Speicherung oder Verwendung von nach Abs. 1 erhobenen personenbezogenen Daten vor, wenn dies zum Erreichen des mit der Videoüberwachung verfolgten Zwecks erforderlich ist und keine Anhaltspunkte dafür bestehen, dass schutzwürdige Interessen der betroffenen Person überwiegen. Abs. 3 Satz 2 bestimmt, unter welchen Voraussetzungen die im Zuge einer Videoüberwachungsmaßnahme erhobenen Daten zu einem anderen Zweck, als zu dem sie erhoben worden sind, weiterverarbeitet werden dürfen. Die Regelung macht von der Öffnungsklausel des Art. 6 Abs. 4 i.V.m. Art. 23 Abs. 1 Buchst. c und d der Verordnung (EU) Nr. 2016/679 Gebrauch. Soweit als anderer Zweck die Verfolgung nicht geringfügiger Ordnungswidrigkeiten genannt wird, ist zur Bestimmung des Begriffs der Geringfügigkeit einer Ordnungswidrigkeit auf die Vorschrift des § 56 Abs. 1 des Gesetzes über Ordnungswidrigkeiten (OWiG) zurückzugreifen.

Abs. 4 regelt nach Maßgabe des Art. 17 Abs. 1 Buchst. a der Verordnung (EU) Nr. 2016/679 die Löschung der im Zuge einer Videoüberwachungsmaßnahme erhobenen und gespeicherten Daten.

Zu §§ 5 bis 7 (Datenschutzbeauftragte öffentlicher Stellen)
Der dritte Abschnitt enthält Vorschriften für die Benennung, die Rechtsstellung und die Aufgaben der Datenschutzbeauftragten öffentlicher Stellen des Landes, der Gemeinden und Landkreise.

Zu § 5 (Benennung)
In Umsetzung des Art. 32 Abs. 1 der Richtlinie (EU) Nr. 2016/680 erfolgt in Abs. 1 eine Übernahme des Art. 37 Abs. 1 Buchst. a der Verordnung (EU) Nr. 2016/679. Neben der Benennung einer oder eines Datenschutzbeauftragten der öffentlichen Stelle sieht Abs. 1 Satz 1 in Fortführung der Vorschrift des § 5 Abs. 1 Satz 1 HDSG das Erfordernis zur Benennung einer Vertreterin oder eines Vertreters weiterhin vor.

Abs. 2, 3 und 5 setzen Art. 32 Abs. 2 bis 4 der Richtlinie (EU) Nr. 2016/680 um. Sie entsprechen Art. 37 Abs. 3, 5 und 7 der Verordnung (EU) Nr. 2016/679.

Abs. 4 überträgt die Regelung des Art. 37 Abs. 6 der Verordnung (EU) Nr. 2016/679, nach welcher sowohl die Benennung interner als auch externer Datenschutzbeauftragte zulässig ist, auf den gesamten Bereich der Landes- und Kommunalverwaltung. Dies geht über die Vorgaben der Richtlinie (EU) Nr. 2016/680 hinaus.

Zu § 6 (Rechtsstellung)
Abs. 1 und 2 setzen Art. 33 der Richtlinie (EU) Nr. 2016/680 um. Sie entsprechen Art. 38 Abs. 1 und 2 der Verordnung (EU) Nr. 2016/679. Abs. 2 Satz 2 führt die Regelung des § 5 Abs. 1 Satz 5 2. Halbsatz HDSG fort.

Abs. 3 und 4 Satz 2 übertragen die Vorgaben des Art. 38 Abs. 3 und 4 der Verordnung (EU) Nr. 2016/679 auf alle öffentlichen Stellen des Landes, der Gemeinden und Landkreise, unabhängig davon, zu welchem Zweck die Datenverarbeitung erfolgt. Dies geht über die Vorgaben der Richtlinie (EU) Nr. 2016/680 hinaus. Durch die Erstreckung der Vorgaben der Verordnung (EU) Nr. 2016/679 auf den Anwendungsbereich der Richtlinie (EU) Nr. 2016/680 und der Datenverarbeitung zu Zwecken, für die der Anwendungsbereich des Rechts der Europäischen Union nicht eröffnet ist, wird die Rechtsstellung der oder des behördlichen Datenschutzbeauftragten in öffentlichen Stellen der Landes- und Kommunalverwaltung einheitlich ausgestaltet.

Abs. 4 Satz 1 nimmt die Vorschrift des § 5 Abs. 1 Satz 7 HDSG auf; Abs. 4 Satz 3 konturiert den Umfang der Verschwiegenheitspflicht der oder des Datenschutzbeauftragten. Das Zeugnisverweigerungsrecht in Abs. 5 sichert die Verschwiegenheitspflicht ab. Die Regelungskompetenz für den Bereich der Verordnung (EU) Nr. 2016/679 folgt aus deren Art. 38 Abs. 5. Die Regelung geht insoweit über die Vorgaben der Richtlinie (EU) Nr. 2016/680 hinaus.

Zu § 7 (Aufgaben)
Abs. 1 Satz 1 setzt Art. 34 der Richtlinie (EU) Nr. 2016/680 um. Um die Aufgaben der oder des Datenschutzbeauftragten einer öffentlichen Stelle für alle Verarbeitungszwecke einheitlich auszugestalten, entspricht die Norm unter lediglich redaktioneller Anpassung zudem Art. 39 der Verordnung (EU) Nr. 2016/679.

Abs. 1 Satz 2 stellt klar, dass sich die Aufgaben einer oder eines Datenschutzbeauftragten eines Gerichts nicht auf das Handeln des Gerichts im Rahmen seiner justiziellen Tätigkeit beziehen. Das Handeln in justizieller Tätigkeit ist als Tätigwerden in richterlicher Unabhängigkeit zu verstehen.

Abs. 2 stellt klar, dass die oder der Datenschutzbeauftragte weitere Aufgaben und Pflichten wahrnehmen kann, sofern diese nicht zu einem Interessenkonflikt führen. Die Regelung entspricht Art. 38 Abs. 6 der Verordnung (EU) Nr. 2016/679, deren Regelungsgehalt auf den Anwendungsbereich der Richtlinie (EU) Nr. 2016/680 und der Datenverarbeitung außerhalb des Anwendungsbereichs des Rechts der Europäischen Union erstreckt wird.

Abs. 3 entspricht Art. 39 Abs. 2 der Verordnung (EU) Nr. 2016/679. Die Regelung hat keine Entsprechung in Art. 34 der Richtlinie (EU) Nr. 2016/680, wird aber auch außerhalb des Anwendungsbereichs der Verordnung (EU) Nr. 2016/679 als allgemeiner Grundsatz festgeschrieben.

Zu §§ 8 bis 18 (Die oder der Hessische Datenschutzbeauftragte)
Der vierte Abschnitt des Ersten Teils passt die Regelungen zu der oder dem Hessischen Datenschutzbeauftragten an die Vorgaben der Verordnung (EU) Nr. 2016/679 an. Zugleich werden die Vorgaben der Richtlinie (EU) Nr. 2016/680 umgesetzt.

Zu § 8 (Rechtsstellung und Unabhängigkeit)
Abs. 1 und 2 ersetzen den bisherigen § 22 HDSG und regeln die Rechtsstellung und Unabhängigkeit der oder des Hessischen Datenschutzbeauftragten.

Die Bestimmung der oder des Hessischen Datenschutzbeauftragten als oberste Landesbehörde in Abs. 1 setzt Art. 44 Abs. 1 Buchst. a der Richtlinie (EU) Nr. 2016/680 (Art. 54 Abs. 1 Buchst. a der Verordnung (EU) Nr. 2016/679) um.

Die in Abs. 2 normierten Grundsätze der Unabhängigkeit und Weisungsfreiheit der oder des Hessischen Datenschutzbeauftragten sind unionsrechtlich vorgegeben (Art. 52 Abs. 1 und 2 der Verordnung (EU) Nr. 2016/679 bzw. Art. 42 Abs. 1 und 2 der Richtlinie (EU) Nr. 2016/680).

Abs. 3 trägt Art. 52 Abs. 6, erster Satzteil der Verordnung (EU) Nr. 2016/679 und Art. 42 Abs. 6, erster Satzteil der Richtlinie (EU) Nr. 2016/680 Rechnung. Jeder Mitgliedstaat hat sicherzustellen, dass jede Aufsichtsbehörde einer Finanzkontrolle unterliegt, die ihre Unabhängigkeit nicht beeinträchtigt. Wie aus Erwägungsgrund 118 der Verordnung (EU) Nr. 2016/679 folgt, bedeutet die Unabhängigkeit der Aufsichtsbehörden nicht, dass sie hinsichtlich ihrer Ausgaben keinem Kontroll- oder Überwachungsmechanismus unterworfen sind. Die Haushalts- und Wirtschaftsführung der oder des Hessischen Datenschutzbeauftragten unterliegt der Prüfung des Hessischen Rechnungshofs.

Abs. 4 übernimmt die Regelung des bisherigen § 21 Abs. 5 HDSG.

Zu § 9 (Wahl)
§ 9 regelt in Durchführung der Art. 53 Abs. 1, 54 Abs. 1 Buchst. c der Verordnung (EU) Nr. 2016/679 sowie in Umsetzung der Art. 43 Abs. 1, 44 Abs. 1 Buchst. c der Richtlinie (EU) Nr. 2016/680 das Verfahren zur Wahl und Ernennung der oder des Hessischen Datenschutzbeauftragten.

Nach Art. 53 Abs. 1 der Verordnung (EU) Nr. 2016/679 und Art. 43 Abs. 1 der Richtlinie (EU) Nr. 2016/680 sehen die Mitgliedstaaten ein transparentes Ernennungsverfahren durch das Parlament, die Regierung, das Staatsoberhaupt oder eine unabhängige Stelle, die nach dem Recht des Mitgliedstaats mit der Ernennung betraut wird, vor. Die Mitgliedstaaten haben zudem die Vorschriften und Verfahren für die Ernennung des Mitglieds oder der Mitglieder jeder Aufsichtsbehörde zu schaffen (Art. 54 Abs. 1 Buchst. c der Verordnung (EU) Nr. 2016/679, Art. 44 Abs. 1 Buchst. c der Richtlinie (EU) Nr. 2016/680). Dem entspricht die bisherige Rechtslage in § 21 Abs. 1 und 2 HDSG.

Zu § 10 (Persönliche Voraussetzungen)
Mit der Vorschrift werden in Durchführung der Art. 53 Abs. 2, 54 Abs. 1 Buchst. b der Verordnung (EU) Nr. 2016/679 und in Umsetzung der Art. 43 Abs. 2, 44 Abs. 1 Buchst. b der Richtlinie (EU) Nr. 2016/680 die Anforderungen an die Qualifikation und sonstigen Voraussetzungen für die Ernennung der oder des Hessischen Datenschutzbeauftragten geregelt. Das in Satz 1 vorgesehene Mindestalter von 35 Jahren ist eine "sonstige" Voraussetzung für die Ernennung im Sinne der vorbezeichneten Art und Weise. Satz 2 setzt Art. 43 Abs. 2 der Richtlinie (EU) Nr. 2016/680 um, nach welchem jedes Mitglied einer Aufsichtsbehörde über die für die Erfüllung seiner Aufgaben und Ausübung seiner Befugnisse erforderliche Qualifikation, Erfahrung und Sachkunde insbesondere im Bereich des Schutzes personenbezogener Daten verfügen muss. Eine wortgleiche Regelung findet sich in Art. 53 Abs. 2 der Verordnung (EU) Nr. 2016/679. Satz 2 konkretisiert die erforderlichen Qualifikationen der oder des Hessischen Datenschutzbeauftragten, die oder der über durch einschlägige Berufserfahrung belegbare

Kenntnisse im Bereich des Schutzes personenbezogener Daten verfügen und die Befähigung zum Richteramt oder höheren Dienst haben muss.

Zu § 11 (Amtsverhältnis)
§ 11 regelt die Ausgestaltung, den Beginn und das Ende des Amtsverhältnisses der oder des Hessischen Datenschutzbeauftragten.

In Abs. 1 Satz 1 wird der bisherige § 21 Abs. 3 Satz 1 HDSG übernommen. Die Ausgestaltung als öffentlich-rechtliches Amtsverhältnis eigener Art sichert die Unabhängigkeit der oder des Hessischen Datenschutzbeauftragten dienstrechtlich ab. Es handelt sich um eine unionsrechtlich nach Art. 54 Abs. 1 Buchst. c der Verordnung (EU) Nr. 2016/679 und Art. 44 Abs. 1 Buchst. c der Richtlinie (EU) Nr. 2016/680 zulässige Konkretisierung der Amtsstellung der oder des Hessischen Datenschutzbeauftragten. Abs. 1 Satz 2 bis 4 ersetzen inhaltlich die Regelungen in § 21 Abs. 1 Satz 2 bis 4 HDSG und entsprechen den Vorgaben des Art. 52 Abs. 3 der Verordnung (EU) Nr. 2016/679 bzw. Art. 42 Abs. 3 der Richtlinie (EU) Nr. 2016/680.

Abs. 2 regelt den Beginn und das Ende der Amtszeit der oder des Hessischen Datenschutzbeauftragten. Die in Abs. 2 Satz 1 aufgenommene Regelung zur Dauer der Amtszeit wird in Abänderung der bisherigen Regelung des § 21 Abs. 4 HDSG von der Dauer der jeweiligen Wahlperiode des Landtags gelöst und mit einer Dauer von fünf Jahren befristet. Die Bestimmungen zur Amtszeit und Wiederwahl in Abs. 2 Satz 4 entsprechen den Vorgaben des Art. 54 Abs. 1 Buchst. d und e der Verordnung (EU) Nr. 2016/679 und Art. 44 Abs. 1 Buchst. d und e der Richtlinie (EU) Nr. 2016/680.

Abs. 2 Satz 2 sieht in Übereinstimmung mit Art. 53 Abs. 3 der Verordnung (EU) Nr. 2016/679 und Art. 43 Abs. 3 der Richtlinie (EU) Nr. 2016/680 als Gründe der Beendigung des Amtsverhältnisses den Ablauf der Amtszeit und den Rücktritt der oder des Hessischen Datenschutzbeauftragten vor. Abs. 2 Satz 4 dient der Umsetzung von Art. 44 Abs. 1 Buchst. e der Richtlinie (EU) Nr. 2016/680 bzw. Art. 54 Abs. 1 Buchst. e der Verordnung (EU) Nr. 2016/679.

Abs. 2 Satz 5 bis 7 konkretisieren die Voraussetzungen und das Verfahren der Beendigung des Amtsverhältnisses im Wege der Amtsenthebung (Art. 53 Abs. 3 und 4, 54 Abs. 1 Buchst. f letzter Satzteil der Verordnung (EU) Nr. 2016/679 und Art. 43 Abs. 3 und 4, Art. 44 Abs. 1 Buchst. f letzter Satzteil der Richtlinie (EU) Nr. 2016/680). Diese orientieren sich unter Anpassung an die Anforderungen der genannten EU-Rechtsakte inhaltlich an der bisherigen Regelung des § 21 Abs. 4 HDSG. Satz 5 sieht - wie bisher - ein Amtsenthebungsverfahren durch Entscheidung des Staatsgerichtshofs auf Antrag von mindestens 15 Mitgliedern des Landtags und der Zustimmung von zwei Dritteln der gesetzlichen Zahl seiner Mitglieder vor. Die aus § 21 Abs. 4 Satz 3 HDSG übernommene Bezugnahme auf die Entlassungsgründe der §§ 22 und 23 Abs. 1 und 3 Nr. 1 Beamtenstatusgesetz sowie auf die Beendigung des Dienstverhältnisses nach § 24 Beamtenstatusgesetz konkretisiert die Vorgaben des Art. 53 Abs. 4 der Verordnung (EU) Nr. 2016/679 bzw. Art. 43 Abs. 4 der Richtlinie (EU) Nr. 2016/680, der eine Amtsenthebung bei einer schweren Verfehlung oder bei Nichterfüllung der Voraussetzungen für die weitere Wahrnehmung des Amtes vorsieht.

In Abs. 5 bis 7 werden die Besoldung, Versorgung und sonstigen Bezüge der oder des Hessischen Datenschutzbeauftragten unter Übernahme des bisherigen § 21 Abs. 6 bis 8 HDSG beibehalten. Es handelt sich um eine notwendige mitgliedstaatliche Begleitvorschrift zur Regelung der Errichtung der Aufsichtsbehörden und des Verfahrens für die Ernennung der Leiterin oder des Leiters der Aufsichtsbehörde (Art. 54 Abs. 1 Buchst. a und c der Verordnung (EU) Nr. 2016/679 und Art. 44 Abs. 1 Buchst. a und c der Richtlinie (EU) Nr. 2016/680).

Zu § 12 (Verschwiegenheitspflicht)
Die Vorschrift setzt Art. 54 Abs. 2 der Verordnung (EU) Nr. 2016/679 und Art. 44 Abs. 2 der Richtlinie (EU) Nr. 2016/680 zur Verschwiegenheitspflicht um. Hierzu wird die Regelung des § 23 Satz 1 und 2 HDSG a. F. zur Verschwiegenheitspflicht der oder des Hessischen Datenschutzbeauftragten nunmehr in Satz 3 des § 12 auf die Beschäftigten der oder des Hessischen Datenschutzbeauftragten erstreckt.

Zu § 13 (Zuständigkeit und Aufgaben)
§ 13 regelt Zuständigkeit und Aufgaben der oder des Hessischen Datenschutzbeauftragten. Art. 51 Abs. 1 der Verordnung (EU) Nr. 2016/679 und Art. 41 Abs. 1 der Richtlinie (EU) Nr. 2016/680 überlassen es den Mitgliedstaaten, eine oder mehrere Aufsichtsbehörden für die Überwachung der Anwendung der Verordnung (EU) Nr. 2016/679 und der Richtlinie (EU) Nr. 2016/680 einzurichten. Nach Art. 41 Abs. 3 der Richtlinie (EU) Nr. 2016/680 können die Mitgliedstaaten vorsehen, dass die gemäß der Verordnung (EU) Nr. 2016/679 in den Mitgliedstaaten errichtete Aufsichtsbehörde zudem die in der Richtlinie genannte Aufsichtsbehörde ist und die Verantwortung für die Aufgaben der nach Art. 41 Abs. 1 der Richtlinie (EU) Nr. 2016/680 zu errichtenden Aufsichtsbehörde übernimmt. Von dieser Regelungsoption wird in der Bestimmung des § 13 Abs. 1 Satz 1 HDSIG-E Gebrauch gemacht.

In Abs. 2 werden die in Art. 57 der Verordnung (EU) Nr. 2016/679 vorgesehenen Aufgaben der Aufsichtsbehörde unter redaktioneller Anpassung des Wortlauts insoweit wiederholt, als sie inhaltlich deckungsgleich mit den Vorgaben der Richtlinie (EU) Nr. 2016/680 sind. Die Vorschrift dient damit vorrangig der Umsetzung der Richtlinie (EU) Nr. 2016/680. Die Regelung gilt unbeschadet anderer Aufgaben nach der Verordnung (EU) Nr. 2016/679. Soweit sich die Auflistung der Aufgaben in Abs. 2 Satz 1 nicht ausdrücklich nur auf die Verordnung oder die Richtlinie bezieht, gelten die Aufgaben der oder des Hessischen Datenschutzbeauftragten auch für Datenverarbeitungen, die nicht in den Anwendungsbereich des Unionsrechts fallen. Abs. 2 Satz 2 setzt zusammen mit § 52 Abs. 7 auch i.V.m. § 51 Abs. 4, § 53 Abs. 7 und § 55 Art. 46 Abs. 1 Buchst. g der Richtlinie (EU) Nr. 2016/680 um; dieser hat in Art. 57 der Verordnung (EU) Nr. 2016/679 keine Entsprechung.

Soweit die oder der Hessische Datenschutzbeauftragte im Rahmen der Aufgabenwahrnehmung nach § 13 Abs. 2 Satz 1 Nr. 2 die Öffentlichkeit über die Risiken, Vorschriften, Garantien und Rechte im Zusammenhang mit der Verarbeitung personenbezogener Daten speziell von Kindern und Jugendlichen sensibilisiert und aufklärt, kann dies insbesondere in Zusammenarbeit mit den für den Kinder- und Jugendschutz zuständigen Stellen erfolgen.

Abs. 3 übernimmt die Regelung des § 24 Abs. 2 HDSG. Abs. 4 Nr. 1 überträgt die Zuständigkeit für die Verfolgung und Ahndung von Ordnungswidrigkeiten nach dem HDSIG-E und Art. 83 der Verordnung (EU) Nr. 2016/679 einheitlich dem Hessischen Datenschutzbeauftragten. Abs. 4 Nr. 2 übernimmt die Regelung des § 24 Abs. 4 Nr. 3 HDSG.

Soweit in Abs. 5 von einem Handeln der Gerichte in justizieller Tätigkeit die Rede ist, ist dies als Tätigwerden in richterlicher Unabhängigkeit zu verstehen.

Abs. 6 konkretisiert die Beratungsbefugnisse der oder des Hessischen Datenschutzbeauftragten für den gesamten Bereich des HDSIG-E. Hierdurch wird Art. 47 Abs. 3 der Richtlinie (EU) Nr. 2016/680 umgesetzt. Zugleich wird der Adressatenkreis des Art. 58 Abs. 3 Buchst. b der Verordnung (EU) Nr. 2016/679 konkretisiert.

Abs. 7 setzt Art. 46 Abs. 2 der Richtlinie (EU) Nr. 2016/680 in Übereinstimmung mit der Regelung des Art. 57 Abs. 2 der Verordnung (EU) Nr. 2016/679 um.

Abs. 8 gestaltet die in Abs. 2 Nr. 7 genannte Aufgabe der oder des Hessischen Datenschutzbeauftragten aus und sieht eine Regelung zur Übermittlung von Informationen und zur Amtshilfeleistung im Verhältnis zu anderen Aufsichtsbehörden vor.

Abs. 9 schafft erstmals eine Rechtsgrundlage für die Erhebung von Kosten durch den Hessischen Datenschutzbeauftragten. Dabei bilden die Vorschriften des Hessischen Verwaltungskostengesetzes die gesetzliche Grundlage. Die Anlage 1 zum HDSIG-E enthält die konkreten Gebührentatbestände, die jeweils Amtshandlungen nach der Verordnung (EU) Nr. 2016/679 und dem HDSIG-E mit Gebühren belegen. Grundsätzlich können sowohl nicht öffentliche Stellen im Sinn des § 2 Abs. 4 Bundesdatenschutzgesetzes als auch öffentliche Stellen nach § 2 Abs. 1 HDSIG-E Kostenschuldner sein, wobei jeweils die Regelungen des Verwaltungskostengesetzes z.B. zur sachlichen Kostenfreiheit und persönlichen Gebührenfreiheit zu beachten sind.

Abs. 10 greift Art. 57 Abs. 3 und 4 der Verordnung (EU) Nr. 2016/679 auf und setzt Art. 46 Abs. 3 und 4 der Richtlinie (EU) Nr. 2016/680 um. Es wird damit der oder dem Hessischen Datenschutzbeauftragten im Falle offenkundig unbegründeter oder exzessiver Anfragen gestattet, eine Missbrauchsgebühr zu erheben.

Abs. 11 ermächtigt dazu, die Anlage 1 zu diesem Gesetz durch Rechtsverordnung zu ändern.

Zu § 14 (Befugnisse)
§ 14 regelt für den gesamten Anwendungsbereich des HDSIG-E die Befugnisse der oder des Hessischen Datenschutzbeauftragten.

Abs. 1 verweist für die Befugnisse und deren Ausübung im Anwendungsbereich der Verordnung (EU) Nr. 2016/679 auf Art. 58 der Verordnung (EU) Nr. 2016/679. Abs. 2 und 3 regeln die Befugnisse der oder des Hessischen Datenschutzbeauftragten im Geltungsbereich der Richtlinie (EU) Nr. 2016/680 sowie bei Datenverarbeitungen, deren Zwecke außerhalb der Verordnung (EU) Nr. 2016/679 und der Richtlinie (EU) Nr. 2016/680 liegen, auch wenn für diese durch die Regelung des § 1 Abs. 8 HDSIG-E die Verordnung (EU) Nr. 2016/679 entsprechend anzuwenden ist. Abs. 4 und 5 gelten sowohl im Anwendungsbereich der Verordnung (EU) Nr. 2016/679 und der Richtlinie (EU) Nr. 2016/680 als auch außerhalb der Vorgaben des europäischen Rechts.

Abs. 1 Satz 1 nimmt im Anwendungsbereich der Verordnung (EU) Nr. 2016/679 aus Gründen der Klarstellung und Lesbarkeit auf die Befugnisse des Art. 58 der Verordnung (EU) Nr. 2016/679 Bezug. Satz 2 bis 5 enthält Verfahrensregelungen im Sinne des Art. 58 Abs. 4 der

Verordnung (EU) Nr. 2016/679. Danach erfolgt die Ausübung der den Aufsichtsbehörden übertragenen Befugnisse vorbehaltlich geeigneter Garantien, einschließlich ordnungsgemäßer Verfahren nach dem Unionsrecht und dem Recht der Mitgliedstaaten. Hierdurch wird sichergestellt, dass von der oder dem Hessischen Datenschutzbeauftragten festgestellte Verstöße gegen die Vorschriften des Datenschutzes der jeweiligen öffentlichen Stelle mitgeteilt werden und vor der Ausübung der aufgezählten Abhilfebefugnisse des Art. 58 Abs. 2 Buchst. b bis g, i und j der Verordnung (EU) Nr. 2016/679 der öffentlichen Stelle unter Setzung einer angemessenen Frist Gelegenheit zur Stellungnahme gegeben wird. Bei den übrigen Abhilfebefugnissen des Art. 58 Abs. 2 der Verordnung (EU) Nr. 2016/679 besteht hingegen kein Bedarf an einer vorherigen Information. Durch die Mitteilung wird insbesondere gewährleistet, dass die öffentliche Stelle - unter den an § 28 Abs. 2 Nr. 1 und Abs. 3 HVwVfG angelehnten Ausnahmen für Eilfälle und entgegenstehende zwingende öffentliche Interessen - vor der Ausübung weitergehender Befugnisse durch die oder den Hessischen Datenschutzbeauftragten rechtliches Gehör findet.

Abs. 2 und 3 regeln die Befugnisse der oder des Hessischen Datenschutzbeauftragten bei allen Datenverarbeitungen, deren Zwecke außerhalb der Verordnung (EU) Nr. 2016/679 liegen, einschließlich solcher im Geltungsbereich der Richtlinie (EU) Nr. 2016/680.

Nach Abs. 2 steht der oder dem Hessischen Datenschutzbeauftragten mit der aus § 27 HDSG übernommenen Beanstandung gegenüber der obersten Landesbehörde oder dem vertretungsberechtigten Organ einer Kommune nebst Unterrichtung der zuständigen Aufsichtsbehörde ein der Datenschutzkontrolle bekanntes Handlungsinstrument zur Verfügung. Die Beanstandung ist vergleichbar mit dem in Art. 58 Abs. 2 Buchst. b der Verordnung (EU) Nr. 2016/679 vorgesehenen Instrument der Verwarnung. Darüber hinaus enthält Abs. 2 als weiteres regelungsbedürftiges Instrument die aus Art. 47 Abs. 2 Buchst. a der Richtlinie (EU) Nr. 2016/680 entnommene Warnung, den an Recht und Gesetz gebundenen Verantwortlichen auf datenschutzrechtliche Verstöße seiner beabsichtigten Verarbeitungsvorgänge aufmerksam zu machen und gibt der oder dem Hessischen Datenschutzbeauftragten damit eine weitere Möglichkeit, rechtswidrigen Zuständen abzuhelfen.

In Abs. 3 werden der oder dem Hessischen Datenschutzbeauftragten in Umsetzung von Art. 47 Abs. 2 Buchst. b der Richtlinie (EU) Nr. 2016/680 im Anwendungsbereich außerhalb der Verordnung (EU) Nr. 2016/679 über die Beanstandung nach Abs. 2 hinaus bestimmte Anordnungsbefugnisse zur Beseitigung erheblicher datenschutzrechtlicher Verstöße als wirksame Abhilfebefugnisse gegeben. HDSIG-E

In Abs. 4 und 5 werden für den gesamten Anwendungsbereich des HDSIG-E § 29 Abs. 1 und 2 HDSG zu den Zugangs- und Informationsrechten der oder des Hessischen Datenschutzbeauftragten in weiten Teilen übernommen. Hierdurch wird zugleich Art. 47 Abs. 1 der Richtlinie (EU) Nr. 2016/680 umgesetzt und die nach Art. 58 Abs. 1 Buchst. f der Verordnung (EU) Nr. 2016/679 zur Ausübung der Untersuchungsbefugnisse notwendigen mitgliedstaatlichen Verfahrensvorschriften für die Zugangs- und Betretungsrechte von Grundstücken und Diensträumen geschaffen (Nr. 3). Das umfassende Informationsrecht der oder des Hessischen Datenschutzbeauftragten in Nr. 1 und 2 erfolgt in Umsetzung des Art. 47 Abs. 1 der Richtlinie (EU) Nr. 2016/680 wortgleicher Anlehnung an Art. 58 Abs. 1 Buchst. a der Verordnung (EU) Nr. 2016/679.

Zu § 15 (Gutachten und Untersuchungen, Tätigkeitsbericht)
§ 15 Abs. 1 und 2 zur Erstattung von Gutachten und zur Durchführung von Untersuchungen in Datenschutzfragen und Fragen des freien Zugangs zu Informationen entsprechen inhaltlich der bisherigen Regelung des § 25 HDSG.

Abs. 3 bestimmt nach den Vorgaben des Art. 59 der Verordnung (EU) Nr. 2016/679 und Art. 49 der Richtlinie (EU) Nr. 2016/680, dass die oder der Hessische Datenschutzbeauftragte einen jährlichen Bericht über ihre oder seine Tätigkeit zu erstellen hat. Der Jahresbericht gilt sowohl für Datenverarbeitungen im Rahmen von Tätigkeiten, die dem Unionsrecht unterfallen als auch für solche, die nicht dem Unionsrecht unterfallen. Abs. 3 Satz 1 konkretisiert die Empfänger des in Art. 59 der Verordnung (EU) Nr. 2016/679 und Art. 49 der Richtlinie (EU) Nr. 2016/680 genannten Tätigkeitsberichts (Jahresbericht). Zudem wird der Bericht nach Abs. 3 Satz 2 der Öffentlichkeit, der Europäischen Kommission und dem Europäischen Datenschutzausschuss zugänglich gemacht (Art. 59 Satz 3 der Verordnung (EU) Nr. 2016/679 und Art. 49 Satz 3 der Richtlinie (EU) Nr. 2016/680). Abs. 4 übernimmt die Vorschrift des § 30 Abs. 2 HDSG. Gegenstand der zu dem Haupt- bzw. Zwischenbericht vorzulegenden Stellungnahme der Landesregierung bleibt dabei - wie im bisherigen Geltungsbereich des HDSG - die Datenverarbeitung durch öffentliche Stellen. Eine darüber hinaus gehende gesetzliche Verpflichtung der Landesregierung, zur Tätigkeit der oder des Hessischen Datenschutzbeauftragten als Aufsichtsbehörde über die nicht öffentlichen Stellen nach § 40 BDSG Stellung zu nehmen, besteht nicht.

Zu § 16 (Informationspflichten)
Abs. 1 der Vorschrift übernimmt die Regelung des § 29 Abs. 3 Var. 1 HDSG und Abs. 2 die Regelung aus § 26 HDSG.

Zu § 17 (Benachteiligungsverbot bei Anrufung der oder des Hessischen Datenschutzbeauftragten)
Ergänzend zu den Maßgaben des Art. 77 der Verordnung (EU) Nr. 2016/679 und § 55 werden die bisherigen Regelungen der § 28 Abs. 1 Satz 2 sowie Abs. 2 HDSG in die Vorschrift des § 17 HDSIG-E aufgenommen.

Zu § 18 (Personal- und Sachausstattung)
§ 18 enthält nach den Vorgaben des Art. 52 Abs. 4 und 5 der Verordnung (EU) Nr. 2016/679 sowie in Umsetzung des Art. 42 Abs. 4 und 5 der Richtlinie (EU) Nr. 2016/680 Regelungen zur näheren Ausgestaltung der Personal- und Sachausstattung der oder des Hessischen Datenschutzbeauftragten als oberster Landesbehörde.

Zu § 19 (Gerichtlicher Rechtsschutz)
§ 19 Abs. 1 stellt deklaratorisch klar, dass für Streitigkeiten zwischen einer natürlichen oder einer juristischen Person und der oder dem Hessischen Datenschutzbeauftragten der Verwaltungsrechtsweg eröffnet ist, soweit nicht durch bereichsspezifische Rechtsvorschriften der Rechtsweg vor anderen Gerichten als den Gerichten der Verwaltungsgerichtsbarkeit eröffnet ist.

Abs. 2 erklärt § 20 Abs. 2, 3, 5 und 7 des Bundesdatenschutzgesetzes für Verfahren nach Abs. 1 Satz 1 für entsprechend anwendbar. Soweit § 73 des Hessischen Verwaltungsvollstreckungsgesetzes (HVwVG) Anwendung findet, ist einstweiliger Rechtsschutz über das Verfahren bei einstweiligen Anordnungen nach § 123 VwGO eröffnet.

Abs. 3 ist eine Bestimmung im Sinne von § 61 Nr. 3 VwGO.

Abs. 4 erklärt für Klagen betroffener Personen gegen einen Verantwortlichen oder einen Auftragsverarbeiter wegen eines Verstoßes gegen datenschutzrechtliche Bestimmungen im Anwendungsbereich der Verordnung (EU) Nr. 2016/679 oder der darin enthaltenen Rechte der betroffenen Person § 44 des Bundesdatenschutzgesetzes für entsprechend anwendbar.

Abs. 5 Satz 1 statuiert - auch in Verbindung mit § 56 - die Zulässigkeit eines Insichprozesses zwischen einer Behörde oder anderen öffentlichen Stelle des Landes einerseits und der oder dem Hessischen Datenschutzbeauftragten andererseits. Satz 2 sieht für die oder den Hessischen Datenschutzbeauftragten die Möglichkeit zur gerichtlichen Feststellung der Rechtmäßigkeit seiner getroffenen verbindlichen Entscheidung vor, sofern die Behörde oder sonstige öffentliche Stelle des Landes nicht innerhalb eines Monats nach Bekanntgabe der verbindlichen Entscheidung Klage hiergegen erhoben hat. Damit wird erreicht, dass den Justizbehörden auch im Innenverhältnis des Landes Verstöße gegen das Datenschutzrecht zur Kenntnis gebracht werden. Abs. 6 sieht vor, dass im Falle der datenschutzaufsichtlichen Anordnung einer Löschung personenbezogener Daten aufgrund deren irreversiblen Charakters einer seitens der betroffenen Behörde oder sonstigen öffentlichen Stelle des Landes erhobenen Klage aufschiebende Wirkung zukommt.

Zu § 20 (Verarbeitung besonderer Kategorien personenbezogener Daten)
Nach Art. 9 Abs. 1 der Verordnung (EU) Nr. 2016/679 ist die Verarbeitung besonderer Kategorien personenbezogener Daten grundsätzlich untersagt. Art. 9 Abs. 2 der Verordnung (EU) Nr. 2016/679 sieht jedoch Ausnahmen von diesem Verbot vor. In den Fällen des Art. 9 Abs. 2 Buchst. b, g, h und i der Verordnung (EU) Nr. 2016/679 sind die Ausnahmen durch nationale Regelungen auszugestalten.

§ 20 Abs. 1 legt in Ausgestaltung des Art. 9 Abs. 2 Buchst. b, g, h und i der Verordnung (EU) Nr. 2016/679 neben den übrigen Ausnahmen des Art. 9 Abs. 2 der Verordnung (EU) Nr. 2016/679 fest, unter welchen Voraussetzungen die Verarbeitung besonderer Kategorien personenbezogener Daten ausnahmsweise zulässig ist. Die Verarbeitung besonderer Kategorien personenbezogener Daten ist nicht nur auf dieser Rechtsgrundlage zulässig, sondern etwa auch auf der Grundlage der sich unmittelbar aus Art. 9 Abs. 2 der Verordnung (EU) Nr. 2016/679 ergebenden Ausnahmetatbestände, einschließlich sonstiger auf der Grundlage der Verordnung (EU) Nr. 2016/679 erlassenen bereichsspezifischen Regelungen.

Im Einzelnen wird mit der Vorschrift von den Öffnungsklauseln des Art. 9 Abs. 2 Buchstabe b der Verordnung (EU) Nr. 2016/679 (in Bezug auf Abs. 1 Nr. 1), des Art. 9 Abs. 2 Buchst. h i.V.m. Abs. 3 der Verordnung (EU) Nr. 2016/679 (in Bezug auf Abs. 1 Nr. 2), des Art. 9 Abs. 2 Buchst. i der Verordnung (EU) Nr. 2016/679 (in Bezug auf Abs. 1 Nr. 3) und des Art. 9 Abs. 2 Buchst. g der Verordnung (EU) Nr. 2016/679 (in Bezug auf Abs. 1 Nr. 4 Buchst a bis d) Gebrauch gemacht.

Abs. 1 Nr. 2, der Art. 9 Abs. 2 Buchst. h der Verordnung (EU) Nr. 2016/679 ausgestaltet, verzichtet auf eine explizite Nennung des öffentlichen Gesundheitsdienstes oder der Arbeitsmedizin, da der Begriff der Gesundheitsvorsorge diese beinhaltet. Die Verarbeitung erfolgt jeweils entsprechend den inhaltlichen Zwecken, die sich aus Nr. 2 oder dem bereichsspezifischen Recht ergeben.

Der zweite Halbsatz in Abs. 1 Nr. 3 dient der Klarstellung des Art. 9 Abs. 2 Buchst. i der Verordnung (EU) Nr. 2016/679: Das deutsche Recht sieht umfangreiche angemessene und spezifische Maßnahmen zum Schutz des Berufsgeheimnisses vor, insbesondere durch § 203 StGB und die einschlägigen Berufsordnungen. Daneben können auch die in § 20 Abs. 2 genannten Maßnahmen der Wahrung des Berufsgeheimnisses dienen.

Die Verarbeitung besonderer Kategorien personenbezogener Daten nach Abs. 1 Nr. 4 Buchst. a bis c erfordert zusätzlich eine Interessenabwägung, wie dies Art. 9 Abs. 2 Buchst. g der Verordnung (EU) Nr. 2016/679 vorsieht, sodass die Verarbeitung in einem angemessenen Verhältnis zu dem verfolgten Zweck stehen und den Wesensgehalt des Rechts auf Datenschutz wahren muss. Ein erhebliches öffentliches Interesse nach Abs. 1 Nr. 4 Buchst. a ist insbesondere in den Fällen anzunehmen, in denen biometrische Daten zu Zwecken der eindeutigen Identifikation Betroffener rechtmäßig verarbeitet werden.

Abs. 2 Satz 1 und 2 setzt das Erfordernis aus Art. 9 Abs. 2 Buchst. b, g und i der Verordnung (EU) Nr. 2016/679 um, "geeignete Garantien für die Grundrechte und die Interessen der betroffenen Person" bzw. "angemessene und spezifische Maßnahmen zur Wahrung der Grundrechte und Interessen der betroffenen Person" vorzusehen.

In Abs. 3 wird die Bestimmung des § 10 Abs. 3 HDSG übernommen.

Zu § 21 (Verarbeitung zu anderen Zwecken)
Mit der Vorschrift wird von dem durch die Verordnung (EU) Nr. 2016/679 eröffneten Regelungsspielraum Gebrauch gemacht, wonach die Mitgliedstaaten nationale Regelungen in Fällen, in denen die Weiterverarbeitung der personenbezogenen Daten nicht dem Zweck bei Erhebung der Daten entspricht, erlassen dürfen, soweit die nationale Regelung eine in einer demokratischen Gesellschaft "notwendige und verhältnismäßige Maßnahme zum Schutz der in Artikel 23 Absatz 1 genannten Ziele darstellt" (Art. 6 Abs. 4 und Erwägungsgrund 50 der Verordnung (EU) Nr. 2016/679). Die Regelung ersetzt teilweise die §§ 11 Abs. 1, 13 Abs. 2 i.V.m. 12 Abs. 2 und 3 sowie § 13 Abs. 4 HDSG.

Abs. 1 schafft für öffentliche Stellen im Rahmen der jeweiligen Aufgabenerfüllung eine landesrechtliche Rechtsgrundlage für die Verarbeitung personenbezogener Daten durch denselben Verarbeiter zu einem anderen Zweck als zu demjenigen, zu dem er sie ursprünglich erhoben hat (Weiterverarbeitung). Soweit eine der tatbestandlichen Voraussetzungen nach Abs. 1 erfüllt ist, kann die Weiterverarbeitung personenbezogener Daten durch öffentliche Stellen auf diese Vorschrift gestützt werden.

Abs. 2 stellt für die Weiterverarbeitung besonderer Kategorien personenbezogener Daten im Sinne des Art. 9 Abs. 1 der Verordnung (EU) Nr. 2016/679 klar, dass neben dem Vorliegen einer der tatbestandlichen Voraussetzungen des Abs. 1 auch ein Ausnahmetatbestand nach Art. 9 Abs. 2 der Verordnung (EU) Nr. 2016/679 oder nach § 20 Abs. 1 HDSIG-E vorliegen muss. Abs. 3 übernimmt die Regelung des § 13 Abs. 5 HDSG.

Zu § 22 (Datenübermittlungen durch öffentliche Stellen)
Die Vorschrift schafft eine Rechtsgrundlage für die Übermittlung personenbezogener Daten durch öffentliche Stellen, soweit diese zu einem anderen Zweck als zu demjenigen, zu dem die Daten erhoben wurden, erfolgt. Die Regelung findet auch auf die Fälle Anwendung, in denen eine öffentliche Stelle Daten, die sie ursprünglich zu Zwecken nach § 40 HDSIG-E erhoben hat, an einen Dritten übermittelt, der die Daten zu Zwecken der Verordnung (EU) Nr. 2016/679 verarbeiten möchte. Die Vorschrift macht von dem durch die Verordnung (EU) Nr. 2016/679 eröffneten Regelungsspielraum Gebrauch (Art. 6 Abs. 4 und Erwägungsgrund 50 der Verordnung (EU) Nr. 2016/679) und ersetzt teilweise die §§ 11 Abs. 1, 13 Abs. 2 i.V.m. 12 Abs. 2 und 3, 13 Abs. 4, 16, 17 Abs. 1 HDSG.

Abs. 1 regelt die tatbestandlichen Voraussetzungen der Datenübermittlung von öffentlichen Stellen an öffentliche Stellen, soweit diese zur Aufgabenerfüllung erforderlich sind. Eine Übermittlung ist zulässig, wenn die Voraussetzungen für eine Verarbeitung zu einem anderen Zweck nach § 21 HDSIG-E vorliegen.

Abs. 2 regelt die tatbestandlichen Voraussetzungen der Datenübermittlung von öffentlichen Stellen an nicht öffentliche Stellen. Die hier entstehenden Informationspflichten ergeben sich unmittelbar aus Art. 13 Abs. 3 bzw. Art. 14 Abs. 4 der Verordnung (EU) Nr. 2016/679.

Abs. 3 stellt für die Übermittlung besonderer Kategorien personenbezogener Daten klar, dass neben dem Vorliegen einer der tatbestandlichen Voraussetzungen der Abs. 1 oder 2 auch ein Ausnahmetatbestand nach Art. 9 Abs. 2 der Verordnung (EU) Nr. 2016/679 oder nach § 20 Abs. 1 HDSIG-E vorliegen muss.

Abs. 4 übernimmt die Regelung des § 14 HDSG zur Verantwortlichkeit für die Zulässigkeit der Datenübermittlung.

Zu § 23 (Datenverarbeitung für Zwecke des Beschäftigungsverhältnisses)
Die Öffnungsklausel des Art. 88 der Verordnung (EU) Nr. 2016/679 lässt nationale Regelungen zur Datenverarbeitung im Beschäftigungskontext zu. Mit § 23 HDSIG-E wird hiervon Gebrauch gemacht.

Abs. 1 regelt, zu welchen Zwecken und unter welchen Voraussetzungen personenbezogene Daten vor, im und nach dem Beschäftigungsverhältnis verarbeitet werden dürfen, wenn dies zum Zweck des Beschäftigungsverhältnisses erforderlich ist. Dabei sind die Interessen des Dienstherrn oder Arbeitgebers an der Datenverarbeitung und das Persönlichkeitsrecht der oder des Beschäftigten zu einem schonenden Ausgleich zu bringen, der beide Interessen möglichst weitgehend berücksichtigt. Abs. 1 Satz 1 i.V.m. Abs. 5 dient auch der Ausgestaltung von Art. 10 der Verordnung (EU) Nr. 2016/679, der es den Mitgliedstaaten ermöglicht, die Verarbeitung personenbezogener Daten über strafrechtliche Verurteilungen und Straftaten oder damit zusammenhängende Sicherungsmaßregeln im Beschäftigungskontext zuzulassen. Satz 3 regelt die Voraussetzungen für die Verarbeitung personenbezogener Daten von Beschäftigten zur Aufdeckung von Straftaten, die im Beschäftigungsverhältnis begangen worden sind.

Abs. 2 regelt die Verarbeitung personenbezogener Daten von Beschäftigten auf Grundlage einer Einwilligung und trägt dabei der Besonderheit des Beschäftigungsverhältnisses als Abhängigkeitsverhältnis und der daraus resultierenden Situation der Beschäftigten Rechnung. Nach Erwägungsgrund 155 der Verordnung (EU) Nr. 2016/679 können insbesondere Vorschriften über die Bedingungen erlassen werden, unter denen personenbezogene Daten im Beschäftigungskontext auf der Grundlage einer Einwilligung der Beschäftigten verarbeitet werden dürfen. Als Voraussetzung einer Einwilligung ist grundsätzlich die Schriftform vorgesehen. Damit wird die Nachweispflicht des Dienstherrn oder Arbeitgebers im Sinne von Art. 7 Abs. 1 der Verordnung (EU) Nr. 2016/679 konkretisiert. Des Weiteren wird der Dienstherr oder Arbeitgeber zur Aufklärung in Textform über den Zweck der Datenverarbeitung und den jederzeit möglichen Widerruf durch die oder den Beschäftigten sowie dessen Folgen nach Art. 7 Abs. 3 der Verordnung (EU) Nr. 2016/679 verpflichtet.

Abs. 3 dient der Ausgestaltung von Art. 9 Abs. 2 Buchst. b der Verordnung (EU) Nr. 2016/679. Die Zulässigkeit der Verarbeitung besonderer Kategorien personenbezogener Daten für andere Zwecke bleibt unberührt; zum Beispiel richtet sich diese im Fall der Verarbeitung zu Zwecken der Gesundheitsvorsorge nach § 20 Abs. 1 Nr. 2 HDSIG-E. Die Vorgaben des Abs. 2 gelten auch für die Einwilligung in die Verarbeitung besonderer Kategorien personenbezogener Daten, wie z.B. von Gesundheitsdaten, wobei sich die Einwilligung ausdrücklich auf diese Daten beziehen muss. Nach Art. 9 Abs. 2 Buchst. b der Verordnung (EU) Nr. 2016/679 muss die nationale Regelung geeignete Garantien für die Grundrechte und die Interessen der betroffenen Person vorsehen, was mit dem Verweis auf § 20 Abs. 2 HDSIG-E geschieht.

Abs. 4 Satz 1 sieht vor, dass die Verarbeitung personenbezogener Beschäftigtendaten aufgrund von Kollektivvereinbarungen zulässig ist. Art. 88 Abs. 1 der Verordnung (EU) Nr. 2016/679 ermöglicht es, spezifischere Regelungen zum Datenschutz im Beschäftigungskontext in Kollektivvereinbarungen zu treffen. Im Hinblick auf besondere Kategorien personenbezogener Daten ist Art. 9 Abs. 2 Buchst. b der Verordnung (EU) Nr. 2016/679 einschlägig. Satz 2 bestimmt, dass auch Art. 88 Abs. 2 der Verordnung (EU) Nr. 2016/679 zu beachten ist.

Abs. 5 bestimmt, dass der Verantwortliche geeignete Maßnahmen zur Wahrung der Grundrechte und Interessen der oder des Beschäftigten ergreifen muss. Dabei wird auch dem Erfordernis aus Art. 10 der Verordnung (EU) Nr. 2016/679 Rechnung getragen, geeignete Garantien für die Rechte und Freiheiten der Beschäftigten vorzusehen.

Abs. 6 stellt klar, dass die Beteiligungsrechte der Interessenvertretungen der Beschäftigten unberührt bleiben.

Abs. 7 Satz 1 legt fest, dass Abs. 1 bis 6 über Art. 2 Abs. 1 der Verordnung (EU) Nr. 2016/679 hinaus auch im Beschäftigungsverhältnis gelten, wenn personenbezogene Daten, einschließlich besonderer Kategorien personenbezogener Daten, von Beschäftigten verarbeitet werden, ohne dass sie in einem Dateisystem gespeichert sind oder gespeichert werden sollen. Satz 2 übernimmt die Regelung des § 34 Abs. 1 Satz 2 HDSG.

Abs. 8 Satz 1 enthält eine Bestimmung des Begriffs "Beschäftigte" im Sinne des HDSIG-E. Abs. 8 Satz 2 stellt klar, dass Bewerberinnen und Bewerber sowie Personen, deren Beschäftigungsverhältnis beendet ist, als Beschäftigte gelten.

Zu § 24 (Datenverarbeitung zu wissenschaftlichen oder historischen Forschungszwecken und zu statistischen Zwecken)
Mit § 24 Abs. 1 HDSIG-E wird von dem Ausnahmetatbestand des Art. 9 Abs. 2 Buchst. j i.V.m. Art. 89 Abs. 1 der Verordnung (EU) Nr. 2016/679 Gebrauch gemacht und eine Regelung für die Zulässigkeit der Verarbeitung besonderer Kategorien personenbezogener Daten zu wissenschaftli-

chen oder historischen Forschungszwecken oder zu statistischen Zwecken geschaffen. Art. 9 Abs. 2 der Verordnung (EU) Nr. 2016/679 sieht Ausnahmen von dem Verbot der Verarbeitung besonderer Kategorien personenbezogener Daten nach Art. 9 Abs. 1 der Verordnung vor. Die Verarbeitung von nicht unter Art. 9 der Verordnung (EU) Nr. 2016/679 fallenden Daten richtet sich nicht nach § 24 HDSIG-E, sondern entweder unmittelbar nach der Verordnung (EU) Nr. 2016/679 (insbesondere nach Art. 6 Abs. 1) oder nach im Einklang mit der Verordnung erlassenen Rechtsgrundlagen. Art. 9 Abs. 2 Buchst. j der Verordnung (EU) Nr. 2016/679 erfordert, dass die Datenverarbeitung für wissenschaftliche oder historische Forschungszwecke in angemessenem Verhältnis zu dem verfolgten Ziel steht, den Wesensgehalt des Rechts auf Datenschutz wahrt sowie angemessene und spezifische Maßnahmen zur Wahrung der Grundrechte und Interessen der betroffenen Person vorsieht. Dem trägt der Verweis auf § 20 Abs. 2 Satz 2 HDSIG-E Rechnung.

Die Weiterverarbeitung personenbezogener Daten durch öffentliche Stellen für wissenschaftliche oder historische Forschungszwecke und für statistische Zwecke gilt nach Art. 5 Abs. 1 Buchst. b der Verordnung (EU) Nr. 2016/679 als nicht unvereinbar mit den ursprünglichen Zwecken. Daher kann sich der Verantwortliche hinsichtlich der Weiterverarbeitung auf diejenige Rechtsgrundlage stützen, die bereits für die Erstverarbeitung Anwendung gefunden hat. Dies trifft auch auf die Weiterverarbeitung besonderer Kategorien personenbezogener Daten zu, für die § 24 Abs. 1 HDSIG-E als Ausnahmetatbestand von dem Verbot des Art. 9 Abs. 1 der Verordnung (EU) Nr. 2016/679 gilt. § 21 HDSIG-E findet insoweit keine Anwendung. Entsprechendes gilt für die Übermittlung besonderer Kategorien von Daten durch öffentliche Stellen zu wissenschaftlichen oder historischen Forschungszwecken und zu statistischen Zwecken. Die Regelung des § 22 HDSIG-E findet ebenfalls keine Anwendung.

§ 24 Abs. 2 Satz 1 HDSIG-E schränkt unter Nutzung der Öffnungsklausel des Art. 89 Abs. 2 der Verordnung (EU) Nr. 2016/679 die Rechte nach Art. 15, 16, 18 und 21 der Verordnung (EU) Nr. 2016/679 ein. Darüber hinaus schränkt Abs. 2 Satz 2 das Auskunftsrecht für die Fälle unverhältnismäßigen Aufwands unter Nutzung der Öffnungsklausel des Art. 23 Abs. 1 Buchst. i der Verordnung (EU) Nr. 2016/679 ein, z.B. bei einem Forschungsvorhaben mit besonders großen Datenmengen. Die Einschränkung der Betroffenenrechte in Abs. 2 gilt für alle Kategorien personenbezogener Daten.

Abs. 3 übernimmt Elemente des § 33 Abs. 2 HDSG; Abs. 4 regelt die Voraussetzungen für eine Veröffentlichung personenbezogener Daten.

Zu § 25 (Datenverarbeitung zu im öffentlichen Interesse liegenden Archivzwecken)
Mit § 25 Abs. 1 wird von dem Ausnahmetatbestand des Art. 9 Abs. 2 Buchst. j der Verordnung (EU) Nr. 2016/679 Gebrauch gemacht und eine Regelung für die Zulässigkeit der Verarbeitung besonderer Kategorien personenbezogener Daten zu im öffentlichen Interesse liegenden Archivzwecken geschaffen. Art. 9 Abs. 2 der Verordnung (EU) Nr. 2016/679 sieht Ausnahmen von dem Verbot der Verarbeitung besonderer Kategorien personenbezogener Daten in Art. 9 Abs. 1 der Verordnung vor. § 25 Abs. 1 HDSIG-E gilt nur für die Verarbeitung von Daten im Sinne von Art. 9 Abs. 1 der Verordnung (EU) Nr. 2016/679. Die Verarbeitung von nicht unter Art. 9 der Verordnung (EU) Nr. 2016/679 fallenden Daten richtet sich nicht nach § 25 HDSIG-E, sondern entweder unmittelbar nach der Verordnung (EU) Nr. 2016/679 (insbesondere Art. 6 Abs. 1) oder nach im Einklang mit der Verordnung erlassenen Rechtsgrundlagen. Art. 9 Abs. 2 Buchst. j der Verordnung (EU) Nr. 2016/679 sieht vor, dass die Datenverarbeitung für im öffentlichen Interesse liegende Archivzwecke in angemessenem Verhältnis zu dem verfolgten Ziel steht, den Wesensgehalt des Rechts auf Datenschutz wahrt sowie angemessene und spezifische Maßnahmen zur Wahrung der Grundrechte und Interessen der betroffenen Person vorsieht. Dem trägt der Verweis auf § 20 Abs. 2 Satz 2 HDSIG-E Rechnung.

Die Weiterverarbeitung personenbezogener Daten durch öffentliche Stellen zu im öffentlichen Interesse liegenden Archivzwecken gilt nach Art. 5 Abs. 1 Buchst. b der Verordnung (EU) Nr. 2016/679 als nicht unvereinbar mit den ursprünglichen Zwecken. Daher kann sich der Verantwortliche hinsichtlich der Weiterverarbeitung auf diejenige Rechtsgrundlage stützen, die bereits für die Erstverarbeitung Anwendung gefunden hat. Dies trifft auch auf die Weiterverarbeitung besonderer Kategorien personenbezogener Daten zu, für die § 25 Abs. 1 HDSIG-E als Ausnahmetatbestand von dem Verbot des Art. 9 Abs. 1 der Verordnung (EU) Nr. 2016/679 gilt. § 21 HDSIG-E findet insoweit keine Anwendung. Entsprechendes gilt für die Übermittlung besonderer Kategorien von Daten durch öffentliche Stellen zu im öffentlichen Interesse liegenden Archivzwecken. Die Regelung des § 22 HDSIG-E findet insoweit keine Anwendung.

Abs. 2 bis 4 schränken unter Nutzung der Öffnungsklausel des Art. 89 Abs. 3 der Verordnung (EU) Nr. 2016/679 die Rechte nach Art. 15, 16, 18, 20 und 21 der Verordnung (EU) Nr. 2016/679 ein. Abs. 2 bezieht sich hierbei auf sämtliche durch Art. 15 der Verordnung (EU) Nr. 2016/679 gewährten Rechte.

Zu § 26 (Rechte der betroffenen Person und aufsichtsbehördliche Untersuchungen im Fall von Geheimhaltungspflichten)
Auf der Grundlage der Öffnungsklausel des Art. 23 Abs. 1 Buchst. i der Verordnung (EU) Nr. 2016/679 beschränkt Abs. 1 das Recht auf Information der betroffenen Person, soweit durch deren Erfüllung Informationen offenbart würden, die geheim gehalten werden müssen. Abs. 1 bezieht sich hierbei nicht auf die nach Rechtsvorschriften bestehenden Geheimhaltungspflichten, da die Informationspflicht insoweit bereits unmittelbar durch Art. 14 Abs. 5 Buchst. d der Verordnung (EU) Nr. 2016/679 beschränkt wird.

Abs. 2 schränkt das Recht auf Auskunft für die Fälle ein, in denen Informationen nach einer Rechtsvorschrift oder ihrem Wesen nach geheim gehalten werden müssen.

Abs. 3 bezieht sich auf eine Beschränkung der Benachrichtigungspflicht nach Art. 34 der Verordnung (EU) Nr. 2016/679.

Die Einschränkung der Informationspflicht nach Abs. 4 beruht auf der Öffnungsklausel des Art. 23 Abs. 1 Buchst. i der Verordnung (EU) Nr. 2016/679 und dient dem Schutz der ungehinderten Kommunikation zwischen Mandant und Berufsgeheimnisträger. Es widerspräche dem besonderen Schutz eines Mandatsverhältnisses, wenn beispielsweise sämtliche durch die Datenübermittlung an den Berufsgeheimnisträger betroffene Personen über die Zwecke der Datenübermittlung und die Identität der beauftragten Berufsgeheimnisträger informiert werden müssten. Durch die in Abs. 2, letzter Halbsatz eingefügte Abwägungsklausel wird den Rechten der Betroffenen angemessen Rechnung getragen.

Abs. 5 erstreckt die Geheimhaltungspflicht auf die oder den Hessischen Datenschutzbeauftragten. Erlangt die oder der Hessische Datenschutzbeauftragte im Rahmen einer Untersuchung Kenntnis von Daten, die einer Geheimhaltungspflicht unterliegen, gilt die Geheimhaltungspflicht auch für die oder den Hessischen Datenschutzbeauftragten und seine Beschäftigten.

Zu § 27 (Datenübermittlung an öffentlich-rechtliche Religionsgemeinschaften)
Die Vorschrift zur Datenübermittlung an öffentlich-rechtliche Religionsgemeinschaften löst die bisherige Regelung des § 35 HDSG ab und trägt den Maßgaben des Art. 91 der Verordnung (EU) Nr. 2016/679 Rechnung.

Zu § 28 (Datenverarbeitung des Hessischen Rundfunks zu journalistischen Zwecken)
Die Vorschrift über die Datenverarbeitung des Hessischen Rundfunks zu journalistischen Zwecken übernimmt die bisherige Regelung des § 37 HDSG und gestaltet den Regelungsauftrag des Art. 85 der Verordnung (EU) Nr. 2016/679 aus.

Zu § 29 (Auskunftsrecht des Landtags und der kommunalen Vertretungsorgane)
Die Vorschrift zum Auskunftsrecht des Landtags und der kommunalen Vertretungsorgane übernimmt die bisherige Regelung des § 38 HDSG.

Zu § 30 (Verarbeitung personenbezogener Daten durch den Landtag und die kommunalen Vertretungsorgane)
Die Vorschrift über die Verarbeitung personenbezogener Daten durch den Landtag und die kommunalen Vertretungsorgane übernimmt die bisherige Regelung des § 39 HDSG.

Zu §§ 31 bis 35 (Rechte der betroffenen Person)
Art. 23 der Verordnung (EU) Nr. 2016/679 sieht vor, dass die Rechte und Pflichten nach Art. 12 bis 22 und Art. 34 sowie die in Art. 5 geregelten Grundsätze für die Verarbeitung personenbezogener Daten, sofern dessen Bestimmungen den in Art. 12 bis 22 vorgesehenen Rechten und Pflichten entsprechen, durch Rechtsvorschriften der Union oder der Mitgliedstaaten beschränkt werden können. Die Beschränkung muss den Wesensgehalt der Grundrechte und Grundfreiheiten achten und in einer demokratischen Gesellschaft eine notwendige und verhältnismäßige Maßnahme darstellen, um die in Art. 23 Abs. 1 Buchst. a bis j aufgezählten Ziele sicherzustellen. Art. 23 der Verordnung (EU) Nr. 2016/679 verlangt besondere Maßnahmen zum Schutz der Grundrechte und Grundfreiheiten der von der Beschränkung betroffenen Person. Insbesondere muss nach Art. 23 Abs. 2 der Verordnung (EU) Nr. 2016/679 jede Gesetzgebungsmaßnahme "insbesondere gegebenenfalls spezifische Vorschriften" zumindest in Bezug auf die in Art. 23 Abs. 2 der Verordnung (EU) Nr. 2016/679 Buchst. a bis h aufgezählten Maßnahmen enthalten.

Die in den Zweiten Abschnitt aufgenommenen Einschränkungen der Betroffenenrechte sowie Pflichten des Verantwortlichen und des Auftragsverarbeiters ergänzen die in der Verordnung (EU) Nr. 2016/679 unmittelbar vorgesehenen Ausnahmen. Die Beschränkungen der Betroffenenrechte finden auch Anwendung auf die in Art. 89 der Verordnung (EU) Nr. 2016/679 geregelte Verarbeitung zu im öffentlichen Interesse liegenden Archivzwecken, zu wissenschaftlichen oder historischen Forschungszwecken und zu statistischen Zwecken. Zwar bestimmt Art. 89 Abs. 2 und 3 der Verordnung (EU) Nr. 2016/679, dass bei einer Verarbeitung zu den dort genannten Forschungs- und statistischen Zwecken Mitgliedstaaten insoweit Ausnahmen von den Rechten nach

Art. 15, 16, 18 und 21 sowie bei der Verarbeitung zu im öffentlichen Interesse liegenden Archivzwecken zusätzlich nach Art. 19 und 20 vorsehen können, als diese Rechte voraussichtlich die Verwirklichung der spezifischen Zwecke unmöglich machen oder ernsthaft beeinträchtigen und solche Ausnahmen für die Erfüllung dieser Zwecke notwendig sind. Eine Beschränkung der Betroffenenrechte muss jedoch nicht nur nach Art. 89 Abs. 2 und 3, sondern auch nach Art. 23 der Verordnung (EU) Nr. 2016/679 möglich sein, da die Verarbeitung zu den in Art. 89 genannten Zwecken andernfalls gegenüber sonstigen Verarbeitungen schlechter gestellt wäre, obwohl der Verordnungsgeber die Verarbeitung zu Archiv-, Forschungs- und Statistikzwecken ausweislich der Sonderregelung in Kapitel IX der Verordnung (EU) Nr. 2016/679 privilegieren wollte.

Zu § 31 (Informationspflicht bei der Erhebung von personenbezogenen Daten bei der betroffenen Person)

Die in Abs. 1 Satz 1 vorgesehene Beschränkung der Informationspflicht gilt nur für die in Art. 13 Abs. 3 der Verordnung (EU) Nr. 2016/679 vorgesehene Fallgruppe, dass der Verantwortliche beabsichtigt, die personenbezogenen Daten für einen anderen Zweck weiterzuverarbeiten als denjenigen, für den die Daten bei der betroffenen Person erhoben wurden. Die Informationspflicht aus Art. 13 Abs. 1 und 2 der Verordnung (EU) Nr. 2016/679 wird demgegenüber nicht beschränkt.

Die mit der Verordnung (EU) Nr. 2016/679 erstmals eingeführte Informationspflicht des Verantwortlichen bei beabsichtigter Zweckänderung findet im HDSG bislang keine Entsprechung. In dieser Konstellation besteht im Gegensatz zu der in Art. 13 Abs. 1 und 2 der Verordnung (EU) Nr. 2016/679 vorgesehenen Informationspflicht zum Zeitpunkt der Erhebung der Daten typischerweise kein unmittelbarer Kontakt zwischen dem Verantwortlichen und der betroffenen Person.

Abs. 1 Satz 1 Nr. 1 enthält eine Ausnahme von der Informationspflicht für mit dem ursprünglichen Erhebungszweck vereinbare Weiterverarbeitungen personenbezogener Daten. Voraussetzung ist, dass die Kommunikation mit der betroffenen Person ausschließlich oder überwiegend nicht in digitaler Form erfolgt und das Interesse der betroffenen Person an der Informationserteilung nach den Umständen des Einzelfalls als gering anzusehen ist. Nr. 2 Buchst. a bis c und Buchst. e enthalten Einschränkungen der Informationspflicht, wenn die Erteilung der Information über die beabsichtigte Weiterverarbeitung die ordnungsgemäße Erfüllung der in der Zuständigkeit des Verantwortlichen liegenden Aufgaben (Nr. 2 Buchst. a), die öffentliche Sicherheit oder Ordnung (Nr. 2 Buchst. b) oder Rechte oder Freiheiten Dritter (Nr. 2 Buchst. c) gefährden oder sonst dem Wohle des Bundes oder eines Landes Nachteile bereiten würde (Nr. 2 Buchst. e). Nr. 2 Buchst. d sieht eine Einschränkung zur Sicherstellung der Geltendmachung, Ausübung oder Verteidigung rechtlicher Ansprüche vor (Art. 23 Abs. 1 Buchst. j der Verordnung (EU) Nr. 2016/679. Nr. 3 schützt die vertrauliche Übermittlung von Daten an öffentliche Stellen (Art. 23 Abs. 1 Buchst. e der Verordnung Nr. 2016/679). Erfasst sind beispielsweise Fallgruppen, in denen die Information der betroffenen Person über die Weiterverarbeitung zu einer Vereitelung oder ernsthaften Beeinträchtigung des - legitimen - Verarbeitungszwecks führen würde, etwa wenn die zuständige Strafverfolgungsbehörde über den Verdacht einer Straftat informiert werden soll. Einschränkende Voraussetzung ist in den Fällen der Nr. 2 Buchst. a bis e, dass die Interessen des Verantwortlichen an der Nichterteilung der Information die Interessen der betroffenen Person überwiegen.

Abs. 1 Satz 2 übernimmt den Rechtsgedanken aus § 18 Abs. 6 Satz 2 HDSG und § 29 Abs. 3 Satz 2 des Hessischen Gesetzes über die öffentliche Sicherheit und Ordnung (HSOG).

Abs. 2 legt fest, dass der Verantwortliche geeignete Maßnahmen zum Schutz der berechtigten Interessen der betroffenen Person zu treffen hat, wenn eine Information der betroffenen Person nach Maßgabe des Abs. 1 unterbleibt. Hierdurch werden die nach Art. 23 Abs. 2 der Verordnung (EU) Nr. 2016/679 erforderlichen Schutzmaßnahmen beachtet. Zu den geeigneten Maßnahmen zählt die Bereitstellung dieser Informationen für die Öffentlichkeit. Eine Veröffentlichung in allgemein zugänglicher Form kann etwa die Bereitstellung der Information auf einer allgemein zugänglichen Internetseite des Verantwortlichen sein (Erwägungsgrund 58 Satz 2 der Verordnung (EU) Nr. 2016/679). Die Information hat in Entsprechung zu Art. 12 Abs. 1 der Verordnung (EU) Nr. 2016/679 in präziser, transparenter, verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache zu erfolgen.

Der Verantwortliche hat schriftlich zu dokumentieren, aus welchen Gründen er von einer Information abgesehen hat. Die Stichhaltigkeit der Gründe unterliegt der Kontrolle durch die zuständige Aufsichtsbehörde, die durch die Dokumentationspflicht ermöglicht wird. Die in Abs. 2 Satz 1 und 2 zum Schutz der berechtigten Interessen der betroffenen Person geforderten Maßnahmen des Verantwortlichen finden im Fall des Abs. 1 Nr. 2 Buchst. d und Nr. 3 keine Anwendung. Andernfalls könnten die in Satz 1 und 2 geforderten Maßnahmen zu einer Vereitelung oder ernsthaften Beeinträchtigung des - legitimen - Verarbeitungszwecks führen.

Abs. 3 bestimmt, dass der Verantwortliche die Information der betroffenen Person zeitnah nachzuholen hat, wenn die Ausschlussgründe des Abs. 1 nur vorübergehend vorliegen.

Zu § 32 (Informationspflicht, wenn die personenbezogenen Daten nicht bei der betroffenen Person erhoben wurden)
§ 32 Abs. 1 Satz 1 HDSIG-E enthält in Ergänzung der in Art. 14 Abs. 5 der Verordnung (EU) Nr. 2016/679 und in § 26 Abs. 1 HDSIG-E genannten Ausnahmen Einschränkungen der Informationspflicht des Verantwortlichen aus Art. 14 Abs. 1, 2 und 4 der Verordnung (EU) Nr. 2016/679. Hinsichtlich der Ausnahmen in Abs. 1 Nr. 1 und 2 wird auf die Begründung zu § 31 Abs. 1 Nr. 2 Buchst. a und b HDSIG-E verwiesen. Abs. 1 Satz 2 übernimmt den Rechtsgedanken aus § 18 Abs. 6 Satz 2 HDSG und § 29 Abs. 3 Satz 2 HSOG.

Abs. 2 entspricht § 31 Abs. 2 Satz 1 und 2 HDSIG-E, sodass auf die dortige Begründung verwiesen wird. Abs. 3 betrifft den Fall der Informationserteilung bei Datenübermittlung durch öffentliche Stellen an die dort aufgeführten Behörden zu Zwecken der nationalen Sicherheit.

Zu § 33 (Auskunftsrecht der betroffenen Person)
§ 33 Abs. 1 HDSIG-E enthält ergänzend zu den in § 24 Abs. 2, § 25 Abs. 2 und § 26 Abs. 2 HDSIG-E genannten Ausnahmen Einschränkungen des Auskunftsrechts der betroffenen Person. Abs. 2 und 3 regeln Maßnahmen zum Schutz der Rechte und Freiheiten der betroffenen Person.

Abs. 1 Nr. 1 verweist für das Auskunftsrecht auf die Beschränkungen des § 32 Abs. 1 und 3 HDSIG-E. Abs. 1 Nr. 2 regelt weitere Beschränkungen des Auskunftsrechts und übernimmt Elemente der Vorschriften des § 18 Abs. 4 HDSG und § 29 Abs. 2 HSOG; eine entsprechende Bestimmung findet sich in § 52 Abs. 2 HDSIG-E.

Die in Abs. 2 und 3 geregelten Beschränkungen sowie Dokumentations- und Begründungspflichten dienen einerseits dem Schutz der öffentlichen Sicherheit (Art. 23 Abs. 1 Buchst. c der Verordnung (EU) Nr. 2016/679) und der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung, einschließlich des Schutzes vor und der Abwehr von Gefahren für die öffentliche Sicherheit (Art. 23 Abs. 1 Buchst. d der Verordnung (EU) Nr. 2016/679), und andererseits dem Schutz der Rechte und Freiheiten der betroffenen Personen im Sinne des Art. 23 Abs. 2 Buchst. c, d, g und h der Verordnung (EU) Nr. 2016/679. Die betroffene Person wird in die Lage versetzt, die Ablehnung der Auskunftserteilung nachzuvollziehen und gegebenenfalls durch die zuständige Aufsichtsbehörde prüfen zu lassen. Abs. 2 Satz 2 enthält die strenge Zweckbindung der zum Zweck der Auskunftserteilung und zu deren Vorbereitung gespeicherten Daten. Ergänzend hierzu hat der Verantwortliche nach Art. 12 Abs. 4 der Verordnung (EU) Nr. 2016/679 die betroffene Person auf die Möglichkeit der Beschwerde bei einer Aufsichtsbehörde und des gerichtlichen Rechtsschutzes hinzuweisen; auf diese Möglichkeit wird in Abs. 3 deklaratorisch noch einmal hingewiesen. Mit der Regelung in Abs. 3 soll zudem ein Gleichlauf mit der Regelung in § 52 Abs. 7 HDSIG-E herbeigeführt werden.

Abs. 4 Satz 1 übernimmt Elemente des § 18 Abs. 5 HDSG sowie des § 29 Abs. 1 Satz 3 und 4 HSOG und sieht die Einschränkung des Auskunftsrechts für personenbezogene Daten vor, die durch öffentliche Stellen weder automatisiert verarbeitet noch - ohne automatisiert verarbeitet zu werden - in einem Dateisystem gespeichert sind oder werden sollen. Darunter fallen insbesondere Akten oder Aktensammlungen sowie ihre Deckblätter, die nicht nach bestimmten Kriterien geordnet sind (vgl. Erwägungsgrund 15 Satz 3 der Verordnung (EU) Nr. 2016/679). Diese Form der Datenverarbeitung ist zwar nach Art. 2 Abs. 1 der Verordnung (EU) Nr. 2016/679 nicht von deren sachlichen Anwendungsbereich erfasst, jedoch gilt nach § 1 Abs. 8 HDSIG-E die Verordnung (EU) Nr. 2016/679 - und mithin das Auskunftsrecht nach deren Art. 15 - auch für diese Form der Datenverarbeitung. Die Einschränkung liegt daher außerhalb des Anwendungsbereichs der Verordnung (EU) Nr. 2016/679. Das Auskunftsrecht besteht nur unter der Voraussetzung, dass die betroffene Person Angaben macht, die dem Verantwortlichen das Auffinden der Daten ermöglichen. Ferner darf der für die Erteilung der Auskunft erforderliche Aufwand nicht außer Verhältnis zu dem von der betroffenen Person geltend gemachten Informationsinteresse stehen. Abs. 4 Satz 2 übernimmt den Rechtsgedanken aus § 29 Abs. 1 Satz 5 HSOG und § 18 Abs. 5 Satz 5 HDSG, stellt der Systematik der Verordnung (EU) Nr. 2016/679 folgend das Auskunftsrecht in den Vordergrund und ermöglicht gleichwohl die Gewährung von Akteneinsicht, wenn personenbezogene Daten durch öffentliche Stellen weder automatisiert verarbeitet noch - ohne automatisiert verarbeitet zu werden - in einem Dateisystem gespeichert sind. Diese Regelung liegt daher ebenfalls außerhalb des Anwendungsbereichs der Verordnung (EU) Nr. 2016/679.

Zu § 34 (Recht auf Löschung ("Recht auf Vergessenwerden"))
§ 34 HDSIG-E schränkt das Recht der betroffenen Person auf Löschung und die damit korrespondierende Pflicht des Verantwortlichen aus Art. 17 Abs. 1 der Verordnung (EU) Nr. 2016/679 in den Fällen der nicht automatisierten Datenverarbeitung ein. Die in Art. 17 Abs. 3 der Verordnung (EU) Nr. 2016/679 genannten Ausnahmen bleiben von der Vorschrift unberührt.

Unter den Voraussetzungen der Abs. 1 bis 3 tritt an die Stelle der Löschung die Einschränkung der Verarbeitung (Art. 18 der Verordnung (EU) Nr. 2016/679). Hierdurch wird die Beschränkung des Rechts auf bzw. der Pflicht zur Löschung personenbezogener Daten auf das erforderliche Maß im Sinne des Art. 23 Abs. 2 Buchst. c der Verordnung (EU) Nr. 2016/679 begrenzt.

Art. 18 Abs. 2 und 3 sowie Art. 19 der Verordnung (EU) Nr. 2016/679 vermitteln effektive Garantien gegen Missbrauch und unrichtige Übermittlung im Sinne des Art. 23 Abs. 2 Buchst. d der Verordnung (EU) Nr. 2016/679.

Der Anwendungsbereich des § 34 Abs. 1 HDSIG-E ist auf Fälle nicht automatisierter Datenverarbeitung beschränkt. Die Einschränkung dient der Konkretisierung des Tatbestandsmerkmals der "besonderen Art der Speicherung". Eine Löschung personenbezogener Daten kommt nicht in Betracht, wenn die Löschung im Fall nicht automatisierter Datenverarbeitung wegen der besonderen Art der Speicherung nicht oder nur mit unverhältnismäßig hohem Aufwand möglich ist. Erfasst werden von der Vorschrift vor allem Archivierungen in Papierform oder die Nutzung früher gebräuchlicher analoger Speichermedien, etwa Mikrofiche, bei denen es nicht oder nur mit unverhältnismäßig hohem Aufwand möglich ist, einzelne Informationen selektiv zu entfernen. Abs. 1 Satz 1 und 2 gelten nach Satz 3 nicht für die Fallgruppe des Art. 17 Buchst. d der Verordnung (EU) Nr. 2016/679, da der Verantwortliche bei einer unrechtmäßigen Datenverarbeitung nicht schutzwürdig ist und sich nicht auf einen unverhältnismäßig hohen Aufwand der Löschung wegen der von ihm selbst gewählten Art der Speicherung berufen kann.

Abs. 2 Satz 1 sieht eine Beschränkung zur Wahrung schutzwürdiger Interessen der betroffenen Person vor (Art. 23 Abs. 1 Buchst. i der Verordnung (EU) Nr. 2016/679). Sie ergänzt in den Fällen, in denen der Verantwortliche die Daten der betroffenen Person nicht länger benötigt oder unrechtmäßig verarbeitet hat (Art. 17 Abs. 1 Buchst. a und d der Verordnung (EU) Nr. 2016/679) die Regelung des Art. 18 Abs. 1 Buchst. b und c der Verordnung (EU) Nr. 2016/679. Nach Art. 18 Abs. 1 Buchst. b der Verordnung (EU) Nr. 2016/679 erfolgt die Einschränkung der Verarbeitung unrechtmäßig verarbeiteter Daten nur auf entsprechendes Verlangen der betroffenen Person. Art. 18 Abs. 1 Buchst. c der Verordnung (EU) Nr. 2016/679 lässt eine Einschränkung der Verarbeitung nicht länger benötigter Daten auf Verlangen der betroffenen Person nur zu, wenn die betroffene Person sie zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen benötigt.

Abs. 2 sieht demgegenüber auch ohne entsprechendes Verlangen der betroffenen Person eine generelle Pflicht des Verantwortlichen zur Einschränkung der Verarbeitung vor, wenn er Grund zu der Annahme hat, dass durch die Löschung schutzwürdige Interessen der betroffenen Person beeinträchtigt würden. Die Regelung ist notwendig, da der Verantwortliche nach Art. 17 der Verordnung (EU) Nr. 2016/679 grundsätzlich verpflichtet ist, nicht mehr erforderliche oder unrechtmäßig verarbeitete Daten zu löschen. Die Einschränkung der Verarbeitung anstelle der Löschung soll die betroffene Person in die Lage versetzen, ihr Verlangen auf Einschränkung der Verarbeitung gegenüber dem Verantwortlichen zu äußern oder sich für eine Löschung der Daten zu entscheiden. Dies wird durch die Unterrichtungspflicht nach Satz 2, welche zugleich eine Maßnahme zum Schutz der Rechte und Freiheiten sowie der berechtigten Interessen der betroffenen Person nach Art. 23 Abs. 2 Buchst. h der Verordnung (EU) Nr. 2016/679 darstellt, gewährleistet. In der Regel wird es sich daher nur um eine vorübergehende Beschränkung der Löschungspflicht des Verantwortlichen handeln (Art. 23 Abs. 2 Buchst. c der Verordnung (EU) Nr. 2016/679).

Abs. 3 sieht eine Beschränkung für den Fall vor, dass einer Löschung nicht mehr erforderlicher Daten satzungsmäßige Aufbewahrungsfristen entgegenstehen. Die vorgesehene ergänzende Einschränkung der gesetzlichen Aufbewahrungsfrist ist in § 34 HDSIG-E über die sich unmittelbar aus der Verordnung (EU) Nr. 2016/679 ergebende Ausnahme des Art. 17 Abs. 3 Buchst. b - Erfüllung einer rechtlichen Verpflichtung nach dem Recht der Union oder der Mitgliedstaaten - erfasst. Die Ausnahme schützt den Verantwortlichen vor einer Pflichtenkollision.

Zu § 35 (Widerspruchsrecht)
§ 35 HDSIG-E schränkt das Recht auf Widerspruch nach Art. 21 Abs. 1 der Verordnung (EU) Nr. 2016/679 ein, soweit an der Verarbeitung ein zwingendes öffentliches Interesse besteht, das die Interessen der betroffenen Person überwiegt, oder eine Rechtsvorschrift zur Verarbeitung verpflichtet. § 35 HDSIG-E setzt öffentliche Interessen des Verantwortlichen im Sinne des Art. 23 Abs. 1 Buchst. e der Verordnung (EU) Nr. 2016/679 voraus, die im konkreten Einzelfall zwingend sein und Vorrang vor den Interessen der betroffenen Person haben müssen. Darüber hinaus ist das Recht auf Widerspruch ausgeschlossen, wenn eine Rechtsvorschrift zur Verarbeitung verpflichtet. § 24 Abs. 2 und § 25 Abs. 4 HDSIG-E enthalten spezifische Einschränkungen des Widerspruchsrechts für die Datenverarbeitung zu Forschungszwecken, statistischen Zwecken und im öffentlichen Interesse liegenden Archivzwecken.

Zu § 36 (Anwendung der Vorschriften über das Bußgeld- und Strafverfahren bei Verstößen nach Artikel 83 der Verordnung (EU) Nr. 2016/679)
Abs. 1 erklärt für Verstöße gegen die in Art. 83 Abs. 4 bis 6 der Verordnung (EU) Nr. 2016/679 zu findenden Ordnungswidrigkeiten, soweit dieses Gesetz nichts anderes bestimmt, § 41 des Bundesdatenschutzgesetzes für entsprechend anwendbar. Die Verordnung (EU) Nr. 2016/679 selbst regelt das Bußgeld- und Strafverfahren nicht.

Mit der Regelung in Abs. 2 wird in Hessen von der Öffnungsklausel des Art. 83 Abs. 7 der Verordnung (EU) Nr. 2016/679 Gebrauch gemacht, national zu regeln, ob und bejahendenfalls in welchem Umfang gegen Behörden und sonstige öffentliche Stellen Geldbußen wegen Verstößen nach Art. 83 verhängt werden können. Die Vorschrift schließt die Verfolgung und Ahndung von Ordnungswidrigkeiten gegen Behörden und andere öffentliche Stellen im Sinne des § 2 Abs. 1 Satz 1 HDSIG-E aus. Von Abs. 2 nicht erfasst werden nicht öffentliche Stellen im Sinne des § 2 Abs. 1 Satz 2, die hoheitliche Aufgaben der öffentlichen Verwaltung wahrnehmen, sowie öffentliche Stellen im Sinne des § 2 Abs. 2, soweit sie als öffentlich-rechtliche Unternehmen am Wettbewerb teilnehmen.

Abs. 3 dient dem verfassungsrechtlichen Verbot einer Selbstbezichtigung. Die Regelung kann auf die Öffnungsklausel des Art. 83 Abs. 8 der Verordnung (EU) Nr. 2016/679 gestützt werden, wonach angemessene Verfahrensgarantien geschaffen werden müssen.

Zu § 37 (Strafvorschriften)
Art. 84 Abs. 1 der Verordnung (EU) Nr. 2016/679 berechtigt und verpflichtet die Mitgliedstaaten, "andere Sanktionen" für Verstöße gegen die Verordnung festzulegen und ist damit insbesondere eine Öffnungsklausel, um neben Geldbußen im Sinne des Art. 83 der Verordnung (EU) Nr. 2016/679 mitgliedstaatlich strafrechtliche Sanktionen vorzusehen. Hiervon macht § 37 HDSIG-E Gebrauch. Abs. 1 ersetzt tatbestandlich sinngemäß die Strafvorschrift des § 40 Abs. 1 HDSG und übernimmt deren Strafrahmen.

Abs. 2 übernimmt die bisherige Bestimmung des § 40 Abs. 2 HDSG. In Abs. 3 wird festgelegt, dass es sich um ein Antragsdelikt handelt.

Abs. 4 dient dem verfassungsrechtlichen Verbot einer Selbstbezichtigung. Die Regelung stützt sich auf die Öffnungsklausel des Art. 84 Abs. 1 der Verordnung (EU) Nr. 2016/679, wonach die Mitgliedstaaten Vorschriften für Verstöße gegen diese Verordnung festlegen und alle zu deren Anwendung erforderlichen Maßnahmen treffen.

Zu § 38 (Bußgeldvorschriften)
Abs. 1 und 2 nehmen Bußgeldtatbestand und Bußgeldrahmen des § 41 HDSG wieder in das HDSIG-E auf.

Zu § 39 (Gemeinsame Verfahren, Gemeinsam Verantwortliche)
Abs. 1 übernimmt die Vorschrift des § 15 Abs. 1 Satz 1 HDSG für die gemeinsamen Verfahren.

Abs. 2 übernimmt die Vorschrift des § 15 Abs. 2, erster Satzteil HDSG und erweitert die in Art. 26 der Verordnung (EU) Nr. 2016/679 genannten Festlegungen der gemeinsam Verantwortlichen um die Bestimmung einer Stelle, der die Planung, Einrichtung und Durchführung des gemeinsamen Verfahrens obliegt.

Abs. 3 erklärt - in Anlehnung an die bestehende Regelung des § 15 Abs. 5 HDSG - Abs. 1 und 2 für die Fälle entsprechend anwendbar, in denen innerhalb einer öffentlichen Stelle ein gemeinsames Verfahren zur Verarbeitung personenbezogener Daten für verschiedene Zwecke eingerichtet wird.

Zu § 40 (Anwendungsbereich)
Die Vorschriften des Dritten Teils dienen der Umsetzung der Richtlinie (EU) Nr. 2016/680.

§ 40 HDSIG-E konturiert in Umsetzung von Art. 2 i.V.m. Art. 1 Abs. 1 der Richtlinie (EU) Nr. 2016/680 deren Anwendungsbereich und gilt vorbehaltlich des § 1 Abs. 2 HDSIG-E für Verarbeitungen durch Behörden und andere öffentliche Stellen, soweit sie für die Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder die Strafvollstreckung, einschließlich des Schutzes vor und der Abwehr von Gefahren für die öffentliche Sicherheit zuständig sind, und auch nur, soweit sie zu diesen Zwecken personenbezogene Daten verarbeiten. Dies sind insbesondere die Polizeibehörden, soweit sie die Daten zu den genannten Zwecken verarbeiten, einschließlich der Datenverarbeitung zu Gefahrenabwehrzwecken.

Der hier geregelte Anwendungsbereich der Richtlinie (EU) Nr. 2016/680 verändert nicht das Gefüge der Gesetzgebungskompetenzen des Bundes nach dem Grundgesetz, wie die konkurrierende Gesetzgebungskompetenz in Art. 74 Abs. 1 Nr. 1 GG für das Strafrecht und gerichtliche Verfahren. So finden die in den Dritten Teil des HDSIG-E aufgenommenen Bestimmungen zur Verarbeitung personenbezogener Daten selbstverständlich keine Anwendung, soweit der Bundesgesetzgeber abschließend über den Datenschutz im Strafverfahren befunden und bspw. mit den §§ 474 ff. Strafprozessordnung (StPO) Vorschriften zum Datenschutz geschaffen hat. Hierbei hat er nicht nur die Verwendung von Daten für verfahrensübergreifende Zwecke (§§ 474 bis 482 StPO) geregelt, sondern auch die Datenverarbeitung für Zwecke des Strafverfahrens (vgl. § 483 StPO). Die vollständige Wiedergabe des Anwendungsbereichs der Richtlinie (EU) Nr. 2016/680 bzw. dessen landesrechtliche Umsetzung soll lediglich sicherstellen, dass bisherige landesrechtliche Regelungen, die etwa über die Vorschrift des § 160 Abs. 4 StPO im Strafver-

fahrensrecht gelten, auch vom Dritten Teil des HDSIG-E erfasst werden und damit in den Anwendungsbereich der Richtlinie fallen. Die hiesigen Regelungen dienen folglich der lückenlosen Richtlinienumsetzung im landesrechtlichen Datenschutzrecht, ohne jedoch die Gesetzgebungskompetenzen von Bund und Ländern zu berühren.

Für die Eröffnung des Anwendungsbereichs des Dritten Teils und damit auch der Richtlinie (EU) Nr. 2016/680 genügt eine Verarbeitung zu den o. g. Zwecken allein nicht. Daneben muss auch eine grundsätzliche Befugnis- und Aufgabenzuweisung (Zuständigkeit) zu Richtlinienzwecken vorliegen.

Die Verhütung, Ermittlung, Verfolgung, Ahndung und Vollstreckung von Ordnungswidrigkeiten ist vom Anwendungsbereich der Richtlinie (EU) Nr. 2016/680 auch ohne deren ausdrückliche Nennung in Art. 1 Abs. 1 umfasst und der Begriff der Ordnungswidrigkeit daher in § 40 Abs. 1 ausdrücklich genannt. Dies schließt auch hierauf bezogene Gefahrenabwehrzwecke, wie im HSOG geregelt, ein. Diese Auslegung wird durch Erwägungsgrund 13 der Richtlinie (EU) Nr. 2016/680 gestützt, wonach es sich bei der Straftat im Sinne der Richtlinie (EU) Nr. 2016/680 um einen eigenständigen Begriff des Unionsrechts handelt. Folglich kann die Ordnungswidrigkeit unter den Begriff der Straftat subsumiert werden, um die unterschiedliche Einordnung eines Sachverhalts als Straftat oder Ordnungswidrigkeit in den EU-Mitgliedstaaten zu kompensieren. Hierdurch wird insbesondere erreicht, dass die polizeiliche Datenverarbeitung einheitlichen Regeln folgt, unabhängig davon, ob eine Straftat oder eine Ordnungswidrigkeit in Rede steht. Dies gilt auch für die Datenverarbeitung durch Behörden, die keine Polizeibehörden sind, soweit sie zu den vorgenannten Zwecken tätig werden.

Um den Anwendungsbereich der Richtlinie (EU) Nr. 2016/680 und der sie betreffenden Umsetzungsnormen jedoch nicht zu überdehnen, gelten die Regelungen des Dritten Teils im Bereich der Gefahrenabwehr nur dann, wenn die Behörden die Datenverarbeitung zum Zwecke der auf die Verhütung von Straftaten oder Ordnungswidrigkeiten bezogenen Gefahrenabwehr vornehmen und eine solche gesetzliche Aufgabenzuweisung besteht. Dies ist im HSOG in Bezug auf die Gefahrenabwehrbehörden dann der Fall, wenn sich etwa die Datenverarbeitung im Rahmen der Maßnahmen aufgrund des HSOG auf die Abwehr von Straftaten und/oder Ordnungswidrigkeiten bezieht. Diese Auslegung kann u.a. auf Erwägungsgrund 11 der Richtlinie (EU) Nr. 2016/680 gestützt werden, wonach zuständige Behörden nicht nur staatliche Stellen wie die Justizbehörden, die Polizei oder andere Strafverfolgungsbehörden sein können, sondern auch alle anderen Stellen oder Einrichtungen, denen durch das Recht der Mitgliedstaaten die Ausübung öffentlicher Gewalt und hoheitlicher Befugnisse für die Zwecke der Richtlinie (EU) Nr. 2016/680 übertragen wurde. Hieraus resultiert, dass die Datenverarbeitung bei Verwaltungsbehörden, deren Aufgabenzuweisung nicht mit den in § 40 HDSIG-E genannten Zwecken übereinstimmt, grundsätzlich solange und soweit nicht in den Anwendungsbereich der Richtlinie fällt, wie die von ihnen geführten Verwaltungsverfahren nicht in ein konkretes Ordnungswidrigkeitsverfahren übergehen. Im Rahmen eines konkreten Ordnungswidrigkeitsverfahrens gelten dann die bundesgesetzlich im Gesetz über Ordnungswidrigkeiten (OWiG) geregelten, bereichsspezifischen Bestimmungen zur Verarbeitung personenbezogener Daten.

Abs. 2 stellt durch die Aufnahme des Begriffs Vollzug klar, dass die in Umsetzung der Richtlinie (EU) Nr. 2016/680 in den Dritten Teil aufgenommenen Bestimmungen auch auf die mit Aufgaben des Strafvollzugs betrauten öffentlichen Stellen Anwendung finden, soweit sie für diesen Zweck personenbezogene Daten verarbeiten. Maßgeblich ist hierfür das Verständnis der in Art. 1 Abs. 1 der Richtlinie (EU) Nr. 2016/680 verwendeten Begriffe der "Strafvollstreckung, einschließlich des Schutzes vor und der Abwehr von Gefahren für die öffentliches Sicherheit", da unabhängig davon, ob eine begriffliche Zusammenfassung von Strafvollstreckung und Strafvollzug in den Rechtssystemen anderer europäischer Staaten üblich ist, der Begriff des Strafvollzugs jedenfalls im deutschen Rechtssystem unter den Begriff der Strafvollstreckung subsumiert werden kann. So wird bezogen auf die Vorschriften der §§ 449 ff. StPO vorwiegend zwischen der Strafvollstreckung im weiteren Sinne und der Strafvollstreckung im engeren Sinne unterschieden. Der Begriff der Strafvollstreckung im weiteren Sinne ist dabei gleichbedeutend wie der Begriff der Strafverwirklichung zu verstehen und umfasst neben der Strafvollstreckung im engeren Sinne auch den Strafvollzug.

Abs. 3 sieht vor, dass Auftragsverarbeiter, deren Tätigkeit sich grundsätzlich dadurch auszeichnet, dass sie Daten zur Erfüllung einer Auftragsverarbeitungsvereinbarung und nicht aufgrund eigener Aufgabenzuschreibung verarbeiten, durch die Regelungen des Dritten Teils nur adressiert sind, sofern sie konkret angesprochen werden. Die von ihnen durchgeführten Verarbeitungen richten sich im Übrigen nach den Regelungen der Verordnung (EU) Nr. 2016/679 bzw. den diese ausformenden Ersten und Zweiten Teil. Das schließt allerdings nicht aus, dass durch den Dritten Teil angesprochene Verantwortliche auch als Auftragsverarbeiter tätig sein können.

Zu § 41 (Begriffsbestimmungen)

Die Begriffsbestimmungen in § 41 Nr. 1 bis 17 HDSIG-E sind zum Zweck der Umsetzung der Richtlinie (EU) Nr. 2016/680 aufgenommen worden. Sie bilden die Begriffsbestimmungen aus Art. 3 der Richtlinie (EU) Nr. 2016/680 ab. Zum Zweck der Übersichtlichkeit wurde die in Art. 10 der Richtlinie (EU) Nr. 2016/680 enthaltene Definition besonderer personenbezogener Daten als Nr. 15

Buchst. a bis e aufgenommen. Zudem wurde die in § 46 HDSIG-E angesprochene Einwilligung unter Übernahme der Definition aus der Verordnung (EU) Nr. 2016/679 in Nr. 18 aufgenommen.

Zu § 42 (Allgemeine Grundsätze für die Verarbeitung personenbezogener Daten)
§ 42 HDSIG-E dient der Umsetzung von Art. 4 Abs. 1 der Richtlinie (EU) Nr. 2016/680 und führt einige allgemeine Verarbeitungsgrundsätze, die in Teilen an späterer Stelle noch einmal aufgenommen werden, an zentraler Stelle zusammen.

Zu § 43 (Verarbeitung besonderer Kategorien personenbezogener Daten)
§ 43 HDSIG-E dient der Umsetzung von Art. 10 der Richtlinie (EU) Nr. 2016/680. Abs. 1 legt fest, dass die Verarbeitung besonderer Kategorien personenbezogener Daten zulässig ist, wenn sie zur Aufgabenerfüllung unbedingt erforderlich ist und schafft damit eine eigene Rechtsgrundlage für diese Verarbeitungen. Das kann auch die Verarbeitung in den in Art. 10 Buchst. b und c der Richtlinie (EU) Nr. 2016/680 genannten Zusammenhängen umfassen, d.h. zur Wahrung lebenswichtiger Interessen der betroffenen Person oder eines Dritten oder wenn Daten verarbeitet werden sollen, die die betroffene Person offensichtlich öffentlich gemacht hat.

Der in Art. 10 der Richtlinie (EU) Nr. 2016/680 verwendete Begriff der "unbedingten" Erforderlichkeit wird in der Richtlinie selbst nicht näher konturiert. Im Allgemeinen erfolgt die Prüfung des auch unionsrechtlich anerkannten Verhältnismäßigkeitsgrundsatzes in drei Stufen, der Geeignetheit, der Erforderlichkeit und der Angemessenheit. Während im Rahmen der Geeignetheit einer Maßnahme danach gefragt wird, ob sie tauglich ist, das legitime Ziel zu erreichen, meint Erforderlichkeit, dass zur Verfolgung der durch die gesetzliche Vorschrift geschützten Interessen kein milderes Mittel, also keine weniger belastende Alternative vorhanden sein darf, die ebenso gut der Zielerreichung wie die gewählte Maßnahme dienen würde. Eine unbedingte Erforderlichkeit ist daher anzunehmen, wenn keine zumutbaren Alternativ- oder Ausgleichsmaßnahmen zur Verfügung stehen, um ein legitimes Ziel zu erreichen.

In Abs. 2 Satz 1 wird geregelt, dass bei der Verarbeitung geeignete Garantien für die Rechte und Freiheiten der betroffenen Personen vorgesehen werden müssen. In Satz 2 werden unverbindliche Beispielsfälle für mögliche Maßnahmen zur Umsetzung dieser Garantien genannt. Die konkrete Ausgestaltung der Maßnahmen kann je nach Fallgestaltung variieren.

Zu § 44 (Verarbeitung zu anderen Zwecken)
Satz 1 setzt Art. 4 Abs. 2 der Richtlinie (EU) Nr. 2016/680 um. Damit wird klargestellt, dass Verantwortliche personenbezogene Daten so lange und so weit zu anderen Zwecken, als zu denen sie ursprünglich erhoben wurden, verarbeiten dürfen, so lange es sich bei diesen anderen Zwecken um einen der in § 40 HDSIG-E genannten Zwecke handelt und diese Verarbeitung erforderlich und verhältnismäßig ist. Grundsätzlich eröffnet Art. 4 Abs. 2 der Richtlinie (EU) Nr. 2016/680 stets die Möglichkeit, die Daten für einen der in § 40 HDSIG-E genannten Zwecke zu verarbeiten und innerhalb des Rahmens der genannten Zwecke auch Zweckänderungen vorzunehmen. Zusätzliche Anforderungen an die Zweckänderung innerhalb der in § 40 HDSIG-E genannten Zwecke aufgrund nationalen Verfassungsrechts (so etwa der Grundsatz der hypothetischen Datenneuerhebung, vgl. BVerfG, Urteil vom 20. April 2016 - 1 BvR 966/09 und 1 BvR 1140/06) werden in den Fachgesetzen, wie dem HSOG-E, umgesetzt.

Satz 2 betrifft die Weiterverarbeitung von zu Zwecken des § 40 HDSIG-E erhobenen Daten zu anderen als den dort genannten Zwecken. Eine solche ist zulässig, wenn dies in einer Rechtsvorschrift vorgesehen ist. Ein Anwendungsfall bildet beispielsweise die Verarbeitung durch Datenübermittlung an nicht für Zwecke der Richtlinie zuständige Behörden in § 22 HDSIG-E.

Zu § 45 (Verarbeitung zu wissenschaftlichen oder historischen Forschungszwecken, zu archivarischen oder statistischen Zwecken)
§ 45 HDSIG-E greift Art. 4 Abs. 3 der Richtlinie (EU) Nr. 2016/680 auf, wonach Verantwortliche Daten auch zu wissenschaftlichen oder historischen, statistischen oder archivarischen Zwecken verarbeiten dürfen, solange diese Verarbeitung unter die in § 40 genannten Zwecke gefasst werden kann. Die Vorschrift ist in ihrer Ausgestaltung an die Struktur der §§ 24, 25 HDSIG-E, um einen Gleichlauf in diesem Bereich der Datenverarbeitung zu ermöglichen.

Voraussetzung für die Datenverarbeitung ist das Vorliegen geeigneter Vorkehrungen zugunsten der Rechte und Freiheiten sowie berechtigten Interessen der betroffenen Personen. Hierzu können insbesondere eine so zeitnah wie möglich erfolgende Anonymisierung von Daten oder die räumliche und organisatorische Abtrennung der Forschung betreibenden Stellen gehören. Hinsichtlich der Begriffsbestimmung "Anonymisierung" ist auf § 2 Abs. 4 zu verweisen.

Abs. 2 fordert im Fall des Abs. 1 Nr. 2 darüber hinaus für die Zulässigkeit der Verarbeitung besonderer Kategorien personenbezogener Daten das Vorliegen einer unbedingten Erforderlichkeit sowie nach Abs. 3 die Durchführung angemessener und spezifischer Maßnahmen im Sinne des § 43 Abs. 3 Satz 1. Ergänzend hierzu sind die besonderen Kategorien personenbezogener Daten nach so zeitnah wie möglich zu anonymisieren. Abs. 3 Satz 3 übernimmt die Regelung des § 33 Abs. 2 HDSG.

Abs. 4 sieht Beschränkungen der Rechte betroffener Personen bei der Verarbeitung personenbezogener Daten zu wissenschaftlichen oder historischen Forschungszwecken oder statistischen Zwecken vor, während sich Abs. 5 auf die Rechte betroffener Personen bei der Verarbeitung zu archivarischen Zwecken bezieht.
Abs. 6 regelt die Voraussetzungen für eine Veröffentlichung personenbezogener Daten.

Zu § 46 (Einwilligung)
In § 46 HDSIG-E finden sich die Voraussetzungen für eine wirksame Einwilligung. Hierbei wurden Elemente aus Art. 7 der Verordnung (EU) Nr. 2016/679 mit Elementen des § 7 Abs. 2 HDSG kombiniert. § 46 Abs. 1 entspricht Art. 7 Abs. 1, § 46 Abs. 2 Art. 7 Abs. 2 und § 46 Abs. 3 Art. 7 Abs. 3 der Verordnung (EU) Nr. 2016/679. § 46 Abs. 4 orientiert sich an Art. 7 Abs. 4 der Verordnung (EU) Nr. 2016/679, wonach für die Beurteilung der Frage, ob die Freiwilligkeit der Einwilligung vorliegt, wesentlich auf die Umstände der Erteilung abzustellen ist. § 46 Abs. 5 entspricht § 7 Abs. 2 Satz 2 HDSG.

Voraussetzung für eine Verarbeitung personenbezogener Daten zu einem der in § 40 HDSIG-E genannten Zwecke ist jedoch, dass die Datenverarbeitung durch (fachgesetzliche) Rechtsvorschrift auf Grundlage der Einwilligung erfolgen kann. Dies folgt auch aus Erwägungsgrund 35 der Richtlinie (EU) Nr. 2016/680.

Zu § 47 (Verarbeitung auf Weisung des Verantwortlichen)
§ 47 HDSIG-E setzt Art. 23 der Richtlinie (EU) Nr. 2016/680 um.

Zu § 48 (Datengeheimnis)
§ 48 HDSIG-E greift die Regelung des § 9 HDSG auf.

Zu § 49 (Automatisierte Einzelentscheidung)
§ 49 HDSIG-E setzt Art. 11 der Richtlinie (EU) Nr. 2016/680 um und regelt das Verbot automatisierter, insbesondere auf Profiling basierender Einzelentscheidungen. Um eine in Abs. 1 genannte, nur unter bestimmten Umständen zulässige "Entscheidung, die eine nachteilige Rechtsfolge für die betroffene Person hat", zu sein, muss es sich bei einer solchen Entscheidung um einen Rechtsakt mit Außenwirkung gegenüber der betroffenen Person - regelmäßig einen Verwaltungsakt - handeln. Interne Zwischenfestlegungen oder -auswertungen, die Ausfluss automatisierter Prozesse sind, fallen nicht hierunter.

Zu § 50 (Allgemeine Informationen zu Datenverarbeitungen)
§ 50 HDSIG-E dient der Umsetzung von Art. 13 Abs. 1 der Richtlinie (EU) Nr. 2016/680. Es geht um aktive Informationspflichten des Verantwortlichen gegenüber betroffenen Personen unabhängig von der Geltendmachung von Betroffenenrechten. Dieser Informationspflicht sollen Verantwortliche in allgemeiner Form nachkommen können. Durch die explizit in Erwägungsgrund 42 der Richtlinie (EU) Nr. 2016/680 aufgenommene Möglichkeit der Information über die Internetseite des Verantwortlichen wird Sinn und Zweck der Regelung klargestellt: Betroffene Personen sollen sich unabhängig von der Datenverarbeitung im konkreten Fall in leicht zugänglicher Form einen Überblick über die Zwecke der beim Verantwortlichen durchgeführten Verarbeitungen verschaffen können und eine Übersicht über die ihnen zur Verfügung stehenden Betroffenenrechte bekommen.

Zu § 51 (Benachrichtigung betroffener Personen)
§ 51 betrifft Fälle, in denen in fachgesetzlichen Regelungen eine aktive Benachrichtigung betroffener Personen vorgesehen ist. Eine Festlegung dieser in Art. 13 Abs. 2 der Richtlinie (EU) Nr. 2016/680 so bezeichneten "besonderen Fälle" ist nicht verallgemeinernd auf Ebene des Landesdatenschutzgesetzes möglich und muss im Fachrecht geleistet werden. Leitend für die Entscheidung, ob eine Benachrichtigung unabhängig von der Geltendmachung eines Betroffenenrechts angezeigt ist, dürfte z.B. sein, ob die Verarbeitung mit oder ohne Wissen der betroffenen Person, ggf. in Verbindung mit einer erhöhten Eingriffstiefe, erfolgt. In letztgenannten Fällen ist eine aktive, ggf. nachträgliche Benachrichtigung die einzige Möglichkeit für die betroffene Person, von der Verarbeitung Kenntnis zu erlangen und ggf. deren Rechtmäßigkeit mithilfe der Geltendmachung von Betroffenenrechten zu prüfen.

Abs. 1 stellt klar, welche Informationen betroffenen Personen von dem Verantwortlichen in diesen Fällen aktiv übermittelt werden müssen und dient dabei der Umsetzung von Art. 13 Abs. 2 der Richtlinie (EU) Nr. 2016/680.

Abs. 2 Satz 1 ermöglicht es in Umsetzung von Art. 13 Abs. 3 der Richtlinie (EU) Nr. 2016/680, zu den dort genannten Zwecken von der Bereitstellung der in Abs. 1 genannten Informationen abzusehen, sie einzuschränken oder sie aufzuschieben. Die Ausnahmen werden u.a. von dem Gedanken getragen, dass die Benachrichtigung nicht zu einer Gefährdung der ordnungsgemäßen Erfüllung der Aufgaben des Verantwortlichen führen soll. Die Nutzung der Möglichkeit, von der Benachrichtigung vollständig oder teilweise abzusehen, muss Verhältnismäßigkeitsgrundsätzen genügen und ihr muss eine nachvollziehbare Interessenabwägung vorausgehen. Die durch das teilweise oder vollständige Absehen von der Benachrichtigung verfolgten Ziele bzw. geschützten

Rechtsgüter müssen mithin in ein angemessenes Verhältnis zur Bedeutung der Benachrichtigung für die spätere Geltendmachung weiterer Betroffenenrechte gebracht werden. So hat der Verantwortliche im Einzelfall zu prüfen, ob die Benachrichtigung etwa nur teilweise eingeschränkt oder zu einem späteren Zeitpunkt erfolgen kann. Mit dieser Interessenabwägung werden die Rechtsgedanken aus § 18 Abs. 6 Satz 1 HDSG und § 29 Abs. 3 Satz 1 HSOG aufgegriffen. Abs. 2 Satz 2 übernimmt den Rechtsgedanken aus § 18 Abs. 6 Satz 2 HDSG und § 29 Abs. 3 Satz 2 HSOG.

Abs. 3 statuiert ein Zustimmungserfordernis der dort genannten Stellen, wenn sich die Benachrichtigung auf die Übermittlung an diese Stellen bezieht.

Abs. 4 verweist im Fall der Einschränkung nach Abs. 2 auf die entsprechende Geltung von § 52 Abs. 7.

Zu § 52 (Auskunftsrecht)
§ 52 HDSIG-E thematisiert das Auskunftsrecht als zentrales Betroffenenrecht und normiert gleichzeitig dessen Einschränkungen. Die Vorschrift dient mithin der Umsetzung der Art. 14 (Bestehen des Auskunftsrechts) und Art. 15 (Ausnahmen) der Richtlinie (EU) Nr. 2016/680. Das Auskunftsrecht setzt - im Gegensatz zu den in § 51 HDSIG-E angesprochenen aktiven Benachrichtigungspflichten - einen entsprechenden Antrag der betroffenen Person voraus.

Abs. 1 legt den Umfang des der betroffenen Person zustehenden Auskunftsrechts fest. Der in Nr. 1 und 4 genannte Begriff "Kategorie" ermöglicht dem Verantwortlichen eine angemessene Generalisierung der Angaben zu den verarbeiteten personenbezogenen Daten sowie zu den Übermittlungsempfängern. Die Angaben nach Nr. 1 zu den verarbeiteten personenbezogenen Daten können im Sinne einer zusammenfassenden Übersicht in verständlicher Form gemacht werden. Die Angaben müssen also nicht in einer Form gemacht werden, welche Aufschluss über die Art und Weise der Speicherung oder Sichtbarkeit der Daten beim Verantwortlichen (im Sinne einer Kopie) zulässt. Ebenso bedeutet die Pflicht zur Angabe der verfügbaren Informationen zur Datenquelle nicht, dass die Identität natürlicher Personen oder gar vertrauliche Informationen preisgegeben werden müssen.

Abs. 2 sorgt mit den hier normierten Beschränkungen des Auskunftsrechts für einen Gleichlauf mit § 33 Abs. 1 Nr. 2 HDSIG-E und übernimmt Elemente der Vorschriften des § 18 Abs. 4 HDSG und § 29 Abs. 2 HSOG.

Abs. 3 sorgt für einen Gleichlauf mit § 33 Abs. 4 HDSIG-E. Dafür übernimmt Abs. 3 Satz 1 Elemente des § 18 Abs. 5 HDSG sowie des § 29 Abs. 1 Satz 3 und 4 HSOG und sieht die Einschränkung des Auskunftsrechts für personenbezogene Daten vor, die durch öffentliche Stellen weder automatisiert verarbeitet noch - ohne automatisiert verarbeitet zu werden - in einem Dateisystem gespeichert sind oder werden sollen. Darunter fallen insbesondere Akten oder Aktensammlungen sowie ihre Deckblätter, die nicht nach bestimmten Kriterien geordnet sind (vgl. Erwägungsgrund 18 Satz 3 der Richtlinie (EU) Nr. 2016/680). Diese Form der Datenverarbeitung ist zwar nach Art. 2 Abs. 2 der Richtlinie (EU) Nr. 2016/680 nicht von deren sachlichen Anwendungsbereich erfasst, jedoch gelten die Vorschriften des Dritten Teils nach § 40 HDSIG-E insgesamt für die Verarbeitung von personenbezogenen Daten und mithin auch für diese Form der Datenverarbeitung. Die Einschränkung liegt daher außerhalb des Anwendungsbereichs der Richtlinie (EU) Nr. 2016/680. Das Auskunftsrecht besteht nur unter der Voraussetzung, dass die betroffene Person Angaben macht, die dem Verantwortlichen das Auffinden der Daten ermöglichen. Ferner darf der für die Erteilung der Auskunft erforderliche Aufwand nicht außer Verhältnis zu dem von der betroffenen Person geltend gemachten Informationsinteresse stehen. Abs. 3 Satz 2 übernimmt den Rechtsgedanken aus § 29 Abs. 1 Satz 5 HSOG und § 18 Abs. 5 Satz 5 HDSG und stellt der Systematik der Richtlinie (EU) Nr. 2016/680 folgend das Auskunftsrecht in den Vordergrund und ermöglicht gleichwohl die Gewährung von Akteneinsicht, wenn personenbezogene Daten durch öffentliche Stellen weder automatisiert verarbeitet noch - ohne automatisiert verarbeitet zu werden - in einem Dateisystem gespeichert sind. Diese Regelung liegt daher ebenfalls außerhalb des Anwendungsbereichs der Richtlinie (EU) Nr. 2016/680.

Abs. 4 normiert in Umsetzung von Art. 15 Abs. 1 der Richtlinie (EU) Nr. 2016/680, zu welchen Zwecken das Auskunftsrecht durch den Verantwortlichen vollständig oder teilweise eingeschränkt werden darf und verweist dafür auf die Voraussetzungen des § 51 Abs. 2 HDSIG-E. Die Ausnahmen werden u.a. von dem Gedanken getragen, dass die Auskunftserteilung nicht zur Behinderung oder Beeinträchtigung der ordnungsgemäßen Erfüllung der Aufgaben des Verantwortlichen führen soll. Die Nutzung der Möglichkeit, von der Auskunftserteilung vollständig oder teilweise abzusehen, muss Verhältnismäßigkeitsgrundsätzen genügen und ihr muss eine nachvollziehbare Interessenabwägung vorausgehen. Die durch das teilweise oder vollständige Absehen von der Auskunftserteilung verfolgten Ziele bzw. geschützten Rechtsgüter müssen mithin in ein angemessenes Verhältnis zur Bedeutung der Auskunftserteilung für die spätere Geltendmachung weiterer Betroffenenrechte gebracht werden. So hat der Verantwortliche im Einzelfall zu prüfen, ob die Auskunft etwa nur teilweise eingeschränkt oder zu einem späteren Zeitpunkt erteilt werden kann.

Abs. 6 Satz 1 und 2 dient der Umsetzung von Art. 15 Abs. 3 Satz 1 und 2 der Richtlinie (EU) Nr. 2016/680. Hierdurch wird dem Verantwortlichen auch gemeinsam mit der sich aus Abs. 4 ergebenden Variante, die Frage nach dem "Ob" der Verarbeitung nicht zu beantworten, die Möglichkeit gegeben, das Auskunftsverlangen unbeantwortet zu lassen. Satz 3 nimmt in Bezug auf das Absehen von einer Begründung der Auskunftsverweigerung zusätzlich Gedanken der Zweckgefährdung auf. Damit wird die Regelung des § 29 Abs. 4 HSOG aufgegriffen.

Abs. 7 thematisiert die Möglichkeiten, die der betroffenen Person im Fall des Absehens von einer Begründung für die vollständige oder teilweise Einschränkung des Auskunftsrechts oder im Fall der ausbleibenden Beantwortung des Auskunftsverlangens bleiben. Nach Satz 1 kann die betroffene Person ihr Auskunftsrecht nach Auskunftsverweigerung durch den Verantwortlichen über die oder den Hessischen Datenschutzbeauftragten ausüben. Dies dient der Umsetzung von Art. 17 Abs. 1 der Richtlinie (EU) Nr. 2016/680 und kommt einer deklaratorischen Wiederholung des auch in § 55 HDSIG-E enthaltenen Grundsatzes gleich, wonach betroffene Personen jederzeit die Hessische Datenschutzbeauftragte oder den Hessischen Datenschutzbeauftragten anrufen können. Satz 2 sieht in Umsetzung von Art. 17 Abs. 2 der Richtlinie (EU) Nr. 2016/680 eine entsprechende Unterrichtung durch den Verantwortlichen vor, die allerdings nicht auf Fälle Anwendung findet, in denen der Verantwortliche nach Abs. 6 berechtigt ist, von einer Information des Antragstellers ganz abzusehen. Mit Satz 3 wird Art. 17 Abs. 3 Satz 1 der Richtlinie (EU) Nr. 2016/680 umgesetzt. Die Regelung betrifft den Inhalt seitens der oder dem Hessischen Datenschutzbeauftragten zur Verfügung gestellten Informationen bezüglich des Ergebnisses der durchgeführten Prüfung. Satz 4 übernimmt die Regelung aus § 29 Abs. 5 Satz 2 HSOG und Satz 5 setzt Art. 17 Abs. 3 Satz 2 der Richtlinie (EU) Nr. 2016/680 um.

Abs. 8 setzt Art. 15 Abs. 4 der Richtlinie (EU) Nr. 2016/680 um.

Zu § 53 (Rechte auf Berichtigung und Löschung sowie Einschränkung der Verarbeitung)
In § 53 HDSIG-E werden die Betroffenenrechte auf Berichtigung, Löschung und Einschränkung der Verarbeitung und deren Ausnahmen geregelt. Die Vorschrift dient der Umsetzung von Art. 16 der Richtlinie (EU) Nr. 2016/680 in seiner Ausformung als Betroffenenrecht.

Abs. 1 betrifft das Recht auf Berichtigung unrichtiger bzw. auf Vervollständigung unvollständiger Daten. Hier wird Art. 16 Abs. 1 der Richtlinie (EU) Nr. 2016/680 umgesetzt. In Satz 2 wird ein in Erwägungsgrund 47 der Richtlinie (EU) Nr. 2016/680 enthaltener Gedanke aufgenommen, wonach zur Vorbeugung massenhafter und nicht erfolgversprechender Anträge klargestellt wird, dass sich die Berichtigung auf Tatsachen bezieht, die die betroffene Person berühren, und nicht etwa auf den Inhalt von Zeugenaussagen. Dies gilt auch für polizeifachliche Bewertungen. In Satz 3 wird Art. 16 Abs. 3 Satz 1 Buchst. a der Richtlinie (EU) Nr. 2016/680 umgesetzt. Zwar sieht die Richtlinienbestimmung hier die Verarbeitungseinschränkung als Alternative zur Löschung vor. Da die Richtlinie allerdings im Fall der Verarbeitung unrichtiger Daten deren Berichtigung, aber nicht deren Löschung vorsieht, wird der in der Richtlinie beschriebene Sachverhalt in Abs. 1 verortet, indem für Fälle, in denen nach Bestreiten der Richtigkeit der Daten deren Richtigkeit oder Unrichtigkeit nicht festgestellt werden kann, an die Stelle der Berichtigung eine Verarbeitungseinschränkung tritt. Für das Bestreiten der Richtigkeit der beim Verantwortlichen verarbeiteten Daten durch die betroffene Person reicht die reine Behauptung der Unrichtigkeit nicht aus, vielmehr müssen die Zweifel an der Unrichtigkeit in geeigneter Weise untermauert werden. Dies dient dem Schutz der polizeilichen Arbeit und der Vermeidung unverhältnismäßigen Prüfaufwands.

Abs. 2 regelt das Recht der betroffenen Person auf Löschung und dient der Umsetzung von Art. 16 Abs. 2 der Richtlinie (EU) Nr. 2016/680, der sowohl das Betroffenenrecht auf Löschung als auch die unabhängig davon bestehende Pflicht des Verantwortlichen zur Löschung vorsieht.

Abs. 3 betrifft die Voraussetzungen, unter denen an die Stelle einer Löschung nach Abs. 2 eine Verarbeitungseinschränkung treten kann und setzt Art. 16 Abs. 2 der Richtlinie (EU) Nr. 2016/680 um. Abs. 3 Satz 1 Nr. 1 greift einen in Erwägungsgrund 47 Satz 4 der Richtlinie (EU) Nr. 2016/680 enthaltenen Gedanken auf. Die Möglichkeit, von der Löschung wegen unverhältnismäßig hohen Aufwands abzusehen, ist als restriktiv auszulegende Ausnahmeregelung zu verstehen. Im Grundsatz sollte die bei Verantwortlichen zum Einsatz kommende IT-Infrastruktur darauf ausgelegt sein, eine Löschungsverpflichtung auch technisch nachvollziehen zu können.

Abs. 4 regelt, dass die Verarbeitungseinschränkung im Kontext automatisierter Verarbeitung eindeutig erkennbar sein muss. Dieser Gedanke wird von Erwägungsgrund 47 Satz 8 bis 10 der Richtlinie (EU) Nr. 2016/680 getragen.

Die in Abs. 5 enthaltene Verpflichtung zur Meldung der Berichtigung an Stellen, von denen die unrichtigen Daten stammen, setzt Art. 16 Abs. 5 der Richtlinie (EU) Nr. 2016/680 um. Eine spiegelbildliche Verpflichtung ist in § 70 Abs. 1 HDSIG-E für Fälle enthalten, in denen der Verantwortliche unabhängig von der Ausübung eines Betroffenenrechts eine Berichtigung durchführt. Darüber hinaus sind in Umsetzung des Art. 16 Abs. 6 der Richtlinie (EU) Nr.

2016/680 nach Abs. 5 Satz 2 und 3 auch andere Stellen, an die Daten übermittelt wurden, über die Berichtigung, Löschung oder Verarbeitungseinschränkung zu benachrichtigen.

Abs. 6 dient der Umsetzung von Art. 16 Abs. 4 der Richtlinie (EU) Nr. 2016/680 und betrifft das zur Anwendung kommende Verfahren, wenn der Verantwortliche dem Verlangen nach Berichtigung oder Löschung nicht oder nur eingeschränkt nachkommt. Die Vorschrift ist § 52 Abs. 6 HDSIG-E nachgebildet.

Abs. 7 verweist für die Fälle des Abs. 6 weitgehend auf die entsprechende Regelung in § 52 Abs. 7 HDSIG-E zur vollständigen oder teilweisen Einschränkung des Auskunftsrechts. Diese Regelung dient der Umsetzung von Art. 17 der Richtlinie (EU) Nr. 2016/680. Zudem wird in Abs. 7 auch die entsprechende Anwendung von § 52 Abs. 8 HDSIG-E statuiert.

Zu § 54 (Verfahren für die Ausübung der Rechte der betroffenen Person)
In § 54 HDSIG-E werden Elemente des Art. 12 der Richtlinie (EU) Nr. 2016/680 umgesetzt. Abs. 1 setzt Art. 12 Abs. 1, Abs. 2 setzt Art. 12 Abs. 3, Abs. 3 setzt Art. 12 Abs. 4 und Abs. 4 setzt Art. 12 Abs. 5 der Richtlinie (EU) Nr. 2016/680 um. Wenngleich es Art. 12 Abs. 5 der Richtlinie (EU) Nr. 2016/680 dem Verantwortlichen in begründeten Zweifelsfällen ermöglicht, zusätzliche Informationen zur Identitätsklärung anzufordern, ergibt sich hierdurch keine Änderung einer bereits bestehenden Praxis, den Nachweis der Identität als Grundvoraussetzung für die Antragsstellung anzusehen.

Zu § 55 (Anrufung der oder des Hessischen Datenschutzbeauftragten)
§ 55 stellt auch für den Bereich der Verarbeitung durch Verantwortliche zu den in § 40 HDSIG-E genannten Zwecken klar, dass sich Betroffene mit Beschwerden über die bei Verantwortlichen durchgeführte Verarbeitung an die Hessische Datenschutzbeauftragte oder den Hessischen Datenschutzbeauftragten wenden können. Insbesondere mit Abs. 1 i.V.m. § 13 Abs. 2 Satz 2 werden gleichzeitig Art. 52 Abs. 1 und 4 sowie Art. 45 Abs. 2 der Richtlinie (EU) Nr. 2016/680 umgesetzt und § 28 Abs. 1 HDSG in das HDSIG-E überführt. Soweit in Abs. 1 Satz 2 von einem Handeln der Gerichte in justizieller Tätigkeit die Rede ist, ist dies als Tätigwerden in richterlicher Unabhängigkeit zu verstehen. Abs. 2 setzt Art. 52 Abs. 2 und 3 der Richtlinie (EU) Nr. 2016/680 um.

Zu § 56 (Rechtsschutz gegen Entscheidungen der oder des Hessischen Datenschutzbeauftragten oder bei deren oder dessen Untätigkeit)
§ 56 setzt Art. 53 Abs. 1 der Richtlinie (EU) Nr. 2016/680 um und bestimmt, dass Adressaten von verbindlichen Entscheidungen der oder des Hessischen Datenschutzbeauftragten Rechtsschutz gegen diese suchen können. In Erwägungsgrund 86 Satz 2 und 3 der Richtlinie (EU) Nr. 2016/680 wird betont, dass sich der Rechtsschutz insbesondere auf die Ausübung von Untersuchungs-, Abhilfe- und Genehmigungsbefugnissen oder die Ablehnung oder Abweisung von Beschwerden durch die oder den Hessischen Datenschutzbeauftragten bezieht; für reine Stellungnahmen oder Empfehlungen hingegen soll der Anwendungsbereich nicht eröffnet sein. Dies schließt insbesondere die Befugnisse in § 14 Abs. 3 ein. In Abs. 2 wird - in Umsetzung von Art. 53 Abs. 2 der Richtlinie (EU) Nr. 2016/680 - der Rechtsschutz auf Fälle der Untätigkeit der oder des Hessischen Datenschutzbeauftragten ausgedehnt.

Zu § 57 (Auftragsverarbeitung)
§ 57 dient der Umsetzung von Art. 22 der Richtlinie (EU) Nr. 2016/680 und stellt Anforderungen für den Fall der Vereinbarung von Auftragsverarbeitungsverhältnissen auf. § 57 ersetzt § 4 HDSG für den Bereich der Richtlinie (EU) Nr. 2016/680.

Abs. 1 greift die Elemente des § 4 Abs. 1 HDSG auf und trifft allgemeine Aussagen zur Auftragsverarbeitung.

Abs. 2 beschreibt an den Auftragsverarbeiter zu stellende Anforderungen und setzt Art. 22 Abs. 1 der Richtlinie (EU) Nr. 2016/680 um.

In Abs. 3 werden Voraussetzungen für die Eingehung von Unterauftragsverarbeitungsverhältnissen normiert und dadurch Art. 22 Abs. 2 der Richtlinie (EU) Nr. 2016/680 umgesetzt.

In Abs. 4 wird in Anlehnung an Art. 28 Abs. 4 der Verordnung (EU) Nr. 2016/679 die Überführung der den Auftragsverarbeiter treffenden Pflichten auf einen Unterauftragnehmer geregelt.

In Abs. 5 werden die erforderlichen Inhalte einer der Auftragsverarbeitung zugrundeliegenden Vereinbarung geregelt und damit Art. 22 Abs. 3 der Richtlinie (EU) Nr. 2016/680 umgesetzt, wobei auch Elemente aus Art. 28 Abs. 3 der Verordnung (EU) Nr. 2016/679 (Buchst. c, f, h) übernommen werden.

Abs. 6 trifft in Umsetzung von Art. 22 Abs. 4 der Richtlinie (EU) Nr. 2016/680 Aussagen zur Form der Vereinbarung und Abs. 7 dient der Umsetzung von Art. 22 Abs. 5 der Richtlinie (EU) Nr. 2016/680.

Zu § 58 (Gemeinsame Verfahren, Gemeinsam Verantwortliche)
§ 58 dient der Umsetzung von Art. 21 der Richtlinie (EU) Nr. 2016/680 zu gemeinsam Verantwortlichen und trifft dabei auch Regelungen zu gemeinsamen Verfahren.

Abs. 1 übernimmt die Vorschrift des § 15 Abs. 1 Satz 1 HDSG für die gemeinsamen Verfahren.

Abs. 2 setzt Art. 21 Abs. 1 Satz 1 der Richtlinie (EU) Nr. 2016/680 zu gemeinsam Verantwortlichen um.

Abs. 3 Satz 1 übernimmt die Vorschrift des § 15 Abs. 2, erster Satzteil HDSG, Abs. 3 Satz 2 setzt Art. 21 Abs. 1 Satz 2 der Richtlinie (EU) Nr. 2016/680 um. Abs. 3 Satz 3 macht von Art. 21 Abs. 2 der Richtlinie (EU) Nr. 2016/680 Gebrauch, wonach die Mitgliedstaaten vorsehen können, dass die betroffene Person ihre Rechte im Rahmen der nach dieser Richtlinie erlassenen Vorschriften bei und gegenüber jedem einzelnen der gemeinsam Verantwortlichen geltend zu machen.

Abs. 4 erklärt in Anlehnung an die bestehende Regelung des § 15 Abs. 5 HDSG Abs. 1 bis 3 für die Fälle entsprechend anwendbar, in denen innerhalb einer öffentlichen Stelle ein gemeinsames Verfahren zur Verarbeitung personenbezogener Daten für verschiedene Zwecke eingerichtet wird.

Zu § 59 (Anforderungen an die Sicherheit der Datenverarbeitung)
§ 59 dient der Umsetzung von Art. 29 der Richtlinie (EU) Nr. 2016/680. Abs. 1 verpflichtet den Verantwortlichen und Auftragsverarbeiter dazu, erforderliche technische und organisatorische Maßnahmen zur Gewährleistung der Sicherheit der Datenverarbeitung zu treffen. Gleichzeitig wird klargestellt, dass die Ausgestaltung der Maßnahmen Ergebnis eines Abwägungsprozesses sein soll, in den insbesondere der Stand der verfügbaren Technik, die entstehenden Kosten und die näheren Umstände der Verarbeitung einzustellen sind. Abs. 1 Satz 1 liegt der schon in § 10 Abs. 1 Satz 2 HDSG enthaltene Gedanke zugrunde, wonach die Erforderlichkeit der Maßnahmen daran zu bemessen ist, ob ihr Aufwand in einem angemessenen Verhältnis zum angestrebten Schutzzweck steht und macht die geeigneten technischen und organisatorischen Maßnahmen zudem von der Eintrittswahrscheinlichkeit und der Schwere eines Risikos für die Rechte und Freiheiten natürlicher Personen abhängig. Die Risiken für die Rechte und Freiheiten der natürlichen Personen werden in Erwägungsgrund 51 der Richtlinie (EU) Nr. 2016/680 beispielhaft aufgeführt. In Erwägungsgrund 52 der Richtlinie (EU) Nr. 2016/680 werden Ausführungen zur Bestimmung des Risikos gemacht. Hiernach sollten Eintrittswahrscheinlichkeit und Schwere des Risikos nach der Art, dem Umfang, den Umständen und den Zwecken der Verarbeitung bestimmt werden. Das Risiko sollte anhand einer objektiven Bewertung beurteilt werden, bei der festgestellt wird, ob die Datenverarbeitung ein hohes Risiko birgt. Ein hohes Risiko ist ein besonderes Risiko der Beeinträchtigung der Rechte und Freiheiten der betroffenen Personen. Abs. 1 Satz 2 bildet als Anwendungshilfe die Gedanken aus Erwägungsgrund 52 ab; in den nachfolgenden Regelungen wird darauf Bezug genommen.

In Abs. 2 werden Inhalte aus Art. 32 Abs. 1 Buchst. a bis c der Verordnung (EU) Nr. 2016/679 übernommen.

Abs. 3 dient der Umsetzung von Art. 29 Abs. 2 der Richtlinie (EU) Nr. 2016/680 und nimmt den wesentlichen Inhalt von § 10 Abs. 2 HDSG auf, um ihn in das HDSIG-E zu überführen. Es werden die Ziele benannt, die im Hinblick auf automatisierte Verarbeitungen durch die Etablierung geeigneter technischer und organisatorischer Maßnahmen verfolgt und erreicht werden sollen.

In Abs. 4 wird die Bestimmung des § 10 Abs. 3 HDSG übernommen.

Zu § 60 (Meldung von Verletzungen des Schutzes personenbezogener Daten an die Hessische Datenschutzbeauftragte oder den Hessischen Datenschutzbeauftragten)
§ 60 dient der Umsetzung von Art. 30 der Richtlinie (EU) Nr. 2016/680 und legt den Umfang und die Modalitäten der Meldung von Verletzungen des Schutzes personenbezogener Daten (in § 41 Nr. 10 definiert) an die oder den Hessischen Datenschutzbeauftragten fest. Ansatzpunkt für eine solche Meldung sind beispielsweise Vorfälle wie Datenabflüsse. Abs. 1 bis 6 setzen jeweils Art. 30 Abs. 1 bis 6 der Richtlinie (EU) Nr. 2016/680 um.

Abs. 1 macht die Meldung der Verletzung vom voraussichtlichen Risiko für die Rechte und Freiheiten natürlicher Personen abhängig und verweist in Satz 3 für die Bestimmung des Risikos auf § 59 Abs. 1 Satz 2.

Die in Abs. 5 geforderte Dokumentation muss so beschaffen sein, dass sie der oder dem Hessischen Datenschutzbeauftragten die Überprüfung der Einhaltung der gesetzlichen Vorgaben ermöglicht.

In Abs. 7 wird durch den Verweis auf § 37 Abs. 4 HDSIG-E an dieser Stelle ebenfalls dem verfassungsrechtlichen Verbot einer Selbstbezichtigung Rechnung getragen. Die Regelung erfolgt in Umsetzung des Art. 57 der Richtlinie (EU) Nr. 2016/680, wonach die Mitgliedstaaten Sanktionen für Verstöße gegen die nach dieser Richtlinie erlassen Vorschriften festlegen und alle zu deren Anwendung erforderlichen Maßnahmen treffen. Die Motivation zur Meldung einer Verletzung des Schutzes personenbezogener Daten soll nicht dadurch verringert werden, dass die durch die Meldung verfügbar werdenden Informationen zur Einleitung eines Strafverfahrens führen können.

Abs. 8 stellt klar, dass die in § 60 HDSIG-E enthaltene Meldepflicht an die Hessische Datenschutzbeauftragte oder den Hessischen Datenschutzbeauftragten andere Meldepflichten nicht ausschließt und diesen auch nicht vorgeht.

Zu § 61 (Benachrichtigung betroffener Personen bei Verletzungen des Schutzes personenbezogener Daten)
§ 61 HDSIG-E setzt Art. 31 der Richtlinie (EU) Nr. 2016/680 um. Abs. 1 bis 5 setzen jeweils Art. 31 Abs. 1 bis 5 der Richtlinie (EU) Nr. 2016/680 um.

Abs. 1 macht die Benachrichtigung über die Verletzung personenbezogener Daten vom voraussichtlichen hohen Risiko für die Rechte und Freiheiten natürlicher Personen abhängig und verweist in Satz 2 für die Bestimmung des Risikos auf § 59 Abs. 1 Satz 2.

In Abs. 6 wird - parallel zu § 60 Abs. 7 HDSIG-E - durch einen Verweis auf § 37 Abs. 4 HDSIG-E wiederum dem verfassungsrechtlichen Verbot einer Selbstbezichtigung Rechnung getragen.

Zu § 62 (Durchführung einer Datenschutz-Folgenabschätzung)
§ 62 HDSIG-E dient der Umsetzung von Art. 27 der Richtlinie (EU) Nr. 2016/680.

In Abs. 1 wird Art. 27 Abs. 1 der Richtlinie (EU) Nr. 2016/680 umgesetzt. Die Voraussetzungen zur Durchführung einer Datenschutz-Folgenabschätzung können gesetzlich nur unvollkommen und nicht abschließend ausgestaltet werden. Die Konkretisierung der in Abs. 1 genannten Voraussetzungen obliegt damit letztlich der Praxis. Dabei ist allerdings zu beachten, dass die entstehenden Aufwände angemessen und beherrschbar bleiben müssen. Nach Erwägungsgrund 58 Satz 2 der Richtlinie (EU) Nr. 2016/680 sollten Datenschutz-Folgenabschätzungen auf maßgebliche Systeme und Verfahren im Rahmen von Verarbeitungsvorgängen, nicht jedoch auf Einzelfälle abstellen. Eine Datenschutz-Folgenabschätzung sollte grundsätzlich nur bei neuen Verarbeitungssystemen oder wesentlichen Veränderungen an bestehenden Systemen durchgeführt werden, soweit die Voraussetzungen des Abs. 1 gegeben sind. Abs. 1 Satz 2 verweist für die Bestimmung des Risikos auf § 59 Abs. 1 Satz 2. Kriterien für die Entscheidung, ob die vorgesehene Verarbeitung qualitativ erhöhte Risiken für die Rechte und Freiheiten der betroffenen natürlichen Person in sich birgt, können beispielsweise der Kreis der betroffenen Personen, die Art der zur Datenerhebung eingesetzten Mittel oder der Kreis der zugriffsberechtigten Personen und damit die Eingriffsintensität der mit der Verarbeitung verbundenen Maßnahmen im Sinne einer Gesamtwürdigung sein.

Abs. 2 übernimmt die Vorgaben des Art. 35 Abs. 1 Satz 2 der Verordnung (EU) Nr. 2016/679 und Abs. 3 die Vorgaben des Art. 35 Abs. 2 der Verordnung (EU) Nr. 2016/679.

Abs. 4 legt den Inhalt der Datenschutz-Folgenabschätzung fest und konkretisiert die in Art. 27 Abs. 2 der Richtlinie (EU) Nr. 2016/680 enthaltenen allgemeinen Angaben unter Übernahme der Inhalte aus Art. 35 Abs. 7 der Verordnung (EU) Nr. 2016/679.

Abs. 5 übernimmt die Vorgaben aus Art. 35 Abs. 11 der Verordnung (EU) Nr. 2016/679.

Zu § 63 (Zusammenarbeit mit der oder dem Hessischen Datenschutzbeauftragten)
§ 63 HDSIG-E setzt Art. 26 der Richtlinie (EU) Nr. 2016/680 um. Die hier angesprochene Pflicht des Verantwortlichen und des Auftragsverarbeiters zur Zusammenarbeit mit der oder dem Hessischen Datenschutzbeauftragten fasst die sich ohnehin aus anderen Vorschriften ergebenden Kooperationsverpflichtungen und Kooperationsbeziehungen zwischen den Vorgenannten zusammen.

Zu § 64 (Vorherige Konsultation der oder des Hessischen Datenschutzbeauftragten)
§ 64 HDSIG-E dient der Umsetzung von Art. 28 der Richtlinie (EU) Nr. 2016/680. Die vorherige Konsultation der oder des Hessischen Datenschutzbeauftragten dient der datenschutzrechtlichen Absicherung in Bezug auf beabsichtigte Verarbeitungen in neu anzulegenden Dateisystemen sowie bei wesentlichen Veränderungen an bestehenden Dateisystemen. Insofern besteht eine enge inhaltliche Verbindung zum Instrument der Datenschutz-Folgenabschätzung (§ 62), die dadurch hergestellt wird, dass nach Abs. 1 Satz 1 Nr. 1 eine vorherige Konsultation durchzuführen ist, wenn aus einer Datenschutz-Folgenabschätzung ein hohes Risikopotential für die Rechte und Freiheiten der betroffenen Personen hervorgeht. Abs. 1 Satz 3 verweist für die Bestimmung des Risikos auf § 59 Abs. 1 Satz 2.

Der Umfang der der oder dem Hessischen Datenschutzbeauftragten vorzulegenden Informationen wird in Abs. 2 durch Zusammenführung der Vorgaben aus Art. 28 Abs. 4 der Richtlinie (EU) Nr. 2016/680 und Art. 36 Abs. 3 der Verordnung (EU) Nr. 2016/679 bestimmt.

Abs. 3 setzt die Vorgaben aus Art. 28 Abs. 5 der Richtlinie (EU) Nr. 2016/680 um.

In Abs. 4 wird eine Eilfallregelung geschaffen, die in Abweichung von der in Abs. 3 vorgesehenen Fristregelung eine Datenverarbeitung vor Ablauf der Frist vorsieht. Zwar wird man im Regelfall den Abschluss der Konsultation im Interesse der Betroffenen abwarten, aber ausnahmsweise kann eine Datenverarbeitung aufgrund bedeutsamer operativer und (polizei-) fachlicher Erfordernisse vor Ablauf der Frist geboten sein. Die Nutzung der Eilfallregelung entbindet den Verantwortlichen gleichwohl nicht davon, die Empfehlungen der oder des Hessischen Datenschutzbeauftragten nach pflichtgemäßem Ermessen zu prüfen und die Verarbeitung gegebenenfalls daraufhin anzupassen.

Abs. 5 dient der Umsetzung von Art. 28 Abs. 2 der Richtlinie (EU) Nr. 2016/680.

Zu § 65 (Verzeichnis von Verarbeitungstätigkeiten)
§ 65 HDSIG-E dient der Umsetzung von Art. 24 der Richtlinie (EU) Nr. 2016/680 und verpflichtet in Abs. 1 den Verantwortlichen zur Führung eines Verzeichnisses über bei ihm durchgeführte Kategorien von Datenverarbeitungstätigkeiten. Dieses Verzeichnis dient vor allem dazu, der oder dem Hessischen Datenschutzbeauftragten einen Überblick über die beim Verantwortlichen durchgeführten Datenverarbeitungen zu geben und die Kontrolle der Verarbeitungsvorgänge zu ermöglichen. Das Zusammenspiel von vorheriger Konsultation (§ 64), Einsicht in das Verzeichnis (§ 65 Abs. 4) und Zurverfügungstellung von Protokolldaten (§ 71 Abs. 4) gewährt der oder dem Hessischen Datenschutzbeauftragten ein umfassendes Bild über die beim Verantwortlichen durchgeführten Datenverarbeitungen. In Abs. 1 werden zudem die in das Verzeichnis aufzunehmenden Angaben benannt und Art. 24 Abs. 1 der Richtlinie (EU) Nr. 2016/680 umgesetzt. Die Begrifflichkeit "Kategorien von Datenverarbeitungstätigkeiten" stellt klar, dass sich das Verzeichnis nicht auf einzelne Datenverarbeitungsvorgänge, sondern auf sinnvoll abgrenzbare Teile der beim Verantwortlichen durchgeführten Datenverarbeitungen bezieht. Es kann sich anbieten, die nach Abs. 1 Satz 2 Nr. 2 aufzunehmenden Angaben zu den Zwecken der Verarbeitung an den gesetzlichen Aufgabenzuschreibungen der betreffenden öffentlichen Stelle auszurichten.

Abs. 2 setzt Art. 24 Abs. 2 der Richtlinie (EU) Nr. 2016/680 für ein vom Auftragsverarbeiter zu führendes Verzeichnis um und verpflichtet dabei den Verantwortlichen, ein Verzeichnis, wenngleich in geringerem Umfang, auch für Verarbeitungen zu führen, wenn er personenbezogene Daten im Auftrag verarbeitet.

In Abs. 3 werden Aussagen zur Form des Verzeichnisses getroffen und Art. 24 Abs. 3 der Richtlinie (EU) Nr. 2016/680 umgesetzt.

Nach Abs. 4 wird das Verzeichnis und seine Aktualisierungen der oder dem Hessischen Datenschutzbeauftragten auf Anfrage zur Verfügung gestellt.

Zu § 66 (Datenschutz durch Technikgestaltung und datenschutzfreundliche Voreinstellungen)
Durch § 66 HDSIG-E wird Art. 20 der Richtlinie (EU) Nr. 2016/680 umgesetzt, der bestimmte allgemeine Anforderungen an den Datenschutz durch Technikgestaltung von Datenverarbeitungssystemen (Privacy by Design) in Abs. 1 und die Implementierung datenschutzfreundlicher Voreinstellungen (Privacy by Default) in Abs. 2 formuliert. Der Norm liegt der Gedanke zugrunde, dass der Aufwand zur Verfolgung der formulierten Ziele und Anforderungen im Sinne eines effizienten Mitteleinsatzes in einem angemessenen Verhältnis zum angestrebten Schutzzweck stehen sollte. Die in Abs. 2 getroffene Regelung, durch Voreinstellungen automatisierte umfassende Zugänglichmachung personenbezogener Daten zu verhindern, mündet in der Vorgabe, eine solche Zugänglichmachung stets durch menschliches Zutun einer Prüfung zu unterziehen.

Zu § 67 (Unterscheidung zwischen verschiedenen Kategorien betroffener Personen)
§ 67 HDSIG-E dient der Umsetzung von Art. 6 Richtlinie (EU) Nr. 2016/680 zur Unterscheidung verschiedener Kategorien betroffener Personen. Die konkreten Rechtsfolgen der vorgesehenen Unterscheidung bei der Verarbeitung personenbezogener Daten, etwa der Unterscheidung entsprechender Aussonderungsprüffristen, Rechte- und Rollenkonzepte oder besonderer Maßnahmen der Datensicherheit, werden dem Fachrecht überlassen.

Zu § 68 (Unterscheidung zwischen Tatsachen und persönlichen Einschätzungen)
§ 68 HDSIG-E dient der Umsetzung von Art. 7 Abs. 1 der Richtlinie (EU) Nr. 2016/680. Die konkreten Ausgestaltungen und Rechtsfolgen der vorgesehenen Unterscheidung zwischen personenbezogenen Daten auf Grundlage von Tatsachen oder persönlichen Einschätzungen werden dem Fachrecht überlassen.

Zu § 69 (Qualitätssicherung personenbezogener Daten vor deren Übermittlung)
§ 69 Abs. 1 HDSIG-E dient der Umsetzung von Art. 7 Abs. 2 der Richtlinie (EU) Nr. 2016/680. Es ist bei der Anwendung und Auslegung des § 69 zu beachten, dass sich die Frage nach der "Aktualität" von Daten und der damit verbundenen Vorgabe, keine "nicht mehr aktuellen" Daten zu übermitteln oder bereitzustellen, stets nur im konkreten Ermittlungszusammenhang und unter Beachtung des konkreten Verarbeitungszwecks beantworten lässt. In bestimmten Ermittlungszusammenhängen kann auch die Übermittlung nicht (mehr) aktueller Daten wie alte Meldeadressen, alte (Geburts-) Namen etc. für die Aufgabenerfüllung erforderlich sein. Gleiches gilt für die Übermittlung unvollständiger Daten. Eine Übermittlung oder sonstige Bereitstellung soll in beiden Fällen nur dann unterbleiben, wenn sie ohne sachlichen Grund erfolgt.

Abs. 2 setzt Art. 9 Abs. 3 der Richtlinie (EU) Nr. 2016/680 um. Beispiele für im Fachrecht vorgesehene Hinweispflichten auf besondere Bedingungen können etwa Zweckbindungsregelungen bei der Weiterverarbeitung durch den Empfänger, das Verbot der Weiterübermittlung ohne Genehmigung oder Konsultationserfordernisse vor der Beauskunftung betroffener Personen durch den Empfänger sein.

Abs. 3 setzt Art. 9 Abs. 4 der Richtlinie (EU) Nr. 2016/680 um.

Zu § 70 (Berichtigung und Löschung personenbezogener Daten sowie Einschränkung der Verarbeitung)
§ 70 HDSIG-E dient der Umsetzung von Art. 16 der Richtlinie (EU) Nr. 2016/680 in seiner Ausformung als Pflicht des Verantwortlichen. Systematisch werden Pflichten des Verantwortlichen zur Berichtigung und Löschung personenbezogener Daten sowie zur Einschränkung ihrer Verarbeitung thematisiert, die unabhängig davon bestehen, ob eine betroffene Person ein darauf gerichtetes Ersuchen gestellt hat. Die spiegelbildlich bestehenden Rechte der betroffenen Person auf Berichtigung, Löschung personenbezogener Daten sowie auf Einschränkung der Verarbeitung durch den Verantwortlichen finden sich in § 53 HDSIG-E.

In Abs. 1 wird die Pflicht des Verantwortlichen zur Berichtigung von personenbezogenen Daten statuiert.

Abs. 2 dient der Umsetzung von Art. 16 Abs. 2 der Richtlinie (EU) Nr. 2016/680, der sowohl das Betroffenenrecht auf Löschung als auch die unabhängig davon bestehende Pflicht des Verantwortlichen zur Löschung vorsieht.

Im Hinblick auf Abs. 3 wird auf die Ausführungen zu § 53 HDSIG-E Bezug genommen.

Abs. 4 dient der Umsetzung von Art. 5 der Richtlinie (EU) Nr. 2016/680 zu Fristen für die Speicherung und Überprüfung.

Zu § 71 (Protokollierung)
§ 71 HDSIG-E dient der Umsetzung von Art. 25 der Richtlinie (EU) Nr. 2016/680 und statuiert in Abs. 1 eine umfassende Pflicht des Verantwortlichen zur Protokollierung der unter seiner Verantwortung durchgeführten Datenverarbeitungen.

Abs. 2 enthält konkrete Vorgaben zum Inhalt der Protokolle und setzt Art. 25 Abs. 1 Satz 2 der Richtlinie (EU) Nr. 2016/680 um.

Abs. 3 statuiert Verwendungsbeschränkungen, wobei von der durch die Richtlinie (EU) Nr. 2016/680 eröffneten Möglichkeit, die Protokolldaten über die Datenschutzkontrolle, Eigenüberwachung und Aufrechterhaltung der Datensicherheit hinaus auch im Zusammenhang mit der Verhütung oder Verfolgung von Straftaten zu verwenden, Gebrauch gemacht wird.

In Abs. 4 wird geregelt, dass die Protokolle der oder dem Hessischen Datenschutzbeauftragten zum Zweck der Datenschutzkontrolle auf Anforderung zur Verfügung stehen müssen.

Zu § 72 (Vertrauliche Meldung von Verstößen)
§ 72 HDSIG-E dient der Umsetzung von Art. 48 der Richtlinie (EU) Nr. 2016/680. Der Verantwortliche hat im Zusammenhang mit der Meldung von Verstößen sowohl interne Meldungen innerhalb der öffentlichen Stelle als auch Hinweise von betroffenen Personen oder sonstigen Dritten in den Blick zu nehmen. Dafür bietet sich als Kontakt- und Beratungsstelle die oder der Datenschutzbeauftragte der öffentlichen Stelle an.

Zu § 73 (Allgemeine Voraussetzungen)
§ 73 HDSIG-E dient der Umsetzung von Art. 35 und 36 Abs. 1 der Richtlinie (EU) Nr. 2016/680 und regelt Voraussetzungen, die bei jeder Übermittlung personenbezogener Daten an Stellen in Drittländern oder an internationale Organisationen vorliegen müssen. Dabei fordert die Vorschrift das Vorliegen der übrigen für Datenübermittlungen geltenden Voraussetzungen, die für alle Datenverarbeitungen gelten, wie etwa die Erforderlichkeit der Übermittlung für die

Zwecke des § 40 HDSIG-E (vgl. Art. 35 Abs. 1 Buchst. a der Richtlinie (EU) Nr. 2016/680) oder die Einhaltung der Vorgaben der §§ 42 und 43 HDSIG-E. Des Weiteren enthält die Vorschrift zusätzliche Anforderungen an die Datenübermittlung an Stellen in Drittländern oder an internationale Organisationen - auch an die insbesondere nach den §§ 74 bis 76 HDSIG-E erforderliche Abwägungsentscheidung - aufgrund der Rechtsprechung des Bundesverfassungsgerichts (so etwa in BVerfG, Urteil vom 20. April 2016 - 1 BvR 966/09 u. 1 BvR 1140/06).

Abs. 1 Nr. 1 setzt Art. 35 Abs. 1 Buchst. b, Abs. 1 Nr. 2 Art. 35 Abs. 1 Buchst. d erste Variante der Richtlinie (EU) Nr. 2016/680 um.

Abs. 2 fordert über die Vorgaben des Art. 35 Abs. 1 Buchst. d und Art. 36 Abs. 1 der Richtlinie (EU) Nr. 2016/680) hinaus ein Unterbleiben der Übermittlung, wenn im Einzelfall Anlass zur Besorgnis besteht, dass ein elementaren rechtsstaatlichen Grundsätzen genügender Umgang mit den übermittelten Daten nicht gesichert ist, und diese Besorgnis auch nach einer Prüfung durch den Verantwortlichen weiter besteht. Hierbei ist nach Abs. 2 Satz 2 besonders zu berücksichtigen, ob der Empfänger einen angemessenen Schutz der Daten garantiert.

In Abs. 3 Satz 1 wird Art. 35 Abs. 1 Buchst. c sowie in Abs. 3 Satz 2 und 3 Art. 35 Abs. 2 der Richtlinie (EU) Nr. 2016/680 umgesetzt. Soweit demnach eine Datenübermittlung nach Abs. 1 des § 73 erfolgen soll und die zugrunde liegenden personenbezogenen Daten ursprünglich aus einem anderen Mitgliedstaat der Europäischen Union übermittelt oder zur Verfügung gestellt wurden, regelt Abs. 3 Satz 1 das Erfordernis zur Einholung der vorherigen Genehmigung des anderen Mitgliedstaats. Abs. 3 Satz 2 befreit unter den dort näher ausgeführten Voraussetzungen von dem vorherigen Genehmigungserfordernis und sieht nach Abs. 3 Satz 3 in diesen Fällen eine unverzügliche Unterrichtung des anderen Mitgliedstaats vor.

Abs. 4 dient der Umsetzung von Art. 35 Abs. 1 Buchst. e der Richtlinie (EU) Nr. 2016/680.

Zu § 74 (Datenübermittlung bei geeigneten Garantien)
§ 74 HDSIG-E dient der Umsetzung von Art. 37 der Richtlinie (EU) Nr. 2016/680 und formuliert § 73 HDSIG-E ergänzende Voraussetzungen für Datenübermittlungen an Stellen in Drittländern oder an internationale Organisationen, zu denen die Europäische Kommission keinen Angemessenheitsbeschluss nach Art. 36 der Richtlinie (EU) Nr. 2016/680 gefasst hat. Hier kommt dem Verantwortlichen - insbesondere nach § 74 Abs. 1 Nr. 2 HDSIG-E - die Aufgabe zu, das Vorliegen geeigneter Garantien für den Schutz personenbezogener Daten beim Empfänger zu beurteilen. Im Zusammenhang mit dem auch hier anwendbaren § 73 Abs. 2 HDSIG-E entfaltet der dort erwähnte Gesichtspunkt der Einzelfallgarantie des Empfängerstaats bei der Prüfung des Vorhandenseins geeigneter Garantien besondere Bedeutung.

Abs. 2 dient der Umsetzung von Art. 37 Abs. 3 der Richtlinie (EU) Nr. 2016/680 zur Dokumentation der Übermittlungen nach § 74.

Abs. 3 dient der Umsetzung von Art. 37 Abs. 2 der Richtlinie (EU) Nr. 2016/680, der die Unterrichtung der oder des Hessischen Datenschutzbeauftragten über Kategorien von Übermittlungen nach Abs. 1 Nr. 2 vorsieht.

Zu § 75 (Ausnahmen für eine Datenübermittlung ohne geeignete Garantien)
§ 75 HDSIG-E dient der Umsetzung von Art. 38 der Richtlinie (EU) Nr. 2016/680 und betrifft Datenübermittlungen, bei denen weder ein Angemessenheitsbeschluss der Europäischen Kommission vorliegt noch die in § 74 HDSIG-E geregelten Garantien in Form eines rechtsverbindlichen Instruments oder nach Beurteilung durch den übermittelnden Verantwortlichen bestehen.

Abs. 1 setzt Art. 38 Abs. 1 der Richtlinie (EU) Nr. 2016/680 und Abs. 2 Art. 38 Abs. 2 der Richtlinie (EU) Nr. 2016/680 um.

Abs. 3 dient der Umsetzung von Art. 38 Abs. 3 der Richtlinie (EU) Nr. 2016/680 zur Dokumentation der Übermittlungen nach § 75 HDSIG-E und ordnet dafür die entsprechende Geltung von § 74 Abs. 2 und 3 HDSIG-E an.

Zu § 76 (Sonstige Übermittlung an Empfänger in Drittländern)
§ 76 HDSIG-E dient der Umsetzung von Art. 39 der Richtlinie (EU) Nr. 2016/680. Der Kreis der möglichen Empfänger wird hier über die in § 73 Abs. 1 Nr. 1 HDSIG-E genannten Stellen hinaus auf sonstige (öffentliche) Stellen oder Einrichtungen und Private in Drittländern ausgeweitet. Dies können etwa Ersuchen an Finanzinstitutionen oder Telekommunikationsdienstleister sein, die notwendigerweise mit der Übermittlung personenbezogener Daten verbunden sind. Für solche Übermittlungen "im besonderen Einzelfall" gelten die in § 76 Abs. 1 HDSIG-E genannten strengen Voraussetzungen.

Abs. 1 setzt Art. 39 Abs. 1 Buchst. a, b, c und e der Richtlinie (EU) Nr. 2016/680 und Abs. 2 Art. 39 Buchst. d der Richtlinie (EU) Nr. 2016/680 um.

Abs. 3 dient der Umsetzung von Art. 39 Abs. 3 und 4 der Richtlinie (EU) Nr. 2016/680 zur Dokumentation der Übermittlungen nach § 76 HDSIG-E und zur Unterrichtung der oder des Hessischen Datenschutzbeauftragten und ordnet dafür die entsprechende Geltung von § 74 Abs. 2 und 3 HDSIG-E an.

In Abs. 4 ist über die Vorgaben des Art. 39 der Richtlinie (EU) Nr. 2016/680 hinaus eine verstärkte Zweckbindung der nach § 76 HDSIG-E übermittelten Daten vorgesehen.

Abs. 5 setzt Art. 39 Abs. 1 i.V.m. Abs. 2 der Richtlinie (EU) Nr. 2016/680 um.

Zu § 77 (Gegenseitige Amtshilfe)
§ 77 HDSIG-E dient der Umsetzung von Art. 50 der Richtlinie (EU) Nr. 2016/680. Dabei setzen Abs. 1 und Abs. 2 Art. 50 Abs. 1 und Abs. 2 der Richtlinie (EU) Nr. 2016/680 um. Abs. 3 bis Abs. 6 dienen der Umsetzung von Art. 50 Abs. 4 bis Abs. 7 der Richtlinie (EU) Nr. 2016/680 und Abs. 7 setzt Art. 50 Abs. 3 der Richtlinie (EU) Nr. 2016/680 um.

Zu § 78 (Schadensersatz und Entschädigung)
Die Vorschrift des § 78 HDSIG-E setzt Art. 56 der Richtlinie (EU) Nr. 2016/680 um. Mit der Schadensersatzregelung wird die Systematik des § 20 HDSG zur verschuldensabhängigen Haftung bei nicht automatisierter Datenverarbeitung und der verschuldensunabhängigen Haftung bei sonstiger (automatisierter) Datenverarbeitung weitgehend erhalten. In Abs. 6 und 7 werden die Regelungen aus § 20 Abs. 3 und 4 HDSG übernommen.

Zu § 79 (Strafvorschriften)
Die Vorschrift des § 79 HDSIG-E setzt Art. 57 der Richtlinie (EU) Nr. 2016/680 um und verweist dafür auf die Strafvorschriften des § 37 HDSIG-E.

Durch § 79 HDSIG-E wird keine dem deutschen Recht grundsätzlich fremde Strafbarkeit öffentlicher Stellen eingeführt. Um das gesetzgeberische Ziel des Gleichlaufs der Sanktionsmöglichkeiten gegenüber öffentlichen Stellen bzw. deren Beschäftigten unabhängig von dem mit der Verarbeitung verfolgten Zweck herzustellen, wird auch für den Dritten Teil mit Blick auf § 38 Abs. 3 HDSIG-E davon ausgegangen, dass gegen Behörden keine Geldbußen verhängt werden. Im Hinblick auf die Strafbarkeit von Handlungen wird auf den für den Zweiten Teil maßgeblichen § 37 HDSIG-E abgestellt.

Zu § 80 (Anspruch auf Auskunft)
§ 80 Abs. 1 HDSIG-E gewährt jedermann einen Anspruch auf Zugang zu den bei öffentlichen Stellen vorhandenen amtlichen Informationen.

Vom Anspruch umfasst sind amtliche Informationen, d.h. die bei einer informationspflichtigen Stelle bereits vorhandenen, amtlichen Zwecken dienenden Aufzeichnungen, unabhängig von der Art ihrer Speicherung, außer Entwürfen und Notizen, die nicht Bestandteil eines Vorgangs werden sollen. Die unberechtigte Verweigerung der Auskunft stellt die Verletzung eines Rechts im Sinne des § 42 Abs. 2 VwGO dar.

Abs. 2 enthält gegenüber § 1 Abs. 2 HDSIG-E eine eigenständige Regelung zum Konkurrenzverhältnis zwischen dem allgemeinen Auskunftsrecht nach § 80 Abs. 1 HDSIG-E und der Vielzahl bereichsspezifischer Informationszugangsrechte. Diese bereichsspezifischen Regelungen verdrängen das allgemeine Auskunftsrecht, soweit sie eigenständige Voraussetzungen für die Gewährung, die Art und Weise oder den Umfang einer Auskunfts- oder sonstigen Form der Informationsgewährung enthalten. Die Anforderungen des Abs. 1 finden dadurch gegenüber Regelungen anderer Rechtsvorschriften über Auskunftsbegehren wie z.B. im Rahmen des Hessischen Umweltinformationsgesetzes, des Hessischen Presserechtsgesetzes, dem Hessischen Sicherheits- und Ordnungsgesetz, dem Hessischen Verfassungsschutzgesetz oder der kommunalrechtlichen Regelungen für Auskunftsrechte von Mandatsträgern keine Anwendung. Hierzu zählen etwa auch die besonderen Auskunftsrechte für Verfahrensbeteiligte nach § 29 HVwVfG oder § 25 SGB X. Dadurch wird sichergestellt, dass für Verfahrensbeteiligte während eines entsprechenden Verfahrens der Vierte Teil des HDSIG-E keine Anwendung findet, sondern diese sich allein auf die insoweit bestehenden Sonderregelungen berufen können. Nicht am Verfahren Beteiligte können entsprechende Auskunftsbegehren dagegen auf § 80 Abs. 1 HDSIG-E stützen, da ihr Auskunftsbegehren nicht Gegenstand fachrechtlicher Informationszugangsregelungen ist. Auch der allgemeine Anspruch auf Akteneinsicht nach den Grundsätzen des § 29 HVwVfG, der nicht am Verfahren Beteiligten zusteht, wenn sie ein berechtigtes Interesse glaubhaft machen, wird durch Abs. 2 nicht ausgeschlossen.

Im Übrigen ergeben sich mittelbar aus der Anknüpfung des Auskunftsrechts an den allgemeinen Anwendungsbereich des HDSIG-E und an den Begriff der öffentlichen Stelle (§ 2 Abs. 1 bis 3 HDSIG-E) weitere Fallgruppen, in denen weiterhin nur nach Maßgabe der jeweiligen bereichsspezifischen Regelungen Auskunftsrechte bestehen, z.B. gegenüber Kirchen und Religionsgemeinschaften, die über eigenständige datenschutzrechtliche Regelungen verfügen, oder dem Hessischen

Rundfunk, auf den das HDSIG-E nach § 1 Abs. 4 nur außerhalb des Bereichs journalistisch-redaktioneller Tätigkeit Anwendung findet. Der Auskunftsanspruch unterliegt weiterhin den allgemeinen Einschränkungen des § 2 Abs. 3 2 HDSIG-E, sodass das Auskunftsrecht etwa nicht gegenüber öffentlichen Stellen gilt, soweit diese als Unternehmen am Wettbewerb teilnehmen.

Zu § 81 (Anwendungsbereich)
§ 81 legt den Anwendungsbereich des Informationszugangsanspruch fest und begrenzt dabei auch den Anspruch auf Auskunft in spezifischen Bereichen öffentlicher Aufgabenerfüllung, bei denen generell vorrangige öffentliche oder private Belange einer Auskunftsgewährung entgegenstehen. Der Begriff der öffentlichen Stelle bemisst sich grundsätzlich nach § 2 Abs. 1-3.

Vor dem Hintergrund der Gewaltenteilung bedarf es bei Vorschriften, deren Gegenstand es vorrangig ist, im Bereich der Exekutive für mehr Transparenz zu sorgen, der ausdrücklichen Bestimmung der von seinen Wirkungen nicht erfassten bzw. aufgrund der Geltung höherrangigen Rechts nicht erfassbaren Stellen.

Satz 1 Nr. 1 schließt daher den Bereich des Landtags von der Anwendung des Vierten Teils des HDSIG-E aus, soweit die Freiheit des Mandats, der Bereich der Abgeordneten- und Fraktionsangelegenheiten sowie die Nicht öffentlichkeit von Landtagsberatungen betroffen ist.

Eine Bereichsausnahme gilt nach Nr. 2 für den Hessischen Rechnungshof und die Hessische Datenschutzbeauftragte bzw. den Hessischen Datenschutzbeauftragten, soweit diese als Kontrollorgan tätig sind. Ein Anspruch auf Auskunft über Inhalte von Dateien und Akten würde in diesem Bereich ein Spannungsverhältnis zur Wahrnehmung der unabhängigen Kontrollaufgaben gegenüber der Exekutive bzw. datenverarbeitenden privaten Stellen schaffen.

Die übrigen in Satz 1 Nrn. 3 bis 6 aufgenommenen Fallgruppen betreffen öffentliches Handeln in Bereichen, die wegen der Art oder des Umfangs der dabei verarbeiteten Daten mit spezifischen Schutzerfordernissen verbunden sind, die der Einräumung allgemeiner Auskunftsansprüche entgegenstehen. Die Abwägung zwischen Informationszugangsinteressen und entgegenstehenden öffentlichen oder privaten Belangen bleibt in diesen Fallgruppen vorrangigen bereichsspezifischen Regelungen vorbehalten.

Satz 1 Nr. 3 nimmt die Gerichte und weitere Organe der Rechtspflege sowie Disziplinarbehörden vom Anwendungsbereich des Auskunftsrechts aus soweit sie als Organe der Rechtspflege oder aufgrund besonderer Rechtsvorschriften in richterlicher oder sachlicher Unabhängigkeit tätig sind. Denn in diesen Fällen werden personenbezogene Daten regelmäßig einer Auskunftserteilung im Wege stehen, sodass auch in diesem Fall typisierend von einem Überwiegen schutzwürdiger Interessen am Ausschluss der Übermittlung auszugehen ist.

Für die Finanzbehörden besteht nach Satz 1 Nr. 4 eine Bereichsausnahme, soweit sie in Verfahren nach der Abgabenordnung tätig sind. § 32e AO in der am 25. Mai 2018 in Kraft tretenden Fassung (siehe Gesetz zur Änderung des Bundesversorgungsgesetzes und anderer Vorschriften vom 17. Juli 2017, BGBl. I Seite 2541) schließt über die besonderen Vorschriften der AO hinausgehende Auskunftsrechte nach dem Informationsfreiheitsgesetz des Bundes oder entsprechenden Gesetzen der Länder grundsätzlich aus.

Unter den Begriff der sonstigen öffentlichen Stellen im Sinne des Satz 1 Nr. 5 fallen im Bereich von Forschung und Lehre, Leistungsbeurteilungen und Prüfungen insbesondere der Prüfungsbereich des Landesjustizprüfungsamts sowie öffentliche Krankenhäuser, die zwar keine Universitätskliniken sind, aber gleichwohl im Bereich der Forschung tätig und insoweit genauso schutzwürdig sind.

Nach Satz 1 Nr. 6 unterliegen die Behörden und sonstigen öffentlichen Stellen der Kommunen nicht der Auskunftspflicht nach den Vorschriften des Vierten Teils des HDSIG-E, es sei denn deren Anwendung wird ausdrücklich durch eine kommunale Satzung bestimmt. Die Erfahrungen der anderen Länder mit Gesetzen zum Informationszugang belegen eindeutig, dass die weit überwiegende Zahl der Auskunftsersuchen an kommunale Stellen gerichtet werden. Eine Verpflichtung aller öffentlichen Stellen im Sinn des § 2 HDSIG-E zur Auskunft nach § 80 Abs. 1 HDSIG-E würde daher insgesamt die kommunalen Stellen stärker belasten, als die Stellen des Landes. Allerdings verfügt das Land dabei nur über unzureichende Möglichkeiten zu beurteilen, ob die Kommunen in der Lage sind, die Gewährung des Informationszugangs mit den zur Verfügung stehenden Mitteln zu bewältigen. Es soll daher der kommunalen Selbstverwaltung und damit der Entscheidung der einzelnen Kommune bzw. deren kommunalen Vereinigung die Entscheidung darüber überlassen bleiben, ob sie den Informationszugang nach den Vorschriften des Vierten Teils des HDSIG-E eröffnen will. Diese Optionsmöglichkeit für die Kommunen stellt zugleich sicher, dass zum Zeitpunkt des Inkrafttretens bereits bestehende, z.B. gemeindliche Informationszugangssatzungen nicht automatisch durch das Landesrecht verdrängt werden. Es bleibt auch in diesen Fällen der Entscheidung der Kommune überlassen, ob sie eine bestehende Satzung aufheben und die Geltung des Auskunftsrechts nach den Vorschriften des HDSIG-E bestimmen will.

Die in Abs. 2 genannten öffentlichen Stellen werden vom Anwendungsbereich der Vorschriften über den Informationszugang nach § 80 Abs. 1 vollständig ausgenommen.

Sowohl die Polizeibehörden als auch das Landesamt für Verfassungsschutz verarbeiten regelmäßig Daten mit spezifischen Schutzerfordernissen, die der Einräumung eines allgemeinen Auskunftsanspruchs entgegenstehen. Der Informationszugang soll in diesem für die innere Sicherheit wichtigen Bereich daher weiterhin nach Maßgabe der bereichsspezifischen Regelungen des HSOG und Hessischen Verfassungsschutzgesetzes gewährt werden.

Das Wirtschaftsministerium, soweit es als Landeskartellbehörde tätig wird, und die Regulierungskammer Hessen sind von dem allgemeinen Auskunftsanspruch ausgenommen, da beide Behörden in erheblichem Umfang Betriebs- und Geschäftsgeheimnisse der von ihnen kontrollierten bzw. regulierten Unternehmen verarbeiten. Allgemeine Auskunftsansprüche beträfen daher von vorne herein nur sehr begrenzte Teilbereiche ihrer Dateien und Akten, die zudem nur mit erheblichem Aufwand oder überhaupt nicht von Betriebs- oder Geschäftsgeheimnissen abgegrenzt werden können. Insbesondere die Regulierungskammer nimmt ihre Aufgaben unabhängig und in einem gerichtsähnlichen Verfahren wahr, dass bereits durch seine Ausgestaltung relative Gewähr für Richtigkeit bietet. Die Landeskartellbehörde wie die Regulierungskammer als Hüterinnen des Wettbewerbs unterliegen außerdem bundesrechtlichen Veröffentlichungspflichten, die nach Auffassung des Bundesgesetzgebers als Informationsinstrument für die Bürgerinnen und Bürger ausreichen. Dem wird im Landesrecht durch die vorliegende Ausnahmeregelung Rechnung getragen.

Auch die Industrie- und Handels- und Handwerkskammern sind wegen ihrer besonderen Aufgabenstellung im Bereich der berufsständischen Selbstverwaltung vom Anwendungsbereich des allgemeinen Auskunftsanspruchs ausgenommen. Die im Prüfprogramm der §§ 82 bis 84 HDSIG-E vorgesehenen Schutztatbestände u.a. zur Wahrung allgemeiner Persönlichkeitsrechte, von Berufs- und Geschäftsgeheimnissen, vertraulicher Beratungsprozesse oder für Prüfungsangelegenheiten vermitteln zwar auch für die Aufgabenerfüllung der Industrie- und Handels- und Handwerkskammern einschlägige einzelfallbezogene oder generelle Lösungen zum Ausgleich zwischen berechtigten Schutzinteressen und Auskunftsanliegen, rechtfertigen aber bei einer Gesamtbetrachtung der Geschäftsvorgänge auch eine eigenständige Bereichsausnahme. Die Regelung dient damit angesichts der großen Bandbreite der von den Kammern wahrgenommenen Aufgaben der gebotenen Verwaltungsvereinfachung und trägt zur effektiven Erfüllung der diesen Selbstverwaltungsorganisationen vorbehaltenen oder ihnen vom Staat übertragenen Aufgaben bei. Der in Satz 1 Nr. 7 geschaffene Ausschlusstatbestand lässt die Befugnis der Industrie- und Handels- und Handwerkskammern unberührt, in Rahmen ihrer Satzungsautonomie im Interesse transparenter Aufgabenerfüllung gleichwohl spezifische Regelungen über Auskunftsersuchen zu treffen, die den Besonderheiten ihrer Aufgabenstellung und der Leistungsfähigkeit ihrer Organisationen angemessen Rechnung tragen.

Nach Abs. 2 Nr. 4 sind auch Notare, die nach § 1 Bundesnotarordnung ein öffentliches Amt bekleiden, vom Anwendungsbereich der Vorschriften über den Informationszugang ausgenommen. Die Offenlegung von Informationen durch Notare wäre mit der Pflicht zur Verschwiegenheit nach § 18 Abs. 1 Bundesnotarordnung nicht zu vereinbaren.

§ 81 Abs. 3 HDSIG-E soll sicherstellen, dass die Regelungen der Abs. 1 und 2 nicht umgangen werden können, wenn und soweit sich Dateien- oder Aktenbestandteile dieser Stellen, die vom Informationszugangsanspruch vollständig oder in bestimmten Tätigkeitsfeldern ausgenommen sind, in Dateien und Akten anderer öffentlicher Stellen befinden. Soweit sich ein Auskunftsbegehren auf Dateien und Akten bezieht, die den Zuständigkeitsbereich mehrerer öffentlicher Stellen betreffen, diese Stellen aber nicht unter § 80 Abs. 1 HDSIG-E fallen, so hat die um Auskunft ersuchte Stelle nach allgemeinen Grundsätzen die mitbetroffenen Stellen vor einer Auskunftsgewährung zu beteiligen.

Zu § 82 (Schutz öffentlicher und privater Belange)
§ 82 HDSIG-E enthält weitere Klarstellungen zum Verhältnis zwischen dem allgemeinen Recht auf Informationszugang und spezifischen Regelungen zum Schutz besonderer öffentlicher oder privater Geheimhaltungspflichten, die an die jeweiligen Informationsinhalte anknüpft.

Die Regelungen in Nrn. 1 und 3 über Verschlusssachen oder berufs- oder funktionsspezifische Geheimhaltungsverpflichtungen begrenzen das allgemeine Informationszugangsrecht. Die Bezeichnung "Berufs- oder besondere Amtsgeheimnisse" stellt anknüpfend an § 1 Abs. 2 Satz 2 HDSIG-E klar, dass das durch § 80 HDSIG-E eingeräumte Auskunftsrecht keine Befugnis zur Offenbarung besonders geschützter Geheimnisse vermittelt. Berufsgeheimnisse sind solche, die für Angehörige bestimmter Berufe gelten (z.B. § 203 Abs. 1 StGB). Besondere Amtsgeheimnisse sind solche, die dem Inhaber eines öffentlichen Amts in dieser Eigenschaft durch Gesetz oder aufgrund Gesetzes auferlegt sind. Es muss sich jedoch um ein "besonderes" Amtsgeheimnis handeln (z.B. das Steuergeheimnis nach § 30 AO oder das Sozialgeheimnis nach § 35 SGB I), die allgemeine Pflicht zur Verschwiegenheit (vgl. § 37 BeamtStG) oder das allgemeine Datengeheimnis nach § 48 HDSIG-E fallen dagegen nicht hierunter.

In Nr. 2 beziehen sich Buchst. a) und b) auf den Schutz der inter- oder supranationale Beziehungen, der Beziehungen zum Bund oder einem anderen Land sowie auf den Schutz der Belange der äußeren oder öffentlichen Sicherheit. Das Bekanntwerden nachteiliger Auswirkungen auf diese Rechtsgüter führt zum Ausschluss des Informationszugangsanspruchs.

Nach Nr. 2 Buchst. c kann die begehrte Auskunft verweigert werden, wenn ihr öffentliche Kontroll- und Aufsichtsaufgaben entgegenstehen. Dieser Versagungsgrund dient dem Schutz der Funktionsfähigkeit öffentlicher Kontroll- und Aufsichtsverfahren, die ihrem Wesen nach als verwaltungsinterne Vorgänge zur Gewährleistung der Recht- und ggf. Zweckmäßigkeit öffentlicher Aufgabenerfüllung durch besondere gewichtige Interessen am Ausschluss einer Informationsübermittlung geprägt sind. Im Rahmen von Kontroll- und Aufsichtsverfahren ist zudem vielfach eine besonders intensive und umfassende Verarbeitung auch von personenbezogenen Daten erforderlich, die besonderen Schutz benötigen, damit z.B. Wettbewerbsverzerrungen durch Auskünfte über aufsichtsbehördliche Erkenntnisse zu Konkurrenten vermieden werden.

Unter Kontroll- und Aufsichtsaufgaben fallen dabei alle Formen staatlicher Aufsicht, also sowohl die klassische Kommunalaufsicht als auch Sonderbereiche wie z.B. die Sparkassenaufsicht. Ein Entgegenstehen erfordert entsprechend dem Begriffsverständnis anderer öffentlichrechtlicher Regelungen ein nachteiliges Berührtsein der betroffenen Schutzgüter. Insoweit bedarf es einer Abwägung zwischen dem Auskunftsinteresse einerseits und der gebotenen ordnungsgemäßen Erfüllung der Kontrollaufgaben andererseits. Es bedarf also Auswirkungen der Informationszugangsgewährung, die die Erfüllung der Kontrollaufgaben zumindest teilweise verhindern würden.

Nr. 2 Buchst. d dient dem Schutz anhängiger Gerichts-, Ordnungswidrigkeiten, Disziplinarverfahren sowie laufender strafrechtlicher Ermittlungen.

Könnten zum persönlichen Lebensbereich gehörende Geheimnisse oder Betriebs- und Geschäftsgeheimnisse mit der Auskunftsgewährung offenbart werden, unterwirft Nr. 4 das Auskunftsrecht einem Einwilligungserfordernis. Dritte, deren schutzwürdige Interessen z.B. wegen möglicher Auswirkungen auf private Verwertungsrechte im Rahmen der nach § 83 HDSIG-E vorzunehmenden Abwägungsentscheidung berührt werden, sind nach allgemeinen verwaltungsverfahrensrechtlichen Regelungen vor der Auskunftsgewährung wie in anderen Fällen drittbelastender Verwaltungsakte anzuhören. Bleibt die Zulässigkeit der Auskunftsgewährung im Hinblick auf den Schutz privater Belange wie z.B. das Bestehen eines Einwilligungserfordernisses umstritten, folgt aus rechtsstaatlichen Grundsätzen außerdem, dass die Auskunftsgewährung erst erfolgen darf, wenn die Behördenentscheidung über den Anspruch auf Auskunft auch gegenüber dem betroffenen Dritten sofort vollziehbar oder unanfechtbar geworden ist.

Darüber hinaus wird nach Nr. 5 kein Zugang zu amtlichen Informationen gewährt, wenn an diesen ein rein wirtschaftliches Interesse besteht.

Zu § 83 (Schutz personenbezogener Daten)
Soweit die Erfüllung des Anspruchs auf Auskunft eine Übermittlung personenbezogener Daten erfordert, gelten weiterhin die datenschutzrechtlichen Übermittlungsvoraussetzungen an nicht öffentliche Stellen, die eine Datenübermittlung u.a. nur erlauben, wenn der Betroffene kein schutzwürdiges Interesse am Ausschluss der Übermittlung hat (vgl. § 22 Abs. 2 Satz 1 Nr. 2 HDSIG-E). Personenbezogene Daten bleiben damit weiterhin umfassend geschützt.

Zu § 84 (Schutz behördlicher Entscheidungsprozesse)
Ziel der Regelung ist die Normierung eines umfassend geschützten Bereichs der Entscheidungsbildung für Entscheidungsträger. Der Schutz interner Verwaltungsabläufe ist für die ordnungsgemäße Erfüllung der gesetzlichen Verwaltungsaufgaben unerlässlich. Das Streben nach Offenheit und Transparenz erfährt dort eine Einschränkung, wo die Effektivität des Verwaltungshandelns gefährdet ist. Neben der ungestörten Entscheidungsfindung ist es auch Zweck des Gesetzes, eine vollständige und unbefangene behördliche Aktenführung zu gewährleisten, die den Gang des Entscheidungsprozesses chronologisch und vollständig nachvollziehbar dokumentiert. Bereits die Überschrift aber stellt klar, dass sich der Schutz im Wesentlichen auf den Prozess der Entscheidungsfindung, nicht aber auf die Ergebnisse des Verwaltungshandelns bezieht. Ein Anspruch auf Zugang zu Information, die Verwaltungshandeln vorbereitet, besteht in der Regel nicht. Erfasst sind solche Entwürfe, die nach den Grundsätzen ordnungsgemäßer Aktenführung Bestandteil eines Vorgangs und damit eine amtliche Information geworden sind. Es sollen vor allem noch nicht endgezeichnete Schriftstücke nicht in die Öffentlichkeit gelangen, ebenso noch nicht vollständige bzw. nicht genügend verifizierte.

Da § 84 den Schutz von Verwaltungsabläufen bezweckt, ist entscheidend, dass die geschützten behördlichen Maßnahmen konkret bevorstehen.

Vereitelt wird der Erfolg der Entscheidung, wenn diese bei Offenbarung der Information voraussichtlich, überhaupt nicht mit anderem Inhalt oder wesentlich später zustande käme.

Nicht geschützt sind in der Regel Ergebnisse von Beweisaufnahmen, Gutachten und Stellungnahmen Dritter. Es handelt sich dabei um abgrenzbare Erkenntnisse, die die Verfahrensherrschaft der Behörde typischerweise nicht beeinträchtigen.

Zu § 85 (Antrag)
Nach Abs. 1 erfolgt der Informationszugang auf Antrag, der schriftlich, mündlich zur Niederschrift oder elektronisch gestellt wird.

In Abs. 2 Satz 1 sind die Anforderungen an den Inhalt eines Antrages geregelt. Es soll ein möglichst schneller und unbürokratischer Informationszugang gewährleistet werden, sodass wenig formale Hürden bei der Antragstellung aufgebaut werden sollen. Gleichfalls dem Ziel eines möglichst schnellen Informationszugangs für alle Bürgerinnen und Bürger dient die Regelung in Satz 2, welche summarische Auskünfte über eine Vielzahl von Einzelentscheidungen für unzulässig erklärt. Erforderlich ist jedoch ein hinreichend bestimmter Antrag, der klar erkennen lassen muss, welche Informationen begehrt werden. Gleichzeitig wird durch Satz 3 klargestellt, dass ein nicht hinreichend bestimmter Antrag nicht ohne Weiteres zurückgewiesen werden darf. Vielmehr hat die ersuchte Stelle auf die fehlenden Angaben hinzuweisen und der antragstellenden Person durch Beratung behilflich zu sein.

Abs. 3 dient der Verpflichtung der informationspflichtigen Stelle, im Falle kollidierender Interessen eine Güterabwägung vorzunehmen.

Der Antrag soll nach Abs. 4 bei der Stelle gestellt werden, bei welcher die begehrten Informationen vorliegen. Bei Unzuständigkeit hat die befragte Stelle die zuständige Stelle zu ermitteln und dem Bürger mitzuteilen.

Zu § 86 (Verfahren bei Beteiligung einer betroffenen Person)
Sind nach § 86 Abs. 1 schutzwürdige Belange i.S. der §§ 82 und 83 beteiligter Dritter betroffen, so sind Letztere innerhalb eines Monats zur Stellungnahme aufzufordern. Um sicherzugehen, dass der Dritte in die Weitergabe ihn betreffender Daten wirklich einverstanden ist, gilt ein Nicht-Antworten der betroffenen Person als Verweigerung der Zustimmung. Die betroffene Person ist über die Entscheidung des Antrages zu Informieren und kann gegebenenfalls bis zur Bestandskraft der Entscheidung dieser noch widersprechen.

Zu § 87 (Entscheidung)
Die in § 86 enthaltenen Fristenregelungen haben eine zentrale Bedeutung, weil ein Informationszugangsrecht ohne zwingende Fristen weitgehend wirkungslos ist. Die Behörde hat nach Abs. 1 die begehrten Informationen unverzüglich, also ohne schuldhaftes Zögern, spätestens aber innerhalb eines Monats zugänglich zu machen. Eine längere Frist gilt, wenn die Rechte Dritter berücksichtigt werden müssen.

Die Begründungspflicht nach Abs. 2 dient der Transparenz und der Verständlichkeit der ergangenen Entscheidung. Zudem hat die zuständige Stelle neben der Ablehnung auch mitzuteilen, ob und wann ein Informationszugang ganz oder teilweise möglich sein könnte. Dies betrifft insbesondere Entscheidungen, die wegen eines laufenden Verwaltungs- oder Gerichtsverfahrens abgelehnt werden müssen.

Nur in besonders schwierigen Fällen, in denen Umfang und Komplexität eine schnelle Zugänglichmachung nicht erlauben, kann nach Abs. 3 die Frist auf bis zu drei Monate verlängert werden.

Zu § 88 (Kosten)
Abs. 1 regelt die Erhebung der Kosten für die Gewährung der Auskunft nach § 80 Abs. 1 HDSIG-E. Die Höhe der etwaigen Gebühren richtet sich nach Maßgabe des Hessischen Verwaltungskostengesetzes in Verbindung mit der hierzu ergangenen Allgemeinen Verwaltungskostenordnung in der jeweils gültigen Fassung. Um einen möglichst einfachen und einheitlichen Vollzug der Kostenregelung durch die Verwaltungsbehörden aller Bereiche zu gewährleisten, übernimmt Abs. 1 im Wesentlichen die bewährte Vorschrift des § 11 Abs. 1 des Hessischen Umweltinformationsgesetzes.

Abs. 1 Satz 4 enthält den Grundsatz, dass Gebühren auch unter Berücksichtigung des Verwaltungsaufwandes so zu bemessen sind, dass die Antragsteller nicht von der Geltendmachung ihres Informationsanspruches nach § 80 Abs. 1 HDSIG-E abgehalten werden. Die auskunftspflichtige Stelle hat im Einzelfall, soweit Informationen zu der wirtschaftlichen Situation der antragstellenden Person vorliegen, in dem von § 88 Abs. 1 Satz 2 und 3 HDSIG-E gesteckten Rahmen zu entscheiden, ob die Geltendmachung der Verwaltungskosten geeignet wäre, die antragstellende Person von der Inanspruchnahme des Auskunftsrechts abzuhalten. In diesem Fall ist die Gebührenhöhe so zu reduzieren, dass eine wirksame Inanspruchnahme des Anspruchs gewährleistet ist. Ggf. kann nach § 17 HVwKostG aus Billigkeitsgründen auf die Gebührenerhebung verzichtet werden.

Abs. 2 bestimmt, dass die Kommunen und kommunalen Vereinigungen, die den Informationszugang nach § 81 Satz 1 Nr. 6 HDSIG-E eröffnet haben, die Erhebung der Gebühren und Auslagen in eigener Zuständigkeit durch Satzung regeln.

Zu § 89 (Die oder der Hessische Informationsfreiheitsbeauftragte)
Das Institut des Informationsfreiheitsbeauftragten hat sich national wie international bewährt. Zur Sicherung des Rechts auf Informationszugang wird daher durch Abs. 1 auch in Hessen eine Informationsfreiheitsbeauftragte bzw. einen Informationsfreiheitbeauftragten geschaffen. Damit wird Antragstellern, deren Antrag auf Informationszugang vollständig oder teilweise abgelehnt wurde, die Möglichkeit eröffnet, unabhängig von den Möglichkeiten zur Einlegung förmlicher Rechtsbehelfe, die oder den Hessischen Informationsfreiheitbeauftragten anzurufen, um die Entscheidung durch eine unabhängige Stelle überprüfen zu lassen. Die Anrufung ist weder an eine bestimmte Form, noch an eine Frist gebunden.

Nach Abs. 2 wird die Aufgabe der oder des Hessischen Informationsfreiheitsbeauftragten der oder dem Hessischen Datenschutzbeauftragten als weitere Aufgabe übertragen.

Soweit eine Überwachungsbefugnis der oder des Hessischen Informationsfreiheitsbeauftragten gegeben ist, sind ihm die öffentlichen Stellen nach Abs. 3 zur Unterstützung verpflichtet. Der oder dem Hessischen Informationsfreiheitsbeauftragten wird ein Akteneinsichts- und Zutrittsrecht zu den Diensträumen gewährt. Die oder der Hessische Informationsfreiheitbeauftragte kann die Verletzung von Bestimmungen nach dem Vierten Teil des Gesetzes beanstanden und ihre Behebung unter Einräumung einer angemessenen Frist fordern. Die zuständige Aufsichtsbehörde ist hierüber zu unterrichten.

Nach Abs. 4 ist die oder der Hessische Informationsfreiheitsbeauftragte verpflichtet, jährlich einen Bericht über ihre bzw. seine Tätigkeit im abgelaufenen Kalenderjahr vorzulegen. Die Regelung entspricht der Berichtspflicht der oder des Hessischen Datenschutzbeauftragten über die Tätigkeit als Aufsichtsbehörde für den Datenschutz.

Zu § 90 (Übergangsvorschrift)
Abs. 1 dient der Umsetzung von Art. 63 Abs. 2 der Richtlinie (EU) Nr. 2016/680.

Mit Abs. 2 wird eine Übergangsvorschrift für die oder den zum Zeitpunkt des Inkrafttretens des Gesetzes im Amt befindliche Hessische Datenschutzbeauftragte oder befindlichen Hessischen Datenschutzbeauftragten geschaffen.

Zu § 91 (Inkrafttreten)
Die Vorschrift regelt das Inkrafttreten des neuen Hessischen Datenschutz- und Informationsfreiheitsgesetzes.

Zu Art. 2 (Änderung des Hessischen Jugendstrafvollzugsgesetzes)

Allgemeines

Auf den Vollzug von Freiheitsstrafen nach § 114 des Jugendgerichtsgesetzes findet grundsätzlich die Richtlinie (EU) Nr. 2016/680 des Europäischen Parlamentes und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zweck der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung sowie zum freien Datenverkehr und zur Aufhebung des Rahmenbeschlusses 2008/977/JI des Rates Anwendung.

In Abgrenzung zur Verordnung (EU) Nr. 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG gilt diese Richtlinie für die Verarbeitung personenbezogener Daten zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung, einschließlich des Schutzes vor und der Abwehr von Gefahren für die öffentliche Sicherheit (Art. 1 Abs. 1 der Richtlinie (EU) Nr. 2016/680).

Der Justizvollzug - einschließlich des Vollzugs von Untersuchungshaft, der Sicherungsverwahrung und des Jugendarrests - fällt insoweit regelmäßig unter den Begriff Strafvollstreckung, bzw. zumindest unter die Ermittlung oder Verfolgung von Straftaten bzw. den Schutz vor und die Abwehr von Gefahren für die öffentliche Sicherheit, was als gesetzgeberischen Handlungsbedarf die Umsetzung der Richtlinie nach sich zieht. Im Wesentlichen sprechen folgende Argumente für diese Bewertung:

Die Subsumtion des Justizvollzugs unter den Begriff der Strafvollstreckung ist dem deutschen Rechtssystem nicht fremd. So wird in der Kommentarliteratur zu den §§ 449 ff. StPO vorwie-

gend zwischen der Strafvollstreckung im weiteren Sinne und der Strafvollstreckung im engeren Sinne unterschieden(vgl. Meyer-Goßner/Schmitt, StPO, vor § 449 Rn. 3). Der Begriff der Strafvollstreckung im weiteren Sinne ist dabei gleichbedeutend wie der Begriff der Strafverwirklichung zu verstehen und umfasst neben der Strafvollstreckung im engeren Sinne auch den Strafvollzug (vgl. Klein, in: Graf, StPO, § 449 Rn. 1; Bringewat, Strafvollstreckung, S. 21 Rn. 1; Pfeiffer, StPO, Vor §§ 449ff. Rn. 1; Appl, in: KK-StPO, vor §§ 449ff. Rn. 3).

Hierunter fallen auch Sanktionen wie die Sicherungsverwahrung und der Jugendarrest, die zwar keine Strafen im eigentlichen Sinne darstellen, aber Sanktionen als Folge von Verstößen gegen strafrechtliche Bestimmungen.

Mit der Anwendbarkeit der Richtlinie (EU) Nr. 2016/680 auf den Justizvollzug ist nach deren eigenem Inhalt (Art. 9 der Richtlinie) jedoch nicht ausgeschlossen, dass auf Tätigkeiten der Justizvollzugsbehörden im Einzelfall auch das Recht der Verordnung (EU) Nr. 2016/679 Anwendung finden kann. Hiernach wird auf die Bestimmungen der Verordnung (EU) Nr. 2016/679 insbesondere dann verwiesen, wenn personenbezogene Daten, die für Zwecke der Richtlinie (EU) Nr. 2016/680 - vorliegend des Strafvollzuges - erhoben werden, für andere Zwecke als derjenigen der Richtlinie (EU) Nr. 2016/680 weiterverarbeitet werden. Dies kann zum Beispiel der Fall sein, wenn personenbezogene Daten zu einem Gefangenen an Behörden der allgemeinen Verwaltung zu deren Aufgabenerfüllung weitergegeben werden, z.B. an Sozialversicherungsbehörden oder im Falle meldepflichtiger Krankheiten an Gesundheitsbehörden. Grenzfälle können sich auch im Bereich der Öffentlichkeitsarbeit ergeben, da diese zwar anlässlich des Vollzuges stattfindet, aber nicht unbedingt erforderlich zum Vollzug einer Freiheitsstrafe sein dürfte.

Im Einzelnen

Zu Nr. 1 (Inhaltsübersicht)
Soweit bei einzelnen Paragrafen die Überschriften geändert werden, ist die Inhaltsübersicht entsprechend anzupassen.

Zu Nr. 2 (§ 24)
Eine Benachrichtigung der nächsten Angehörigen ist im Falle der schweren Erkrankung von der Einwilligung des Gefangenen abhängig zu machen; ein entsprechender Vorbehalt wurde zu Satz 1 als 2. Halbsatz angefügt. Dies entspricht den Maßgaben von Art. 9 Abs. 1 Satz 2 der Richtlinie (EU) Nr. 2016/680 i.V.m. Art. 9 Abs. 1 und 2 Buchst. a der Verordnung (EU) Nr. 2016/679, da insoweit die Verarbeitung (durch Übermittlung) von besonderen Kategorien personenbezogener Daten (in Form von Gesundheitsdaten, vgl. § 41 Nr. 14 HDSIG-E) zu Zwecken erfolgt, die nicht ohne Weiteres der Durchführung des Strafvollzuges dient, sondern zunächst einmal der allgemeinen Information der Angehörigen. Auf eine mutmaßliche Einwilligung i.S.v. Art. 9 Abs. 2 Buchst. c kann insoweit nicht abgestellt werden, da die Übermittlung des Gesundheitszustandes an Angehörige auch bei Lebensgefahr kein lebenswichtiges Interesse der betroffenen Personen darstellt; dies dürfte nur für die Durchführung lebenserhaltender Maßnahmen zutreffen. Um auch in Situationen handeln zu können, in denen eine Einwilligung nicht mehr eingeholt werden kann, sollte die Einwilligung - die insoweit den Anforderungen der Verordnung (EU) Nr. 2016/679 genügen muss - bereits bei Aufnahme eingeholt werden; zu diesem Zweck wurde als neuer Satz 3 eine Belehrungspflicht aufgenommen. Handelt es sich bei den Betroffenen um Minderjährige, so sind die besonderen Grundsätze für die Einwilligung Minderjähriger zu beachten.

Im Falle des Todes ist weiterhin eine Benachrichtigung auch ohne Einwilligung angezeigt und nach §§ 22 Abs. 3 i.V.m. Abs. 2 Nr. 3 und Art. 9 Abs. 2 Buchst. f der Verordnung (EU) Nr. 2016/679 möglich.

Zu Nr. 3 (§ 33)

Zu Buchst. a
Als neuer zweiter Halbsatz wurde eine Regelung zu Satz 1 hinzugefügt, wonach sich die Überwachung sowohl auf Gefangene wie Besucher bezieht; dies dient der Klarstellung im Sinne von § 67 HDSIG-E, da die Überwachung sich sowohl auf die Gefangenen als verurteilte Straftäter (dort Nr. 3) wie auch auf den Besuch (dort nur Nr. 5) beziehen kann.

In Satz 2 wird klargestellt, dass die Überwachung der Unterhaltung, sofern sie besondere Kategorien personenbezogener Daten zum Gegenstand hat, nur noch im Falle unbedingter Erforderlichkeit erfolgt, um insbesondere den Anforderungen aus § 43 Abs. 1 HDSIG-E bzw. Art. 10 der Richtlinie (EU) Nr. 2016/680 Rechnung zu tragen. Eine Verarbeitung besonderer Kategorien personenbezogener Daten - legaldefiniert in § 41 Nr. 15 HDSIG-E, insoweit gleichlaufend Art. 9 der Verordnung (EU) Nr. 2016/679 - ist nur bei unbedingter Erforderlichkeit zulässig. Der Begriff der "unbedingten Erforderlichkeit" ist weder in der Verordnung (EU) Nr. 2016/679 noch der Richtlinie (EU) Nr. 2016/680 legaldefiniert. Da er nach dem Wortlaut ein gesteigertes Maß der Erforderlichkeit vorsieht, kann er wie der bisher im Rahmen des Strafvollzugsrechts verwendete

Begriff "unerlässlich" im Sinne eines gesteigerten Maßes der Erforderlichkeit verstanden werden. Eine Maßnahme ist dann unerlässlich, wenn tatsächlich keinerlei weniger eingriffsintensive und mit vertretbarem Aufwand durchführbare Maßnahmen zur Zweckerreichung zur Verfügung stehen; darüber hinaus darf die Art der datenschutzrelevanten Maßnahme schutzwürdige Interessen der Betroffenen nicht beeinträchtigen (vgl. Arloth/Krä StVollzG 4. Auflage § 59 HStVollzG Rd.-Nr. 2, Laubenthal/Nestler/Neubacher/Verrel O Rd.-Nr. 35ff). In die Abwägung einzustellen sind somit sämtliche mit hinreichender Wahrscheinlichkeit mit der Datenverarbeitung für die Betroffenen im persönlichen Nahbereich einhergehenden Konsequenzen, einschließlich der Auswirkungen auf die Beziehungen zu Verwandten, zum sozialen Wohnumfeld sowie zum Arbeitgeber (vgl. Laubenthal/Nestler/Neubacher/Verrel aaO.). Wie in der Begründung zu § 43 HDSIG-E ausgeführt ist eine unbedingte Erforderlichkeit anzunehmen, wenn keine zumutbare Alternativ- oder Ausgleichsmaßnahme zur Verfügung steht, um ein legitimes Ziel zu erreichen.

Inwieweit der Begriff der "unbedingten Erforderlichkeit" in der Rechtspraxis zu anderen Ergebnissen führen wird als eine konsequente Anwendung des Erforderlichkeitsprinzips im Rahmen der Verhältnismäßigkeitsprüfung bleibt abzuwarten. So wird in anderen Regelungsbereichen z.B. zur Durchführung einer sachgerechten medizinischen Betreuung bereits bei jeder Anamnese die umfassende Erhebung von Gesundheitsdaten regelmäßig unbedingt erforderlich sein, ebenso wie es für jeden Vollzugsbediensteten regelmäßig unbedingt erforderlich sein dürfte, auf die Gesichtsbilder der Gefangenen in der Gefangenenpersonalakte zugreifen zu können, um dessen Person in praxisgerechter Weise identifizieren zu können.

Die Überwachung von Besuchen ist elementar für die Sicherheit oder Ordnung der Anstalt. Die permanente Überwachung der Unterhaltung wird daher im Regelfall unbedingt erforderlich sein, auch wenn sie besondere Kategorien personenbezogener Daten zum Inhalt hat. In vielen Fällen ist es allerdings praktisch unvermeidbar, dass die Vollzugsbediensteten Informationen zur Kenntnis nehmen, bevor sie deren besonderen datenschutzrechtlichen Bezug erkennen. In derartigen Fällen ist es in Anlehnung an die Entscheidung BVerfGE 129, S. 208ff. (Rd.-Nr. 209ff,) verfassungsrechtlich nicht gefordert, den Zugriff wegen des Risikos einer Kernbereichsverletzung auf der Erhebungsebene von vornherein zu unterlassen. In Fällen dieser Art ist es geboten, aber auch ausreichend, für hinreichenden Schutz in der Auswertungsphase zu sorgen, insbesondere durch Gewährung eines entsprechenden Schutzes durch Löschung von Aufzeichnungen.

Zu Buchst. b
In Satz 1 wird ein neuer zweiter Halbsatz eingeführt, wonach die Überwachung auch durch optisch-elektronische Einrichtungen erfolgen kann, die als Videoüberwachung legaldefiniert wird, da dieser Begriff im Gesetz mehrfach verwendet wird.

Satz 2 wird dahin gehend neu gefasst, dass die Aufzeichnung und Speicherung von Daten gemäß Satz 1 nur im Falle unbedingter Erforderlichkeit erfolgt. Dies ist dem Umstand geschuldet, dass für den Geltungsbereich der Richtlinie (EU) Nr. 2016/680 je nach Qualität des Überwachungssystems Gesichtsbilder unter die besondere Kategorie personenbezogener Daten fallen können, insbesondere bei der Verwendung spezieller Gesichtserkennungssoftware. Darüber hinaus ist eine Videoüberwachung von Besuchen besonders geneigt, durch Aufzeichnung des Verhaltens der überwachten Personen Informationen zu besonderen Kategorien personenbezogener Daten im Sinne von Art. 10 der Richtlinie (EU) Nr. 2016/680 zu generieren. Die Einfügung des Tatbestandsmerkmals der unbedingten Erforderlichkeit trägt im Interesse einer möglichst sicheren Umsetzung der Richtlinie (EU) Nr. 2016/680 entsprechend deren Art. 10 bzw. § 43 Abs. 1 HDSIG-E Rechnung, um eine Videoüberwachung in jedem Fall datenschutzrechtlich abzusichern. Dies gilt insbesondere für Gesichtsbilder, die im Rahmen einer Videoüberwachung anfallen.

Zu Buchst. c
Der Verweis in Satz 6 wurde dahin gehend redaktionell berichtigt, dass es sich bei der in Bezug genommenen Norm um die des § 46 Abs. 3 handelt und nicht die des § 47 Abs. 3.

Zu Nr. 4 (§ 34)
Der zu überwachende Schriftwechsel wird häufig mit einer gewissen Wahrscheinlichkeit besondere Kategorien personenbezogener Daten enthalten, ohne dass dies vor Beginn der Überwachung klar ist. Diesbezüglich ist grundsätzlich der Anwendungsbereich der Richtlinie (EU) Nr. 2016/680 auch im Bereich des Schriftwechsels nicht in jedem Fall ausgeschlossen. Es ist insbesondere nach Abs. 3 auch möglich, angehaltenen Schriftwechsel zu verwahren, regelmäßig in einer körperlichen Akte, aber auch nach Scannen in einer elektronischen Akte, mithin analogen oder digitalen Dateisystemen.

Insoweit besteht eine geringere Flexibilität als bei der Überwachung eines Besuchs, bei dem sich die besondere datenschutzrechtliche Relevanz bei den besonderen Kategorien aus dem überwachten Verlauf des Besuchs selbst ergeben kann. Um das Schutzniveau für die besonderen Kategorien personenbezogener Daten von Anfang an zu gewährleisten, ist nach § 43 Abs. 1 HDSIG-E daher prophylaktisch sicherzustellen, dass die Überwachung des Schriftwechsels nur im Falle unbedingter Erforderlichkeit erfolgt, was durch einen entsprechenden Einschub in Satz 1 erfolgt. Da die

Überwachung des Schriftwechsels für Sicherheit oder Ordnung unverzichtbar sind, wird das Kriterium der unbedingten Erforderlichkeit regelmäßig erfüllt sein. Darüber hinaus sollten Gefangene frühzeitig (d.h. bei Aufnahme) auf die Möglichkeit der Überwachung hingewiesen werden, um den Eingriff in das Postgeheimnis nicht zu einer verdeckten Maßnahme zu machen, an die - insbesondere angesichts des Urteils des Bundesverfassungsgerichts vom 20.04.2016, Aktenzeichen 1 BvR 966/09 und 1BvR 1140/09 - bei der Datenverarbeitung erheblich höhere Anforderungen zu stellen wären; eine entsprechende Hinweispflicht wurde als neuer Halbsatz an Satz 1 angefügt.

Zu Nr. 5 (§ 44)
In Abs. 2 Satz 2 wird - auch im Sinne einer einheitlichen Terminologie - ferner klargestellt, dass die technischen Hilfsmittel auch optisch-elektronische Einrichtungen (Videoüberwachung) umfassen. Da diese - unabhängig von der Einstufung eines Gesichtsbildes als biometrisches Datum - besonders geeignet sind, insgesamt besondere Kategorien personenbezogener Daten zu liefern, sei es in Form von Gesundheitsdaten oder anderen Unterfällen, ist nach § 43 Abs. 1 HDSIG-E in Satz 2 nunmehr vorgesehen, dass die entsprechende Verarbeitung nur im Falle unbedingter Erforderlichkeit zulässig ist. Auch hier wird wegen der Unverzichtbarkeit einer entsprechenden Überwachung für Sicherheit oder Ordnung der Anstalt das Kriterium der unbedingten Erforderlichkeit regelmäßig erfüllt sein.

Zu Nr. 6 (§ 49)

Zu Buchst. a
Es wird - auch im Sinne einer einheitlichen Terminologie - in Abs. 2 Nr. 2 klargestellt, dass die technischen Hilfsmittel auch optisch-elektronische Einrichtungen (Videoüberwachung) umfassen. Da diese regelmäßig besondere Kategorien personenbezogener Daten liefern können, insbesondere Gesundheitsdaten zur Kontrolle des Gesundheitszustandes der Gefangenen, ist nach § 43 Abs. 1 HDSIG-E vorgesehen, dass die entsprechende Verarbeitung nur im Falle unbedingter Erforderlichkeit zulässig erfolgt. Da die entsprechende Kontrolle für die Information des Gesundheitszustandes des Gefangenen unverzichtbar ist, wird das Kriterium der unbedingten Erforderlichkeit regelmäßig erfüllt sein.

Zu Buchst. b
Da die dauerhafte Überwachung nach Abs. 2 Nr. 2 regelmäßig Gesundheitsdaten, aber auch Gesundheitsdaten liefern kann und somit besondere Kategorien personenbezogener Daten, ist in Abs. 6 Satz 2 klargestellt, dass dies im Sinne von § 43 Abs. 1 HDSIG-E nur im Falle unbedingter Erforderlichkeit zulässig ist. Auch hier gilt, dass, da die entsprechende Kontrolle für die Information des Gesundheitszustandes des Gefangenen unverzichtbar ist, das Kriterium der unbedingten Erforderlichkeit regelmäßig erfüllt sein wird.

Zu Nr. 7 (§§ 58 bis 61)

Zu § 58

Zu Abs. 1
In Satz 1 wird in Anlehnung an § 41 Nr. 2 des HDSIG-E statt an die Alternativen Datenerhebung bzw. -weiterverarbeitung an den einheitlichen Begriff der Verarbeitung angeknüpft; ebenfalls wurde vor dem Wort "verarbeiten" ein "nur" eingefügt, um das Prinzip des Verbots mit Erlaubnisvorbehalts hervorzuheben. Ferner erfolgt in Satz 1 die systematische Klarstellung, dass zunächst eine gesetzliche Spezialregelung Anwendung findet und nur in letzter Linie die Generalklausel, die insoweit grundsätzlich auf die Erforderlichkeit für den Vollzug abstellt. Bei der Verarbeitung besonderer Kategorien personenbezogener Daten - legaldefiniert in § 41 Nr. 15 HDSIG-E - muss allerdings insoweit die unbedingte Erforderlichkeit gegeben sein. Gestrichen wurde die Einwilligung als allgemeiner Rechtsgrund für eine Datenverarbeitung. Dies trägt dem Umstand Rechnung, dass die Richtlinie (EU) Nr. 2016/680 eine Einwilligung im Rahmen ihres Geltungsbereichs grundsätzlich nicht mehr als alleinige Grundlage hierfür ausreichen lässt, wie sich aus Ziffer 35 der Erwägungen zur Richtlinie (EU) Nr. 2016/680 ergibt. Wie weit dieser Grundsatz reicht, ist derzeit noch nicht abschließend geklärt. Der letzte Satz der vorgenannten Erwägungen führt hierzu aus: "Dies sollte die Mitgliedstaaten nicht daran hindern, durch Rechtsvorschriften vorzusehen, dass die betroffenen Personen der Verarbeitung ihrer personenbezogenen Daten für die Zwecke dieser Richtlinie zustimmen kann, beispielsweise im Falle von DNA-Tests in strafrechtlichen Ermittlungen oder zur Überwachung ihres Aufenthaltsortes mittels elektronischer Fußfessel zur Strafvollstreckung." In den Artikeln der Richtlinie (EU) Nr. 2016/680 findet sich die Einwilligung dann jedoch - anders als in der Verordnung (EU) Nr. 2016/679 - als Rechtsgrund einer Datenverarbeitung nicht mehr. Daher wird die entsprechende Erwägung dahin gehend auszulegen sein, dass die Einwilligung in der Einzelvorschrift ausdrücklich aufgeführt sein muss; konsequenterweise sieht § 46 HDSIG-E die Möglichkeit einer Einwilligung in solchen Fällen vor. Tatbestände, bei denen ein solcher Einwilligungsvorbehalt gegeben ist, werden nunmehr durch den Tatbestand der "Rechtsvorschrift" mit abgedeckt.

Die Verweisung auf die Bestimmungen des subsidiär geltenden Hessischen Datenschutz- und Informationsfreiheitsgesetzes in Satz 2 wird faktisch als dynamische Verweisung ausgestaltet, um zukünftige Änderungen abzubilden. Zu Satz 2 wurde ein weiterer Halbsatz angehängt, durch den klargestellt wird, dass die Datenverarbeitung durch die Justizvollzugsbehörden zu Vollzugszwecken grundsätzlich - aber nicht ausschließlich, da insoweit auch die allgemeinen Bestimmungen, insbesondere Teil 1 gelten - unter dem Regime des Teils 3 des HDSIG-E erfolgt, um der Praxis angesichts der - in Art. 9 der Richtlinie (EU) Nr. 2016/680 selbst vorgesehenen Zweiteilung der datenschutzrechtlichen Regelungssysteme - eine grundsätzliche Entscheidungshilfe an die Hand zu geben. Dies hat daher nicht allein deklaratorische Wirkung; die Entscheidung kann im Einzelfall schwierig werden, s. hierzu die Ausführungen in den Vorbemerkungen zur Begründung.

Neu hinzugefügt wurde Satz 3, der den Verhältnismäßigkeitsgrundsatz konkretisiert und im Hinblick auf Art. 1 Abs. 1 GG ein Verarbeitungsverbot ausspricht, da der Gesetzgeber den Kernbereich privater Lebensgestaltung zu schützen hat (vgl. BVerfGE 129, S. 208ff. [S. 245]). Ob ein Sachverhalt dem unantastbaren Kernbereich zuzuordnen ist, hängt davon ab, ob er nach seinem Inhalt höchstpersönlichen Charakters ist, also auch in welcher Art und Intensität er aus sich heraus die Sphäre anderer oder Belange der Gemeinschaft berührt (vgl. BVerfGE 80, 367 [374] = NJW 1990, 563).

Zu Abs. 2
Die Präzisierung, dass die Verarbeitung für Ziel und Aufgaben des Vollzugs nach § 2 erfolgt, dient der Klarstellung, dass die Verantwortlichen im Sinne des Datenschutzes im vorliegenden Fall Daten grundsätzlich zu Zwecken des Strafvollzuges verarbeiten. Klarstellend wird ferner eingefügt, dass die Verarbeitung der aufgezählten personenbezogenen Daten auch zur Aufrechterhaltung der medizinischen Versorgung und Gesundheitsfürsorge verarbeitet werden können, was Art. 8 Abs. 2 der Richtlinie (EU) Nr. 2016/680 Rechnung trägt.

Ferner wird auf den einheitlichen Tatbestand einer Verarbeitung abgestellt.

Da die bisherigen Nummern 1 bis 4 bereits zumeist besondere Kategorien personenbezogener Daten i.S.v. § 41 Nr. 15 des HDSIG-E darstellen, wurde durch die Ergänzung um Nr. 5 insoweit eine Gesamtregelung für die Verarbeitung entsprechender Informationen geschaffen. Dabei wurden die Gesundheitsdaten in Hinblick auf ihre besondere Bedeutung, aber auch ihre bisher schon separate Speicherung herausgehoben.

Die Verarbeitung besonderer Kategorien personenbezogener Daten wurde nach § 43 Abs. 1 HDSIG-E an das Erfordernis unbedingter Erforderlichkeit geknüpft. Die beibehaltene Beschränkung auf Gefangene als verurteilte Straftäter trägt darüber hinaus § 67 HDSIG-E Rechnung, der wiederum aus Art. 6 der Richtlinie (EU) Nr. 2016/680 folgt.

Zu Abs. 3
Es erfolgt in Satz 1 eine Anpassung der separat zu führenden personenbezogenen Daten an die Neunummerierung in Abs. 2.
In Satz 2 wird statt auf "Daten, die den Gesundheitszustand betreffen" auf "Gesundheitsdaten" abgestellt, da letzter Begriff in § 41 Nr. 14 HDSIG-E legaldefiniert ist. Der Begriff "Personalakte" in Satz 2 wurde durch den der "Gefangenenpersonalakte" präzisiert.

Zu Abs. 4
Satz 2 wurde neu eingeführt, um klarzustellen, dass bei der Verarbeitung besonderer Kategorien personenbezogener Daten dies nur bei unbedingter Erforderlichkeit zulässig ist, s. § 43 Abs. 1 HDSIG-E. Es wurde insoweit auf dieselbe Begrifflichkeit abgestellt wie in Satz 1.

Zu Abs. 5
Neu eingefügt wurde Satz 2, sofern hierbei die Verarbeitung biometrischer Daten notwendig werden sollte. Dies würde die Verarbeitung von besonderen Kategorien personenbezogener Daten darstellen, die wiederum gemäß § 43 Abs. 1 HDSIG-E nur bei unbedingter Erforderlichkeit zulässig ist.

Zu Abs. 6
Die Neufassung der Vorschrift orientiert sich an § 4 HDSIG-E. Da die Außensicherung sowohl öffentliche wie nicht öffentliche Plätze abdecken kann, konnte insoweit nicht lediglich auf die vorgenannte Vorschrift verwiesen werden.

Soweit in Satz 1 zusätzlich darauf abgestellt wird, dass schutzwürdige Interessen der Betroffenen nicht überwiegen dürfen, erfolgt dies in Orientierung an § 4 Abs. 1 HDSIG-E.

Satz 2 wurde dahin gehend ergänzt, dass neben der Überwachung auch der Name und die Kontaktdaten des Verantwortlichen zum frühestmöglichen Zeitpunkt erkennbar zu machen sind. Verantwortlicher wird dabei regelmäßig keine natürliche, mit Namen zu benennende Person sein, sondern die Anstalt als zuständige Behörde, vgl. § 41 Nr. 8 HDSIG-E.

Ergänzend wird klargestellt, dass eine Speicherung nur zulässig ist, wenn keine Anhaltspunkte dafür bestehen, dass schutzwürdige Interessen der Betroffenen überwiegen; dies trägt § 4 Abs. 3 S. 1 HDSIG-E Rechnung.

Zu § 58a

Zu Abs. 1
In Satz 2 wurde klargestellt, dass die Zuverlässigkeitsüberprüfung zur Aufrechterhaltung der Sicherheit oder Ordnung der Anstalt erfolgt.

Die Verweisung auf das Hessische Sicherheitsüberprüfungsgesetz (HSÜG) in Satz 5 wurde durch eine dynamische Verweisung ersetzt, um zukünftige Änderungen abzubilden.

Zu Abs. 2
In Satz 1 wurde klargestellt, dass die Zuverlässigkeitsüberprüfung zur Aufrechterhaltung der Sicherheit oder Ordnung der Anstalt und zur Abwendung von Gefahren hierfür erfolgt.
In Satz 2 wurde präzisiert, dass - in Hinblick auf § 67 HDSIG-E - die Zulassung zum Gefangenbesuch überhaupt erfolgt und nicht nur für welche Gefangene.

Zu Abs. 4
Hinsichtlich der Benachrichtigungspflicht wurde ausdrücklich auf § 51 HDSIG-E Bezug genommen.

Zu Abs. 6
In Satz 1 wurde in Hinblick auf den in Art. 8 der Richtlinie (EU) Nr. 2016/680 normierten Erforderlichkeitsgrundsatz ergänzend eingeführt, dass die Wiederholung der Zulässigkeitsprüfung zu erfolgen hat, sofern ihre Erforderlichkeit fortbesteht.

Zu § 59
Der bisherige § 59 HJStVollzG war mit seinem bisherigen Regelungsgehalt aufzuheben. Die Vorschrift ging von dem Grundsatz aus, dass personenbezogene Daten grundsätzlich bei den Betroffenen zu erheben sind. Ein solcher Grundsatz wird weder in der Richtlinie (EU) Nr. 2016/680 noch in der Verordnung (EU) Nr. 2016/680 statuiert. Da nicht ausgeschlossen werden kann, dass auch eine Vollzugseinrichtung im Bereich der Verordnung (EU) Nr. 2106/679 tätig wird, könnte die Beibehaltung eines entsprechenden Grundsatzes insoweit als Verstoß gegen europäisches Recht gelten. Darüber hinaus ist davon auszugehen, dass die Datenerhebung auch in Zukunft hauptsächlich bei den Betroffenen erfolgen werden wird. Sollte dies nicht der Fall sein, sind diese im Übrigen auch nicht rechtlos, wie sich aus § 64 ergibt.

Stattdessen wird eine neue Vorschrift an dieser Stelle eingefügt, die eine spezielle Befugnis zum Auslesen unzulässig in die Justizvollzugsanstalten eingebrachter Datenträger darstellt. Eine spezielle Ermächtigung hierfür ist sinnvoll und erforderlich, da die unkontrollierte Kommunikation über Speichermedien eine erhebliche Gefährdung der Sicherheit oder Ordnung der Anstalten darstellt. Die Neuregelung erfolgt im Rahmen der datenschutzrechtlichen Bestimmungen, da damit gerechnet werden kann, dass die entsprechenden Speichermedien aufgrund ihrer Bestimmung zur Kommunikation zahlreiche personenbezogene Daten, auch solche besonderer Kategorien, enthalten.

In diesem Zusammenhang ist aus Gründen des Verhältnismäßigkeitsgrundsatzes zu differenzieren, dass nicht jeder Datenspeicher auszulesen ist, sondern nur dann, wenn konkrete Anhaltspunkte für eine Gefährdung hierdurch sprechen. Solche konkreten Anhaltspunkte werden dann regelmäßig vorliegen, wenn Hinweise für ein heimliches Verbringen des Datenspeichers in die Anstalt sprechen, z.B. beim Auffinden in einem Haftraum. Anders dürfte die Lage z.B. zu beurteilen sein, wenn Kommunikationssysteme als notwendiger Bestandteil z.B. von Baugeräten im Rahmen von Baumaßnahmen in eine Anstalt verbracht werden, ohne dass das Baugerät hierauf gezielt kontrolliert wurde.

Die Regelung orientiert sich im Wesentlichen an § 23 des rheinland-pfälzischen Landesjustizvollzugsdatenschutzgesetzes, zuletzt geändert durch § 44 des Gesetzes vom 6. Oktober 2015 (GVBl. S. 354). Diese Vorschrift lautet in ihrer derzeitigen Fassung wie folgt:

"§ 23
Auslesen von Datenspeichern

(1) Elektronische Datenspeicher sowie elektronische Geräte mit Datenspeicher, die ohne Erlaubnis in die Anstalt eingebracht wurden, dürfen auf schriftliche Anordnung der Anstaltsleiterin oder des Anstaltsleiters ausgelesen werden, soweit konkrete Anhaltspunkte die Annahme rechtfertigen, dass dies für die Erfüllung der Aufgaben des Vollzugs erforderlich ist. Die Gründe sind in der Anordnung festzuhalten. Sind die Betroffenen bekannt, sind ihnen die Gründe vor dem Auslesen mitzuteilen. Beim Auslesen sind ihre schutzwürdigen Interessen zu berücksichtigen, insbesondere der Kernbereich privater

Lebensgestaltung. Das Auslesen ist möglichst auf die Inhalte zu beschränken, die zur Erreichung der die Anordnung begründenden Zwecke erforderlich sind.

(2) Die nach Absatz 1 erhobenen Daten dürfen verarbeitet werden, soweit dies aus den in der Anordnung genannten Gründen erforderlich ist. Aus anderen Gründen ist die Verarbeitung der Daten nur zulässig, soweit dies für die Erfüllung der Aufgaben des Vollzugs zwingend erforderlich ist und schutzwürdige Interessen der Betroffenen dem nicht entgegenstehen.

(3) Die Verarbeitung der nach Absatz 1 erhobenen Daten ist unzulässig, soweit sie dem Kernbereich der privaten Lebensgestaltung Gefangener oder Dritter unterfallen. Diese Daten sind unverzüglich zu löschen. Die Tatsachen der Erfassung und der Löschung der Daten sind zu dokumentieren. Die Dokumentation darf ausschließlich für Zwecke der Datenschutzkontrolle verwendet werden. Sie ist zu löschen, wenn sie für diese Zwecke nicht mehr erforderlich ist, spätestens jedoch am Ende des Kalenderjahres, das dem Jahr der Dokumentation folgt.

(4) Die Gefangenen sind bei der Aufnahme über die Möglichkeit des Auslesens von nicht gestatteten Datenspeichern zu belehren."

Ein besonderer Hinweis auf die Berücksichtigung schutzwürdiger Interessen und eine Beschränkung auf die Inhalte, die zur Erreichung der die Anordnung begründenden Zwecke erforderlich sind, ist indes nicht erforderlich, da dies durch die allgemeine Bestimmung in § 58 Abs. 1 bzw. die Beschränkung innerhalb der Vorschrift "soweit" bereits abgedeckt wird. In Hinblick auf die Möglichkeit, dass die auszulesenden Datenträger auch besondere Kategorien personenbezogener Daten enthalten können, sollte von der Maßnahme nur bei unbedingter Erforderlichkeit Gebrauch gemacht werden. Ebenfalls nicht notwendig ist eine Beschränkung der Verarbeitung auf die Zwecke ihrer Erhebung, da dies ebenfalls durch § 58 Abs. 1 und 2 abgedeckt ist. Einer besonderen Löschungsbestimmung bedarf es nicht, diese ist durch die Neuregelung in § 65 Abs. 2 erfasst.

Zu § 60

Zu Abs. 1
Zunächst waren die Bestimmungen über die Verarbeitung personenbezogener Daten zu anderen Zwecken, als zu denen, für die sie erhoben wurden, an die entsprechenden Bestimmungen des HDSIG-E anzupassen, d.h. an dessen §§ 20 bis 27 und 44 bis 45. Da nach Art. 9 der Richtlinie (EU) Nr. 2016/680 auch für Justizvollzugsbehörden der Anwendungsbereich der Verordnung (EU) Nr. 2016/679 eröffnet sein kann, war insoweit auch auf die Normen zu deren Umsetzung abzustellen.

Soweit darüber hinaus in einer Aufzählung nurmehr besondere Regelbeispiele ("insbesondere") für eine Datenverarbeitung zu namentlich genannten Zwecken genannt werden, ist dies wie folgt zu begründen:

Die neue Nr. 1 stellt die Umsetzung von Art. 4 Abs. 2 der Richtlinie (EU) Nr. 2016/680 dar. Die bisherige Nr. 1 wird Nr. 2. Die bisherige Nr. 2 kann gestrichen werden, da sie in der neuen Nr. 1 aufgeht. Die Nennung von Nr. 3 bis 5 wäre über die neue Nr. 1 erfasst. Eine Streichung der vorgenannten Vorschriften könnte aber eine erhebliche Rechtsunklarheit in der Praxis auslösen, da durch die Verweisung auf allgemeine Bestimmungen die Rechtsanwendung nicht nur vereinfacht wird. Eine entsprechende Unklarheit sollte im Sinne einer effizienten Rechtshandhabung - auch im Sinne der Betroffenen - vermieden werden. Insoweit erscheint es sinnvoll, den bisherigen Katalog weitestgehend beizubehalten.

Dies gilt im Ergebnis und mit derselben Begründung auch für die übrigen Nr. 6 bis 12, zu deren Zweck die Verarbeitung anderweitig erhobener personenbezogener Daten jedenfalls nach Art. 9 Abs. 1 Satz 2 der Richtlinie (EU) Nr. 2016/680 i.V.m. Art. 9 Abs. 2 der Verordnung (EU) Nr. 2016/679 zulässig ist, was wiederum über die Verweisung auf § 22 HDSIG-E abgedeckt wird. Auch insoweit soll jedoch Rechtsunklarheit in der Praxis vermieden werden, sodass es geboten erscheint, die bisherigen Tatbestände als Regelbeispiele ebenfalls beizubehalten.

Die Einführung des Erfordernisses der unbedingten Erforderlichkeit bei besonderen Kategorien personenbezogener Daten trägt insoweit § 43 Abs. 1 HDSIG-E Rechnung und betrifft z.B. Maßnahmen nach § 25 Abs. 3.

Zu Abs. 2
Die Vorschrift dient dem besonderen Schutz von Daten, die bei besonders erheblichen Eingriffen in Grundrechte anfallen.

Das Telekommunikationsgeheimnis steht den bisherigen Ausnahmetatbeständen insoweit gleich, weshalb die Überwachung der Telekommunikation (vgl. § 35) und das Auslesen von Datenspeichern (vgl. § 59 HJStVollzG-E) in Satz 1 ebenfalls aufgeführt werden. Entsprechend der syste-

matischen Bedeutung der Vorschrift wird in Satz 1 wie für Abs. 1 klargestellt, dass die Regelung für Datenverarbeitungen gilt, die über die reine Erfassung und Speicherung hinausgehen, insbesondere für die Übermittlung.

Die Gründe, aus denen bei den entsprechenden sensiblen Daten eine Weiterverarbeitung weiterhin möglich sein soll, werden nunmehr unter Nr. 1 bis 3 aufgezählt.

Nr. 1 erweitert den bisherigen Regelungsgehalt auf andere Zwecke, wie sie in § 40 HDSIG-E vorgesehen werden.

Nr. 2 entspricht der bisherigen Verweisung auf § 12 Abs. 2 Nr. 1 des derzeit noch geltenden Hessischen Datenschutzgesetzes. Die übrigen Verweisungen auf das derzeit noch geltende Hessische Datenschutzgesetz werden obsolet; der bisherige Verweis auf § 12 Abs. 2 Nr. 3 und 4 des Hessischen Datenschutzgesetzes erübrigt sich durch die Verweisung auf Abs. 1 Nr. 1 neuer Fassung.

Nr. 3 stellt einen Auffangtatbestand dar, der beibehalten werden sollte, um die Praxis bei der bisherigen Rechtsanwendung fortzuführen. Die bisherige Nr. 3 - die Einwilligung - wurde wegen der besonderen Problematik dieser Rechtsgrundlage im Geltungsbereich der Richtlinie (EU) Nr. 2016/680 gestrichen.

Darüber hinaus soll die Weiterverarbeitung, insbesondere die Übermittlung, nur bei unbedingter Erforderlichkeit vorgenommen werden, wie dies in Satz 1 eingefügt wurde. Das Bundesverfassungsgericht hat in seinem Urteil vom 20. April 2016, Aktenzeichen 1 BvR 966/09 und 1BvR 1140/09 in Hinblick auf das BKAG in der damals geltenden Fassung ausgeführt, dass die Verhältnismäßigkeit eines Eingriffs von dessen Intensität abhängt und angemessen ausgestaltet sein muss. Je tiefer Überwachungsmaßnahmen in das Privatleben eingreifen, desto strenger sind die Anforderungen, was insbesondere für die Wohnraumüberwachung und den Zugriff auf informationstechnische Systeme gilt. Die in der Entscheidung zu beurteilenden Sachverhalte betrafen zwar verdeckte Datenverarbeitungen, während die im Hessischen Jugendstrafvollzugsgesetz vorgesehenen Maßnahmen regelmäßig nicht verdeckt erfolgen, was insbesondere durch die Offenlegung von Überwachungsmaßnahmen gilt. Auch stellt insbesondere der Haftraum keine Wohnung i.S.d. Art. 13 GG dar (vgl. BVerfG NJW 1996, 2643). Schließlich müssen bei den Eingriffen nicht notwendigerweise auch besondere Kategorien personenbezogener Daten geschützt werden. Dennoch erscheinen vor diesem Hintergrund die aufgeführten Daten besonders schützenswert - nachdem es sich zwar um offene, aber tiefe Eingriffe in die Kommunikation handelt - sodass ihre Weitergabe nur zu eingeschränkten Zwecken und im Fall der unbedingten Erforderlichkeit erfolgen sollte. Durch diese Beschränkung wird sichergestellt, dass insbesondere die Übermittlung der entsprechenden Daten nur zu Zwecken erfolgt, für die sie selbst hätten erhoben werden können (Grundsatz der hypothetischen Datenneuerhebung).

Um im Falle ihrer Übermittlung sicherzustellen, dass die entsprechenden Daten mit der erforderlichen Sensibilität behandelt werden, sind sie entsprechend dem neu eingefügten Satz 2 eindeutig zu kennzeichnen.

Es wird ferner klargestellt, dass § 4 Abs. 3 Satz 2 HDSIG-E unberührt bleibt. Diese Vorschrift regelt den Sonderfall einer Übermittlung von Videoaufzeichnungen, die bei der Überwachung öffentlich zugänglicher Räume angefallen sind.

Zu Abs. 3
Es handelt sich insoweit um Sonderfälle des Abs. 1.

Der neue Verweis in Satz 1 auf Abs. 1 soll auch insoweit eine Rechtsunsicherheit in der Praxis vermeiden.

Zu Abs. 5
Der neue Hinweis in Satz 3 a. E. an jeden Empfänger, was die Einstufung besonderer Kategorien personenbezogener Daten angeht, entspricht insbesondere der Pflicht zur Schaffung geeigneter Garantien nach § 43 Abs. 2 Nr. 8 HDSIG-E im Falle der Übermittlung besonderer Kategorien personenbezogener Daten, die wiederum auf Art. 10 der Richtlinie (EU) Nr. 2016/680 zurückgeht

Zu Abs. 6
Die Nennung der Gerichtszuständigkeit wurde an die Neufassung des Kataloges in Abs. 1 angepasst; desgleichen der Verweis auf die Vorschrift in § 65.

Zu § 61

Zu Abs. 1
Der Schutzbereich der Vorschrift in Satz 1 wurde auf alle besonderen Kategorien personenbezogener Daten nach § 41 Nr. 15 HDSIG-E erweitert. Die Erweiterung des Schutzes für alle be-

sonderen Kategorien personenbezogener Daten trägt dessen § 43 Abs. 2 Rechnung. Weitere Schutzvorschriften enthalten insoweit § 58 Abs. 2 und § 60 Abs. 1.

Zu Abs. 2
Die Verwendung des Begriffs "unbedingt erforderlich" in Satz 2 statt bisher "unerlässlich" stellt auf die Terminologie in § 43 Abs. 1 HDSIG-E ab. Passend zu Satz 2 wird in Satz 3 ebenfalls auf den Begriff der "Offenbarung" abgestellt.

Zu Abs. 3
Die Vorschrift betrifft die Weitergabe von Informationen, die von externen Dienstleistern nicht unmittelbar zu Vollzugszwecken - sondern primär zum Zwecke der Behandlung - erhoben, aber zu Zwecken des Vollzuges weitergegeben werden. Insoweit ist der Anwendungsbereich der Verordnung (EU) Nr. 2016/679 eröffnet.

Redaktionell wird ferner in Satz 2 klargestellt, dass die vorgenannten Personen lediglich zu einer Offenbarung befugt sind.

Zu Abs. 5
Der Terminus "unerlässlich" wurde an den Begriff "unbedingt erforderlich" angepasst.

Zu Nr. 8 (§ 62)
Das entsprechende Verfahren ist nunmehr in § 58 HDSIG-E geregelt, sodass die Verweisung entsprechend anzupassen war.

Zu Nr. 9 (§§ 63 bis 65)

Zu § 63

Zu Abs. 1
Die Bestimmung ist neu eingeführt.

Die Sätze 1, 2 und 4 geben insoweit die Bestimmung von § 48 HDSIG-E wieder. Die Wiedergabe erfolgt, weil der Hinweis in Satz 3 sonst nicht ohne weiteres aus sich heraus verständlich wäre.

Der gesonderte Hinweis nach Satz 3 entspricht insoweit dem Regelungsgehalt von § 43 Abs. 2 Satz 2 Nr. 3 HDSIG-E für die Sicherung besonderer Kategorien personenbezogener Daten, ist jedoch aufgrund der besonderen datenschutzrechtlichen Sensibilität der weiteren aufgeführten Arten von Daten erforderlich.

Zu Abs. 2
Entsprechend der Einführung eines neuen Abs. 1 ist der bisherige Inhalt von § 63 HJStVollzG als Abs. 2 zu bezeichnen. Die Verweisung auf die Vorschrift des bisherigen § 10 HDSG in Satz 1 war an § 59 HDSIG-E entsprechend anzupassen.

Zu § 64
Die Vorschrift wird komplett neu gefasst.

In die Überschrift wurde der Begriff der Information aufgenommen, da dies der Terminologie des HDSIG-E entspricht, vgl. dort § 50.

Entsprechend der Formulierungen des HDSIG-E wird auf dessen §§ 50 bis 52 verwiesen, soweit die Datenverarbeitung zu Zwecken der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung und des Strafvollzuges erfolgt; im Übrigen auf dessen §§ 31 bis 33. Die Zweiteilung der Informations- und Auskunftsrechte folgt aus der nichtausschließlichen Anwendbarkeit von Richtlinie (EU) Nr. 2016/680 und Verordnung (EU) Nr. 2016/679 im Bereich des Hessischen Justizvollzugs. Dabei erscheint es sinnvoll, den Gefangenen zur Aufnahme z.B. ein entsprechendes Formblatt als Information zu Datenverarbeitungen auszuhändigen - § 8 Abs. 1 sieht insoweit die Information über Rechte und Pflichten vor - und dgl. Besuchern bei Betreten der Anstalt.

Zur Gewährung eines effektiven Rechtsschutzes wird im neuen Satz 2 die Möglichkeit einer Akteneinsicht beibehalten und auf das insgesamt Erforderliche ausgedehnt werden. Insbesondere bei Einsichtnahmen in Gesundheitsakten wird hierbei großzügig zu verfahren sein, vgl. BVerfG, Beschluss der 2. Kammer des Zweiten Senats vom 20.Dezember 2016 - 2 BvR 1541/15.

Zu § 65
Die Vorschrift wird weitestgehend neu gefasst.

Zur Überschrift
Der Begriff "Sperrung" wurde durch den Begriff "Einschränkung der Verarbeitung" ersetzt.

Nach der Systematik des HDSIG-E kann, vgl. dort § 53 Abs. 3, an Stelle einer Löschung von personenbezogenen Daten bei diesen eine Einschränkung der Verarbeitung vorgenommen werden. Nach § 41 Nr. 3 HDSIG-E ist hierunter "die Markierung gespeicherter personenbezogener Daten mit dem Ziel, ihre künftige Verarbeitung einzuschränken" zu verstehen.

Nach der bisherigen Systematik, vgl. § 65 Abs. 1 HJStVollzG in seiner jetzigen Fassung, sind personenbezogene Daten auch jetzt schon unverzüglich zu löschen, sobald feststeht, dass ihre Speicherung nicht mehr erforderlich ist, um die Zwecke zu erfüllen, für die sie erhoben worden sind oder für die sie nach § 13 Abs. 2 und 4 HDSG weiterverarbeitet werden dürfen; wenn bei der Speicherung nicht absehbar ist, wie lange die Daten benötigt werden, ist nach einer aufgrund der Erfahrung zu bestimmenden Frist zu prüfen, ob die Erforderlichkeit der Speicherung noch besteht, vgl. § 19 Abs. 3 HDSG in seiner jetzigen Fassung.

Grundsätzlich sollte für die zukünftige Rechtslage - wie bisher auch - zwischen besonders sensiblen Daten, Daten in Gefangenenakten- und -dateien und sonstigen Daten hinsichtlich der Frage ihrer Löschung oder - an deren Stelle - der Einschränkung ihrer Verarbeitung unterschieden werden.

Zu Abs. 1
Der Absatz entspricht in seinem Regelungsgehalt dem bisherigen Abs. 1. Es wurde der Begriff "in der Verarbeitung einzuschränken" anstelle der bisherigen Sperrung verwendet und auf die einschlägigen Bestimmungen des HDSIG-E verwiesen, je nachdem, ob die Verarbeitung zu den Zwecken nach § 40 HDSIG-E erfolgt oder nicht.

Zu Abs. 2
Abs. 2 befasst sich entsprechend der bisherigen Systematik mit der Verfahrensweise bei personenbezogenen Daten, die aufgrund besonders intensiver Eingriffe erhoben wurden. Insoweit liegt hierin eine Konkretisierung auch von § 4 Abs. 4 HDSIG-E.

In Satz 1 wurden Ergebnisse von Maßnahmen nach § 59 den Videoaufnahmen gleichgestellt, da insoweit ein gleiches Maß an Schutzwürdigkeit gegeben ist. Ebenfalls wird klargestellt, dass eine Löschung nur dann nicht erfolgt, wenn zum Zeitpunkt der Entscheidung über die Löschung zu konkreten Beweiszwecken die weitere Aufbewahrung bei gleichzeitiger Einschränkung der Verarbeitung unbedingt erforderlich ist; insoweit ist eine Angleichung an die Terminologie der Bestimmungen des HDSIG-E vorgenommen worden, was die Verarbeitung von besonderen Kategorien personenbezogener Daten angeht.

Im neu eingeführten Satz 2 wird eine verkürzte Frist zur Löschung von Daten eingeführt, die entgegen dem Grundsatz verarbeitet, insbesondere erhoben wurden, dass der Kernbereich der Lebensgestaltung nicht zum Gegenstand der Verarbeitung personenbezogener Daten gemacht werden darf. Dies trägt der besonderen Schutzwürdigkeit der Betroffenen in diesem Fall Rechnung.

Der ebenfalls neu eingeführte Satz 3 statuiert insoweit eine Dokumentationspflicht zur kontrollierbaren Löschung der in Satz 1 und 2 aufgeführten, besonders sensiblen Daten, vgl. BVerfGE 274 S. 337ff. [S. 339]).

Zu Abs. 3
Die Vorschrift befasst sich mit der Löschung von personenbezogenen Daten und differenziert hierbei zwischen Akten und Dateien zum Gefangenen und sonstigen Akten und Dateien. Dabei ist eine Gleichbehandlung von Dateien im Sinne einer elektronischen Datei mit einer Papierakte geboten, da auch eine ordnungsgemäß geführte Gefangenenpersonalakte regelmäßig ein Dateisystem im datenschutzrechtlichen Sinne darstellen wird (vgl. zum Begriff Gola DS-GVO Art. 4 Rd.-Nr. 46). Die Vorschrift orientiert sich insoweit an der Struktur des Abs. 3 Satz 1 in der derzeit geltenden Fassung, wobei aber entsprechend der Systematik der Richtlinie (EU) Nr. 2016/680 statt einer grundsätzlichen Sperrung der Daten jetzt vorrangig deren Löschung zu erfolgen hat.

In Satz 1 wird zunächst redaktionell klargestellt, dass der Abs. sich - wie Abs. 1 und 2 - auf personenbezogene Daten bezieht. § 53 Abs. 2 HDSIG-E sieht in Umsetzung von Art. 16 der Richtlinie (EU) Nr. 2016/680 die Löschung vor, wenn die Kenntnis der Daten für die Aufgabenerfüllung nicht mehr erforderlich ist. Das ist grundsätzlich dann der Fall, wenn ein Gefangener endgültig entlassen wird. Dies ist jedoch nicht der Fall, sofern die begonnene Freiheitsentziehung wiederaufgenommen werden kann - insbesondere bei Aussetzung des Strafrestes zur Bewährung. Entsprechend ist der Anstalt eine Frist für die Löschung der personenbezogenen Daten jedenfalls bis zum Ende einer möglichen Bewährungsfrist einzuräumen. Wird ein Gefangener nach Verbüßung einer Jugendstrafe auf Bewährung entlassen, dauert die Bewährungszeit bis zu drei Jahre, § 22 Abs. 1 Satz 2 JGG. Wird die Strafaussetzung widerrufen, müssen die Daten aus der vorhergehenden Inhaftierung dem Justizvollzug zur Verfügung stehen, da das Vollstreckungsverhältnis gerade nicht beendet wurde. Außerdem sollen die gespeicherten Daten gemäß BVerfGE 116, 69-95,

Rdnr. 64, der Evaluation des Justizvollzuges dienen. Besteht zum Zeitpunkt des Fristablaufs ein konkreter Anhaltspunkt dafür, dass eine Aufbewahrung von Daten zur Abwicklung des Vollstreckungsverhältnisses weiter erforderlich ist, kann dem durch die weitere Speicherung bei Einschränkung der Verarbeitung nach Abs. 4 Rechnung getragen werden.

Satz 2 ersetzt den bisherigen Abs. 4 der Bestimmung in seiner derzeit geltenden Fassung.

Zu Abs. 4
Der besseren Nachvollziehbarkeit halber sollen die Bestimmungen zur Einschränkung der Verarbeitung personenbezogener Daten in einem eigenen Absatz dargestellt werden. Aus demselben Grund wird in Satz 1 auf die Normen verwiesen, aus denen sich grundsätzlich ergibt, wann und wie die Einschränkung der Verarbeitung zu erfolgen hat.

Anstelle einer Löschung der Daten können diese unter den Voraussetzungen des § 53 Abs. 3 bis 7 des HDSIG-E in der Verarbeitung eingeschränkt werden, Satz 1 Nr. 1. Wie in § 53 Abs. 3 HDSIG-E erscheint eine weitergehende Speicherung bei Einschränkung der Verarbeitung zu Beweiszwecken insgesamt sinnvoll. Art. 16 Abs. 3 Satz 1 Buchst. b der Richtlinie (EU) Nr. 2016/680 lässt dies grundsätzlich zu und beschränkt Beweiszwecke nicht ausdrücklich auf den Anwendungsbereich der Richtlinie. Dies deckt auch die Beweiszwecke z.B. auch jenen Konstellationen ab, in denen ein ehemaliger Gefangener Haftungsansprüche gegen das Land geltend macht, z.B. wegen fehlerhafter ärztlicher Behandlung in der Haft. Einen ähnlichen Weg geht insoweit auch § 78 Abs. 2 bzw. 3 des Bundeskriminalamtgesetzes in seiner Neufassung durch das Gesetz zur Neustrukturierung des Bundeskriminalamtgesetzes; dort wird ebenfalls nur von der Aufbewahrung für "gerichtliche Verfahren" bzw. der Behebung "einer Beweisnot" gesprochen, ohne nach der Art des Verfahrens zu differenzieren, in dem die Daten benötigt werden. Sofern eine Einschränkung der Verarbeitung zu Beweiszwecken erfolgt, ist aber darauf zu achten, dass die Entscheidung hierüber grundsätzlich eine Einzelfallentscheidung darstellt und zum Zeitpunkt ihrer Entscheidung konkrete Anhaltspunkte für die Notwendigkeit einer späteren Verwendung vorliegen müssen. Eine abstrakte Vorratsdatenspeicherung ohne konkreten Anlass - der sinnvollerweise zu dokumentieren ist - dürfte unzulässig sein. Anders ist dies bei normierten Dokumentationspflichten zu beurteilen, wie insbesondere z.B. nach § 10 der Berufsordnung für die Ärztinnen und Ärzte in Hessen für die im Rahmen der Freiheitsentziehung erfolgten ärztlichen Maßnahmen; ein hierauf bezogenes Regelbeispiel wurde zur Erleichterung der Rechtspraxis in Nr. 1 aufgeführt.

Satz 1 Nr. 2 stellt insoweit einen Auffangtatbestand dar, soweit Daten nicht im Geltungsbereich der Richtlinie (EU) Nr. 2016/680 gespeichert wurden.

Die Kennzeichnung von in der Verarbeitung eingeschränkten personenbezogenen Daten trägt insbesondere § 53 Abs. 4 HDSIG-E Rechnung. Die in Satz 2 ebenfalls geregelte Heranziehung in der Verarbeitung eingeschränkter personenbezogener Daten, im Regelfall durch Übermittlung, zu anderen Zwecken als des § 40 HDSIG-E, muss den Anforderungen der Verordnung (EU) Nr. 2016/679 genügen (vgl. Art. 9 Abs. 1 und 2 der Richtlinie (EU) Nr. 2016/680; insoweit gestattet Art. 18 Abs. 1 Buchst. a bzw. c der Verordnung (EU) Nr. 2016/679 aber auch die Verwertung zu Beweiszwecken). Wie sich aus Art. 9 der Richtlinie (EU) Nr. 2016/680 ergibt, muss die Verarbeitung zu Vollzugszwecken erhobener Daten auch nicht auf den sachlichen Bereich der Richtlinie (EU) Nr. 2016/680 beschränkt sein.

Satz 3 entspricht dem bisherigen Regelungsgehalt von § 65 Abs. 3 S. 4 HJStVollzG in seiner jetzigen Fassung. Auch insoweit bleibt eine Einwilligung weiter zulässig: entweder dient die Aufhebung der Einschränkung der Verarbeitung Zwecken der Richtlinie (EU) Nr. 2016/680, sodass § 46 HDSIG-E Anwendung findet; oder die Verarbeitung dient anderen Zwecken, sodass über Art. 9 Abs. 1 der Richtlinie (EU) Nr. 2016/680 die Bestimmungen der Verordnung (EU) Nr. 2016/679 gelten.

Satz 4 entspricht dem bisherigen Regelungsgehalt von § 65 Abs. 3 S. 2 HJStVollzG in seiner jetzigen Fassung.

Zu Abs. 5
Entsprechend § 70 Abs. 4 HDSIG-E wurde eine jährliche Kontrollfrist eingeführt, differenzierend zwischen Gefangenendateien und -akten einerseits sowie sonstigen Dateien und Akten andererseits.

Zu Abs. 6
Der Absatz entspricht im Wesentlichen dem bisherigen Abs. 5 in der derzeit geltenden Fassung. Redaktionell wurde die Herkunft der Daten danach präzisiert, aus welchen Akten etc. sie stammen. Hinsichtlich der Gefangenenbücher ist darauf hinzuweisen, dass es sich hierbei um Bestandsverzeichnisse in Buchform handelt, die mittlerweile elektronisch geführt werden. Die Aufbewahrungsfristen beziehen sich daher im Wesentlichen auf Altfälle, die sich bereits in der Aufbewahrung befinden.

In Satz 4 wurde die Verweisung auf das Hessische Archivgesetz in eine dynamische Verweisung umgewandelt, um zukünftige Änderungen abzubilden.

Zu Nr. 10 (§ 66)

Zu Buchst. a
In Satz 2 wurde ergänzend eingefügt, dass die Ergebnisse dem öffentlichen Interesse dienen, um den Maßgaben von § 45 HDSIG-E zu entsprechen.

Zu Buchst. b
Der Verweis auf § 476 StPO ist dahin gehend zu aktualisieren, dass er den Anforderungen an eine Verarbeitung besonderer Kategorien personenbezogener Daten gemäß § 43 Abs. 1 HDSIG-E Rechnung trägt (Nr. 2), sodass eine Übermittlung nur bei unbedingter Erforderlichkeit möglich ist.

Zu Art. 3 (Änderung des Hessischen Strafvollzugsgesetzes)

Allgemeines
Auf den Strafvollzug findet grundsätzlich die Richtlinie (EU) Nr. 2016/680 des Europäischen Parlamentes und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zweck der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung sowie zum freien Datenverkehr und zur Aufhebung des Rahmenbeschlusses 2008/977/JI des Rates Anwendung. Insoweit wird auf die Ausführungen zur Begründung zur Änderung des Hessischen Jugendstrafvollzugsgesetzes Bezug genommen.

Im Einzelnen

Zu Nr. 1 (Inhaltsübersicht)
Soweit bei einzelnen Paragrafen die Überschriften geändert werden, ist die Inhaltsübersicht entsprechend anzupassen.

Zu Nr. 2 (§ 24)
Eine Benachrichtigung der nächsten Angehörigen ist im Falle der schweren Erkrankung von der Einwilligung des Gefangenen abhängig zu machen; ein entsprechender Vorbehalt wurde zu Satz 1 als 2. Halbsatz angefügt. Dies entspricht den Maßgaben von Art. 9 Abs. 1 S. 2 der Richtlinie (EU) Nr. 2016/680 i.V.m. Art. 9 Abs. 1 und 2 Buchst. a der Verordnung (EU) Nr. 2016/679, da insoweit die Verarbeitung (durch Übermittlung) von besonderen Kategorien personenbezogener Daten (in Form von Gesundheitsdaten, vgl. § 41 Nr. 14 HDSIG-E) zu Zwecken erfolgt, die nicht ohne Weiteres der Durchführung des Strafvollzuges dient, sondern zunächst einmal der allgemeinen Information der Angehörigen. Auf eine mutmaßliche Einwilligung i.S.v. Art. 9 Abs. 2 Buchst. c kann insoweit nicht abgestellt werden, da die Übermittlung des Gesundheitszustandes an Angehörige auch bei Lebensgefahr kein lebenswichtiges Interesse der betroffenen Personen darstellt; dies dürfte nur für die Durchführung lebenserhaltender Maßnahmen zutreffen. Um auch in Situationen handeln zu können, in denen eine Einwilligung nicht mehr eingeholt werden kann, sollte die Einwilligung - die insoweit den Anforderungen der Verordnung (EU) Nr. 2016/679 genügen muss - bereits bei Aufnahme eingeholt werden; zu diesem Zweck wurde als neuer Satz 3 eine Belehrungspflicht aufgenommen.

Im Falle des Todes ist weiterhin eine Benachrichtigung auch ohne Einwilligung angezeigt und nach §§ 22 Abs. 3 i.V.m. Abs. 2 Nr. 3 und Art. 9 Abs. 2 Buchst. f der Verordnung (EU) Nr. 2016/679 möglich.

Zu Nr. 3 (§ 34)

Zu Buchst. a
Als neuer zweiter Halbsatz wurde eine Regelung zu Satz 1 hinzugefügt, wonach sich die Überwachung sowohl auf Gefangene wie Besucher bezieht; dies dient der Klarstellung im Sinne von § 67 HDSIG-E, da die Überwachung sich sowohl auf die Gefangenen als verurteilte Straftäter (dort Nr. 3) wie auch auf den Besuch (dort nur Nr. 5) beziehen kann.

In Satz 2 wird klargestellt, dass die Überwachung der Unterhaltung, sofern sie besondere Kategorien personenbezogener Daten zum Gegenstand hat, nur noch im Falle unbedingter Erforderlichkeit erfolgt, um insbesondere den Anforderungen aus § 43 Abs. 1 HDSIG-E bzw. Art. 10 der Richtlinie (EU) Nr. 2016/680 Rechnung zu tragen. Eine Verarbeitung besonderer Kategorien personenbezogener Daten - legaldefiniert in § 41 Nr. 15 HDSIG-E, insoweit gleichlaufend Art. 9 der Verordnung (EU) Nr. 2016/679 - ist nur bei unbedingter Erforderlichkeit zulässig. Der Begriff der "unbedingten Erforderlichkeit" ist weder in der Verordnung (EU) Nr. 2016/679 noch der Richtlinie (EU) Nr. 2016/680 legaldefiniert. Da er nach dem Wortlaut ein gesteigertes Maß der Erforderlichkeit vorsieht, kann er wie der bisher im Rahmen des Strafvollzugsrechts verwendete

Begriff "unerlässlich" im Sinne eines gesteigerten Maßes der Erforderlichkeit verstanden werden. Eine Maßnahme ist dann unerlässlich, wenn tatsächlich keinerlei weniger eingriffsintensive und mit vertretbarem Aufwand durchführbare Maßnahmen zur Zweckerreichung zur Verfügung stehen; darüber hinaus darf die Art der datenschutzrelevanten Maßnahme schutzwürdige Interessen der Betroffenen nicht beeinträchtigen (vgl. Arloth/Krä StVollzG 4. Auflage § 59 HStVollzG Rd.-Nr. 2, Laubenthal/Nestler/Neubacher/Verrel O Rd.-Nr. 35ff). In die Abwägung einzustellen sind somit sämtliche mit hinreichender Wahrscheinlichkeit mit der Datenverarbeitung für die Betroffenen im persönlichen Nahbereich einhergehenden Konsequenzen, einschließlich der Auswirkungen auf die Beziehungen zu Verwandten, zum sozialen Wohnumfeld sowie zum Arbeitgeber (vgl. Laubenthal/Nestler/Neubacher/Verrel aaO.).Wie in der Begründung zu § 43 HDSIG-E ausgeführt ist eine unbedingte Erforderlichkeit anzunehmen, wenn keine zumutbare Alternativ- oder Ausgleichsmaßnahme zur Verfügung steht, um ein legitimes Ziel zu erreichen.

Inwieweit der Begriff der "unbedingten Erforderlichkeit" in der Rechtspraxis zu anderen Ergebnissen führen wird als eine konsequente Anwendung des Erforderlichkeitsprinzips im Rahmen der Verhältnismäßigkeitsprüfung bleibt abzuwarten. So wird in anderen Regelungsbereichen z.B. zur Durchführung einer sachgerechten medizinischen Betreuung bereits bei jeder Anamnese die umfassende Erhebung von Gesundheitsdaten regelmäßig unbedingt erforderlich sein, ebenso wie es für jeden Vollzugsbediensteten regelmäßig unbedingt erforderlich sein dürfte, auf die Gesichtsbilder der Gefangenen in der Gefangenenpersonalakte zugreifen zu können, um dessen Person in praxisgerechter Weise identifizieren zu können.

Die Überwachung von Besuchen ist elementar für die Sicherheit oder Ordnung der Einrichtung. Die permanente Überwachung der Unterhaltung wird daher im Regelfall unbedingt erforderlich sein, auch wenn sie besondere Kategorien personenbezogener Daten zum Inhalt hat. In vielen Fällen ist es allerdings praktisch unvermeidbar, dass die Vollzugsbediensteten Informationen zur Kenntnis nehmen, bevor sie deren besonderen datenschutzrechtlichen Bezug erkennen. In derartigen Fällen ist es in Anlehnung an die Entscheidung BVerfGE 129, S. 208ff. (Rn. 209ff) verfassungsrechtlich nicht gefordert, den Zugriff wegen des Risikos einer Kernbereichsverletzung auf der Erhebungsebene von vornherein zu unterlassen. In Fällen dieser Art ist es geboten, aber auch ausreichend, für hinreichenden Schutz in der Auswertungsphase zu sorgen, insbesondere durch Gewährung eines entsprechenden Schutzes durch Löschung von Aufzeichnungen.

Zu Buchst. b
In Satz 1 wird ein neuer zweiter Halbsatz eingeführt, wonach die Überwachung auch durch optisch-elektronische Einrichtungen erfolgen kann, die als Videoüberwachung legaldefiniert wird, da dieser Begriff im Gesetz mehrfach verwendet wird.

Satz 2 wird dahin gehend neu gefasst, dass die Aufzeichnung und Speicherung von Daten gemäß Satz 1 nur im Falle unbedingter Erforderlichkeit erfolgt. Dies ist dem Umstand geschuldet, dass für den Geltungsbereich der Richtlinie (EU) Nr. 2016/680 je nach Qualität des Überwachungssystems Gesichtsbilder unter die besondere Kategorie personenbezogener Daten fallen können, insbesondere bei Verwendung spezieller Gesichtserkennungssoftware. Darüber hinaus ist eine Videoüberwachung von Besuchen besonders geneigt, durch Aufzeichnung des Verhaltens der überwachten Personen Informationen zu besonderen Kategorien personenbezogener Daten im Sinne von Art. 10 der Richtlinie (EU) Nr. 2016/680 zu generieren. Die Einfügung des Tatbestandsmerkmals der unbedingten Erforderlichkeit trägt im Interesse einer möglichst sicheren Umsetzung der Richtlinie (EU) Nr. 2016/680 entsprechend deren Art. 10 bzw. § 43 Abs. 1 HDSIG-E Rechnung, um eine Videoüberwachung in jedem Fall datenschutzrechtlich abzusichern.

Zu Nr. 4 (§ 35)
In Satz 1 wird eingefügt, dass die Erforderlichkeit sich auf Ziel und Aufgaben des Vollzugs der Freiheitsstrafe gemäß § 2, insbesondere auf Gründe der Sicherheit oder Ordnung der Anstalt bezieht; insoweit wird Art. 8 Abs. 2 der Richtlinie (EU) Nr. 2016/680 Rechnung getragen. Deren Anwendungsbereich ist auch im Bereich des Schriftwechsels nicht in jedem Fall ausgeschlossen. Es ist insbesondere nach Abs. 3 auch möglich, angehaltenen Schriftwechsel zu verwahren, regelmäßig in einer körperlichen Akte, aber auch nach Scannen in einer elektronischen Akte, mithin analogen oder digitalen Dateisystemen. Der zu überwachende Schriftwechsel wird häufig mit einer gewissen Wahrscheinlichkeit besondere Kategorien personenbezogener Daten enthalten, ohne dass dies vor Beginn der Überwachung klar ist. Insoweit besteht eine geringere Flexibilität als bei der Überwachung eines Besuchs, bei dem sich die besondere datenschutzrechtliche Relevanz bei den besonderen Kategorien aus dem überwachten Verlauf des Besuchs selbst ergeben kann. Um das Schutzniveau für die besonderen Kategorien personenbezogener Daten von Anfang an zu gewährleisten, ist nach § 43 Abs. 1 HDSIG-E daher prophylaktisch sicherzustellen, dass die Überwachung des Schriftwechsels nur im Falle unbedingter Erforderlichkeit erfolgt, was durch einen entsprechenden Einschub in Satz 1 erfolgt. Da die Überwachung des Schriftwechsels für Sicherheit oder Ordnung unverzichtbar sind, wird das Kriterium der unbedingten Erforderlichkeit regelmäßig erfüllt sein. Darüber hinaus sollten Gefangene frühzeitig (d.h. bei Aufnahme) auf die Möglichkeit der Überwachung hingewiesen werden, um den Eingriff in das Postgeheimnis nicht zu einer verdeckten Maßnahme zu machen, an die - insbesondere angesichts des Urteils des Bundesverfas-

sungsgerichts vom 20. April 2016, Aktenzeichen 1 BvR 966/09 und 1BvR 1140/09 - bei der Datenverarbeitung erheblich höhere Anforderungen zu stellen wären; eine entsprechende Hinweispflicht wurde als neuer Halbsatz an Satz 1 angefügt.

Zu Nr. 5 (§ 45)
In Satz 2 wird - auch im Sinne einer einheitlichen Terminologie - ferner klargestellt, dass die technischen Hilfsmittel auch optisch-elektronische Einrichtungen (Videoüberwachung) umfassen. Da diese - unabhängig von der Einstufung eines Gesichtsbildes als biometrisches Datum - besonders geeignet sind, insgesamt besondere Kategorien personenbezogener Daten zu liefern, sei es in Form von Gesundheitsdaten oder anderen Unterfällen, ist nach § 43 Abs. 1 HDSIG-E in Satz 2 nunmehr vorgesehen, dass die entsprechende Verarbeitung nur im Falle unbedingter Erforderlichkeit zulässig ist. Auch hier wird wegen der Unverzichtbarkeit einer entsprechenden Überwachung für Sicherheit oder Ordnung der Anstalt das Kriterium der unbedingten Erforderlichkeit regelmäßig erfüllt sein.

Zu Nr. 6 (§ 50)

Zu Buchst. a
Es wird - auch im Sinne einer einheitlichen Terminologie - in Nr. 2 klargestellt, dass die technischen Hilfsmittel auch optisch-elektronische Einrichtungen (Videoüberwachung) umfassen. Da diese regelmäßig besondere Kategorien personenbezogener Daten liefern können, insbesondere Gesundheitsdaten zur Kontrolle des Gesundheitszustandes des Gefangenen, ist nach § 43 Abs. 1 HDSIG-E vorgesehen, dass die entsprechende Verarbeitung nur im Falle unbedingter Erforderlichkeit zulässig erfolgt. Da die entsprechende Kontrolle für die Information des Gesundheitszustandes des Gefangenen unverzichtbar ist, wird das Kriterium der unbedingten Erforderlichkeit regelmäßig erfüllt sein.

Zu Buchst. b
Da die dauerhafte Überwachung nach Abs. 2 Nr. 2 regelmäßig Gesundheitsdaten liefern kann und somit besondere Kategorien personenbezogener Daten, ist in Satz 2 klargestellt, dass dies im Sinne von § 43 Abs. 1 HDSIG-E nur im Falle unbedingter Erforderlichkeit zulässig ist. Auch hier gilt, dass, da die entsprechende Kontrolle für die Information des Gesundheitszustandes des Gefangenen unverzichtbar ist, das Kriterium der unbedingten Erforderlichkeit regelmäßig erfüllt sein wird.

Zu Nr. 7 (§§ 58 bis 61)

Zu § 58

Zu Abs. 1
In Satz 1 wird in Anlehnung an § 41 Nr. 2 HDSIG-E statt an die Alternativen Datenerhebung bzw. -weiterverarbeitung an den einheitlichen Begriff der Verarbeitung angeknüpft; ebenfalls wurde vor dem Wort "verarbeiten" ein "nur" eingefügt, um das Prinzip des Verbots mit Erlaubnisvorbehalt hervorzuheben. Ferner erfolgt in Satz 1 die systematische Klarstellung, dass zunächst eine gesetzliche Spezialregelung Anwendung findet und nur in letzter Linie die Generalklausel, die insoweit grds. auf die Erforderlichkeit für den Vollzug abstellt. Bei der Verarbeitung besonderer Kategorien personenbezogener Daten - legaldefiniert § 41 Nr. 15 HDSIG-E - muss allerdings insoweit die unbedingte Erforderlichkeit gegeben sein. Gestrichen wurde die Einwilligung als allgemeiner Rechtsgrund für eine Datenverarbeitung. Dies trägt dem Umstand Rechnung, dass die Richtlinie (EU) Nr. 2016/680 eine Einwilligung im Rahmen ihres Geltungsbereichs grundsätzlich nicht mehr als alleinige Grundlage hierfür ausreichen lässt, wie sich aus Ziffer 35 der Erwägungen zur Richtlinie ergibt. Wie weit dieser Grundsatz reicht, ist derzeit noch nicht abschließend geklärt. Der letzte Satz der vorgenannten Erwägungen führt hierzu aus: "Dies sollte die Mitgliedstaaten nicht daran hindern, durch Rechtsvorschriften vorzusehen, dass die betroffene Person der Verarbeitung ihrer personenbezogenen Daten für die Zwecke dieser Richtlinie zustimmen kann, beispielsweise im Falle von DNA-Tests in strafrechtlichen Ermittlungen oder zur Überwachung ihres Aufenthaltsortes mittels elektronischer Fußfessel zur Strafvollstreckung." In den Artikeln der Richtlinie (EU) Nr. 2016/680 findet sich die Einwilligung dann jedoch - anders als in der Verordnung (EU) Nr. 2016/679 - als Rechtsgrund einer Datenverarbeitung nicht mehr. Daher wird die entsprechende Erwägung dahin gehend auszulegen sein, dass die Einwilligung in der Einzelvorschrift ausdrücklich aufgeführt sein muss; konsequenterweise sieht § 46 HDSIG-E die Möglichkeit einer Einwilligung in solchen Fällen vor. Tatbestände, bei denen ein solcher Einwilligungsvorbehalt gegeben ist, werden nunmehr durch den Tatbestand der "Rechtsvorschrift" mit abgedeckt.

Die Verweisung auf die Bestimmungen des subsidiär geltenden Hessischen Datenschutz- und Informationsfreiheitsgesetzes in Satz 2 wird faktisch als dynamische Verweisung ausgestaltet, um zukünftige Änderungen abzubilden. Zu Satz 2 wurde ein weiterer Halbsatz angehängt, durch den klargestellt wird, dass die Datenverarbeitung durch die Justizvollzugsbehörden zu Vollzugszwecken grundsätzlich - aber nicht ausschließlich, da insoweit auch die allgemeinen Bestimmungen,

insbesondere Teil 1 gelten - unter dem Regime des Teils 3 des HDSIG-E erfolgt, um der Praxis angesichts der - in Art. 9 der Richtlinie (EU) Nr. 2016/680 selbst vorgesehenen Zweiteilung der datenschutzrechtlichen Regelungssysteme - eine grundsätzliche Entscheidungshilfe an die Hand zu geben. Dies hat daher nicht allein deklaratorische Wirkung; die Entscheidung kann im Einzelfall schwierig werden, s. hierzu die Ausführungen in den Vorbemerkungen zur Begründung.

Neu hinzugefügt wurde Satz 3, der den Verhältnismäßigkeitsgrundsatz konkretisiert und in Hinblick auf Art. 1 Abs. 1 GG ein Verarbeitungsverbot ausspricht, da der Gesetzgeber den Kernbereich privater Lebensgestaltung zu schützen hat (vgl. BVerfGE 129, S. 208ff. [S. 245]). Ob ein Sachverhalt dem unantastbaren Kernbereich zuzuordnen ist, hängt davon ab, ob er nach seinem Inhalt höchstpersönlichen Charakters ist, also auch in welcher Art und Intensität er aus sich heraus die Sphäre anderer oder Belange der Gemeinschaft berührt (vgl. BVerfGE 80, 367 [374] = NJW 1990, 563).

Zu Abs. 2
Die Präzisierung, dass die Verarbeitung für Ziel und Aufgaben des Vollzugs nach § 2 erfolgt, dient der Klarstellung, dass die Verantwortlichen im Sinne des Datenschutzes im vorliegenden Fall Daten grundsätzlich zu Zwecken des Strafvollzuges verarbeiten. Klarstellend wird ferner eingefügt, dass die Verarbeitung der aufgezählten personenbezogenen Daten auch zur Aufrechterhaltung der medizinischen Versorgung und Gesundheitsfürsorge verarbeitet werden können, was Art. 8 Abs. 2 der Richtlinie (EU) Nr. 2016/680 Rechnung trägt.

Ferner wird auf den einheitlichen Tatbestand einer Verarbeitung abgestellt.

Da die bisherigen Nummern 1 bis 4 bereits zumeist besondere Kategorien personenbezogener Daten i.S.v. § 41 Nr. 15 HDSIG-E darstellen, wurde durch die Ergänzung um Nr. 5 eine Gesamtregelung für die Verarbeitung entsprechender Informationen geschaffen. Dabei wurden die Gesundheitsdaten in Hinblick auf ihre besondere Bedeutung, aber auch ihre bisher schon separate Speicherung herausgehoben. Deren Verarbeitung ist insbesondere bei Maßnahmen nach §§ 24 Abs. 1, 25 Abs. 4, 46 Abs. 2 und 3 sowie 47 relevant.

Die Verarbeitung besonderer Kategorien personenbezogener Daten wurde nach § 43 Abs. 1 HDSIG-E an das Erfordernis unbedingter Erforderlichkeit geknüpft.
Die beibehaltene Beschränkung auf Gefangene als verurteilte Straftäter trägt darüber hinaus § 67 HDSIG-E Rechnung, der wiederum aus Art. 6 der Richtlinie (EU) Nr. 2016/680 folgt.

Zu Abs. 3
Es erfolgt in Satz 1 eine Anpassung der separat zu führenden personenbezogenen Daten an die Neunummerierung in Abs. 2.

In Satz 2 wird statt auf "Daten, die den Gesundheitszustand betreffen" auf "Gesundheitsdaten" abgestellt, da letzter Begriff in § 41 Nr. 14 HDSIG-E legaldefiniert ist. Der Begriff "Personalakte" in Satz 2 wurde durch den der "Gefangenenpersonalakte" präzisiert.

Zu Abs. 4
Satz 2 wurde neu eingeführt, um klarzustellen, dass bei der Verarbeitung besonderer Kategorien personenbezogener Daten dies nur bei unbedingter Erforderlichkeit zulässig ist, s. § 43 Abs. 1 HDSIG-E.

Zu Abs. 5
Neu eingefügt wurde Satz 2, sofern hierbei die Verarbeitung biometrischer Daten notwendig werden sollte. Dies würde die Verarbeitung von besonderen Kategorien personenbezogener Daten darstellen, die wiederum gemäß § 43 Abs. 1 HDSIG-E nur bei unbedingter Erforderlichkeit zulässig ist.

Zu Abs. 6
Die Neufassung der Vorschrift orientiert sich an § 4 HDSIG-E. Da die Außensicherung sowohl öffentliche wie nicht öffentliche Plätze abdecken kann, konnte insoweit nicht lediglich auf die vorgenannte Vorschrift verwiesen werden.

Soweit in Satz 1 zusätzlich darauf abgestellt wird, dass schutzwürdige Interessen der Betroffenen nicht überwiegen dürfen, erfolgt dies in Orientierung an § 4 Abs. 1 HDSIG-E.

Satz 2 wurde dahin gehend ergänzt, dass neben der Überwachung auch der Name und die Kontaktdaten des Verantwortlichen zum frühestmöglichen Zeitpunkt erkennbar zu machen sind. Verantwortlicher wird dabei regelmäßig keine natürliche, mit Namen zu benennende Person sein, sondern die Anstalt als zuständige Behörde, vgl. § 41 Nr. 8 HDSIG-E.

Ergänzend wird klargestellt, dass eine Speicherung nur zulässig ist, wenn keine Anhaltspunkte dafür bestehen, dass schutzwürdige Interessen der Betroffenen überwiegen; dies trägt § 4 Abs. 3 Satz 1 HDSIG-E Rechnung.

Zu § 58a

Zu Abs. 1
In Satz 2 wurde klargestellt, dass die Zuverlässigkeitsüberprüfung zur Aufrechterhaltung der Sicherheit oder Ordnung der Anstalt und zur Abwendung von Gefahren hierfür erfolgt.
Die Verweisung auf das HSÜG in Satz 5 wurde durch eine dynamische Verweisung ersetzt, um zukünftige Änderungen abzubilden.

Zu Abs. 2
In Satz 1 wurde klargestellt, dass die Zuverlässigkeitsüberprüfung zur Aufrechterhaltung der Sicherheit oder Ordnung der Anstalt hierfür erfolgt.

In Satz 2 wurde präzisiert, dass - in Hinblick auf § 67 HDSIG-E - die Zulassung zum Gefangenenbesuch überhaupt erfolgt und nicht nur für welche Gefangene.

Zu Abs. 4
Hinsichtlich der Benachrichtigungspflicht wurde ausdrücklich auf § 51 HDSIG-E Bezug genommen.

Zu Abs. 6
In Satz 1 wurde in Hinblick auf den in Art. 8 der Richtlinie (EU) Nr. 2016/680 normierten Erforderlichkeitsgrundsatz ergänzend eingeführt, dass die Wiederholung der Zulässigkeitsprüfung zu erfolgen hat, sofern ihre Erforderlichkeit fortbesteht.

Zu § 59
Der bisherige § 59 HStVollzG war mit seinem bisherigen Regelungsgehalt aufzuheben. Die Vorschrift ging von dem Grundsatz aus, dass personenbezogene Daten grundsätzlich bei den Betroffenen zu erheben sind. Ein solcher Grundsatz wird weder in der Richtlinie (EU) Nr. 2016/680 noch der Verordnung (EU) Nr. 2016/679 statuiert. Da nicht ausgeschlossen werden kann, dass auch eine Vollzugseinrichtung im Bereich der Verordnung (EU) Nr. 2016/679 tätig wird, könnte die Beibehaltung eines entsprechenden Grundsatzes insoweit als Verstoß gegen europäisches Recht gelten. Darüber hinaus ist davon auszugehen, dass die Datenerhebung auch in Zukunft hauptsächlich bei den Betroffenen erfolgen werden wird. Sollte dies nicht der Fall sein, sind diese im Übrigen auch nicht rechtlos, wie sich aus § 64 ergibt.

Stattdessen wird eine neue Vorschrift an dieser Stelle eingefügt, die eine spezielle Befugnis zum Auslesen unzulässig in die Justizvollzugsanstalten eingebrachter Datenträger darstellt. Eine spezielle Ermächtigung hierfür ist sinnvoll und erforderlich, da die unkontrollierte Kommunikation über Speichermedien eine erhebliche Gefährdung der Sicherheit oder Ordnung der Anstalten darstellt. Die Neuregelung erfolgt im Rahmen der datenschutzrechtlichen Bestimmungen, da damit gerechnet werden kann, dass die entsprechenden Speichermedien aufgrund ihrer Bestimmung zur Kommunikation zahlreiche personenbezogene Daten, auch solche besonderer Kategorien, enthalten.

In diesem Zusammenhang ist aus Gründen der Verhältnismäßigkeitsgrundsatzes zu differenzieren, dass nicht jeder Datenspeicher auszulesen ist, sondern nur dann, wenn konkrete Anhaltspunkte für eine Gefährdung hierdurch sprechen. Solche konkreten Anhaltspunkte werden dann regelmäßig vorliegen, wenn Hinweise für ein heimliches Verbringen des Datenspeichers in die Anstalt sprechen, z.B. bei Auffinden in einem Haftraum. Anders dürfte die Lage z.B. zu beurteilen sein, wenn Kommunikationssysteme als notwendiger Bestandteil z.B. von Baugeräten im Rahmen von Baumaßnahmen in eine Anstalt verbracht werden, ohne dass das Baugerät hierauf gezielt kontrolliert wurde.

Die Regelung orientiert sich im Wesentlichen an § 23 des rheinland-pfälzischen Landesjustizvollzugsdatenschutzgesetzes, zuletzt geändert durch § 44 des Gesetzes vom 6. Oktober 2015 (GVBl. S. 354). Diese Vorschrift lautet in ihrer derzeitigen Fassung wie folgt:

"§ 23
Auslesen von Datenspeichern

(1) Elektronische Datenspeicher sowie elektronische Geräte mit Datenspeicher, die ohne Erlaubnis in die Anstalt eingebracht wurden, dürfen auf schriftliche Anordnung der Anstaltsleiterin oder des Anstaltsleiters ausgelesen werden, soweit konkrete Anhaltspunkte die Annahme rechtfertigen, dass dies für die Erfüllung der Aufgaben des Vollzugs erforderlich ist. Die Gründe sind in der Anordnung festzuhalten. Sind die Betroffenen bekannt, sind ihnen die Gründe vor dem Auslesen mitzuteilen. Beim Auslesen sind ihre schutzwürdigen Interessen zu berücksichtigen, insbesondere der Kernbereich privater Lebensgestaltung. Das Auslesen ist möglichst auf die Inhalte zu beschränken, die zur Erreichung der die Anordnung begründenden Zwecke erforderlich sind.

(2) Die nach Absatz 1 erhobenen Daten dürfen verarbeitet werden, soweit dies aus den in der Anordnung genannten Gründen erforderlich ist. Aus anderen Gründen ist die Ver-

arbeitung der Daten nur zulässig, soweit dies für die Erfüllung der Aufgaben des Vollzugs zwingend erforderlich ist und schutzwürdige Interessen der Betroffenen dem nicht entgegenstehen.

(3) Die Verarbeitung der nach Absatz 1 erhobenen Daten ist unzulässig, soweit sie dem Kernbereich der privaten Lebensgestaltung Gefangener oder Dritter unterfallen. Diese Daten sind unverzüglich zu löschen. Die Tatsachen der Erfassung und der Löschung der Daten sind zu dokumentieren. Die Dokumentation darf ausschließlich für Zwecke der Datenschutzkontrolle verwendet werden. Sie ist zu löschen, wenn sie für diese Zwecke nicht mehr erforderlich ist, spätestens jedoch am Ende des Kalenderjahres, das dem Jahr der Dokumentation folgt.

(4) Die Gefangenen sind bei der Aufnahme über die Möglichkeit des Auslesens von nicht gestatteten Datenspeichern zu belehren."

Ein besonderer Hinweis auf die Berücksichtigung schutzwürdiger Interessen und eine Beschränkung auf die Inhalte, die zur Erreichung der die Anordnung begründenden Zwecke erforderlich sind, ist indes nicht erforderlich, da dies durch die allgemeine Bestimmung in § 58 Abs. 1 bzw. die Beschränkung innerhalb der Vorschrift "soweit" bereits abgedeckt wird. In Hinblick auf die Möglichkeit, dass die auszulesenden Datenträger auch besondere Kategorien personenbezogener Daten enthalten können, sollte von der Maßnahme nur bei unbedingter Erforderlichkeit Gebrauch gemacht werden. Ebenfalls nicht notwendig ist eine Beschränkung der Verarbeitung auf die Zwecke ihrer Erhebung, da dies ebenfalls durch § 58 Abs. 1 und 2 abgedeckt ist. Einer besonderen Löschungsbestimmung bedarf es nicht, diese ist durch die Neuregelung in § 65 Abs. 2 erfasst.

Zu § 60

Zu Abs. 1
Zunächst waren die Bestimmungen über die Verarbeitung personenbezogener Daten zu anderen Zwecken, als zu denen, für die sie erhoben wurden, an die entsprechenden Bestimmungen des HDSIG-E anzupassen, d.h. an dessen §§ 20 bis 27 und 44 bis 45. Danach Art. 9 der Richtlinie (EU) Nr. 2016/680 auch für Justizvollzugsbehörden der Anwendungsbereich der Verordnung (EU) Nr. 2016/679 eröffnet sein kann, war insoweit auch auf die Normen zu deren Umsetzung abzustellen.

Soweit darüber hinaus in einer Aufzählung nurmehr besondere Regelbeispiele ("insbesondere") für eine Datenverarbeitung zu namentlich genannten Zwecken genannt werden, ist dies wie folgt zu begründen:

Die neue Nr. 1 stellt die Umsetzung von Art. 4 Abs. 2 der Richtlinie (EU) Nr. 2016/680 dar. Die bisherige Nr. 1 wird Nr. 2. Die bisherige Nr. 2 kann gestrichen werden, da sie in der neuen Nr. 1 aufgeht. Die Nennung von Nr. 3 bis 5 wäre über die neue Nr. 1 erfasst. Eine Streichung der vorgenannten Vorschriften könnte aber eine erhebliche Rechtsunklarheit in der Praxis auslösen, da durch die Verweisung auf allgemeine Bestimmungen die Rechtsanwendung nicht nur vereinfacht wird. Eine entsprechende Unklarheit sollte im Sinne einer effizienten Rechtshandhabung - auch im Sinne der Betroffenen - vermieden werden. Insoweit erscheint es sinnvoll, den bisherigen Katalog weitestgehend beizubehalten.

Dies gilt im Ergebnis und mit derselben Begründung auch für die übrigen Nr. 6 bis 12, zu deren Zweck die Verarbeitung anderweitig erhobener personenbezogener Daten jedenfalls nach Art. 9 Abs. 1 S. 2 der Richtlinie (EU) Nr. 2016/680 i.V.m. Art. 9 Abs. 2 der Verordnung (EU) Nr. 2016/679 zulässig ist, was wiederum über die Verweisung auf § 22 HDSIG-E abgedeckt wird. Auch insoweit soll jedoch Rechtsunklarheit in der Praxis vermieden werden, sodass es geboten erscheint, die bisherigen Tatbestände als Regelbeispiele ebenfalls beizubehalten.

Die Einführung des Erfordernisses der unbedingten Erforderlichkeit bei besonderen Kategorien personenbezogener Daten trägt insoweit § 43 Abs. 1 HDSIG-E Rechnung und betrifft z.B. Maßnahmen nach § 25 Abs. 3.

Zu Abs. 2
Die Vorschrift dient dem besonderen Schutz von Daten, die bei besonders erheblichen Eingriffen in Grundrechte anfallen.

Das Telekommunikationsgeheimnis steht den bisherigen Ausnahmetatbeständen insoweit gleich, weshalb die Überwachung der Telekommunikation (vgl. § 36) und das Auslesen von Datenspeichern (vgl. § 59 HStVollzG-E) in Satz 1 ebenfalls aufgeführt werden. Entsprechend der systematischen Bedeutung der Vorschrift wird in Satz 1 wie für Abs. 1 klargestellt, dass die Regelung für Datenverarbeitungen gilt, die über die reine Erfassung und Speicherung hinausgehen, insbesondere für die Übermittlung.

Die Gründe, aus denen bei den entsprechenden sensiblen Daten eine Weiterverarbeitung weiterhin möglich sein soll, werden nunmehr unter Nr. 1 bis 3 aufgezählt.

Nr. 1 erweitert den bisherigen Regelungsgehalt auf andere Zwecke, wie sie in § 40 HDSIG-E vorgesehen werden.

Nr. 2 entspricht der bisherigen Verweisung auf § 12 Abs. 2 Nr. 1 des derzeit noch geltenden Hessischen Datenschutzgesetzes. Die übrigen Verweisungen auf das derzeit noch geltende Hessische Datenschutzgesetz werden obsolet; der bisherige Verweis auf § 12 Abs. 2 Nr. 3 und 4 des Hessischen Datenschutzgesetzes erübrigt sich durch die Verweisung auf Abs. 1 Nr. 1 neuer Fassung.

Nr. 3 stellt insoweit einen Auffangtatbestand dar, um die Praxis bei der bisherigen Rechtsanwendung fortzuführen. Die bisherige Nr. 3 - die Einwilligung - wurde wegen der besonderen Problematik dieser Rechtsgrundlage im Geltungsbereich der Richtlinie (EU) Nr. 2016/680 gestrichen.

Darüber hinaus soll die Weiterverarbeitung, insbesondere die Übermittlung, nur bei unbedingter Erforderlichkeit vorgenommen werden, wie dies in Satz 1 eingefügt wurde. Das Bundesverfassungsgericht hat in seinem Urteil vom 20. April 2016, Aktenzeichen 1 BvR 966/09 und 1BvR 1140/09 in Hinblick auf das BKAG in der damals geltenden Fassung ausgeführt, dass die Verhältnismäßigkeit eines Eingriffs von dessen Intensität abhängt und angemessen ausgestaltet sein muss. Je tiefer Überwachungsmaßnahmen in das Privatleben eingreifen, desto strenger sind die Anforderungen, was insbesondere für die Wohnraumüberwachung und den Zugriff auf informationstechnische Systeme gilt. Die in der Entscheidung zu beurteilenden Sachverhalte betrafen zwar verdeckte Datenverarbeitungen, während die im Hessischen Strafvollzugsgesetz vorgesehenen Maßnahmen regelmäßig nicht verdeckt erfolgen, was insbesondere durch die Offenlegung von Überwachungsmaßnahmen gilt. Auch stellt insbesondere der Haftraum keine Wohnung i.S.d. Art. 13 GG dar (vgl. BVerfG NJW 1996, 2643). Schließlich müssen bei den Eingriffen nicht notwendigerweise auch besondere Kategorien personenbezogener Daten geschützt werden. Dennoch erscheinen vor diesem Hintergrund die aufgeführten Daten besonders schützenswert - nachdem es sich zwar um offene, aber tiefe Eingriffe in die Kommunikation handelt - sodass ihre Weitergabe nur zu eingeschränkten Zwecken und im Fall der unbedingten Erforderlichkeit erfolgen sollte. Durch diese Beschränkung wird sichergestellt, dass insbesondere die Übermittlung der entsprechenden Daten nur zu Zwecken erfolgt, für die sie selbst hätten erhoben werden können (Grundsatz der hypothetischen Datenneuerhebung).

Um im Falle ihrer Übermittlung sicherzustellen, dass die entsprechenden Daten mit der erforderlichen Sensibilität behandelt werden, sind sie entsprechend dem neu eingefügten Satz 2 eindeutig zu kennzeichnen.

Es wird ferner klargestellt, dass § 4 Abs. 3 Satz 2 HDSIG-E unberührt bleibt. Diese Vorschrift regelt den Sonderfall einer Übermittlung von Videoaufzeichnungen, die bei der Überwachung öffentlich zugänglicher Räume angefallen sind.

Zu Abs. 3
E handelt sich insoweit um Sonderfälle des Abs. 1.

Der neue Verweis in Satz 1 auf Abs. 1 soll ebenfalls der Vermeidung eine Rechtsunsicherheit dienen.

Zu Abs. 5
Der neue Hinweis in Satz 3 a. E. an jeden Empfänger, was die Einstufung besonderer Kategorien personenbezogener Daten angeht, entspricht insbesondere der Pflicht zur Schaffung geeigneter Garantien nach § 43 Abs. 2 Nr. 8 HDSIG-E im Falle der Übermittlung besonderer Kategorien personenbezogener Daten, die wiederum auf Art. 10 der Richtlinie (EU) Nr. 2016/680 zurückgeht.

Zu Abs. 6
Die Nennung der Gerichtszuständigkeit wurde an die Neufassung des Kataloges in Abs. 1 angepasst; desgleichen der Verweis auf die Vorschriften in § 65.

Zu § 61

Zu Abs. 1
Der Schutzbereich der Vorschrift in Satz 1 wurde auf alle besonderen Kategorien personenbezogener Daten nach § 41 Nr. 15 HDSIG-E erweitert. Die Erweiterung des Schutzes für alle besonderen Kategorien personenbezogener Daten trägt dessen § 43 Abs. 2 Rechnung. Weitere Schutzvorschriften enthalten insoweit § 58 Abs. 2 und § 60 Abs. 1.

Zu Abs. 2
Die Verwendung des Begriffs "unbedingt erforderlich" in Satz 2 statt bisher "unerlässlich" stellt auf die Terminologie in § 43 Abs. 1 HDSIG-E ab. Passend zu Satz 2 wird in Satz 3 ebenfalls auf den Begriff der "Offenbarung" abgestellt.

Zu Abs. 3
Die Vorschrift betrifft die Weitergabe von Informationen, die von externen Dienstleistern nicht unmittelbar zu Vollzugszwecken - sondern primär zum Zwecke der Behandlung - erhoben, aber zu Zwecken des Vollzuges weitergegeben werden. Insoweit ist der Anwendungsbereich der Verordnung (EU) Nr. 2016/679 eröffnet.

Redaktionell wird ferner in Satz 2 klargestellt, dass die vorgenannten Personen lediglich zu einer Offenbarung befugt sind.

Zu Abs. 5
Der Terminus "unerlässlich" wurde an den Begriff "unbedingt erforderlich" angepasst.

Zu Nr. 8 (§ 62)
Das entsprechende Verfahren ist nunmehr in § 58 HDSIG-E geregelt, sodass die Verweisung entsprechend anzupassen war.

Zu Nr. 9 (§§ 63 bis 65)

Zu § 63

Zu Abs. 1
Die Bestimmung ist neu eingeführt.

Die Sätze 1, 2 und 4 geben insoweit die Bestimmung von § 48 HDSIG-E wieder. Die Wiedergabe erfolgt, weil der Hinweis in Satz 3 sonst nicht ohne weiteres aus sich heraus verständlich wäre.

Der gesonderte Hinweis nach Satz 3 entspricht insoweit dem Regelungsgehalt von § 43 Abs. 2 Satz 2 Nr. 3 HDSIG-E für die Sicherung besonderer Kategorien personenbezogener Daten, ist jedoch aufgrund der besonderen datenschutzrechtlichen Sensibilität der weiteren aufgeführten Arten von Daten erforderlich.

Zu Abs. 2

Entsprechend der Einführung eines neuen Abs. 1 ist der bisherige Inhalt von § 63 HStVollzG als Abs. 2 zu bezeichnen. Die Verweisung auf die Vorschrift des bisherigen § 10 HDSG in Satz 1 war an § 59 HDSIG-E entsprechend anzupassen.

Zu § 64
Die Vorschrift wird komplett neu gefasst.

In die Überschrift wurde der Begriff der Information aufgenommen, da dies der Terminologie des HDSIG-E entspricht, vgl. dort § 50.

Entsprechend der Formulierungen des HDSIG-E wird auf dessen §§ 50 bis 52 verwiesen, soweit die Datenverarbeitung zu Zwecken der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung und des Strafvollzuges, einschließlich des Schutzes vor und der Abwehr von Gefahren für die öffentliche Sicherheit erfolgt; im Übrigen auf dessen §§ 31 bis 33. Die Zweiteilung der Informations- und Auskunftsrechte folgt aus der nicht-ausschließlichen Anwendbarkeit von Richtlinie (EU) Nr. 2016/680 und Verordnung (EU) Nr. 2016/679 im Bereich des Hessischen Justizvollzugs. Dabei erscheint es sinnvoll, den Gefangenen bei Aufnahme z.B. ein entsprechendes Formblatt als Information zu Datenverarbeitungen auszuhändigen - § 8 Abs. 1 sieht insoweit die Information über Rechte und Pflichten vor - und dgl. Besuchern bei Betreten der Anstalt.

Zur Gewährung eines effektiven Rechtsschutzes wird im neuen Satz 2 die Möglichkeit einer Akteneinsicht beibehalten werden und dahin gehend erweitert, dass sie insgesamt im Rahmen des Erforderlichen gewährt wird. Insbesondere bei Einsichtnahmen in Gesundheitsakten wird hierbei großzügig zu verfahren sein, vgl. BVerfG, Beschluss der 2. Kammer des Zweiten Senats vom 20. Dezember 2016 - 2 BvR 1541/15.

Zu § 65
Die Vorschrift wird weitestgehend neu gefasst.

Zur Überschrift
Der Begriff "Sperrung" wurde durch den Begriff "Einschränkung der Verarbeitung" ersetzt.

Nach der Systematik des HDSIG-E kann, vgl. dort § 53 Abs. 3, an Stelle einer Löschung von personenbezogenen Daten bei diesen eine Einschränkung der Verarbeitung vorgenommen werden. Nach § 41 Nr. 3 HDSIG-E ist hierunter "die Markierung gespeicherter personenbezogener Daten mit dem Ziel, ihre künftige Verarbeitung einzuschränken" zu verstehen.

Nach der bisherigen Systematik, vgl. § 65 Abs. 1 HStVollzG in seiner jetzigen Fassung, sind personenbezogene Daten auch jetzt schon unverzüglich zu löschen, sobald feststeht, dass ihre Speicherung nicht mehr erforderlich ist, um die Zwecke zu erfüllen, für die sie erhoben worden sind oder für die sie nach § 13 Abs. 2 und 4 HDSG weiterverarbeitet werden dürfen; wenn bei der Speicherung nicht absehbar ist, wie lange die Daten benötigt werden, ist nach einer aufgrund der Erfahrung zu bestimmenden Frist zu prüfen, ob die Erforderlichkeit der Speicherung noch besteht, vgl. § 19 Abs. 3 HDSG in seiner jetzigen Fassung.

Grundsätzlich sollte für die zukünftige Rechtslage - wie bisher auch - zwischen besonders sensiblen Daten, Daten in Gefangenenakten und -dateien und sonstigen Daten hinsichtlich der Frage ihrer Löschung oder - an deren Stelle - der Einschränkung ihrer Verarbeitung unterschieden werden.

Zu Abs. 1
Abs. 1 entspricht in seinem Regelungsgehalt dem bisherigen Abs. 1. Es wurde der Begriff "in der Verarbeitung einzuschränken" anstelle der bisherigen Sperrung verwendet und auf die einschlägigen Bestimmungen des HDSIG-E verwiesen, je nachdem, ob die Verarbeitung zu den Zwecken nach § 40 HDSIG-E erfolgt oder nicht.

Zu Abs. 2

Abs. 2 befasst sich entsprechend der bisherigen Systematik mit der Verfahrensweise bei personenbezogenen Daten, die aufgrund besonders intensiver Eingriffe erhoben wurden.

In Satz 1 wurden Ergebnisse von Maßnahmen nach § 59 den Videoaufnahmen gleichgestellt, da insoweit ein gleiches Maß an Schutzwürdigkeit gegeben ist. Ebenfalls wird klargestellt, dass eine Löschung nur dann nicht erfolgt, wenn zum Zeitpunkt der Entscheidung über die Löschung zu konkreten Beweiszwecken die weitere Aufbewahrung bei gleichzeitiger Einschränkung der Verarbeitung unbedingt erforderlich ist; insoweit ist eine Angleichung an die Terminologie der Bestimmungen des HDSIG-E vorgenommen worden, was die Verarbeitung von besonderen Kategorien personenbezogener Daten angeht.

Im neu eingeführten Satz 2 wird eine verkürzte Frist zur Löschung von Daten eingeführt, die entgegen dem Grundsatz verarbeitet, insbesondere erhoben wurden, dass der Kernbereich der Lebensgestaltung nicht zum Gegenstand der Verarbeitung personenbezogener Daten gemacht werden darf. Dies trägt der besonderen Schutzwürdigkeit der Betroffenen in diesem Fall Rechnung.

Der ebenfalls neu eingeführte Satz 3 statuiert insoweit eine Dokumentationspflicht zur kontrollierbaren Löschung der in Satz 1 und 2 aufgeführten, besonders sensiblen Daten, vgl. BVerfGE 274 S. 337ff. [S. 339]).

Zu Abs. 3
Die Vorschrift befasst sich mit der Löschung von personenbezogenen Daten und differenziert hierbei zwischen Akten und Dateien zum Gefangenen und sonstigen Akten und Dateien. Dabei ist eine Gleichbehandlung von Dateien im Sinne einer elektronischen Datei mit einer Papierakte geboten, da auch eine ordnungsgemäß geführte Gefangenenpersonalakte regelmäßig ein Dateisystem im datenschutzrechtlichen Sinne darstellen wird (vgl. zum Begriff Gola DS-GVO Art. 4 Rd.-Nr. 46). Die Vorschrift orientiert sich insoweit an der Struktur des Abs. 3 Satz 1 in der derzeit geltenden Fassung, wobei aber entsprechend der Systematik der Richtlinie (EU) Nr. 2016/680 statt einer grundsätzlichen Sperrung der Daten jetzt vorrangig deren Löschung zu erfolgen hat.

In Satz 1 wird zunächst redaktionell klargestellt, dass Abs. 3 sich - wie Abs. 1 und 2 - auf personenbezogene Daten bezieht. § 53 Abs. 2 des HDSIG-E sieht in Umsetzung von Art. 16 der Richtlinie (EU) Nr. 2016/680 die Löschung vor, wenn die Kenntnis der Daten für die Aufgabenerfüllung nicht mehr erforderlich ist. Das ist grundsätzlich dann der Fall, wenn ein Gefangener endgültig entlassen wird. Dies ist jedoch nicht der Fall, sofern die begonnene Freiheitsentziehung wiederaufgenommen werden kann - insbesondere bei Aussetzung des Strafrestes zur Bewährung. Entsprechend ist der Anstalt eine Frist für die Löschung der personenbezogenen Daten jedenfalls bis zum Ende einer möglichen Bewährungsfrist einzuräumen. Wird ein Strafgefangener auf Bewährung entlassen, dauert die Bewährungszeit bis zu fünf Jahre, § 56a Abs. 1 Satz 2 StGB. Wird die Strafaussetzung widerrufen, müssen die Daten aus der vorhergehenden Inhaftierung dem Justizvollzug zur Verfügung stehen, da das Vollstreckungsverhältnis gerade nicht beendet wurde. Außerdem sollen die gespeicherten Daten gemäß BVerfGE 116, 69-95, Rn. 64, der Evaluation des Justizvollzuges dienen. Besteht zum Zeitpunkt des Fristablaufs ein konkreter Anhaltspunkt dafür, dass eine Aufbewahrung von Daten zur Abwicklung des Vollstreckungsverhältnisses weiter erforderlich ist, kann dem durch die weitere Speicherung bei Einschränkung der Verarbeitung nach Abs. 4 Rechnung getragen werden.

Satz 2 ersetzt den bisherigen Abs. 4 der Bestimmung in seiner derzeit geltenden Fassung.

Zu Abs. 4
Der besseren Nachvollziehbarkeit halber sollen die Bestimmungen zur Einschränkung der Verarbeitung personenbezogener Daten in einem eigenen Absatz dargestellt werden. Aus demselben Grund wird in Satz 1 auf die Normen verwiesen, aus denen sich grundsätzlich ergibt, wann und wie die Einschränkung der Verarbeitung zu erfolgen hat.

Anstelle einer Löschung der Daten können diese unter den Voraussetzungen des § 53 Abs. 3 bis 7 HDSIG-E in der Verarbeitung eingeschränkt werden, Satz 1 Nr. 1. Wie in § 53 Abs. 3 HDSIG-E erscheint eine weitergehende Speicherung bei Einschränkung der Verarbeitung zu Beweiszwecken insgesamt sinnvoll. Art. 16 Abs. 3 Satz 1 Buchst. b der Richtlinie (EU) Nr. 2016/680 lässt dies grundsätzlich zu und beschränkt Beweiszwecke nicht ausdrücklich auf den Anwendungsbereich der Richtlinie. Dies deckt auch die Beweiszwecke z.B. auch jenen Konstellationen ab, in denen ein ehemaliger Gefangener Haftungsansprüche gegen das Land geltend macht, z.B. wegen fehlerhafter ärztlicher Behandlung in der Haft. Einen ähnlichen Weg geht insoweit auch § 78 Abs. 2 bzw. 3 des Bundeskriminalamtgesetzes in seiner Neufassung durch das Gesetz zur Neustrukturierung des Bundeskriminalamtgesetzes; dort wird ebenfalls nur von der Aufbewahrung für "gerichtliche Verfahren" bzw. der Behebung "einer Beweisnot" gesprochen, ohne nach der Art des Verfahrens zu differenzieren, in dem die Daten benötigt werden. Sofern eine Einschränkung der Verarbeitung zu Beweiszwecken erfolgt, ist aber darauf zu achten, dass die Entscheidung hierüber grundsätzlich eine Einzelfallentscheidung darstellt und zum Zeitpunkt ihrer Entscheidung konkrete Anhaltspunkte für die Notwendigkeit einer späteren Verwendung vorliegen müssen. Eine abstrakte Vorratsdatenspeicherung ohne konkreten Anlass - der sinnvollerweise zu dokumentieren ist - dürfte unzulässig sein. Anders ist dies bei normierten Dokumentationspflichten zu beurteilen, wie insbesondere z.B. nach § 10 der Berufsordnung für die Ärztinnen und Ärzte in Hessen für die im Rahmen der Freiheitsentziehung erfolgten ärztlichen Maßnahmen; ein hierauf bezogenes Regelbeispiel wurde zur Erleichterung der Rechtspraxis in Nr. 1 aufgeführt.

Satz 1 Nr. 2 stellt insoweit einen Auffangtatbestand dar, soweit Daten nicht im Geltungsbereich der Richtlinie (EU) Nr. 2016/680 gespeichert wurden.

Die Kennzeichnung von in der Verarbeitung eingeschränkten personenbezogenen Daten trägt insbesondere § 53 Abs. 4 HDSIG-E Rechnung. Die in Satz 2 ebenfalls geregelte Heranziehung in der Verarbeitung eingeschränkter personenbezogener Daten, im Regelfall durch Übermittlung, zu anderen Zwecken als des § 40 HDSIG-E, muss den Anforderungen der Verordnung (EU) Nr. 2016/679 genügen (vgl. Art. 9 Abs. 1 und 2 der Richtlinie (EU) Nr. 2016/680; insoweit gestattet Art. 18 Abs. 1 Buchst. a bzw. c der Verordnung (EU) Nr. 2016/679 aber auch die Verwertung zu Beweiszwecken). Wie sich aus Art. 9 der Richtlinie (EU) Nr. 2016/680 ergibt, muss die Verarbeitung zu Vollzugszwecken erhobener Daten auch nicht auf den sachlichen Bereich der Richtlinie beschränkt sein.

Satz 3 entspricht dem bisherigen Regelungsgehalt von § 65 Abs. 3 S. 4 HStVollzG in seiner jetzigen Fassung. Auch insoweit bleibt eine Einwilligung weiter zulässig: entweder dient die Aufhebung der Einschränkung der Verarbeitung zu Zwecken der Richtlinie (EU) Nr. 2016/680, sodass § 46 HDSIG-E Anwendung findet; oder die Verarbeitung dient anderen Zwecken, sodass über Art. 9 Art. 1 der Richtlinie (EU) Nr. 2016/680 die Bestimmungen der Verordnung (EU) Nr. 2016/679 gelten.

Satz 4 entspricht dem bisherigen Regelungsgehalt von § 65 Abs. 3 S. 2 HStVollzG in seiner jetzigen Fassung.

Zu Abs. 5
Entsprechend § 70 Abs. 4 HDSIG-E wird eine jährliche Kontrollfrist eingeführt, differenzierend zwischen Gefangenendateien und -akten einerseits sowie sonstigen Dateien und Akten andererseits.

Zu Abs. 6
Der Absatz entspricht im Wesentlichen dem bisherigen Abs. 5 in der derzeit geltenden Fassung. Redaktionell wurde die Herkunft der Daten danach präzisiert, aus welchen Akten etc. sie stammen. Hinsichtlich der Gefangenenbücher ist darauf hinzuweisen, dass es sich hierbei um Bestandsverzeichnisse in Buchform handelt, die mittlerweile elektronisch geführt werden. Die Aufbewahrungsfristen beziehen sich daher im Wesentlichen auf Altfälle, die sich bereits in der Aufbewahrung befinden.

In Satz 4 wurde die Verweisung auf das Hessische Archivgesetz in eine dynamische Verweisung umgewandelt, um zukünftige Änderungen abzubilden.

Zu Nr. 10 (§ 69)

Buchst. a
In Satz 2 wurde ergänzend eingefügt, dass die Ergebnisse dem öffentlichen Interesse dienen, um den Maßgaben von § 45 HDSIG-E zu entsprechen.

Buchst. b
Der Verweis auf § 476 StPO ist dahin gehend zu aktualisieren, dass er den Anforderungen an eine Verarbeitung besonderer Kategorien personenbezogener Daten gemäß § 43 Abs. 1 HDSIG-E Rechnung trägt (Nr. 2), sodass eine Übermittlung nur bei unbedingter Erforderlichkeit möglich ist.

Zu Art. 4 (Änderung des Hessischen Untersuchungshaftvollzugsgesetzes)

Allgemeines
Auf den Vollzug der Untersuchungshaft findet ebenfalls grundsätzlich die Richtlinie (EU) Nr. 2016/680 des Europäischen Parlamentes und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zweck der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung sowie zum freien Datenverkehr und zur Aufhebung des Rahmenbeschlusses 2008/977/JI des Rates Anwendung. Insoweit wird auf die Vorbemerkung zur Begründung zur Änderung des Hessischen Jugendstrafvollzugsgesetzes Bezug genommen.

Im Einzelnen

Zu Nr. 1 (Inhaltsübersicht)
Soweit bei einzelnen Paragrafen die Überschriften geändert werden, ist die Inhaltsübersicht entsprechend anzupassen.

Zu Nr. 2 (§ 17)
Eine Benachrichtigung der nächsten Angehörigen ist im Falle der schweren Erkrankung von der Einwilligung der Untersuchungsgefangenen abhängig zu machen; ein entsprechender Vorbehalt wurde zu Satz 1 als 2. Halbsatz angefügt. Dies entspricht den Maßgaben von Art. 9 Abs. 1 Satz 2 der Richtlinie (EU) Nr. 2106/680 i.V.m. Art. 9 Abs. 1 und 2 Buchst. a der Verordnung (EU) Nr. 2016/679, da insoweit die Verarbeitung (durch Übermittlung) von besonderen Kategorien personenbezogener Daten (in Form von Gesundheitsdaten, vgl. § 41 Nr. 14 HDSIG-E) zu Zwecken erfolgt, die nicht ohne Weiteres der Durchführung des Strafvollzuges dient, sondern zunächst einmal der allgemeinen Information der Angehörigen. Auf eine mutmaßliche Einwilligung i.S.v. Art. 9 Abs. 2 Buchst. c kann insoweit nicht abgestellt werden, da die Übermittlung des Gesundheitszustandes an Angehörige auch bei Lebensgefahr kein lebenswichtiges Interesse der betroffenen Personen darstellt; dies dürfte nur für die Durchführung lebenserhaltender Maßnahmen zutreffen. Um auch in Situationen handeln zu können, in denen eine Einwilligung nicht mehr eingeholt werden kann, sollte die Einwilligung - die insoweit den Anforderungen der Verordnung (EU) Nr. 2016/679 genügen muss - bereits bei Aufnahme eingeholt werden; zu diesem Zweck wurde als neuer Satz 3 eine Belehrungspflicht aufgenommen. Handelt es sich bei den Betroffenen um Minderjährige, so sind die besonderen Grundsätze für die Einwilligung Minderjähriger zu beachten.

Im Falle des Todes ist weiterhin eine Benachrichtigung auch ohne Einwilligung angezeigt und nach §§ 22 Abs. 3 i.V.m. Abs. 2 Nr. 3 und Art. 9 Abs. 2 Buchst. f der Verordnung (EU) Nr. 2016/679 möglich.

Zu Nr. 3 (§ 26)

Zu Buchst. a
Als neuer zweiter Halbsatz wurde eine Regelung zu Satz 1 hinzugefügt, wonach sich die Überwachung sowohl auf Untersuchungsgefangene wie Besucher bezieht; dies dient der Klarstellung im Sinne von § 67 HDSIG-E, da die Überwachung sich sowohl auf die Untersuchungsgefangenen als Personen bezieht, gegen die ein begründeter Verdacht besteht, dass sie eine Straftat begangen haben (dort Nr. 1) wie auch auf den Besuch (dort nur Nr. 5) beziehen kann.

In Satz 2 wird klargestellt, dass die Überwachung der Unterhaltung, sofern sie besondere Kategorien personenbezogener Daten zum Gegenstand hat, nur noch im Falle unbedingter Erforderlichkeit erfolgt, um insbesondere den Anforderungen aus § 43 Abs. 1 HDSIG-E bzw. Art. 10 der Richtlinie (EU) Nr. 2016/680 Rechnung zu tragen. Eine Verarbeitung besonderer Kategorien personenbezogener Daten - legaldefiniert in § 41 Nr. 15 HDSIG-E, insoweit gleichlaufend Art. 9 der Verordnung (EU) Nr. 2016/679 - ist nur bei unbedingter Erforderlichkeit zulässig.

Der Begriff der "unbedingten Erforderlichkeit" ist weder in der Verordnung (EU) Nr. 2016/679 noch der Richtlinie (EU) Nr. 2016/680 legaldefiniert. Da er nach dem Wortlaut ein gesteigertes Maß der Erforderlichkeit vorsieht, kann er wie der bisher im Rahmen des Vollzugsrechts verwendete Begriff "unerlässlich" im Sinne eines gesteigerten Maßes der Erforderlichkeit verstanden werden. Eine Maßnahme ist dann unerlässlich, wenn tatsächlich keinerlei weniger eingriffsintensive und mit vertretbarem Aufwand durchführbare Maßnahmen zur Zweckerreichung zur Verfügung stehen; darüber hinaus darf die Art der datenschutzrelevanten Maßnahme schutzwürdige Interessen der Betroffenen nicht beeinträchtigen (vgl. Arloth/Krä StVollzG 4. Auflage § 59 HStVollzG Rd.-Nr. 2, Laubenthal/Nestler/Neubacher/Verrel O Rd.-Nr. 35ff). In die Abwägung

einzustellen sind somit sämtliche mit hinreichender Wahrscheinlichkeit mit der Datenverarbeitung für die Betroffenen im persönlichen Nahbereich einhergehenden Konsequenzen, einschließlich der Auswirkungen auf die Beziehungen zu Verwandten, zum sozialen Wohnumfeld sowie zum Arbeitgeber (vgl. Laubenthal/Nestler/Neubacher/Verrel aaO.). Wie in der Begründung zu § 43 HDSIG-E ausgeführt ist eine unbedingte Erforderlichkeit anzunehmen, wenn keine zumutbare Alternativ- oder Ausgleichsmaßnahme zur Verfügung steht, um ein legitimes Ziel zu erreichen.

Inwieweit der Begriff der "unbedingten Erforderlichkeit" in der Rechtspraxis zu anderen Ergebnissen führen wird als eine konsequente Anwendung des Erforderlichkeitsprinzips im Rahmen der Verhältnismäßigkeitsprüfung bleibt abzuwarten. So wird in anderen Regelungsbereichen z.B. zur Durchführung einer sachgerechten medizinischen Betreuung bereits bei jeder Anamnese die umfassende Erhebung von Gesundheitsdaten regelmäßig unbedingt erforderlich sein, ebenso wie es für jeden Vollzugsbediensteten regelmäßig unbedingt erforderlich sein dürfte, auf die Gesichtsbilder der Untersuchungsgefangenen in deren Personalakte zugreifen zu können, um deren Person in praxisgerechter Weise identifizieren zu können.

Die Überwachung von Besuchen ist elementar für die Sicherheit oder Ordnung der Anstalt. Die permanente Überwachung der Unterhaltung wird daher im Regelfall unbedingt erforderlich sein, auch wenn sie besondere Kategorien personenbezogener Daten zum Inhalt hat. In vielen Fällen ist es allerdings praktisch unvermeidbar, dass die Vollzugsbediensteten Informationen zur Kenntnis nehmen, bevor sie deren besonderen datenschutzrechtlichen Bezug erkennen. In derartigen Fällen ist es in Anlehnung an die Entscheidung BVerfGE 129, S. 208ff. (Rn. 209ff) verfassungsrechtlich nicht gefordert, den Zugriff wegen des Risikos einer Kernbereichsverletzung auf der Erhebungsebene von vornherein zu unterlassen. In Fällen dieser Art ist es geboten, aber auch ausreichend, für hinreichenden Schutz in der Auswertungsphase zu sorgen, insbesondere durch Gewährung eines entsprechenden Schutzes durch Löschung von Aufzeichnungen.

Buchst. b
In Satz 1 wird ein neuer zweiter Halbsatz eingeführt, wonach die Überwachung auch durch optisch-elektronische Einrichtungen erfolgen kann, die als Videoüberwachung legaldefiniert wird, da dieser Begriff im Gesetz mehrfach verwendet wird.

Satz 2 wird dahin gehend neu gefasst, dass die Aufzeichnung und Speicherung von Daten gemäß Satz 1 nur im Falle unbedingter Erforderlichkeit erfolgt. Dies ist dem Umstand geschuldet, dass für den Geltungsbereich der Richtlinie (EU) Nr. 2016/680 je nach Qualität des Überwachungssystems Gesichtsbilder unter die besondere Kategorie personenbezogener Daten fallen können, insbesondere bei Verwendung spezieller Gesichtserkennungssoftware. Darüber hinaus ist eine Videoüberwachung von Besuchen besonders geneigt, durch Aufzeichnung des Verhaltens der überwachten Personen Informationen zu besonderen Kategorien personenbezogener Daten im Sinne von Art. 10 der Richtlinie (EU) Nr. 2016/680 zu generieren. Die Erfüllung des Tatbestandsmerkmals der unbedingten Erforderlichkeit trägt im Interesse einer möglichst sicheren Umsetzung der Richtlinie entsprechend deren Art. 10 bzw. § 43 Abs. 1 HDSIG-E Rechnung, um eine Videoüberwachung in jedem Fall datenschutzrechtlich abzusichern.

Zu Nr. 4 (§ 27)
Der Anwendungsbereich der Richtlinie (EU) Nr. 2016/680 ist auch im Bereich des Schriftwechsels nicht in jedem Fall ausgeschlossen. Es ist insbesondere nach Abs. 3 auch möglich, angehaltenen Schriftwechsel zu verwahren, regelmäßig in einer körperlichen Akte, aber auch nach Scannen in einer elektronischen Akte, mithin analogen oder digitalen Dateisystemen. Der zu überwachende Schriftwechsel wird häufig mit einer gewissen Wahrscheinlichkeit besondere Kategorien personenbezogener Daten enthalten, ohne dass dies vor Beginn der Überwachung klar ist. Insoweit besteht eine geringere Flexibilität als bei der Überwachung eines Besuchs, bei dem sich die besondere datenschutzrechtliche Relevanz bei den besonderen Kategorien aus dem überwachten Verlauf des Besuchs selbst ergeben kann. Um das Schutzniveau für die besonderen Kategorien personenbezogener Daten von Anfang an zu gewährleisten, ist nach § 43 Abs. 1 HDSIG-E daher prophylaktisch sicherzustellen, dass die Überwachung des Schriftwechsels nur im Falle unbedingter Erforderlichkeit erfolgt, was durch einen entsprechenden Einschub in Satz 1 erfolgt. Da die Überwachung des Schriftwechsels für Sicherheit oder Ordnung unverzichtbar sind, wird das Kriterium der unbedingten Erforderlichkeit regelmäßig erfüllt sein.

Darüber hinaus sollten Untersuchungsgefangene frühzeitig (d.h. bei Aufnahme) auf die Möglichkeit der Überwachung hingewiesen werden, um den Eingriff in das Postgeheimnis nicht zu einer verdeckten Maßnahme zu machen, an die - insbesondere angesichts des Urteils des Bundesverfassungsgerichts vom 20. April 2016, Aktenzeichen 1 BvR 966/09 und 1BvR 1140/09 - bei der Datenverarbeitung erheblich höhere Anforderungen zu stellen wären; eine entsprechende Hinweispflicht wurde als neuer Halbsatz an Satz 1 angefügt.

Zu Nr. 5 (§ 30)
In Satz 2 wird - auch im Sinne einer einheitlichen Terminologie klargestellt, dass die technischen Hilfsmittel auch optisch-elektronische Einrichtungen (Videoüberwachung) umfassen. Da

diese - unabhängig von der Einstufung eines Gesichtsbildes als biometrisches Datum - besonders geeignet sind, insgesamt besondere Kategorien personenbezogener Daten zu liefern, sei es in Form von Gesundheitsdaten oder anderen Unterfällen, ist nach § 43 Abs. 1 HDSIG-E in Satz 2 nunmehr vorgesehen, dass die entsprechende Verarbeitung nur im Falle unbedingter Erforderlichkeit zulässig ist. Auch hier wird wegen der Unverzichtbarkeit einer entsprechenden Überwachung für Sicherheit oder Ordnung der Anstalt das Kriterium der unbedingten Erforderlichkeit regelmäßig erfüllt sein.

Zu Nr. 6 (§ 35)

Zu Buchst. a
Es wird - auch im Sinne einer einheitlichen Terminologie - in Nr. 2 klargestellt, dass die technischen Hilfsmittel auch optisch-elektronische Einrichtungen (Videoüberwachung) umfassen. Da diese regelmäßig besondere Kategorien personenbezogener Daten liefern können, insbesondere Gesundheitsdaten zur Kontrolle des Gesundheitszustandes, ist nach § 43 Abs. 1 HDSIG-E vorgesehen, dass die entsprechende Verarbeitung nur im Falle unbedingter Erforderlichkeit zulässig erfolgt. Da die entsprechende Kontrolle für die Information des Gesundheitszustandes des Gefangenen unverzichtbar ist, wird das Kriterium der unbedingten Erforderlichkeit regelmäßig erfüllt sein.

Zu Buchst. b
Da die dauerhafte Überwachung nach Abs. 2 Nr. 2 regelmäßig Gesundheitsdaten liefern kann und somit besondere Kategorien personenbezogener Daten, ist in Satz 2 klargestellt, dass dies im Sinne von § 43 Abs. 1 HDSIG-E nur im Falle unbedingter Erforderlichkeit zulässig ist. Auch hier gilt, dass, da die entsprechende Kontrolle für die Information des Gesundheitszustandes des Gefangenen unverzichtbar ist, das Kriterium der unbedingten Erforderlichkeit regelmäßig erfüllt sein wird.

Zu Nr. 7 (§ 46)
Die bezeichnete Passage in Abs. 5 kann gestrichen werden, da die Regelung inhaltlich nicht mehr von § 55 Abs. 1 abweicht.

Zu Nr. 8 (§§ 54 bis 57)

Zu § 54

Zu Abs. 1
In Satz 1 wird in Anlehnung an § 41 Nr. 2 HDSIG-E statt an die Alternativen Datenerhebung bzw. -weiterverarbeitung an den einheitlichen Begriff der Verarbeitung angeknüpft; ebenfalls wurde vor dem Wort "verarbeiten" ein "nur" eingefügt, um das Prinzip des Verbots mit Erlaubnisvorbehalt hervorzuheben. Ferner erfolgt in Satz 1 die systematische Klarstellung, dass zunächst eine gesetzliche Spezialregelung Anwendung findet und nur in letzter Linie die Generalklausel, die insoweit grundsätzlich auf die Erforderlichkeit für den Vollzug abstellt. Bei der Verarbeitung besonderer Kategorien personenbezogener Daten - legaldefiniert § 41 Nr. 15 HDSIG-E - muss allerdings insoweit die unbedingte Erforderlichkeit gegeben sein. Gestrichen wurde die Einwilligung als allgemeiner Rechtsgrund für eine Datenverarbeitung. Dies trägt dem Umstand Rechnung, dass die Richtlinie (EU) Nr. 2016/680 eine Einwilligung im Rahmen ihres Geltungsbereichs grundsätzlich nicht mehr als alleinige Grundlage hierfür ausreichen lässt, wie sich aus Ziffer 35 der Erwägungen zur Richtlinie ergibt. Wie weit dieser Grundsatz reicht, ist derzeit noch nicht abschließend geklärt. Der letzte Satz der vorgenannten Erwägungen führt hierzu aus: "Dies sollte die Mitgliedstaaten nicht daran hindern, durch Rechtsvorschriften vorzusehen, dass die betroffene Person der Verarbeitung ihrer personenbezogenen Daten für die Zwecke dieser Richtlinie zustimmen kann, beispielsweise im Falle von DNA-Tests in strafrechtlichen Ermittlungen oder zur Überwachung ihres Aufenthaltsortes mittels elektronischer Fußfessel zur Strafvollstreckung." In den Artikeln der Richtlinie (EU) Nr. 2016/680 findet sich die Einwilligung dann jedoch - anders als in der Verordnung (EU) Nr. 2016/679 - als Rechtsgrund einer Datenverarbeitung nicht mehr. Daher wird die entsprechende Erwägung dahin gehend auszulegen sein, dass die Einwilligung in der Einzelvorschrift ausdrücklich aufgeführt sein muss; konsequenterweise sieht § 46 HDSIG-E die Möglichkeit einer Einwilligung in solchen Fällen vor. Tatbestände, bei denen ein solcher Einwilligungsvorbehalt gegeben ist, werden nunmehr durch den Tatbestand der "Rechtsvorschrift" mit abgedeckt.

Die Verweisung auf die Bestimmungen des subsidiär geltenden Hessischen Datenschutz- und Informationsfreiheitsgesetzes in Satz 2 wird faktisch als dynamische Verweisung ausgestaltet, um zukünftige Änderungen abzubilden. Zu Satz 2 wurde ein weiterer Halbsatz angehängt, durch den klargestellt wird, dass die Datenverarbeitung durch die Justizvollzugsbehörden zu Vollzugszwecken grundsätzlich - aber nicht ausschließlich, da insoweit auch die allgemeinen Bestimmungen, insbesondere Teil 1 gelten - unter dem Regime des Teils 3 des HDSIG-E erfolgt, um der Praxis angesichts der - in Art. 9 der Richtlinie (EU) Nr. 2016/680 selbst vorgesehenen Zweiteilung der datenschutzrechtlichen Regelungssysteme - eine grundsätzliche Entscheidungs-

hilfe an die Hand zu geben. Dies hat daher nicht allein deklaratorische Wirkung; die Entscheidung kann im Einzelfall schwierig sein, s. hierzu die Vorabbemerkungen unter Verweis auf die entsprechenden Ausführungen zum HStVollzG.

Neu hinzugefügt wurde Satz 3, der den Verhältnismäßigkeitsgrundsatz konkretisiert und in Hinblick auf Art. 1 Abs. 1 GG ein Verarbeitungsverbot ausspricht, da der Gesetzgeber den Kernbereich privater Lebensgestaltung zu schützen hat (vgl. BVerfGE 129, S. 208ff. [S. 245]). Ob ein Sachverhalt dem unantastbaren Kernbereich zuzuordnen ist, hängt davon ab, ob er nach seinem Inhalt höchstpersönlichen Charakters ist, also auch in welcher Art und Intensität er aus sich heraus die Sphäre anderer oder Belange der Gemeinschaft berührt (vgl. BVerfGE 80, 367 [374] = NJW 1990, 563).

Zu Abs. 2
Die Präzisierung, dass die Verarbeitung für Ziel und Aufgaben des Vollzugs nach § 2 erfolgt, dient der Klarstellung, dass die Verantwortlichen im Sinne des Datenschutzes im vorliegenden Fall Daten grundsätzlich zu Zwecken des Vollzuges von Untersuchungshaft verarbeiten. Klarstellend wird ferner eingefügt, dass die Verarbeitung der aufgezählten personenbezogenen Daten auch zur Aufrechterhaltung der medizinischen Versorgung und Gesundheitsfürsorge verarbeitet werden können, was Art. 8 Abs. 2 der Richtlinie (EU) Nr. 2016/680 Rechnung trägt.

Ferner wird auf den einheitlichen Tatbestand einer Verarbeitung abgestellt.

Da die bisherigen Nummern 1 bis 4 bereits zumeist besondere Kategorien personenbezogener Daten i.S.v. § 41 Nr. 15 HDSIG-E darstellen, wurde durch die Ergänzung um Nr. 5 insoweit eine Gesamtregelung für die Verarbeitung entsprechender Informationen geschaffen. Dabei wurden die Gesundheitsdaten in Hinblick auf ihre besondere Bedeutung, aber auch ihre bisher schon separate Speicherung herausgehoben.

Die Verarbeitung besonderer Kategorien personenbezogener Daten wurde nach § 43 Abs. 1 HDSIG-E an das Erfordernis unbedingter Erforderlichkeit geknüpft.

Die beibehaltene Beschränkung auf Untersuchungsgefangene als Personen, gegen die der begründete Verdacht besteht, dass sie eine Straftat begangen haben, trägt darüber hinaus § 67 HDSIG-E Rechnung, der wiederum aus Art. 6 der Richtlinie (EU) Nr. 2016/680 folgt.

Zu Abs. 3
Es erfolgt in Satz 1 eine Anpassung der separat zu führenden personenbezogenen Daten an die Neunummerierung in Abs. 2.

In Satz 2 wird statt auf "Daten, die den Gesundheitszustand betreffen" auf "Gesundheitsdaten" abgestellt, da letzter Begriff in § 41 Nr. 14 HDSIG-E legaldefiniert ist. Der Begriff "Personalakte" in Satz 2 wurde durch den der "Gefangenenpersonalakte" präzisiert.

Zu Abs. 4
Satz 2 wurde neu eingeführt, um klarzustellen, dass bei der Verarbeitung besonderer Kategorien personenbezogener Daten dies nur bei unbedingter Erforderlichkeit zulässig ist, s. § 43 Abs. 1 HDSIG-E.

Zu Abs. 5
Neu eingefügt wurde Satz 2, sofern hierbei die Verarbeitung biometrischer Daten notwendig werden sollte. Dies würde die Verarbeitung von besonderen Kategorien personenbezogener Daten darstellen, die wiederum gemäß § 43 Abs. 1 HDSIG-E nur bei unbedingter Erforderlichkeit zulässig ist.

Zu Abs. 6
Die Neufassung der Vorschrift orientiert sich an § 4 HDSIG-E. Da die Außensicherung sowohl öffentliche wie nicht öffentliche Plätze abdecken kann, konnte insoweit nicht lediglich auf die vorgenannte Vorschrift verwiesen werden.

Soweit in Satz 1 zusätzlich darauf abgestellt wird, dass schutzwürdige Interessen der Betroffenen nicht überwiegen dürfen, erfolgt dies in Orientierung an § 4 Abs. 1 HDSIG-E.

Satz 2 wurde dahin gehend ergänzt, dass neben der Überwachung auch der Name und die Kontaktdaten des Verantwortlichen zum frühestmöglichen Zeitpunkt erkennbar zu machen sind. Verantwortlicher wird dabei regelmäßig keine natürliche, mit Namen zu benennende Person sein, sondern die Anstalt als zuständige Behörde, vgl. § 41 Nr. 8 HDSIG-E.

Ergänzend wird klargestellt, dass eine Speicherung nur zulässig ist, wenn keine Anhaltspunkte dafür bestehen, dass schutzwürdige Interessen der Betroffenen überwiegen; dies trägt § 4 Abs. 3 Satz 1 HDSIG-E Rechnung.

Zu § 54a

Zu Abs. 1
In Satz 2 wurde klargestellt, dass die Zuverlässigkeitsüberprüfung zur Aufrechterhaltung der Sicherheit oder Ordnung der Anstalt hierfür erfolgt.
Die Verweisung auf das HSÜG in Satz 5 wurde durch eine dynamische Verweisung ersetzt, um zukünftige Änderungen abzubilden.

Zu Abs. 2
In Satz 1 wurde klargestellt, dass die Zuverlässigkeitsüberprüfung zur Aufrechterhaltung der Sicherheit oder Ordnung der Anstalt hierfür erfolgt.
In Satz 2 wurde präzisiert, dass - in Hinblick auf § 67 HDSIG-E - die Zulassung zum Besuch von Untersuchungsgefangenen überhaupt erfolgt und nicht nur für welche Gefangene.

Zu Abs. 4
Hinsichtlich der Benachrichtigungspflicht wurde ausdrücklich auf § 51 HDSIG-E Bezug genommen.

Zu Abs. 6
In Satz 1 wurde in Hinblick auf den in Art. 8 der Richtlinie (EU) Nr. 2016/680 normierten Erforderlichkeitsgrundsatz ergänzend eingeführt, dass die Wiederholung der Zulässigkeitsprüfung zu erfolgen hat, sofern ihre Erforderlichkeit fortbesteht.

Zu § 55
Der bisherige § 55 HUVollzG war mit seinem bisherigen Regelungsgehalt aufzuheben. Die Vorschrift ging von dem Grundsatz aus, dass personenbezogene Daten grundsätzlich bei den Betroffenen zu erheben sind. Ein solcher Grundsatz wird weder in der Richtlinie (EU) Nr. 2016/680 noch der Verordnung (EU) Nr. 2016/679 statuiert. Da nicht ausgeschlossen werden kann, dass auch eine Vollzugseinrichtung im Bereich der Verordnung (EU) Nr. 2016/679 tätig wird, könnte die Beibehaltung eines entsprechenden Grundsatzes insoweit als Verstoß gegen europäisches Recht gelten. Darüber hinaus ist davon auszugehen, dass die Datenerhebung auch in Zukunft hauptsächlich bei den Betroffenen erfolgen werden wird. Sollte dies nicht der Fall sein, sind diese im Übrigen auch nicht rechtlos, wie sich aus § 60 ergibt.

Stattdessen wird eine neue Vorschrift an dieser Stelle eingefügt, die eine spezielle Befugnis zum Auslesen unzulässig in die Justizvollzugsanstalten eingebrachter Datenträger darstellt. Eine spezielle Ermächtigung hierfür ist sinnvoll und erforderlich, da die unkontrollierte Kommunikation über Speichermedien eine erhebliche Gefährdung der Sicherheit oder Ordnung der Anstalten darstellt. Die Neuregelung erfolgt im Rahmen der datenschutzrechtlichen Bestimmungen, da damit gerechnet werden kann, dass die entsprechenden Speichermedien aufgrund ihrer Bestimmung zur Kommunikation zahlreiche personenbezogene Daten, auch solche besonderer Kategorien, enthalten.

In diesem Zusammenhang ist aus Gründen des Verhältnismäßigkeitsgrundsatzes zu differenzieren, dass nicht jeder Datenspeicher auszulesen ist, sondern nur dann, wenn konkrete Anhaltspunkte für eine Gefährdung hierdurch sprechen. Solche konkreten Anhaltspunkte werden dann regelmäßig vorliegen, wenn Hinweise für ein heimliches Verbringen des Datenspeichers in die Anstalt sprechen, z.B. beim Auffinden in einem Haftraum. Anders dürfte die Lage z.B. zu beurteilen sein, wenn Kommunikationssysteme als notwendiger Bestandteil z.B. von Baugeräten im Rahmen von Baumaßnahmen in eine Anstalt verbracht werden, ohne dass das Baugerät hierauf gezielt kontrolliert wurde.

Die Regelung orientiert sich im Wesentlichen an § 23 des rheinland-pfälzischen Landesjustizvollzugsdatenschutzgesetzes, zuletzt geändert durch § 44 des Gesetzes vom 6. Oktober 2015 (GVBl. S. 354). Diese Vorschrift lautet in ihrer derzeitigen Fassung wie folgt:

"§ 23
Auslesen von Datenspeichern

(1) Elektronische Datenspeicher sowie elektronische Geräte mit Datenspeicher, die ohne Erlaubnis in die Anstalt eingebracht wurden, dürfen auf schriftliche Anordnung der Anstaltsleiterin oder des Anstaltsleiters ausgelesen werden, soweit konkrete Anhaltspunkte die Annahme rechtfertigen, dass dies für die Erfüllung der Aufgaben des Vollzugs erforderlich ist. Die Gründe sind in der Anordnung festzuhalten. Sind die Betroffenen bekannt, sind ihnen die Gründe vor dem Auslesen mitzuteilen. Beim Auslesen sind ihre schutzwürdigen Interessen zu berücksichtigen, insbesondere der Kernbereich privater Lebensgestaltung. Das Auslesen ist möglichst auf die Inhalte zu beschränken, die zur Erreichung der die Anordnung begründenden Zwecke erforderlich sind.

(2) Die nach Absatz 1 erhobenen Daten dürfen verarbeitet werden, soweit dies aus den in der Anordnung genannten Gründen erforderlich ist. Aus anderen Gründen ist die Verarbeitung der Daten nur zulässig, soweit dies für die Erfüllung der Aufgaben des Voll-

zugs zwingend erforderlich ist und schutzwürdige Interessen der Betroffenen dem nicht entgegenstehen.

(3) Die Verarbeitung der nach Absatz 1 erhobenen Daten ist unzulässig, soweit sie dem Kernbereich der privaten Lebensgestaltung Gefangener oder Dritter unterfallen. Diese Daten sind unverzüglich zu löschen. Die Tatsachen der Erfassung und der Löschung der Daten sind zu dokumentieren. Die Dokumentation darf ausschließlich für Zwecke der Datenschutzkontrolle verwendet werden. Sie ist zu löschen, wenn sie für diese Zwecke nicht mehr erforderlich ist, spätestens jedoch am Ende des Kalenderjahres, das dem Jahr der Dokumentation folgt.

(4) Die Gefangenen sind bei der Aufnahme über die Möglichkeit des Auslesens von nicht gestatteten Datenspeichern zu belehren."

Ein besonderer Hinweis auf die Berücksichtigung schutzwürdiger Interessen und eine Beschränkung auf die Inhalte, die zur Erreichung der die Anordnung begründenden Zwecke erforderlich sind, ist indes nicht erforderlich, da dies durch die allgemeine Bestimmung in § 54 Abs. 1 bzw. die Beschränkung innerhalb der Vorschrift "soweit" bereits abgedeckt wird. In Hinblick auf die Möglichkeit, dass die auszulesenden Datenträger auch besondere Kategorien personenbezogener Daten enthalten können, sollte von der Maßnahme nur bei unbedingter Erforderlichkeit Gebrauch gemacht werden. Ebenfalls nicht notwendig ist eine Beschränkung der Verarbeitung auf die Zwecke ihrer Erhebung, da dies ebenfalls durch § 54 Abs. 1 und 2 abgedeckt ist. Einer besonderen Löschungsbestimmung bedarf es nicht, diese ist durch die Neuregelung in § 61 Abs. 2 erfasst.

Zu § 56

Zu Abs. 1
Zunächst waren die Bestimmungen über die Verarbeitung personenbezogener Daten zu anderen Zwecken, als zu denen, für die sie erhoben wurden, an die entsprechenden Bestimmungen des HDSIG-E anzupassen, d.h. an dessen §§ 20 bis 27 und 44 bis 45. Da nach Art. 9 der Richtlinie (EU) Nr. 2016/680 auch für Justizvollzugsbehörden der Anwendungsbereich der Verordnung (EU) Nr. 2016/679 eröffnet sein kann, war insoweit auch auf die Normen zu deren Umsetzung abzustellen.

Soweit darüber hinaus in einer Aufzählung nurmehr besondere Regelbeispiele ("insbesondere") für eine Datenverarbeitung zu namentlich genannten Zwecken genannt werden, ist dies wie folgt zu begründen:

Die neue Nr. 1 stellt die Umsetzung von Art. 4 Abs. 2 der Richtlinie (EU) Nr. 2016/680 dar. Die bisherige Nr. 1 wird Nr. 2. Die bisherige Nr. 2 kann gestrichen werden, da sie in der neuen Nr. 1 aufgeht. Die Nennung von Nr. 3 und 5 wäre über die neue Nr. 1 erfasst. Eine Streichung der vorgenannten Vorschriften könnte aber eine erhebliche Rechtsunklarheit in der Praxis auslösen, da durch die Verweisung auf allgemeine Bestimmungen die Rechtsanwendung nicht nur vereinfacht wird. Eine entsprechende Unklarheit sollte im Sinne einer effizienten Rechtshandhabung - auch im Sinne der Betroffenen - vermieden werden. Insoweit erscheint es sinnvoll, den bisherigen Katalog trotz seiner deklaratorischen Natur weitestgehend beizubehalten. Neu hinzugefügt wurde Nr. 4, um insoweit einen Gleichlauf mit dem Hessischen Strafvollzugsgesetz sicherzustellen.

Dies gilt im Ergebnis und mit derselben Begründung auch für die übrigen Nr. 6 bis 12, zu deren Zweck die Verarbeitung anderweitig erhobener personenbezogener Daten jedenfalls nach Art. 9 Abs. 1 Satz 2 der Richtlinie (EU) Nr. 2016/680 i.V.m. Art. 9 Abs. 2 der Verordnung (EU) Nr. 2016/679 zulässig ist, was wiederum über die Verweisung auf § 22 HDSIG-E abgedeckt wird. Auch insoweit soll jedoch Rechtsunklarheit in der Praxis vermieden werden, sodass es geboten erscheint, die bisherigen Tatbestände als Regelbeispiele ebenfalls beizubehalten.

Die Einführung des Erfordernisses der unbedingten Erforderlichkeit bei besonderen Kategorien personenbezogener Daten trägt insoweit § 43 Abs. 1 HDSIG-E Rechnung und betrifft z.B. Maßnahmen nach § 18 Abs. 3.

Zu Abs. 2
Die Vorschrift dient dem besonderen Schutz von Daten, die bei besonders erheblichen Eingriffen in Grundrechte anfallen.

Das Telekommunikationsgeheimnis steht den bisherigen Ausnahmetatbeständen insoweit gleich, weshalb die Überwachung der Telekommunikation (vgl. § 36) und das Auslesen von Datenspeichern (vgl. § 55 HUVollzG-E) in Satz 1 ebenfalls aufgeführt werden. Entsprechend der systematischen Bedeutung der Vorschrift wird in Satz 1 wie für Abs. 1 klargestellt, dass die Regelung für Datenverarbeitungen gilt, die über die reine Erfassung und Speicherung hinausgehen, insbesondere für die Übermittlung.

Die Gründe, aus denen bei den entsprechenden sensiblen Daten eine Weiterverarbeitung weiterhin möglich sein soll, werden nunmehr unter Nr. 1 bis 3 aufgezählt.

Nr. 1 erweitert den bisherigen Regelungsgehalt auf andere Zwecke, wie sie in § 40 HDSIG-E vorgesehen werden.

Nr. 2 entspricht der bisherigen Verweisung auf § 12 Abs. 2 Nr. 1 des derzeit noch geltenden Hessischen Datenschutzgesetzes; insoweit war klarzustellen, dass die Befugnis zur Verarbeitung auch aus Normen des Hessischen Strafvollzugsgesetzes folgen kann. Die übrigen Verweisungen auf das derzeit noch geltende Hessische Datenschutzgesetz werden obsolet; der bisherige Verweis auf § 12 Abs. 2 Nr. 3 und 4 des Hessischen Datenschutzgesetzes erübrigt sich durch die Verweisung auf Abs. 1 Nr. 1 neuer Fassung.

Nr. 3 stellt insoweit einen Auffangtatbestand dar, um die Praxis bei der bisherigen Rechtsanwendung fortzuführen. Die bisherige Nr. 3 - die Einwilligung - wurde wegen der besonderen Problematik dieser Rechtsgrundlage im Geltungsbereich der Richtlinie (EU) Nr. 2016/680 gestrichen.

Darüber hinaus soll die Weiterverarbeitung, insbesondere die Übermittlung, nur bei unbedingter Erforderlichkeit vorgenommen werden, wie dies in Satz 1 eingefügt wurde. Das Bundesverfassungsgericht hat in seinem Urteil vom 20. April 2016, Aktenzeichen 1 BvR 966/09 und 1BvR 1140/09 in Hinblick auf das BKAG in der damals geltenden Fassung ausgeführt, dass die Verhältnismäßigkeit eines Eingriffs von dessen Intensität abhängt und angemessen ausgestaltet sein muss. Je tiefer Überwachungsmaßnahmen in das Privatleben eingreifen, desto strenger sind die Anforderungen, was insbesondere für die Wohnraumüberwachung und den Zugriff auf informationstechnische Systeme gilt. Die in der Entscheidung zu beurteilenden Sachverhalte betrafen zwar verdeckte Datenverarbeitungen, während die im Hessischen Untersuchungshaftvollzugsgesetz vorgesehenen Maßnahmen regelmäßig nicht verdeckt erfolgen, was insbesondere durch die Offenlegung von Überwachungsmaßnahmen gilt. Auch stellt insbesondere der Haftraum keine Wohnung i.S.d. Art. 13 GG dar (vgl. BVerfG NJW 1996, 2643). Schließlich müssen bei den Eingriffen nicht notwendigerweise auch besondere Kategorien personenbezogener Daten geschützt werden. Dennoch erscheinen vor diesem Hintergrund die aufgeführten Daten besonders schützenswert - nachdem es sich zwar um offene, aber tiefe Eingriffe in die Kommunikation handelt - sodass ihre Weitergabe nur zu eingeschränkten Zwecken und im Fall der unbedingten Erforderlichkeit erfolgen sollte. Durch diese Beschränkung wird sichergestellt, dass insbesondere die Übermittlung der entsprechenden Daten nur zu Zwecken erfolgt, für die sie selbst hätten erhoben werden können (Grundsatz der hypothetischen Datenneuerhebung).

Um im Falle ihrer Übermittlung sicherzustellen, dass die entsprechenden Daten mit der erforderlichen Sensibilität behandelt werden, sind sie entsprechend dem neu eingefügten Satz 2 eindeutig zu kennzeichnen.

Es wird ferner klargestellt, dass § 4 Abs. 3 Satz 2 HDSIG-E unberührt bleibt. Diese Vorschrift regelt den Sonderfall einer Übermittlung von Videoaufzeichnungen, die bei der Überwachung öffentlich zugänglicher Räume angefallen sind.

Zu Abs. 3
Es handelt sich insoweit um Sonderfälle des Abs. 1.

Der neue Verweis in Satz 1 auf Abs. 1 dient ebenfalls der Vermeidung von Rechtsunsicherheit in der Praxis.

Zu Abs. 5
Der neue Hinweis in Satz 3 a. E. an jeden Empfänger, was die Einstufung besonderer Kategorien personenbezogener Daten angeht, entspricht insbesondere der Pflicht zur Schaffung geeigneter Garantien nach § 43 Abs. 2 Nr. 8 HDSIG-E im Falle der Übermittlung besonderer Kategorien personenbezogener Daten, die wiederum auf Art. 10 der Richtlinie (EU) Nr. 2016/680 zurückgeht.

Zu Abs. 6
Die Nennung der Gerichtszuständigkeit wurde an die Neufassung des Kataloges in Abs. 1 angepasst; desgleichen der Verweis auf die Vorschriften in § 61.

Zu § 57

Zu Abs. 1
Der Schutzbereich der Vorschrift in Satz 1 wurde auf alle besonderen Kategorien personenbezogener Daten nach § 41 Nr. 15 HDSIG-E erweitert. Die Erweiterung des Schutzes für alle besonderen Kategorien personenbezogener Daten trägt dessen § 43 Abs. 2 Rechnung. Weitere Schutzvorschriften enthalten insoweit § 54 Abs. 2 und § 56 Abs. 1.

Zu Abs. 2
Die Verwendung des Begriffs "unbedingt erforderlich" in Satz 2 statt bisher "unerlässlich" stellt auf die Terminologie in § 43 Abs. 1 HDSIG-E ab. Passend zu Satz 2 wird in Satz 3 ebenfalls auf den Begriff der "Offenbarung" abgestellt.

Zu Abs. 3
Die Vorschrift betrifft die Weitergabe von Informationen, die von externen Dienstleistern nicht unmittelbar zu Vollzugszwecken - sondern primär zum Zwecke der Behandlung - erhoben, aber zu Zwecken des Vollzuges weitergegeben werden. Insoweit ist der Anwendungsbereich der Verordnung (EU) Nr. 2016/679 eröffnet.
Redaktionell wird ferner in Satz 2 klargestellt, dass die vorgenannten Personen lediglich zu einer Offenbarung befugt sind.

Zu Abs. 5
Der Terminus "unerlässlich" wurde an den Begriff "unbedingt" erforderlich angepasst.

Zu Nr. 9 (§ 58)
Das entsprechende Verfahren ist nunmehr in § 58 HDSIG-E geregelt, sodass die Verweisung entsprechend anzupassen war.

Zu Nr. 10 (§§ 59 bis 61)

Zu § 59

Zu Abs. 1
Die Bestimmung ist neu eingeführt.

Die Sätze 1, 2 und 4 geben insoweit die Bestimmung von § 48 HDSIG-E wieder.

Der gesonderte Hinweis nach Satz 3 entspricht insoweit dem Regelungsgehalt von § 43 Abs. 2 Satz 2 Nr. 3 HDSIG-E für die Sicherung besonderer Kategorien personenbezogener Daten, ist jedoch aufgrund der besonderen datenschutzrechtlichen Sensibilität der weiteren aufgeführten Arten von Daten erforderlich.

Zu Abs. 2

Entsprechend der Einführung eines neuen Abs. 1 ist der bisherige Inhalt von § 59 HUVollzG als Abs. 2 zu bezeichnen. Die Verweisung auf die Vorschrift des bisherigen § 10 HDSG in Satz 1 war an § 59 HDSIG-E entsprechend anzupassen.

Zu § 60
Die Vorschrift wird komplett neu gefasst.

In die Überschrift wurde der Begriff der Information aufgenommen, da dies der Terminologie des HDSIG-E entspricht, vgl. dort § 50.

Entsprechend der Formulierungen des HDSIG-E wird auf dessen §§ 50 bis 52 verwiesen, soweit die Datenverarbeitung zu Zwecken der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung und des Strafvollzuges, einschließlich des Schutzes vor und der Abwehr von Gefahren für die öffentliche Sicherheit erfolgt; im Übrigen auf dessen §§ 31 bis 33. Die Zweiteilung der Informations- und Auskunftsrechte folgt aus der nicht-ausschließlichen Anwendbarkeit von Richtlinie (EU) Nr. 2016/680 und Verordnung (EU) Nr. 2016/679 im Bereich des Hessischen Justizvollzugs. Dabei erscheint es sinnvoll, den Untersuchungsgefangenen bei Aufnahme z.B. ein entsprechendes Formblatt als Information zu Datenverarbeitungen auszuhändigen - § 6 Abs. 1 sieht insoweit die Information über Rechte und Pflichten vor - und dgl. Besuchern bei Betreten der Anstalt.

Zur Gewährung eines effektiven Rechtsschutzes wird im neuen Satz 2 die Möglichkeit einer Akteneinsicht beibehalten und dahin gehend erweitert, dass sie im Rahmen des Erforderlichen insgesamt möglich ist. Insbesondere bei Einsichtnahmen in Gesundheitsakten wird hierbei großzügig zu verfahren sein, vgl. BVerfG, Beschluss der 2. Kammer des Zweiten Senats vom 20. Dezember 2016 - 2 BvR 1541/15.

Zu § 61
Die Vorschrift wird weitestgehend neu gefasst.

Zur Überschrift
Der Begriff "Sperrung" wurde durch den Begriff "Einschränkung der Verarbeitung" ersetzt.

Nach der Systematik des HDSIG-E kann, vgl. dort § 53 Abs. 3, an Stelle einer Löschung von personenbezogenen Daten bei diesen eine Einschränkung der Verarbeitung vorgenommen werden. Nach § 41 Nr. 3 HDSIG-E ist hierunter "die Markierung gespeicherter personenbezogener Daten mit dem Ziel, ihre künftige Verarbeitung einzuschränken" zu verstehen.

Nach der bisherigen Systematik, vgl. § 61 Abs. 1 HUVollzG in seiner jetzigen Fassung, sind personenbezogene Daten auch jetzt schon unverzüglich zu löschen, sobald feststeht, dass ihre Speicherung nicht mehr erforderlich ist, um die Zwecke zu erfüllen, für die sie erhoben worden sind oder für die sie nach § 13 Abs. 2 und 4 HDSG weiterverarbeitet werden dürfen; wenn bei der Speicherung nicht absehbar ist, wie lange die Daten benötigt werden, ist nach einer aufgrund der Erfahrung zu bestimmenden Frist zu prüfen, ob die Erforderlichkeit der Speicherung noch besteht, vgl. § 19 Abs. 3 HDSG in seiner jetzigen Fassung.

Grundsätzlich sollte für die zukünftige Rechtslage - wie bisher auch - zwischen besonders sensiblen Daten, Daten in Gefangenenakten und -dateien und sonstigen Daten hinsichtlich der Frage ihrer Löschung oder - an deren Stelle - der Einschränkung ihrer Verarbeitung unterschieden werden.

Zu Abs. 1
Der Absatz entspricht in seinem Regelungsgehalt dem bisherigen Abs. 1. Es wurde der Begriff "in der Verarbeitung einzuschränken" anstelle der bisherigen Sperrung verwendet und auf die einschlägigen Bestimmungen des HDSIG-E verwiesen, je nachdem, ob die Verarbeitung zu den Zwecken nach § 40 HDSIG-E erfolgt oder nicht.

Zu Abs. 2
Abs. 2 befasst sich entsprechend der bisherigen Systematik mit der Verfahrensweise bei personenbezogenen Daten, die aufgrund besonders intensiver Eingriffe erhoben wurden.

In Satz 1 wurden Ergebnisse von Maßnahmen nach § 55 den Videoaufnahmen gleichgestellt, da insoweit ein gleiches Maß an Schutzwürdigkeit gegeben ist. Ebenfalls wird klargestellt, dass eine Löschung nur dann nicht erfolgt, wenn zum Zeitpunkt der Entscheidung über die Löschung zu konkreten Beweiszwecken die weitere Aufbewahrung bei gleichzeitiger Einschränkung der Verarbeitung unbedingt erforderlich ist; insoweit ist eine Angleichung an die Terminologie der Bestimmungen des Entwurfs zum Hessischen Datenschutz- und Informationsfreiheitsgesetz vorgenommen worden, was die Verarbeitung von besonderen Kategorien personenbezogener Daten angeht.

Im neu eingeführten Satz 2 wird eine verkürzte Frist zur Löschung von Daten eingeführt, die entgegen dem Grundsatz verarbeitet, insbesondere erhoben wurden, dass der Kernbereich der Lebensgestaltung nicht zum Gegenstand der Verarbeitung personenbezogener Daten gemacht werden darf. Dies trägt der besonderen Schutzwürdigkeit der Betroffenen in diesem Fall Rechnung.

Der ebenfalls neu eingeführte Satz 3 statuiert insoweit eine Dokumentationspflicht zur kontrollierbaren Löschung der in Satz 1 und 2 aufgeführten, besonders sensiblen Daten, vgl. BVerfGE 274 S. 337ff. [S. 339]).

Zu Abs. 3
Die Vorschrift befasst sich mit der Löschung von personenbezogenen Daten und differenziert hierbei zwischen Akten und Dateien zum Gefangenen und sonstigen Akten und Dateien. Dabei ist eine Gleichbehandlung von Dateien im Sinne einer elektronischen Datei mit einer Papierakte geboten, da auch eine ordnungsgemäß geführte Gefangenenpersonalakte regelmäßig ein Dateisystem im datenschutzrechtlichen Sinne darstellen wird (vgl. zum Begriff Gola DS-GVO Art. 4 Rd.-Nr. 46). Die Vorschrift orientiert sich insoweit an der Struktur des Abs. 3 Satz 1 in der derzeit geltenden Fassung, wobei aber entsprechend der Systematik der Richtlinie (EU) Nr. 2016/680 statt einer grundsätzlichen Sperrung der Daten jetzt vorrangig deren Löschung zu erfolgen hat.

In Satz 1 wird zunächst redaktionell klargestellt, dass der Abs. 3 sich - wie Abs. 1 und 2 - auf personenbezogene Daten bezieht. § 53 Abs. 2 HDSIG-E sieht in Umsetzung von Art. 16 der Richtlinie (EU) Nr. 2016/680 die Löschung vor, wenn die Kenntnis der Daten für die Aufgabenerfüllung nicht mehr erforderlich ist. Das ist grundsätzlich dann der Fall, wenn ein Untersuchungsgefangener entlassen oder verlegt wird. Dies ist jedoch nicht der Fall, sofern die Daten zur Abwicklung der Freiheitsentziehung notwendig verfügbar sein müssen (z.B. zur Abrechnung von Geldern), oder die Freiheitsentziehung wieder aufgenommen werden kann. Entsprechend ist der Anstalt eine Frist für die Löschung der personenbezogenen Daten von bis zu zwei Jahren für die Löschung der personenbezogenen Daten zuzubilligen, wie dies z.B. auch Art. 41 Nr. 3 BayUVollzG vorsieht; im Falle eines Freispruchs etc. ist der Untersuchungsgefangene vor einer übermäßig langen Speicherung durch die Sondervorschrift des Abs. 5 hinreichend geschützt. Besteht zum Zeitpunkt des Fristablaufs ein konkreter Anhaltspunkt dafür, dass eine Aufbewahrung von Daten zur Abwicklung des Vollstreckungsverhältnisses weiter erforderlich ist, kann dem durch die weitere Speicherung bei Einschränkung der Verarbeitung nach Abs. 4 Rechnung getragen werden.

Satz 2 ersetzt den bisherigen Abs. 4 der Bestimmung in seiner derzeit geltenden Fassung.

Zu Abs. 4
Der besseren Nachvollziehbarkeit halber sollen die Bestimmungen zur Einschränkung der Verarbeitung personenbezogener Daten in einem eigenen Abs. 4 dargestellt werden. Aus demselben Grund wird in Satz 1 auf die Normen verwiesen, aus denen sich grundsätzlich ergibt, wann und wie die Einschränkung der Verarbeitung zu erfolgen hat.

Anstelle einer Löschung der Daten können diese unter den Voraussetzungen des § 53 Abs. 3 bis 7 HDSIG-E in der Verarbeitung eingeschränkt werden, Satz 1 Nr. 1. Wie in § 53 Abs. 3 HDSIG-E erscheint eine weitergehende Speicherung bei Einschränkung der Verarbeitung zu Beweiszwecken insgesamt sinnvoll. Art. 16 Abs. 3 Satz 1 Buchst. b der Richtlinie (EU) Nr. 2016/680 lässt dies grundsätzlich zu und beschränkt Beweiszwecke nicht ausdrücklich auf den Anwendungsbereich der Richtlinie. Dies deckt auch die Beweiszwecke z.B. auch jenen Konstellationen ab, in denen ein ehemaliger Gefangener Haftungsansprüche gegen das Land geltend macht, z.B. wegen fehlerhafter ärztlicher Behandlung in der Haft. Einen ähnlichen Weg geht insoweit auch § 78 Abs. 2 bzw. 3 des Bundeskriminalamtgesetzes in seiner Neufassung durch das Gesetz zur Neustrukturierung des Bundeskriminalamtgesetzes; dort wird ebenfalls nur von der Aufbewahrung für "gerichtliche Verfahren" bzw. der Behebung "einer Beweisnot" gesprochen, ohne nach der Art des Verfahrens zu differenzieren, in dem die Daten benötigt werden. Sofern eine Einschränkung der Verarbeitung zu Beweiszwecken erfolgt, ist aber darauf zu achten, dass die Entscheidung hierüber grundsätzlich eine Einzelfallentscheidung darstellt und zum Zeitpunkt ihrer Entscheidung konkrete Anhaltspunkte für die Notwendigkeit einer späteren Verwendung vorliegen müssen. Eine abstrakte Vorratsdatenspeicherung ohne konkreten Anlass - der sinnvollerweise zu dokumentieren ist - dürfte unzulässig sein. Anders ist dies bei normierten Dokumentationspflichten zu beurteilen, wie insbesondere z.B. nach § 10 der Berufsordnung für die Ärztinnen und Ärzte in Hessen für die im Rahmen der Freiheitsentziehung erfolgten ärztlichen Maßnahmen; ein hierauf bezogenes Regelbeispiel wurde zur Erleichterung der Rechtspraxis in Nr. 1 aufgeführt.

Satz 1 Nr. 2 stellt insoweit einen Auffangtatbestand dar, soweit Daten nicht im Geltungsbereich der Richtlinie (EU) Nr. 2016/680 gespeichert wurden.

Die Kennzeichnung von in der Verarbeitung eingeschränkten personenbezogenen Daten trägt insbesondere § 53 Abs. 4 HDSIG-E Rechnung. Die in Satz 2 ebenfalls geregelte Heranziehung in der Verarbeitung eingeschränkter personenbezogener Daten, im Regelfall durch Übermittlung, zu anderen Zwecken als des § 40 HDSIG-E, muss den Anforderungen der Verordnung (EU) Nr. 2016/679 genügen (vgl. Art. 9 Abs. 1 und 2 der Richtlinie (EU) Nr. 2016/680; insoweit gestattet Art. 18 Abs. 1 Buchst. a bzw. c der Verordnung (EU) Nr. 2016/679 aber auch die Verwertung zu Beweiszwecken). Wie sich aus Art. 9 der Richtlinie (EU) Nr. 2016/680 ergibt, muss die Verarbeitung zu Vollzugszwecken erhobener Daten auch nicht auf den sachlichen Bereich der Richtlinie (EU) Nr. 2016/680 beschränkt sein.

Satz 3 entspricht dem bisherigen Regelungsgehalt von § 61 Abs. 3 Satz 4 HUVollzG in seiner jetzigen Fassung. Auch insoweit bleibt eine Einwilligung weiter zulässig: entweder dient die Aufhebung der Einschränkung der Verarbeitung Zwecken der Richtlinie, sodass § 46 HDSIG-E Anwendung findet; oder die Verarbeitung dient anderen Zwecken, sodass über Art. 9 Abs. 1 der Richtlinie (EU) Nr. 2016/680 die Bestimmungen der Verordnung (EU) Nr. 2016/679 gelten.

Satz 4 entspricht dem bisherigen Regelungsgehalt von § 61 Abs. 3 Satz 2 HUVollzG in seiner jetzigen Fassung.

Zu Abs. 5

Entsprechend § 70 Abs. 4 HDSIG-E wurde eine jährliche Kontrollfrist eingeführt, differenzierend zwischen Gefangenendateien und -akten einerseits sowie sonstigen Dateien und Akten andererseits.

Zu Abs. 6
Die Vorschrift entspricht im Wesentlichen dem Regelungsgehalt des bisherigen Abs. 5.

Zu Abs. 7
Der Absatz entspricht im Wesentlichen dem bisherigen Abs. 6 in der derzeit geltenden Fassung. Redaktionell wurde die Herkunft der Daten danach präzisiert, aus welchen Akten etc. sie stammen. Hinsichtlich der Gefangenenbücher ist darauf hinzuweisen, dass es sich hierbei um Bestandsverzeichnisse in Buchform handelt, die mittlerweile elektronisch geführt werden. Die Aufbewahrungsfristen beziehen sich daher im Wesentlichen auf Altfälle, die sich bereits in der Aufbewahrung befinden.

In Satz 4 wurde die Verweisung auf das Hessische Archivgesetz in eine dynamische Verweisung umgewandelt, um zukünftige Änderungen abzubilden.

Zu Art. 5 (Änderung des Hessischen Sicherungsverwahrungsvollzugsgesetzes)

Allgemeines
Auf die Sicherungsverwahrung findet grundsätzlich die Richtlinie (EU) Nr. 2016/680 des Europäischen Parlamentes und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zweck der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung sowie zum freien Datenverkehr und zur Aufhebung des Rahmenbeschlusses 2008/977/JI des Rates Anwendung. Insoweit wird ebenfalls auf die Vorbemerkungen zur Änderung des Hessischen Jugendstrafvollzugsgesetzes Bezug genommen.

Zu Nr. 1 (Inhaltsübersicht)
Soweit bei einzelnen Paragrafen die Überschriften geändert werden, ist die Inhaltsübersicht entsprechend anzupassen.

Zu Nr. 2 (§ 24)
Eine Benachrichtigung der nächsten Angehörigen ist im Falle der schweren Erkrankung von der Einwilligung des Untergebrachten abhängig zu machen; ein entsprechender Vorbehalt wurde zu Satz 1 als 2. Halbsatz angefügt. Dies entspricht den Maßgaben von Art. 9 Abs. 1 Satz 2 der Richtlinie (EU) Nr. 2016/680 i.V.m. Art. 9 Abs. 1 und 2 Buchst. a der Verordnung (EU) Nr. 2016/679, da insoweit die Verarbeitung (durch Übermittlung) von besonderen Kategorien personenbezogener Daten (in Form von Gesundheitsdaten, vgl. § 41 Nr. 14 HDSIG-E) zu Zwecken erfolgt, die nicht ohne Weiteres der Durchführung des Strafvollzuges dient, sondern zunächst einmal der allgemeinen Information der Angehörigen. Auf eine mutmaßliche Einwilligung i.S.v. Art. 9 Abs. 2 Buchst. c kann insoweit nicht abgestellt werden, da die Übermittlung des Gesundheitszustandes an Angehörige auch bei Lebensgefahr kein lebenswichtiges Interesse der betroffenen Personen darstellt; dies dürfte nur für die Durchführung lebenserhaltender Maßnahmen zutreffen. Um auch in Situationen handeln zu können, in denen eine Einwilligung nicht mehr eingeholt werden kann, sollte die Einwilligung - die insoweit den Anforderungen der Verordnung (EU) Nr. 2016/679 genügen muss - bereits bei Aufnahme eingeholt werden; zu diesem Zweck wurde als neuer Satz 3 eine Belehrungspflicht aufgenommen.

Im Falle des Todes ist weiterhin eine Benachrichtigung auch ohne Einwilligung angezeigt und nach §§ 22 Abs. 3 i.V.m. Abs. 2 Nr. 3 und Art. 9 Abs. 2 Buchst. f der Verordnung (EU) Nr. 2016/679 möglich.

Zu § 34

Zu Buchst. a
Als neuer zweiter Halbsatz wurde eine Regelung zu Satz 1 hinzugefügt, wonach sich die Überwachung sowohl auf Untergebrachte wie Besucher bezieht; dies dient der Klarstellung im Sinne von § 67 HDSIG-E, da die Überwachung sich sowohl auf die Untergebrachten als verurteilte Straftäter (dort Nr. 3) wie auch auf den Besuch (dort nur Nr. 5) beziehen kann.

In Satz 2 wird klargestellt, dass die Überwachung der Unterhaltung, sofern sie besondere Kategorien personenbezogener Daten zum Gegenstand hat, nur noch im Falle unbedingter Erforderlichkeit erfolgt, um insbesondere den Anforderungen aus § 43 Abs. 1 HDSIG-E bzw. Art. 10 der Richtlinie (EU) Nr. 2016/680 Rechnung zu tragen. Eine Verarbeitung besonderer Kategorien personenbezogener Daten - legaldefiniert in § 41 Nr. 15 HDSIG-E, insoweit gleichlaufend Art. 9 der Verordnung (EU) Nr. 2016/679 - ist nur bei unbedingter Erforderlichkeit zulässig. Der Begriff der "unbedingten Erforderlichkeit" ist weder in der Verordnung (EU) Nr. 2016/679 noch der Richtlinie (EU) Nr. 2016/680 legaldefiniert. Da er nach dem Wortlaut ein gesteigertes Maß der Erforderlichkeit vorsieht, kann er wie der bisher im Rahmen des Strafvollzugsrechts verwendete Begriff "unerlässlich" im Sinne eines gesteigerten Maßes der Erforderlichkeit verstanden werden. Eine Maßnahme ist dann unerlässlich, wenn tatsächlich keinerlei weniger eingriffsintensive und mit vertretbarem Aufwand durchführbare Maßnahmen zur Zweckerreichung zur Verfügung stehen; darüber hinaus darf die Art der datenschutzrelevanten Maßnahme schutzwürdige Interessen der Betroffenen nicht beeinträchtigen (vgl. Arloth/Krä StVollzG 4. Auflage § 59 HStVollzG Rd.-Nr. 2, Laubenthal/Nestler/Neubacher/Verrel O Rd.-Nr. 35ff). In die Abwägung einzustellen sind somit sämtliche mit hinreichender Wahrscheinlichkeit mit der Datenverarbeitung für die Betroffenen im persönlichen Nahbereich einhergehenden Konsequenzen, einschließlich der Auswirkungen auf die Beziehungen zu Verwandten, zum sozialen Wohnumfeld sowie zum Arbeitgeber (vgl. Laubenthal/Nestler/Neubacher/Verrel aaO.). Wie in der Begründung zu § 43 HDSIG-E ausgeführt ist eine unbedingte Erforderlichkeit anzunehmen, wenn keine zumutbare Alternativ- oder Ausgleichsmaßnahme zur Verfügung steht, um ein legitimes Ziel zu erreichen.

Inwieweit der Begriff der "unbedingten Erforderlichkeit" in der Rechtspraxis zu anderen Ergebnissen führen wird als eine konsequente Anwendung des Erforderlichkeitsprinzips im Rahmen der Verhältnismäßigkeitsprüfung bleibt abzuwarten. So wird in anderen Regelungsbereichen z.B. zur Durchführung einer sachgerechten medizinischen Betreuung bereits bei jeder Anamnese die umfassende Erhebung von Gesundheitsdaten regelmäßig unbedingt erforderlich sein, ebenso wie es für jeden Vollzugsbediensteten regelmäßig unbedingt erforderlich sein dürfte, auf die Gesichtsbilder der Untergebrachten in der Untergebrachtenpersonalakte zugreifen zu können, um dessen Person in praxisgerechter Weise identifizieren zu können.

Die Überwachung von Besuchen ist elementar für die Sicherheit oder Ordnung der Einrichtung. Die permanente Überwachung der Unterhaltung wird daher im Regelfall unbedingt erforderlich sein, auch wenn sie besondere Kategorien personenbezogener Daten zum Inhalt hat. In vielen Fällen ist es allerdings praktisch unvermeidbar, dass die Vollzugsbediensteten Informationen zur Kenntnis nehmen, bevor sie deren besonderen datenschutzrechtlichen Bezug erkennen. In derartigen Fällen ist es in Anlehnung an die Entscheidung BVerfGE 129, S. 208ff. (Rn. 209ff) verfassungsrechtlich nicht gefordert, den Zugriff wegen des Risikos einer Kernbereichsverletzung auf der Erhebungsebene von vornherein zu unterlassen. In Fällen dieser Art ist es geboten, aber auch ausreichend, für hinreichenden Schutz in der Auswertungsphase zu sorgen, insbesondere durch Gewährung eines entsprechenden Schutzes durch Löschung von Aufzeichnungen.

Zu Buchst. b
In Satz 1 wird ein neuer zweiter Halbsatz eingeführt, wonach die Überwachung auch durch optisch-elektronische Einrichtungen erfolgen kann, die als Videoüberwachung legaldefiniert wird, da dieser Begriff im Gesetz mehrfach verwendet wird.

Satz 2 wird dahin gehend neu gefasst, dass die Aufzeichnung und Speicherung von Daten gemäß Satz 1 nur im Falle unbedingter Erforderlichkeit erfolgt. Dies ist dem Umstand geschuldet, dass für den Geltungsbereich der Richtlinie (EU) Nr. 2016/680 je nach Qualität des Überwachungssystems Gesichtsbilder unter die besondere Kategorie personenbezogener Daten fallen können, insbesondere bei der Verwendung spezieller Gesichtserkennungssoftware. Darüber hinaus ist eine Videoüberwachung von Besuchen besonders geneigt, durch Aufzeichnung des Verhaltens der überwachten Personen Informationen zu besonderen Kategorien personenbezogener Daten im Sinne von Art. 10 der Richtlinie (EU) Nr. 2016/680 zu generieren. Die Einfügung des Tatbestandsmerkmals der unbedingten Erforderlichkeit trägt im Interesse einer möglichst sicheren Umsetzung der Richtlinie (EU) Nr. 2016/680 entsprechend deren Art. 10 bzw. § 43 Abs. 1 HDSIG-E Rechnung, um eine Videoüberwachung in jedem Fall datenschutzrechtlich abzusichern.

Zu Nr. 4 (§ 35)
In Satz 1 wird eingefügt, dass die Erforderlichkeit sich auf Ziel und Aufgaben des Vollzugs der Freiheitsstrafe gemäß § 2, insbesondere auf Gründe der Sicherheit oder Ordnung der Einrichtung bezieht; insoweit wird Art. 8 Abs. 2 der Richtlinie (EU) Nr. 2016/680 Rechnung getragen. Deren Anwendungsbereich ist auch im Bereich des Schriftwechsels nicht in jedem Fall ausgeschlossen. Es ist insbesondere nach Abs. 3 auch möglich, angehaltenen Schriftwechsel zu verwahren, regelmäßig in einer körperlichen Akte, aber auch nach Scannen in einer elektronischen Akte, mithin analogen oder digitalen Dateisystemen. Der zu überwachende Schriftwechsel wird häufig mit einer gewissen Wahrscheinlichkeit besondere Kategorien personenbezogener Daten enthalten, ohne dass dies vor Beginn der Überwachung klar ist. Insoweit besteht eine geringere Flexibilität als bei der Überwachung eines Besuchs, bei dem sich die besondere datenschutzrechtliche Relevanz bei den besonderen Kategorien aus dem überwachten Verlauf des Besuchs selbst ergeben kann. Um das Schutzniveau für die besonderen Kategorien personenbezogener Daten von Anfang an zu gewährleisten, ist nach § 43 Abs. 1 HDSIG-E daher prophylaktisch sicherzustellen, dass die Überwachung des Schriftwechsels nur im Falle unbedingter Erforderlichkeit erfolgt, was durch einen entsprechenden Einschub in Satz 1 erfolgt. Da die Überwachung des Schriftwechsels für Sicherheit oder Ordnung unverzichtbar sind, wird das Kriterium der unbedingten Erforderlichkeit regelmäßig erfüllt sein. Darüber hinaus sollten Untergebrachte frühzeitig (d.h. bei Aufnahme) auf die Möglichkeit der Überwachung hingewiesen werden, um den Eingriff in das Postgeheimnis nicht zu einer verdeckten Maßnahme zu machen, an die - insbesondere angesichts des Urteils des Bundesverfassungsgerichts vom 20. April 2016, Aktenzeichen 1 BvR 966/09 und 1BvR 1140/09 - bei der Datenverarbeitung erheblich höhere Anforderungen zu stellen wären; eine entsprechende Hinweispflicht wurde als neuer Halbsatz an Satz 1 angefügt.

Zu Nr. 5 (§ 45)

Zu Abs. 2
In Satz 2 wird - auch im Sinne einer einheitlichen Terminologie - ferner klargestellt, dass die technischen Hilfsmittel auch optisch-elektronische Einrichtungen (Videoüberwachung) umfassen. Da diese - unabhängig von der Einstufung eines Gesichtsbildes als biometrisches Datum - besonders geeignet sind, insgesamt besondere Kategorien personenbezogener Daten zu liefern, sei es in Form von Gesundheitsdaten oder anderen Unterfällen, ist nach § 43 Abs. 1 HDSIG-E in Satz 2 nunmehr vorgesehen, dass die entsprechende Verarbeitung nur im Falle unbedingter

Erforderlichkeit zulässig ist. Auch hier wird wegen der Unverzichtbarkeit einer entsprechenden Überwachung für Sicherheit oder Ordnung der Einrichtung das Kriterium der unbedingten Erforderlichkeit regelmäßig erfüllt sein.

Zu Nr. 6 (§ 50)

Zu Abs. 2
Es wird - auch im Sinne einer einheitlichen Terminologie - in Nr. 2 klargestellt, dass die technischen Hilfsmittel auch optisch-elektronische Einrichtungen (Videoüberwachung) umfassen. Da diese regelmäßig besondere Kategorien personenbezogener Daten liefern können, insbesondere Gesundheitsdaten zur Kontrolle des Gesundheitszustandes des Untergebrachten und somit besondere Kategorien personenbezogener Daten, ist nach § 43 Abs. 1 HDSIG-E vorgesehen, dass die entsprechende Verarbeitung nur im Falle unbedingter Erforderlichkeit zulässig erfolgt. Da die entsprechende Kontrolle für die Information des Gesundheitszustandes des Untergebrachten unverzichtbar ist, wird das Kriterium der unbedingten Erforderlichkeit regelmäßig erfüllt sein.

Zu Abs. 6
Da die dauerhafte Überwachung nach Abs. 2 Nr. 2 regelmäßig Gesundheitsdaten liefern kann und somit besondere Kategorien personenbezogener Daten, ist in Satz 2 klargestellt, dass dies im Sinne von § 43 Abs. 1 HDSIG-E nur im Falle unbedingter Erforderlichkeit zulässig ist. Auch hier gilt, dass, da die entsprechende Kontrolle für die Information des Gesundheitszustandes des Untergebrachten unverzichtbar ist, das Kriterium der unbedingten Erforderlichkeit regelmäßig erfüllt sein wird.

Zu Nr. 7 (§§ 58 bis 61)

Zu § 58

Zu Abs. 1
In Satz 1 wird in Anlehnung an § 41 Nr. 2 HDSIG-E statt an die Alternativen Datenerhebung bzw. -weiterverarbeitung an den einheitlichen Begriff der Verarbeitung angeknüpft; ebenfalls wurde vor dem Wort "verarbeiten" ein "nur" eingefügt, um das Prinzip des Verbots mit Erlaubnisvorbehalt hervorzuheben. Ferner erfolgt in Satz 1 die systematische Klarstellung, dass zunächst eine gesetzliche Spezialregelung Anwendung findet und nur in letzter Linie die Generalklausel, die insoweit grundsätzlich auf die Erforderlichkeit für den Vollzug abstellt. Bei der Verarbeitung besonderer Kategorien personenbezogener Daten - legaldefiniert § 41 Nr. 15 HDSIG-E - muss allerdings insoweit die unbedingte Erforderlichkeit gegeben sein. Gestrichen wurde die Einwilligung als allgemeiner Rechtsgrund für eine Datenverarbeitung. Dies trägt dem Umstand Rechnung, dass die Richtlinie (EU) Nr. 2016/680 eine Einwilligung im Rahmen ihres Geltungsbereichs grundsätzlich nicht mehr als alleinige Grundlage hierfür ausreichen lässt, wie sich aus Ziffer 35 der Erwägungen zur Richtlinie ergibt. Wie weit dieser Grundsatz reicht, ist derzeit noch nicht abschließend geklärt. Der letzte Satz der vorgenannten Erwägungen führt hierzu aus: "Dies sollte die Mitgliedstaaten nicht daran hindern, durch Rechtsvorschriften vorzusehen, dass die betroffene Person der Verarbeitung ihrer personenbezogenen Daten für die Zwecke dieser Richtlinie zustimmen kann, beispielsweise im Falle von DNA-Tests in strafrechtlichen Ermittlungen oder zur Überwachung ihres Aufenthaltsortes mittels elektronischer Fußfessel zur Strafvollstreckung." In den Artikeln der Richtlinie (EU) Nr. 2016/680 findet sich die Einwilligung dann jedoch - anders als in der Verordnung (EU) Nr. 2016/679 - als Rechtsgrund einer Datenverarbeitung nicht mehr. Daher wird die entsprechende Erwägung dahin gehend auszulegen sein, dass die Einwilligung in der Einzelvorschrift ausdrücklich aufgeführt sein muss; konsequenterweise sieht § 46 HDSIG-E die Möglichkeit einer Einwilligung in solchen Fällen vor. Tatbestände, bei denen ein solcher Einwilligungsvorbehalt gegeben ist, werden nunmehr durch den Tatbestand der "Rechtsvorschrift" mit abgedeckt.

Die Verweisung auf die Bestimmungen des subsidiär geltenden Hessischen Datenschutz- und Informationsfreiheitsgesetzes in Satz 2 wird faktisch als dynamische Verweisung ausgestaltet, um zukünftige Änderungen abzubilden. Zu Satz 2 wurde ein weiterer Halbsatz angehängt, durch den klargestellt wird, dass die Datenverarbeitung durch die Justizvollzugsbehörden zu Vollzugszwecken grundsätzlich - aber nicht ausschließlich, da insoweit auch die allgemeinen Bestimmungen, insbesondere Teil 1 gelten - unter dem Regime des Teils 3 des HDSIG-E erfolgt, um der Praxis angesichts der - in Art. 9 der Richtlinie (EU) Nr. 2016/680 selbst vorgesehenen Zweiteilung der datenschutzrechtlichen Regelungssysteme - eine grundsätzliche Entscheidungshilfe an die Hand zu geben. Dies hat daher nicht allein deklaratorische Wirkung; die Entscheidung kann im Einzelfall schwierig sein, s. hierzu die Ausführungen in den Vorbemerkungen zur Begründung der Änderung des HstVollzG

Neu hinzugefügt wurde Satz 3, der den Verhältnismäßigkeitsgrundsatz konkretisiert und in Hinblick auf Art. 1 Abs. 1 GG ein Verarbeitungsverbot ausspricht, da der Gesetzgeber den Kernbereich privater Lebensgestaltung zu schützen hat (vgl. BVerfGE 129, S. 208ff. [S. 245]). Ob ein Sachverhalt dem unantastbaren Kernbereich zuzuordnen ist, hängt davon ab, ob er nach seinem

Inhalt höchstpersönlichen Charakters ist, also auch in welcher Art und Intensität er aus sich heraus die Sphäre anderer oder Belange der Gemeinschaft berührt (vgl. BVerfGE 80, 367 [374] = NJW 1990, 563).

Zu Abs. 2
Die Präzisierung, dass die Verarbeitung für Ziel und Aufgaben des Vollzugs nach § 2 erfolgt, dient der Klarstellung, dass die Verantwortlichen im Sinne des Datenschutzes im vorliegenden Fall Daten grundsätzlich zu Zwecken der Sicherungsverwahrung verarbeiten. Klarstellend wird ferner eingefügt, dass die Verarbeitung der aufgezählten personenbezogenen Daten auch zur Aufrechterhaltung der medizinischen Versorgung und Gesundheitsfürsorge verarbeitet werden können, was Art. 8 Abs. 2 der Richtlinie (EU) Nr. 2016/680 Rechnung trägt.

Ferner wird auf den einheitlichen Tatbestand einer Verarbeitung abgestellt.

Da die bisherigen Nummern 1 bis 4 zumeist bereits besondere Kategorien personenbezogener Daten i.S.v. § 41 Nr. 15 HDSIG-E darstellen, wurde durch die Ergänzung um Nr. 5 insoweit eine Gesamtregelung für die Verarbeitung entsprechender Informationen geschaffen. Dabei wurden die Gesundheitsdaten in Hinblick auf ihre besondere Bedeutung, aber auch ihre bisher schon separate Speicherung herausgehoben. Deren Verarbeitung ist insbesondere bei Maßnahmen nach §§ 24 Abs. 1, 25 Abs. 4, 46 Abs. 2 und 3 sowie 47 relevant.

Die Verarbeitung besonderer Kategorien personenbezogener Daten wurde nach § 43 Abs. 1 HDSIG-E an das Erfordernis unbedingter Erforderlichkeit geknüpft.

Die beibehaltene Beschränkung auf Untergebrachte als verurteilte Straftäter trägt darüber hinaus § 67 HDSIG-E Rechnung, der wiederum aus Art. 6 der Richtlinie (EU) Nr. 2016/680 folgt.

Zu Abs. 3
Es erfolgt in Satz 1 eine Anpassung der separat zu führenden personenbezogenen Daten an die Neunummerierung in Abs. 2.

In Satz 2 wird statt auf "Daten, die den Gesundheitszustand betreffen" auf "Gesundheitsdaten" abgestellt, da letzter Begriff in § 41 Nr. 14 HDSIG-E legaldefiniert ist. Der Begriff "Personalakte" in Satz 2 wurde durch den der "Untergebrachtenpersonalakte" präzisiert.

Zu Abs. 4

Satz 2 wurde neu eingeführt, um klarzustellen, dass bei der Verarbeitung besonderer Kategorien personenbezogener Daten dies nur bei unbedingter Erforderlichkeit zulässig ist, s. § 43 Abs. 1 HDSIG-E.

Zu Abs. 5
Neu eingefügt wurde Satz 2, sofern hierbei die Verarbeitung biometrischer Daten notwendig werden sollte. Dies würde die Verarbeitung von besonderen Kategorien personenbezogener Daten darstellen, die wiederum gemäß § 43 Abs. 1 HDSIG-E nur bei unbedingter Erforderlichkeit zulässig ist.

Zu Abs. 6
Die Neufassung der Vorschrift orientiert sich an § 4 HDSIG-E. Da die Außensicherung sowohl öffentliche wie nicht öffentliche Plätze abdecken kann, konnte insoweit nicht lediglich auf die vorgenannte Vorschrift verwiesen werden.

Soweit in Satz 1 zusätzlich darauf abgestellt wird, dass schutzwürdige Interessen der Betroffenen nicht überwiegen dürfen, erfolgt dies in Orientierung an § 4 Abs. 1 HDSIG-E.

Satz 2 wurde dahin gehend ergänzt, dass neben der Überwachung auch der Name und die Kontaktdaten des Verantwortlichen zum frühestmöglichen Zeitpunkt erkennbar zu machen sind. Verantwortlicher wird dabei regelmäßig keine natürliche, mit Namen zu benennende Person sein, sondern die Einrichtung als zuständige Behörde, vgl. § 41 Nr. 8 HDSIG-E.

Ergänzend wird klargestellt, dass eine Speicherung nur zulässig ist, wenn keine Anhaltspunkte dafür bestehen, dass schutzwürdige Interessen der Betroffenen überwiegen; dies trägt § 4 Abs. 3 Satz 1 HDSIG-E Rechnung.

Zu § 58a

Zu Abs. 1
In Satz 2 wurde klargestellt, dass die Zuverlässigkeitsüberprüfung zur Aufrechterhaltung der Sicherheit oder Ordnung der Einrichtung hierfür erfolgt.

Die Verweisung auf das HSÜG in Satz 5 wurde durch eine dynamische Verweisung ersetzt, um zukünftige Änderungen abzubilden.

Zu Abs. 2
In Satz 1 wurde klargestellt, dass die Zuverlässigkeitsüberprüfung zur Aufrechterhaltung der Sicherheit oder Ordnung der Einrichtung hierfür erfolgt.

In Satz 2 wurde präzisiert, dass - in Hinblick auf § 67 HDSIG-E - die Zulassung zum Untergebrachtenbesuch überhaupt erfolgt und nicht nur für welche Untergebrachte.

Zu Abs. 4

Hinsichtlich der Benachrichtigungspflicht wurde ausdrücklich auf § 51 HDSIG-E Bezug genommen.

Zu Abs. 6
In Satz 1 wurde in Hinblick auf den in Art. 8 der Richtlinie (EU) Nr. 2016/680 normierten Erforderlichkeitsgrundsatz ergänzend eingeführt, dass die Wiederholung der Zulässigkeitsprüfung zu erfolgen hat, sofern ihre Erforderlichkeit fortbesteht.

Zu § 59
Der bisherige § 59 HSVVollzG war mit seinem bisherigen Regelungsgehalt aufzuheben. Die Vorschrift ging von dem Grundsatz aus, dass personenbezogene Daten grundsätzlich bei den Betroffenen zu erheben sind. Ein solcher Grundsatz wird weder in der Richtlinie (EU) Nr. 2016/680 noch der Verordnung (EU) Nr. 2016/679 statuiert. Da nicht ausgeschlossen werden kann, dass auch eine Vollzugseinrichtung im Bereich der Verordnung (EU) Nr. 2016/679 tätig wird, könnte die Beibehaltung eines entsprechenden Grundsatzes insoweit als Verstoß gegen europäisches Recht gelten. Darüber hinaus ist davon auszugehen, dass die Datenerhebung auch in Zukunft hauptsächlich bei den Betroffenen erfolgen werden wird. Sollte dies nicht der Fall sein, sind diese im Übrigen auch nicht rechtlos, wie sich aus § 64 ergibt.

Stattdessen wird eine neue Vorschrift an dieser Stelle eingefügt, die eine spezielle Befugnis zum Auslesen unzulässig in die Einrichtungen eingebrachter Datenträger darstellt. Eine spezielle Ermächtigung hierfür ist sinnvoll und erforderlich, da die unkontrollierte Kommunikation über Speichermedien eine erhebliche Gefährdung der Sicherheit oder Ordnung der Einrichtungen darstellt. Die Neuregelung erfolgt im Rahmen der datenschutzrechtlichen Bestimmungen, da damit gerechnet werden kann, dass die entsprechenden Speichermedien aufgrund ihrer Bestimmung zur Kommunikation zahlreiche personenbezogene Daten, auch solche besonderer Kategorien, enthalten.

In diesem Zusammenhang ist aus Gründen des Verhältnismäßigkeitsgrundsatzes zu differenzieren, dass nicht jeder Datenspeicher auszulesen ist, sondern nur dann, wenn konkrete Anhaltspunkte für eine Gefährdung hierdurch sprechen. Solche konkreten Anhaltspunkte werden dann regelmäßig vorliegen, wenn Hinweise für ein heimliches Verbringen des Datenspeichers in die Einrichtung sprechen, z.B. dessen Auffinden im Zimmer eines Sicherungsverwahrten. Anders dürfte die Lage z.B. zu beurteilen sein, wenn Kommunikationssysteme als notwendiger Bestandteil z.B. von Baugeräten im Rahmen von Baumaßnahmen in eine Einrichtung verbracht werden, ohne dass das Baugerät hierauf gezielt kontrolliert wurde.

Die Regelung orientiert sich im Wesentlichen an § 23 des rheinland-pfälzischen Landesjustizvollzugsdatenschutzgesetzes, zuletzt geändert durch § 44 des Gesetzes vom 6. Oktober 2015 (GVBl. S. 354). Diese Vorschrift lautet in ihrer derzeitigen Fassung wie folgt:

"§ 23
Auslesen von Datenspeichern

(1) Elektronische Datenspeicher sowie elektronische Geräte mit Datenspeicher, die ohne Erlaubnis in die Einrichtung eingebracht wurden, dürfen auf schriftliche Anordnung der Einrichtungsleiterin oder des Einrichtungsleiters ausgelesen werden, soweit konkrete Anhaltspunkte die Annahme rechtfertigen, dass dies für die Erfüllung der Aufgaben des Vollzugs erforderlich ist. Die Gründe sind in der Anordnung festzuhalten. Sind die Betroffenen bekannt, sind ihnen die Gründe vor dem Auslesen mitzuteilen. Beim Auslesen sind ihre schutzwürdigen Interessen zu berücksichtigen, insbesondere der Kernbereich privater Lebensgestaltung. Das Auslesen ist möglichst auf die Inhalte zu beschränken, die zur Erreichung der die Anordnung begründenden Zwecke erforderlich sind.

(2) Die nach Absatz 1 erhobenen Daten dürfen verarbeitet werden, soweit dies aus den in der Anordnung genannten Gründen erforderlich ist. Aus anderen Gründen ist die Verarbeitung der Daten nur zulässig, soweit dies für die Erfüllung der Aufgaben des Vollzugs zwingend erforderlich ist und schutzwürdige Interessen der Betroffenen dem nicht entgegenstehen.

(3) Die Verarbeitung der nach Absatz 1 erhobenen Daten ist unzulässig, soweit sie dem Kernbereich der privaten Lebensgestaltung Gefangener oder Dritter unterfallen. Diese Daten sind unverzüglich zu löschen. Die Tatsachen der Erfassung und der Löschung der Daten sind zu dokumentieren. Die Dokumentation darf ausschließlich für Zwecke der Datenschutzkontrolle verwendet werden. Sie ist zu löschen, wenn sie für diese Zwecke nicht mehr erforderlich ist, spätestens jedoch am Ende des Kalenderjahres, das dem Jahr der Dokumentation folgt.

(4) Die Gefangenen sind bei der Aufnahme über die Möglichkeit des Auslesens von nicht gestatteten Datenspeichern zu belehren."

Ein besonderer Hinweis auf die Berücksichtigung schutzwürdiger Interessen und eine Beschränkung auf die Inhalte, die zur Erreichung der die Anordnung begründenden Zwecke erforderlich sind, ist indes nicht erforderlich, da dies durch die allgemeine Bestimmung in § 58 Abs. 1 bzw. die Beschränkung innerhalb der Vorschrift "soweit" bereits abgedeckt wird. In Hinblick auf die Möglichkeit, dass die auszulesenden Datenträger auch besondere Kategorien personenbezogener Daten enthalten können, sollte von der Maßnahme nur bei unbedingter Erforderlichkeit Gebrauch gemacht werden. Ebenfalls nicht notwendig ist eine Beschränkung der Verarbeitung auf die Zwecke ihrer Erhebung, da dies ebenfalls durch § 58 Abs. 1 und 2 abgedeckt ist. Einer besonderen Löschungsbestimmung bedarf es nicht, diese ist durch die Neuregelung in § 65 Abs. 2 erfasst.

Zu § 60

Zu Abs. 1
Zunächst waren die Bestimmungen über die Verarbeitung personenbezogener Daten zu anderen Zwecken, als zu denen, für die sie erhoben wurden, an die entsprechenden Bestimmungen des HDSIG-E anzupassen, d.h. an dessen §§ 20 bis 27 und 44 bis 45. Danach Art. 9 der Richtlinie (EU) Nr. 2016/680 auch für Justizvollzugsbehörden der Anwendungsbereich der Verordnung (EU) Nr. 2016/679 eröffnet sein kann, war insoweit auch auf die Normen zu deren Umsetzung abzustellen.

Soweit darüber hinaus in einer Aufzählung nurmehr besondere Regelbeispiele ("insbesondere") für eine Datenverarbeitung zu namentlich genannten Zwecken genannt werden, ist dies wie folgt zu begründen:

Die neue Nr. 1 stellt die Umsetzung von Art. 4 Abs. 2 der Richtlinie (EU) Nr. 2016/680 dar. Die bisherige Nr. 1 wird Nr. 2. Die bisherige Nr. 2 kann gestrichen werden, da sie in der neuen Nr. 1 aufgeht. Die Nennung von Nr. 3 bis 5 wäre über die neue Nr. 1 erfasst. Eine Streichung der vorgenannten Vorschriften könnte aber eine erhebliche Rechtsunklarheit in der Praxis auslösen, da durch die Verweisung auf allgemeine Bestimmungen die Rechtsanwendung nicht nur vereinfacht wird. Eine entsprechende Unklarheit sollte im Sinne einer effizienten Rechtshandhabung - auch im Sinne der Betroffenen - vermieden werden. Insoweit erscheint es sinnvoll, den bisherigen Katalog trotz seiner deklaratorischen Natur weitestgehend beizubehalten.

Dies gilt im Ergebnis und mit derselben Begründung auch für die übrigen Nr. 6 bis 12, zu deren Zweck die Verarbeitung anderweitig erhobener personenbezogener Daten jedenfalls nach Art. 9 Abs. 1 Satz 2 der Richtlinie (EU) Nr. 2016/680 i.V.m. Art. 9 Abs. 2 der Verordnung (EU) Nr. 2016/679 zulässig ist, was wiederum über die Verweisung auf § 22 HDSIG-E abgedeckt wird. Auch insoweit soll jedoch Rechtsunklarheit in der Praxis vermieden werden, sodass es geboten erscheint, die bisherigen Tatbestände als Regelbeispiele ebenfalls beizubehalten.

Die Einführung des Erfordernisses der unbedingten Erforderlichkeit bei besonderen Kategorien personenbezogener Daten trägt insoweit § 43 Abs. 1 HDSIG-E Rechnung und betrifft z.B. Maßnahmen nach § 25 Abs. 3.

Zu Abs. 2
Die Vorschrift dient dem besonderen Schutz von Daten, die bei besonders erheblichen Eingriffen in Grundrechte anfallen.

Das Telekommunikationsgeheimnis steht den bisherigen Ausnahmetatbeständen insoweit gleich, weshalb die Überwachung der Telekommunikation (vgl. § 36) und das Auslesen von Datenspeichern (vgl. § 59) in Satz 1 ebenfalls aufgeführt werden. Entsprechend der systematischen Bedeutung der Vorschrift wird in Satz 1 wie für Abs. 1 klargestellt, dass die Regelung für Datenverarbeitungen gilt, die über die reine Erfassung und Speicherung hinausgehen, insbesondere für die Übermittlung.

Die Gründe, aus denen bei den entsprechenden sensiblen Daten eine Weiterverarbeitung weiterhin möglich sein soll, werden nunmehr unter Nr. 1 bis 3 aufgezählt.

Nr. 1 erweitert den bisherigen Regelungsgehalt auf andere Zwecke, wie sie in § 40 HDSIG-E vorgesehen werden.

Nr. 2 entspricht der bisherigen Verweisung auf § 12 Abs. 2 Nr. 1 des derzeit noch geltenden Hessischen Datenschutzgesetzes; insoweit war klarzustellen, dass die Befugnis zur Verarbeitung auch aus Normen des Hessischen Strafvollzugsgesetzes folgen kann. Die übrigen Verweisungen auf das derzeit noch geltende Hessische Datenschutzgesetz werden obsolet; der bisherige Verweis auf § 12 Abs. 2 Nr. 3 und 4 des Hessischen Datenschutzgesetzes erübrigt sich durch die Verweisung auf Abs. 1 Nr. 1 neuer Fassung.

Nr. 3 stellt insoweit einen Auffangtatbestand dar, der jedoch beibehalten werden sollte, um die Praxis bei der bisherigen Rechtsanwendung fortzuführen. Die bisherige Nr. 3 - die Einwilligung - wurde wegen der besonderen Problematik dieser Rechtsgrundlage im Geltungsbereich der Richtlinie (EU) Nr. 2016/680 gestrichen.

Darüber hinaus soll die Weiterverarbeitung, insbesondere die Übermittlung, nur bei unbedingter Erforderlichkeit vorgenommen werden, wie dies in Satz 1 eingefügt wurde. Das Bundesverfassungsgericht hat in seinem Urteil vom 20. April 2016, Aktenzeichen 1 BvR 966/09 und 1BvR 1140/09 in Hinblick auf das BKAG in der damals geltenden Fassung ausgeführt, dass die Verhältnismäßigkeit eines Eingriffs von dessen Intensität abhängt und angemessen ausgestaltet sein muss. Je tiefer Überwachungsmaßnahmen in das Privatleben eingreifen, desto strenger sind die Anforderungen, was insbesondere für die Wohnraumüberwachung und den Zugriff auf informationstechnische Systeme gilt. Die in der Entscheidung zu beurteilenden Sachverhalte betrafen zwar verdeckte Datenverarbeitungen, während die im Hessischen Sicherungsverwahrungsvollzugsgesetz vorgesehenen Maßnahmen regelmäßig nicht verdeckt erfolgen, was insbesondere durch die Offenlegung von Überwachungsmaßnahmen gilt. Auch stellt insbesondere der Haftraum, dann konsequenterweise auch die Zimmer des Sicherungsverwahrten keine Wohnung i.S.d. Art. 13 GG dar (vgl. BVerfG NJW 1996, 2643). Schließlich müssen bei den Eingriffen nicht notwendigerweise auch besondere Kategorien personenbezogener Daten geschützt werden. Dennoch erscheinen vor diesem Hintergrund die aufgeführten Daten besonders schützenswert - nachdem es sich zwar um offene, aber tiefe Eingriffe in die Kommunikation handelt - sodass ihre Weitergabe nur zu eingeschränkten Zwecken und im Fall der unbedingten Erforderlichkeit erfolgen sollte. Durch diese Beschränkung wird sichergestellt, dass insbesondere die Übermittlung der entsprechenden Daten nur zu Zwecken erfolgt, für die sie selbst hätten erhoben werden können (Grundsatz der hypothetischen Datenneuerhebung).

Um im Falle ihrer Übermittlung sicherzustellen, dass die entsprechenden Daten mit der erforderlichen Sensibilität behandelt werden, sind sie entsprechend dem neu eingefügten Satz 2 eindeutig zu kennzeichnen.

Es wird ferner klargestellt, dass § 4 Abs. 3 Satz 2 HDSIG-E unberührt bleibt. Diese Vorschrift regelt den Sonderfall einer Übermittlung von Videoaufzeichnungen, die bei der Überwachung öffentlich zugänglicher Räume angefallen sind.

Zu Abs. 3
Es handelt sich insoweit um Sonderfälle des Abs. 1.

Der neue Verweis in Satz 1 auf Abs. 1 ist insoweit zwar auch wegen der §§ 22 und 44 HDSIG-E nur deklaratorisch, jedoch sollte auch insoweit eine Rechtsunsicherheit in der Praxis durch eine Streichung der Bestimmung vermieden werden.

Zu Abs. 5
Der neue Hinweis in Satz 3 a.E. an jeden Empfänger, was die Einstufung besonderer Kategorien personenbezogener Daten angeht, entspricht insbesondere der Pflicht zur Schaffung geeigneter Garantien nach § 43 Abs. 2 Nr. 8 HDSIG-E im Falle der Übermittlung besonderer Kategorien personenbezogener Daten, die wiederum auf Art. 10 Richtlinie (EU) Nr. 2016/680 zurückgeht.

Zu Abs. 6
Die Nennung der Gerichtszuständigkeit wurde an die Neufassung des Kataloges in Abs. 1 angepasst; desgleichen der Verweis auf die Vorschriften in § 65.

Zu § 61

Zu Abs. 1
Der Schutzbereich der Vorschrift in Satz 1 wurde auf alle besonderen Kategorien personenbezogener Daten nach § 41 Nr. 15 HDSIG-E erweitert. Die Erweiterung des Schutzes für alle besonderen Kategorien personenbezogener Daten trägt dessen § 43 Abs. 2 Rechnung. Weitere Schutzvorschriften enthalten insoweit § 58 Abs. 2 und § 60 Abs. 1.

Zu Abs. 2
Die Verwendung des Begriffs "unbedingt erforderlich" in Satz 2 statt bisher "unerlässlich" stellt auf die Terminologie in § 43 Abs. 1 HDSIG-E ab. Passend zu Satz 2 wird in Satz 3 ebenfalls auf den Begriff der "Offenbarung" abgestellt.

Zu Abs. 3
Die Vorschrift betrifft die Weitergabe von Informationen, die von externen Dienstleistern nicht unmittelbar zu Vollzugszwecken - sondern primär zum Zwecke der Behandlung - erhoben, aber zu Zwecken des Vollzuges weitergegeben werden. Insoweit ist der Anwendungsbereich der Verordnung (EU) Nr. 2016/679 eröffnet.

Redaktionell wird ferner in Satz 2 klargestellt, dass die vorgenannten Personen lediglich zu einer Offenbarung befugt sind.

Zu Abs. 5
Der Terminus "unerlässlich" wurde an den Begriff "unbedingt erforderlich" angepasst.

Zu Nr. 8 (§ 62)
Das entsprechende Verfahren ist nunmehr in § 58 HDSIG-E geregelt, sodass die Verweisung entsprechend anzupassen war.

Zu Nr. 9 (§§ 63 bis 65)

Zu Abs. 1
Die Bestimmung ist neu eingeführt.

Die Sätze 1, 2 und 4 geben insoweit die Bestimmung von § 48 HDSIG-E wieder. Die Wiedergabe erfolgt, weil der Hinweis in Satz 3 sonst nicht ohne weiteres aus sich heraus verständlich wäre.

Der gesonderte Hinweis nach Satz 3 entspricht insoweit dem Regelungsgehalt von § 43 Abs. 2 Satz 2 Nr. 3 HDSIG-E für die Sicherung besonderer Kategorien personenbezogener Daten, ist jedoch aufgrund der besonderen datenschutzrechtlichen Sensibilität der weiteren aufgeführten Arten von Daten erforderlich.

Zu Abs. 2
Entsprechend der Einführung eines neuen Abs. 1 ist der bisherige Inhalt von § 63 HSVVollzG als Abs. 2 zu bezeichnen. Die Verweisung auf die Vorschrift des bisherigen § 10 HDSG in Satz 1 war an § 59 HDSIG-E entsprechend anzupassen.

Zu § 64
Die Vorschrift wird komplett neu gefasst.

In die Überschrift wurde der Begriff der Information aufgenommen, da dies der Terminologie des HDSIG-E entspricht, vgl. dort § 50.

Entsprechend der Formulierungen des HDSIG-E wird auf dessen §§ 50 bis 52 verwiesen, soweit die Datenverarbeitung zu Zwecken der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung und des Strafvollzuges, einschließlich des Schutzes vor und der Abwehr von Gefahren für die öffentliche Sicherheit erfolgt; im Übrigen auf dessen §§ 31 bis 33. Die Zweiteilung der Informations- und Auskunftsrechte folgt aus der nicht-ausschließlichen Anwendbarkeit von Richtlinie (EU) Nr. 2016/680 und Verordnung (EU) Nr. 2016/679 im Bereich des Hessischen Justizvollzugs. Dabei erscheint es sinnvoll, den Untergebrachten bei Aufnahme z.B. ein entsprechendes Formblatt als Information zu Datenverarbeitungen auszuhändigen - § 8 Abs. 1 sieht insoweit die Information über Rechte und Pflichten vor - und dgl. Besuchern bei Betreten der Anstalt.

Zur Gewährung eines effektiven Rechtsschutzes wird im neuen Satz 2 die Möglichkeit einer Akteneinsicht beibehalten und auf das im Rahmen des Erforderlichen erweitert werden. Insbesondere bei Einsichtnahmen in Gesundheitsakten wird hierbei großzügig zu verfahren sein, vgl. BVerfG, Beschluss der 2. Kammer des Zweiten Senats vom 20. Dezember 2016 - 2 BvR 1541/15.

Zu § 65
Die Vorschrift wird weitestgehend neu gefasst.

Zur Überschrift
Der Begriff "Sperrung" wurde durch den Begriff "Einschränkung der Verarbeitung" ersetzt.

Nach der Systematik des HDSIG-E kann, vgl. dort § 53 Abs. 3, an Stelle einer Löschung von personenbezogenen Daten bei diesen eine Einschränkung der Verarbeitung vorgenommen werden. Nach § 41 Nr. 3 HDSIG-E ist hierunter "die Markierung gespeicherter personenbezogener Daten mit dem Ziel, ihre künftige Verarbeitung einzuschränken" zu verstehen.

Nach der bisherigen Systematik, vgl. § 65 Abs. 1 HSVVollzG in seiner jetzigen Fassung, sind personenbezogene Daten auch jetzt schon unverzüglich zu löschen, sobald feststeht, dass ihre Speicherung nicht mehr erforderlich ist, um die Zwecke zu erfüllen, für die sie erhoben worden sind oder für die sie nach § 13 Abs. 2 und 4 HDSG weiterverarbeitet werden dürfen; wenn bei der Speicherung nicht absehbar ist, wie lange die Daten benötigt werden, ist nach einer aufgrund der Erfahrung zu bestimmenden Frist zu prüfen, ob die Erforderlichkeit der Speicherung noch besteht, vgl. § 19 Abs. 3 HDSG in seiner jetzigen Fassung.

Grundsätzlich sollte für die zukünftige Rechtslage - wie bisher auch - zwischen besonders sensiblen Daten, Daten in Untergebrachtenakten und -dateien und sonstigen Daten hinsichtlich der Frage ihrer Löschung oder - an deren Stelle - der Einschränkung ihrer Verarbeitung unterschieden werden.

Zu Abs. 1
Der Absatz entspricht in seinem Regelungsgehalt dem bisherigen Abs. 1. Es wurde der Begriff "in der Verarbeitung einzuschränken" anstelle der bisherigen Sperrung verwendet und auf die einschlägigen Bestimmungen des HDSIG-E verwiesen, je nachdem, ob die Verarbeitung zu den Zwecken nach § 40 HDSIG-E erfolgt oder nicht.

Zu Abs. 2
Abs. 2 befasst sich entsprechend der bisherigen Systematik mit der Verfahrensweise bei personenbezogenen Daten, die aufgrund besonders intensiver Eingriffe erhoben wurden. Insoweit liegt hierin eine Konkretisierung auch von § 4 Abs. 4 HDSIG-E.

In Satz 1 wurden Ergebnisse von Maßnahmen nach § 59 den Videoaufnahmen gleichgestellt, da insoweit ein gleiches Maß an Schutzwürdigkeit gegeben ist. Ebenfalls wird klargestellt, dass eine Löschung nur dann nicht erfolgt, wenn zum Zeitpunkt der Entscheidung über die Löschung zu konkreten Beweiszwecken die weitere Aufbewahrung bei gleichzeitiger Einschränkung der Verarbeitung unbedingt erforderlich ist; insoweit ist eine Angleichung an die Terminologie der Bestimmungen des HDSIG-E vorgenommen worden, was die Verarbeitung von besonderen Kategorien personenbezogener Daten angeht.

Im neu eingeführten Satz 2 wird eine verkürzte Frist zur Löschung von Daten eingeführt, die entgegen dem Grundsatz verarbeitet, insbesondere erhoben wurden, dass der Kernbereich der Lebensgestaltung nicht zum Gegenstand der Verarbeitung personenbezogener Daten gemacht werden darf. Dies trägt der besonderen Schutzwürdigkeit der Betroffenen in diesem Fall Rechnung.

Der ebenfalls neu eingeführte Satz 3 statuiert insoweit eine Dokumentationspflicht zur kontrollierbaren Löschung der in Satz 1 und 2 aufgeführten, besonders sensiblen Daten, vgl. BVerfGE 274 S. 337ff. [S. 339]).

Zu Abs. 3
Die Vorschrift befasst sich mit der Löschung von personenbezogenen Daten und differenziert hierbei zwischen Akten und Dateien der Untergebrachten und sonstigen Akten und Dateien. Dabei ist eine Gleichbehandlung von Dateien im Sinne einer elektronischen Datei mit einer Papierakte geboten, da auch eine ordnungsgemäß geführte Untergebrachtenpersonalakte regelmäßig ein Dateisystem im datenschutzrechtlichen Sinne darstellen wird (vgl. zum Begriff Gola DS-GVO Art. 4 Rd.-Nr. 46). Die Vorschrift orientiert sich insoweit an der Struktur des Abs. 3 Satz 1 in der derzeit geltenden Fassung, wobei aber entsprechend der Systematik der Richtlinie (EU) Nr. 2016/680 statt einer grundsätzlichen Sperrung der Daten jetzt vorrangig deren Löschung zu erfolgen hat.

In Satz 1 wird zunächst redaktionell klargestellt, dass der Abs. 3 sich - wie Abs. 1 und 2 - auf personenbezogene Daten bezieht. § 53 Abs. 2 HDSIG-E sieht in Umsetzung von Art. 16 der Richtlinie (EU) Nr. 2016/680 die Löschung vor, wenn die Kenntnis der Daten für die Aufgabenerfüllung nicht mehr erforderlich ist. Das ist grundsätzlich dann der Fall, wenn Untergebrachte endgültig entlassen werden. Dies ist jedoch nicht der Fall, sofern die begonnene Unterbringung wiederaufgenommen werden kann - insbesondere bei Aussetzung zur Bewährung. Entsprechend ist der Einrichtung eine Frist für die Löschung der personenbezogenen Daten jedenfalls bis zum Ende einer möglichen Führungsaufsicht im Anschluss an die Aussetzung der Sicherungsverwahrung zur Bewährung einzuräumen. Wird die Sicherungsverwahrung zur Bewährung ausgesetzt, schließt sich die Führungsaufsicht an, die im Regelfall bis zu fünf Jahre dauert, § 68c Abs. 1 Satz 1 StGB. Wird die Aussetzung widerrufen, müssen die Daten aus der vorhergehenden Unterbringung dem Justizvollzug zur Verfügung stehen, da das Vollstreckungsverhältnis gerade nicht beendet wurde. Außerdem sollen die gespeicherten Daten gemäß BVerfGE 116, 69-95, Rdnr. 64, der Evaluation des Justizvollzuges dienen. Besteht zum Zeitpunkt des Fristablaufs ein konkreter Anhaltspunkt dafür, dass eine Aufbewahrung von Daten zur Abwicklung des Vollstreckungsverhältnisses weiter erforderlich ist, kann dem durch die weitere Speicherung bei Einschränkung der Verarbeitung nach Abs. 4 Rechnung getragen werden.

Satz 2 ersetzt den bisherigen Abs. 4 der Bestimmung in seiner derzeit geltenden Fassung.

Zu Abs. 4
Der besseren Nachvollziehbarkeit halber sollen die Bestimmungen zur Einschränkung der Verarbeitung personenbezogener Daten in einem eigenen Abs. 4 dargestellt werden. Aus demselben Grund wird in Satz 1 auf die Normen verwiesen, aus denen sich grundsätzlich ergibt, wann und wie die Einschränkung der Verarbeitung zu erfolgen hat.

Anstelle einer Löschung der Daten können diese unter den Voraussetzungen des § 53 Abs. 3 bis 7 HDSIG-E in der Verarbeitung eingeschränkt werden, Satz 1 Nr. 1. Wie in § 53 Abs. 3 HDSIG-E erscheint eine weitergehende Speicherung bei Einschränkung der Verarbeitung zu Beweiszwecken insgesamt sinnvoll. Art. 16 Abs. 3 Satz 1 Buchst. b der Richtlinie (EU) Nr. 2016/680 lässt dies grundsätzlich zu und beschränkt Beweiszwecke nicht ausdrücklich auf den Anwendungsbereich der Richtlinie. Dies deckt auch die Beweiszwecke z.B. auch jenen Konstellationen ab, in denen ein ehemaliger Gefangener Haftungsansprüche gegen das Land geltend macht, z.B. wegen fehlerhafter ärztlicher Behandlung in der Haft. Einen ähnlichen Weg geht insoweit auch § 78 Abs. 2 bzw. 3 des Bundeskriminalamtgesetzes in seiner Neufassung durch das Gesetz zur Neustrukturierung des Bundeskriminalamtgesetzes; dort wird ebenfalls nur von der Aufbewahrung für "gerichtliche Verfahren" bzw. der Behebung "einer Beweisnot" gesprochen, ohne nach der Art des Verfahrens zu differenzieren, in dem die Daten benötigt werden. Sofern eine Einschränkung der Verarbeitung zu Beweiszwecken erfolgt, ist aber darauf zu achten, dass die Entscheidung hierüber grundsätzlich eine Einzelfallentscheidung darstellt und zum Zeitpunkt ihrer Entscheidung konkrete Anhaltspunkte für die Notwendigkeit einer späteren Verwendung vorliegen müssen. Eine abstrakte Vorratsdatenspeicherung ohne konkreten Anlass - der sinnvollerweise zu dokumentieren ist - dürfte unzulässig sein. Anders ist dies bei normierten Dokumentationspflichten zu beurteilen, wie insbesondere z.B. nach § 10 der Berufsordnung für die Ärztinnen und Ärzte in Hessen für die im Rahmen der Freiheitsentziehung erfolgten ärztlichen Maßnahmen; ein hierauf bezogenes Regelbeispiel wurde zur Erleichterung der Rechtspraxis in Nr. 1 aufgeführt.

Satz 1 Nr. 2 stellt insoweit einen Auffangtatbestand dar, soweit Daten nicht im Geltungsbereich der Richtlinie (EU) Nr. 2016/680 gespeichert wurden.

Die Kennzeichnung von in der Verarbeitung eingeschränkten personenbezogenen Daten trägt insbesondere § 53 Abs. 4 HDSIG-E Rechnung. Die in Satz 2 ebenfalls geregelte Heranziehung in der Verarbeitung eingeschränkter personenbezogener Daten, im Regelfall durch Übermittlung, zu anderen Zwecken als des § 40 HDSIG-E, muss den Anforderungen der Verordnung (EU) Nr. 2016/679 genügen (vgl. Art. 9 Abs. 1 und 2 der Richtlinie (EU) Nr. 2016/680; insoweit gestattet Art. 18 Abs. 1 Buchst. a bzw. Buchst. c der Verordnung (EU) Nr. 2016/679 aber auch die Verwertung zu Beweiszwecken). Wie sich aus Art. 9 der Richtlinie (EU) Nr. 2016/680 ergibt, muss die Verarbeitung zu Vollzugszwecken erhobener Daten auch nicht auf den sachlichen Bereich der Richtlinie beschränkt sein.

Satz 3 entspricht dem bisherigen Regelungsgehalt von § 65 Abs. 3 Satz 4 HSVVollzG in seiner jetzigen Fassung. Auch insoweit bleibt eine Einwilligung weiter zulässig: entweder dient die Aufhebung der Einschränkung der Verarbeitung zu Zwecken der Richtlinie (EU) Nr. 2016/680, sodass § 46 HDSIG-E Anwendung findet; oder die Verarbeitung dient anderen Zwecken, sodass über Art. 9 Abs. 1 der Richtlinie (EU) Nr. 2016/680 die Bestimmungen der Verordnung (EU) Nr. 2016/679 gelten.

Satz 4 entspricht dem bisherigen Regelungsgehalt von § 65 Abs. 3 Satz 2 HSVVollzG in seiner jetzigen Fassung.

Zu Abs. 5
Entsprechend § 70 Abs. 4 HDSIG-E wurde eine jährliche Kontrollfrist eingeführt, differenzierend zwischen Untergebrachtendateien und -akten einerseits sowie sonstigen Dateien und Akten andererseits.

Zu Abs. 6
Abs. 6 entspricht im Wesentlichen dem bisherigen Abs. 5 in der derzeit geltenden Fassung. Redaktionell wurde die Herkunft der Daten danach präzisiert, aus welchen Akten etc. sie stammen. Hinsichtlich der Untergebrachtenbücher ist darauf hinzuweisen, dass es sich hierbei um Bestandsverzeichnisse in Buchform handelt, die mittlerweile elektronisch geführt werden. Die Aufbewahrungsfristen beziehen sich daher im Wesentlichen auf Altfälle, die sich bereits in der Aufbewahrung befinden.

In Satz 4 wurde die Verweisung auf das Hessische Archivgesetz in eine dynamische Verweisung umgewandelt, um zukünftige Änderungen abzubilden.

Zu Nr. 10 (§ 66)

Zu Buchst. a
In Satz 2 wurde ergänzend eingefügt, dass die Ergebnisse dem öffentlichen Interesse dienen, um den Maßgaben von § 45 HDSIG-E zu entsprechen.

Zu Buchst. b
Der Verweis auf § 476 StPO ist dahin gehend zu aktualisieren, dass er den Anforderungen an eine Verarbeitung besonderer Kategorien personenbezogener Daten gemäß § 43 Abs. 1 HDSIG-E Rechnung trägt (Nr. 2), sodass eine Übermittlung nur bei unbedingter Erforderlichkeit möglich ist.

Zu Art. 6 (Änderung des Hessischen Jugendarrestvollzugsgesetzes)

Allgemeines
Auf den Vollzug von Jugendarrest findet ebenfalls grundsätzlich die Richtlinie (EU) Nr. 2016/680 des Europäischen Parlamentes und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zweck der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung sowie zum freien Datenverkehr und zur Aufhebung des Rahmenbeschlusses 2008/977/JI des Rates Anwendung. Insoweit wird auf die Vorbemerkung zur Begründung zur Änderung des Hessischen Jugendstrafvollzugsgesetzes Bezug genommen.

Hinsichtlich der datenschutzrechtlichen Bestimmungen wird in § 38 weitestgehend auf die Bestimmungen des Hessischen Jugendstrafvollzuges verwiesen.

Zu Nr. 1 (§ 19)
In Hinblick auf Abs. 2 Satz 1 ist in Anlehnung an die übrigen Vollzugsgesetze klar- bzw. festzustellen, dass - wie bei anderen Eingriffsnormen des Gesetzes - ein Tätigwerden auch zum Zweck der Ordnung der Anstalt möglich ist.

In Satz 3 wurde zunächst klargestellt, dass Abs. 3 Ausnahmeregelungen enthält; als neuer zweiter Halbsatz wurde eine Regelung zu Satz 3 hinzugefügt, wonach sich die Überwachung sowohl auf die Jugendlichen wie Besucher bezieht - dies dient der Klarstellung im Sinne von § 67 HDSIG-E.

Im neuen Satz 4 wird klargestellt, dass die Überwachung von Besuchen und Telefongesprächen, sofern sie besondere Kategorien personenbezogener Daten zum Gegenstand hat, nur noch im Falle unbedingter Erforderlichkeit erfolgt, um den Anforderungen aus § 43 Abs. 1 HDSIG-E bzw. Art. 10 der Richtlinie (EU) Nr. 2016/680 Rechnung zu tragen. Der Begriff der "unbedingten Erforderlichkeit" ist hierbei zu verstehen wie in der Begründung zu § 33 Abs. 4 HJStVollzG-E ausgeführt; auf die dortigen Ausführungen wird insoweit verwiesen. Sind die Gründe einer Überwachung nach Satz 3 gegeben, wird das Kriterium der unbedingten Erforderlichkeit regelmäßig erfüllt sein, da die Wahrung von Sicherheit oder Ordnung der Einrichtung unverzichtbar sind.

Im jetzigen Satz 7 wird die Überwachung durch optisch-elektronische Einrichtungen eingeführt und diese als Videoüberwachung legaldefiniert. Auch insoweit wird darauf hingewiesen, dass die Videoüberwachung besonders geneigt ist, besondere Kategorien personenbezogener Daten zu generieren. Für diese Form der Überwachung ist daher der neue Satz 4 einschlägig.

Zu Nr. 2 (§ 26)

Zu Buchst. a
Es wird - auch im Sinne einer einheitlichen Terminologie - in Nr. 2 klargestellt, dass die technischen Hilfsmittel auch optisch-elektronische Einrichtungen (Videoüberwachung) umfassen. Da diese regelmäßig biometrische Daten, aber auch Gesundheitsdaten liefern können und somit besondere Kategorien personenbezogener Daten, ist nach § 43 Abs. 1 HDSIG-E vorgesehen, dass die entsprechende Verarbeitung nur im Falle unbedingter Erforderlichkeit zulässig erfolgt. Da die entsprechende Kontrolle für die Information des Gesundheitszustandes des Jugendlichen unverzichtbar ist, wird das Kriterium der unbedingten Erforderlichkeit regelmäßig erfüllt sein.
Insoweit wird ebenfalls klargestellt, dass die Videoüberwachung nur zu Zwecken des Abs. 1 durchgeführt werden darf.

Zu Buchst. b
Da die dauerhafte Überwachung nach Abs. 2 Nr. 2 regelmäßig Gesundheitsdaten liefern wird und somit besondere Kategorien personenbezogener Daten, ist in Satz 2 klargestellt, dass die Aufzeichnung nur im Falle unbedingter Erforderlichkeit im Sinne von § 43 Abs. 1 HDSIG-E zulässig ist. Auch hier gilt, dass, da die entsprechende Kontrolle für die Information des Gesundheitszustandes des Jugendlichen unverzichtbar ist, das Kriterium der unbedingten Erforderlichkeit regelmäßig erfüllt sein wird.

Zu Nr. 3 (§ 27)
In Abs. 1 S. 1 wird die Änderung des HJStVollzG durch das vorliegende Gesetz aufgenommen.

Zu Nr. 4 (§§ 37, 38)

Zu § 37

Zu Abs. 1
Die Vorschrift wurde weitgehend an § 69 Abs. 1 HStVollzG-E angeglichen. Insbesondere wurde in Satz 2 ergänzend eingefügt, dass die Ergebnisse dem öffentlichen Interesse dienen, um den Maßgaben von § 45 HDSIG-E zu entsprechen.

Zu Abs. 2
Der Verweis auf § 476 StPO ist dahin gehend zu aktualisieren, dass er den Anforderungen an eine Verarbeitung besonderer Kategorien personenbezogener Daten gemäß § 43 Abs. 1 HDSIG-E Rechnung trägt (Nr. 2), sodass eine Übermittlung nur bei unbedingter Erforderlichkeit möglich ist.

Zu § 38
§ 38 wird dahin gehend geändert, dass der Verweis auf die frühere Sperrfrist in § 65 Abs. 1 Satz 1 HJStVollzG (richtigerweise Abs. 3 S. 1) in einen solchen auf die Löschungsfrist nach § 65 Abs. 3 Satz 1 HJStVollzG umgewandelt wird. Darüber hinaus wird im Wege einer dynamischen Verweisung klargestellt, dass auf die Bestimmungen des HJStVollzG in seiner jeweils geltenden Fassung verwiesen wird.

Zu Art. 7 (Änderung des Hessischen Justizkostengesetzes)

Zu Nr. 1
Abs. 2 Nr. 1 Buchst. c ist aufgrund der auf Bundesebene vorgenommenen Anpassungen an die Vorgaben der Verordnung (EU) Nr. 2016/679 und der damit einhergehenden Aufhebung des § 10 Abs. 4 des Bundesdatenschutzgesetzes in der Fassung der Bekanntmachung vom 14. Januar 2003 (BGBl. I S. 66), zuletzt geändert durch Gesetz vom 14. August 2009 (BGBl. I S. 2814), obsolet geworden.

Zu Nr. 2
Aufgrund der Neufassung des Hessischen Datenschutz- und Informationsfreiheitsgesetzes wird der Verweis auf dieses Gesetz entsprechend angepasst.

Zu Nr. 3
Die Begrifflichkeit in Abs. 6 Satz 3 ist entsprechend Art. 4 Nr. 3 der Verordnung (EU) Nr. 2016/679 anzupassen.

Zu Art. 8 (Änderung der Hessischen Landeshaushaltsordnung)

§ 95 der Hessischen Landeshaushaltsordnung (LHO) erfüllt die Anforderungen der Verordnung (EU) Nr. 2016/679 und insbesondere die des dortigen Art. 6. Danach ist die Verarbeitung personenbezogener Daten rechtmäßig für die Wahrnehmung einer Aufgabe, die im öffentlichen Interesse liegt oder in Ausübung öffentlicher Gewalt erfolgt (Art. 6 Abs. 1 Buchst. e (EU) Nr. 2016/679), wobei die Rechtsgrundlage sich aus dem nationalen Recht (hier: § 95 LHO) ergeben kann (Art. 6 Abs. 3 Buchst. b der Verordnung (EU) Nr. 2016/679).

Mit der Ergänzung erhält die nationale Rechtsgrundlage des § 95 LHO künftig eine Regelung im Sinne des Art. 6 Abs. 3 Satz 3 der Verordnung (EU) Nr. 2016/679 ("..., welche Arten von Daten verarbeitet werden, ... und welche Verarbeitungsvorgänge und -verfahren angewendet werden dürfen, ..."). Hierdurch wird für die Prüfungstätigkeit des Hessischen Rechnungshofs klargestellt, dass er Zugang zu solchen elektronisch gespeicherten Informationen hat. Zu den Verarbeitungsverfahren zählt ausdrücklich auch der automatisierte Abruf von Daten.

Zu Art. 9 (Änderung des Gesetzes über die Hessische Steuerberaterversorgung)

Es handelt sich um eine redaktionelle Anpassung des § 11 Satz 2 Nr. 5 des Gesetzes über die Hessische Steuerberaterversorgung (StBVG). Es wird der dortige Widerspruch bezüglich des Verweises auf § 6 Abs. 3 StBVG behoben, da es Abs. 3 in § 6 StBVG nicht gibt und somit der Verweis darauf ins Leere geht. Auslegungsprobleme, mithin Rechtsunsicherheiten auf Seiten der Betroffenen werden künftig vermieden.

Die generelle und für die Leistungsfestsetzung entscheidende Auskunftspflicht der Mitglieder, der sonstigen Leistungsempfänger und der Steuerberaterkammer Hessen gegenüber dem Versorgungswerk ergibt sich aus § 12 StBVG. Die Vorschrift entspricht den Vorgaben der Verordnung (EU) Nr. 2016/679. Die Verarbeitung personenbezogener Daten ist nach Art. 6 der Ver-

ordnung (EU) Nr. 2016/679 rechtmäßig für die Wahrnehmung einer Aufgabe, die im öffentlichen Interesse liegt oder in Ausübung öffentlicher Gewalt erfolgt (Art. 6 Abs. 1 Buchst. e der Verordnung (EU) Nr. 2016/679); die Rechtsgrundlage kann sich dabei aus dem nationalen Recht ergeben (Art. 6 Abs. 3 Buchst. b der Verordnung (EU) Nr. 2016/679).

Nach § 11 Satz 2 Nr. 5 StBVG-E wird alles Weitere dazu durch die Satzung des Versorgungswerks der Steuerberater in Hessen vom 11. Februar 2002 (StAnz. S. 707), zuletzt geändert am 11. September 2013 (StAnz. S. 1262), geregelt.

Zu Art. 10 (Änderung des Hessischen Ingenieurgesetzes)

Zur Klarstellung, dass die Staatsaufsicht das unmittelbar geltende EU-Recht inhaltlich mitumfasst, wird dieses ausdrücklich benannt. Mit der Formulierung erfolgt eine Anpassung an § 19 Abs. 1 Satz 2 des Hessischen Architekten- und Stadtplanergesetzes (HASG) vom 30. November 2015 (GVBl. S. 457, 478).

Zu Art. 11 (Änderung des Hessischen Straßengesetzes)

Die bisherige Regelung erlaubt dem Vorhabenträger, in den auszulegenden Planunterlagen die betroffenen Grundstückseigentümer mit vollem Namen und Anschrift aufzuführen. Diese Regelung diente dazu, den Betroffenen die Erkennbarkeit ihrer Beeinträchtigung zu erleichtern. Sie wurde bisher vor dem Hintergrund, dass die Auslegung der Planunterlagen räumlich und zeitlich begrenzt erfolgte und die Planunterlagen somit nur einem begrenzten Personenkreis zugänglich waren, als datenschutzrechtlich zulässig angesehen. Aufgrund der zuletzt erfolgten Änderungen des Hessischen Verwaltungsverfahrensgesetzes (Gesetz zur Änderung des Hessischen Verwaltungsverfahrensgesetzes und anderer Vorschriften vom 26. Juni 2015 [GVBl. S. 254]) und der damit erfolgten Einführung des § 27a HVwVfG, der eine Veröffentlichung der Planunterlagen auch im Internet vorschreibt, wären die Daten der Betroffenen nunmehr für jedermann frei und zeitlich unbefristet zugänglich. Vor dem Hintergrund dieser neuen rechtlichen Situation und des in der Verordnung (EU) 2016/679 enthaltenen Gebots einer möglichst schonenden Verarbeitung personenbezogener Daten ist es erforderlich, die Namen und Adressdaten zukünftig durchgehend zu anonymisieren, was bereits heute häufig der gängigen Praxis entspricht. Dementsprechend wird durch die Änderung des § 33 Abs. 2 zukünftig von der ausdrücklichen Nennung der Namen und Anschriften der Grundstückseigentümer als notwendige Bestandteile des Planes abgesehen. Mit der Streichung des § 33 Abs. 2 Satz 1, 2. Halbs. entfällt auch die Notwendigkeit der Erweiterung des Anwendungsbereichs des Satzes 1 auf Planfeststellungsverfahren für Bundesfernstraßen durch Satz 2. Er ist als überflüssig zu streichen.

Zu Art. 12 (Änderung des Hessischen Gesetzes über den Bau und die Finanzierung öffentlicher Straßen durch Private)

Der Verweis auf das HDSG in § 9 Abs. 5 ist anzupassen. Das Nebeneinander der Bußgeldvorschriften in § 13 Abs. 1 Nr. 2 und 3 und Art. 83 der Verordnung (EU) Nr. 2016/679 ist wegen unerwünschter bzw. unzulässiger Doppelung zu beseitigen.

Zu Art. 13 (Änderung des Hessischen Schulgesetzes)

Zu Nr. 1 (§ 83)
Die Verarbeitung personenbezogener Daten im Rahmen von Evaluationen bzw. wissenschaftlicher Forschung ist künftig nur unter den Voraussetzungen der Verordnung (EU) Nr. 2016/679 und des HDSIG-E möglich, ohne dass es hierzu eines ausdrücklichen Anwendungsbefehls bedürfte. § 83 Abs. 4 Satz 5 des Hessischen Schulgesetzes (HSchG) ist daher zu streichen.

Zu Nr. 2 (§ 84)
Die genannten Vorschriften des HDSG sind nach dessen anstehender Neufassung nicht mehr einschlägig und es bedarf aufgrund der Bestimmung des § 1 Abs. 2 HDSIG-E keines Verweises auf das insoweit zur Anwendung kommende HDSIG-E. § 84 Abs. 2 Satz 6 HSchG ist daher zu streichen.

Zu Art. 14 (Änderung des Hessischen Pressegesetzes)

Allgemeines
Durch das in § 41 Abs. 1 Bundesdatenschutzgesetz (BDSG) in der Fassung der Bekanntmachung vom 14. Januar 2003 (BGBl. I S. 66), zuletzt geändert durch Gesetz vom 30. Juni 2017 (BGBl. I S. 2097), geregelte Medienprivileg, das in § 10 des Hessischen Pressegesetzes (HPres-

seG) transferiert wurde, wird die Anwendbarkeit des Datenschutzrechts auf die Pressetätigkeit im journalistisch-redaktionellen und literarischen Bereich weitgehend und die Datenschutzaufsicht über die genannte Pressetätigkeit durch die Datenschutzbeauftragten der Länder vollständig ausgeschlossen. Mit § 41 Abs. 1 BDSG setzte der Bundesgesetzgeber im Jahre 2001 Art. 9 der Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr (ABl. EG L Nr. 281 S. 31 ff.; im Folgenden: DSRL) um. Art. 9 DSRL wird am 25. Mai 2018 von Art. 85 der Verordnung (EU) Nr. 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung) (ABl. EU Nr. L 119 S. 1) abgelöst. § 41 BSDG wird mit dem BDSG vom 14. Januar 2003 zum gleichen Zeitpunkt außer Kraft treten. Im neuen Bundesdatenschutzgesetz vom 30. Juni 2017 (BGBl. I S. 2097, im Folgenden: BDSG n.F.), das gleichzeitig am 25. Mai 2018 in Kraft treten wird, ist das Medienprivileg nicht mehr geregelt. Die Bundesregierung hat in der Gesetzesbegründung zum Entwurf des Datenschutz-Anpassungs- und -Umsetzungsgesetzes-EU (DSAnpUG-EU) erklärt, dass für das Pressewesen nunmehr ausschließlich die Länder zuständig seien. Es werde davon ausgegangen, dass die zuständigen Landesgesetzgeber das Presseprivileg wie bisher absichern würden. (Vgl. BT-Drs. 18/11325 vom 24. Februar 2017, S. 79). Diese Absicherung des Presseprivilegs erfolgt durch die Neufassung des § 10 HPresse, mit welcher der Regelungsauftrag des Art. 85 Abs. 1 der Verordnung (EU) Nr. 2016/679 umgesetzt wird. Der Regelungsauftrag beinhaltet, dass das Recht auf Schutz der personenbezogenen Daten mit der Freiheit der Meinungsäußerung und der Informationsfreiheit in Einklang zu bringen ist.

Die im neugefassten § 10 HPresseG-E geregelte Absicherung des Presseprivilegs ist nach Art. 85 Abs. 2 der Verordnung (EU) Nr. 2016/679 zulässig. Art. 85 Abs. 2 der Verordnung (EU) Nr. 2016/679 erlaubt für die Verarbeitung von personenbezogenen Daten, die zu journalistischen Zwecken oder zu wissenschaftlichen, künstlerischen oder literarischen Zwecken erfolgt, Abweichungen und Ausnahmen von der Verordnung (EU) Nr. 2016/679, wenn dies erforderlich ist, um das Recht auf Schutz der personenbezogenen Daten mit der Freiheit der Meinungsäußerung und der Informationsfreiheit in Einklang zu bringen. Nach dem Erwägungsgrund 153 der Verordnung (EU) Nr. 2016/679 müssen Begriffe wie Journalismus weit ausgelegt werden, um der Bedeutung des Rechts auf freie Meinungsäußerung in einer demokratischen Gesellschaft Rechnung zu tragen. Die auf den Journalismus bezogene Meinungsäußerungsfreiheit beinhaltet die Pressefreiheit.

Nach der ständigen Rechtsprechung des Bundesverfassungsgerichts seit 1966 ist eine freie, nicht von der öffentlichen Gewalt gelenkte, keiner Zensur unterworfene Presse ein Wesenselement des freiheitlichen Staates und für die moderne Demokratie unentbehrlich (vgl. BVerfGE 20, 162 ff.). Die in Art. 5 Abs. 1 Satz 2 GG gesicherte Eigenständigkeit der Presse reicht von der Beschaffung der Information bis zur Verbreitung der Nachrichten und Meinungen. Die Gewährleistung der Pressefreiheit schließt nach dem Bundesverfassungsgericht auch diejenigen Voraussetzungen und Hilfstätigkeiten mit ein, ohne die die Presse ihre Funktion nicht in angemessener Weise erfüllen kann. Geschützt sind daher auch die Geheimhaltung der Informationsquellen und das Vertrauensverhältnis zwischen Presse und Informanten (BVerfGE 117, 244, 258 f., Urteil vom 27. Februar 2007 m.w.Nachw.).

Die Pressefreiheit wird neben Art. 5 Abs. 1 Satz 2 GG durch Art. 11 der Charta der Grundrechte der Europäischen Union (GRC) und Art. 10 Abs. 1 Satz 2 der Europäischen Menschenrechtskonvention (EMRK) geschützt. Auf die besondere Bedeutung des durch Art. 11 GRC gewährleisteten Grundrechts der Meinungs- bzw. Pressefreiheit als "eine der wesentlichen Grundlagen einer demokratischen und pluralistischen Gesellschaft", die nur soweit erforderlich eingeschränkt werden darf, hat der Gerichtshof der Europäischen Union (EuGH) mehrfach hingewiesen (vgl. Urteil der Großen Kammer vom 21. Dezember 2016 - Rs. C-203/15 m.w.N.; Urteil des EuG vom 12. September 2007 - Rs. T-36/04). Ebenso hat der Europäische Gerichtshof für Menschenrechte (EGMR) in seiner Rechtsprechung die grundlegende Bedeutung und das große Gewicht der Pressefreiheit für eine demokratische Gesellschaft, die unentbehrliche Rolle der Presse als Kontrollorgan und die staatliche Verpflichtung, die Pressefreiheit zu gewährleisten und zu erhalten, betont und insbesondere auch den Quellenschutz als Eckstein der Pressefreiheit bezeichnet, ohne den Informanten davon abgehalten werden könnten, der Presse bei der Unterrichtung der Öffentlichkeit über Fragen öffentlichen Interesses zu helfen. Ein Eingriff in den Quellenschutz wäre mit Art. 10 EMRK nur vereinbar, wenn er durch übergeordnete Erfordernisse des öffentlichen Interesses gerechtfertigt wäre (vgl. EGMR, V. Sektion, Urteil vom 29. Juni 2012 -15054/07,15066/07 in NJW 2013, 3709, und EGMR, II. Sektion, Urteil vom 19. Januar 2016 - 49085/07 in NJW 2017, 1533, jeweils m.w.N.).

Die Presse ist bei Erfüllung ihrer verfassungs- und europarechtlich verbürgten Aufgaben zwingend auf die Verwendung personenbezogener Daten ohne Einwilligung der betroffenen Personen angewiesen. Journalistische Arbeit und vor allem auch eine verdeckte Recherche im Rahmen eines investigativen Journalismus wären nicht möglich, wenn personenbezogene Daten nur

mit Einwilligung der betroffenen Personen erhoben, gespeichert und genutzt werden dürften oder den betroffenen Personen konkrete Auskunfts- und daraus folgende Berichtigungsansprüche zu nicht veröffentlichten redaktionellen Daten eingeräumt würden. Einflüsse von außen auf die Datenverarbeitung der Presse, insbesondere im Vorfeld der Berichterstattung, müssen zum Schutz der Pressefreiheit vermieden werden. Die Presse könnte ihre nach Art. 5 Abs. 1 Satz 2 GG, Art. 10 Abs. 1 Satz 2 EMRK und Art. 11 GRC zuerkannten und garantierten Aufgaben in dem Umfang, wie er von dem Bundesverfassungsgericht, dem Gerichtshof der Europäischen Union und dem Europäischen Gerichtshof für Menschenrechte anerkannt ist, nicht wahrnehmen (vgl. BVerwG, Beschluss vom 29. Oktober 2015 - 1 B 32.15;)

Für die von Art. 85 Abs. 2 der Verordnung (EU) Nr. 2016/679 geforderte Abwägung sind die oben angeführten Gründe für den Schutz der Pressefreiheit, die bereits für das bisherige Presseprivileg galten, wesentlich. Sie können nicht weiter als bisher durch den Schutz der personenbezogenen Daten zurückgedrängt werden. Andernfalls würde in den Wesensgehalt der Pressefreiheit eingegriffen. Der Schutz der personenbezogenen Daten kann gegenüber dem Schutz der Pressefreiheit nicht als höherrangig angesehen werden. Das bisherige Schutzniveau für die personenbezogenen Daten hat sich nicht als ungeeignet und unzumutbar erwiesen. Es hat sich vielmehr seit 2001 bewährt. Auch werden keine weitergehenden Persönlichkeitsrechte der Betroffenen durch die Verordnung (EU) Nr. 2016/679 geschaffen, die im Rahmen der verfassungs- und europarechtlichen Abwägung einen Vorrang gegenüber der Pressefreiheit beanspruchen könnten. Ein solcher Vorrang würde im Widerspruch zu Art. 5 Abs. 1 Satz 2 GG, Art. 10 Abs. 1 Satz 2 EMRK und Art. 11 GRC stehen.

Für den Datenschutz ausreichend und für die Pressefreiheit erforderlich ist es danach, wenn in § 10 HPresseG-E eine Umstellung in dem Sinne erfolgt, dass die am 25. Mai 2018 außer Kraft tretenden Vorschriften des BDSG a.F. zur Datensicherheit einschließlich des darauf bezogenen Schadensersatzes bei Verletzung der Datensicherheit durch Vorschriften aus der Verordnung (EU) Nr. 2016/679 und die zum Datengeheimnis durch Anlehnung an die Formulierung in § 53 BDSG n.F. mit der Regelung über die Schadensersatzpflicht nach § 83 BDSG n.F. ersetzt werden.

Im Einzelnen

Zu § 10 Satz 1 bis 3 HPresseG-E
Mit der Regelung des Datengeheimnisses in § 10 Satz 1 bis 3 HPresseG-E bleibt die bisherige Rechtslage weitgehend erhalten. Im Einklang mit Art. 85 Abs. 2 der Verordnung (EU) Nr. 2016/679 wird neben den literarischen Zwecken nur noch von "journalistischen" und nicht wie bisher von "journalistisch-redaktionellen Zwecken" gesprochen. Dadurch wird die gesamte journalistische Datenverarbeitung von der Beschaffung der Informationen über die Verarbeitung in der Redaktion bis hin zur Veröffentlichung und Aufnahme in Presse- bzw. Redaktionsarchiven einschließlich deren Nutzung erfasst. Auch werden Kooperationen mit anderen journalistischen Einheiten (z.B. Rechercheverbünde) vom Presseprivileg des § 10 HPresseG-E erfasst, weil nicht mehr auf eigene journalistische Zwecke abgestellt wird. Neben den Presseunternehmen werden wie bisher die Hilfsunternehmen der Presse genannt. Nicht erfasst werden Beteiligungsunternehmen der Presse, weil für sie das Presseprivileg nur gelten kann, wenn ihre Tätigkeit der Erfüllung der Kernaufgaben der Presse dient. Sie können nicht berücksichtigt werden, wenn ein Sachzusammenhang mit der Hauptaufgabe der Presse nicht besteht. Erfüllen sie die Anforderungen, können sie aber als Unternehmen oder Hilfsunternehmen der Presse angesehen werden.

Zu § 10 Satz 4 bis 6 HPresseG-E
Durch das Zitat der Kapitel I, X und XI der Verordnung (EU) Nr. 2016/679 in § 10 Satz 4 HPresseG-E wird der Einschränkung des Art. 85 Abs. 2 der Verordnung (EU) Nr. 2016/679 Rechnung getragen, dass von den genannten Kapiteln keine Abweichungen oder Ausnahmen zulässig sind. Der Schutz der Pressefreiheit steht ihrer Anwendung nicht entgegen.

Art. 5 Abs. 1 Buchst. f der Verordnung (EU) Nr. 2016/679 hat zum Inhalt, dass personenbezogene Daten in einer Weise verarbeitet werden müssen, die eine angemessene Sicherheit der personenbezogenen Daten gewährleistet, einschließlich Schutz vor unbefugter oder unrechtmäßiger Verarbeitung und vor unbeabsichtigtem Verlust, unbeabsichtigter Zerstörung oder unbeabsichtigter Schädigung durch geeignete technische und organisatorische Maßnahmen ("Integrität und Vertraulichkeit"). Erfasst wird dadurch auch die Absicherung gegen eine Zweckentfremdung der personenbezogenen Daten für nicht journalistische oder literarische Zwecke. Art. 5 Abs. 1 Buchst. f der Verordnung (EU) Nr. 2016/679 kann mit § 9 BDSG a.F. verglichen werden, der die Verpflichtung zur Datensicherheit durch technische und organisatorische Maßnahmen regelt. Durch Art. 5 Abs. 2 der Verordnung (EU) Nr. 2016/679 wird sichergestellt, dass der Verantwortliche für die Einhaltung des Abs. 1 verantwortlich ist und dessen Einhaltung nachweisen können muss (Rechenschaftspflicht). Diese Pflicht besteht nur in Bezug auf Art. 5 Abs. 1 Buchst. f der Verordnung (EU) Nr. 2016/679.

Für die technischen und organisatorischen Maßnahmen werden zudem Art. 24 Abs. 1 Satz 1 und Abs. 2, Art. 32 Abs. 1 Buchst. b bis d, Abs. 2 und 4 der Verordnung (EU) Nr. 2016/679 für anwendbar erklärt, die sich auf den für die Verarbeitung der personenbezogenen Daten Verantwortlichen, das Schutzniveau für die technischen und organisatorischen Maßnahmen und die Anweisungen gegenüber den dem Verantwortlichen unterstellten Personen beziehen.

Art. 82 der Verordnung (EU) Nr. 2016/679 regelt die Haftung und das Recht auf Schadenersatz, wenn wegen eines Verstoßes gegen die Verordnung ein materieller oder immaterieller Schaden entstanden ist. Die Vorschrift ist in § 10 Satz 4 und 5 HPresseG-E für den Fall aufgenommen, dass gegen die in Art. 5 Abs. 1 Buchst. f, Art. 24 Abs. 1 Satz 1 und Abs. 2, Art. 32 Abs. 1 Buchst. b bis d, Abs. 2 und 4 der Verordnung (EU) Nr. 2016/679 geregelten Verpflichtungen zur Datensicherheit durch geeignete technische und organisatorische Maßnahmen bzw. Datenschutzvorkehrungen verstoßen wird.

Anstelle von Art. 82 der Verordnung (EU) Nr. 2016/679 wird § 83 BDSG n.F. für den Schadensersatz (materieller Schaden) und die Entschädigung (immaterieller Schaden) bei Verletzung des Datengeheimnisses in § 10 Satz 4 und 6 HPresseG-E genannt, weil Art. 82 der Verordnung (EU) Nr. 2016/679 voraussetzt, dass gegen die Verordnung (EU) Nr. 2016/679 verstoßen wurde, das Datengeheimnis aber nicht in der Verordnung (EU) Nr. 2016/679 explizit geregelt ist. Durch den Verweis auf § 83 BDSG n.F. werden Rechtsgrund und Rechtsfolge für den Anspruch auf Schadensersatz und Entschädigung bei Verletzung des Dienstgeheimnisses eigenständig (ohne den im BDSG n.F. bestehenden Regelungszusammenhang) in § 10 Satz 4 und 6 HPresseG-E geregelt. Durch die Formulierung in § 10 Satz 4 HPresseG-E und der damit einhergehenden Regelungstechnik, dass im Übrigen für die Datenverarbeitung zu journalistischen oder literarischen Zwecken außer den Kapiteln I, X und XI nur Art. 5 Abs. 1 Buchst. f in Verbindung mit Abs. 2, Art. 24 Abs. 1 Satz 1 und Abs. 2, Art. 32 Abs. 1 Buchst. b bis d, Abs. 2 und 4, Art. 82 der Verordnung (EU) Nr. 2016/679 sowie § 83 des Bundesdatenschutzgesetzes vom 30. Juni 2017 (BGBl. I S. 2097) in der jeweils geltenden Fassung Anwendung finden, wird außerdem klargestellt, dass nicht nur die anderen Vorschriften der Verordnung (EU) Nr. 2016/679, sondern auch die des Bundesdatenschutzgesetzes n.F. nicht anwendbar sind.

In § 10 HPresseG-E erfolgt keine Regelung, dass Kapitel VIII der Verordnung (EU) Nr. 2016/679 anwendbar ist. Eine Aussage über die Anwendbarkeit von Kapitel VIII (Art. 77 bis 84) der Verordnung (EU) Nr. 2016/679 in § 10 HPresseG-E mit Ausnahme des Art. 82 der Verordnung (EU) Nr. 2016/679 wäre irreführend, weil die anderen Artikel von Kapitel VIII der Verordnung (EU) Nr. 2016/679 entweder nicht greifen oder aber bereits erfüllt sind. Infolgedessen handelt es sich auch nicht um eine unzulässige Abweichung von Art. 85 Abs. 2 der Verordnung (EU) Nr. 2016/679, der Kapitel VIII nicht für Ausnahmen und Abweichungen nennt. Aus der Entstehungsgeschichte und der Systematik des Art. 85 der Verordnung (EU) Nr. 2016/679 ergibt sich, dass auch von Kapitel VIII abgewichen werden kann, wenn dies zum Schutz des Rechts auf freie Meinungsäußerung und Informationsfreiheit, mithin für den Schutz der Pressefreiheit erforderlich ist. Von Kapitel VIII sind Art. 77, 78 und 83 der Verordnung (EU) Nr. 2016/679 unanwendbar, weil sie die Aufsichtsbehörde betreffen. Über die Unternehmen und Hilfsunternehmen der Presse gibt es aufgrund des in § 10 HPresseG-E geregelten Presseprivilegs keine Aufsicht einer Aufsichtsbehörde im Sinne der Verordnung (EU) Nr. 2016/679. Der Ausschluss der Aufsicht über die Unternehmen und Hilfsunternehmen der Presse ist nach Art. 85 Abs. 2 der Verordnung (EU) Nr. 2016/679 zum Schutz der Pressefreiheit nach Art. 5 Abs. 1 Satz 2 GG, Art. 10 Abs. 1 Satz 2 EMRK und Art. 11 GRC - wie oben dargelegt - notwendig. Für die Presse ist eine journalistische Tätigkeit mit der hierfür erforderlichen Verarbeitung personenbezogener Daten ohne staatliche Einfluss- und Kontrollmöglichkeiten von elementarer Bedeutung und ein unverzichtbares, verfassungs- und europarechtlich gebotenes Element. Damit ist aber auch der Ausschluss von Art. 77 der Verordnung (EU) Nr. 2016/679 erforderlich, mit dem jede betroffene Person das Recht auf Beschwerde bei einer Aufsichtsbehörde eingeräumt wird, wenn die betroffene Person der Ansicht ist, dass die Verarbeitung der sie betreffenden personenbezogenen Daten gegen diese Verordnung verstößt. Aufgrund einer Beschwerde würde die Aufsichtsbehörde die Datenverarbeitung der Presse kontrollieren. Dies widerspricht dem Schutz der Pressefreiheit. Nach Art. 4 Nr. 21 der Verordnung (EU) Nr. 2016/679 ist "Aufsichtsbehörde" eine von einem Mitgliedstaat gemäß Art. 51 der Verordnung (EU) Nr. 2016/679 eingerichtete unabhängige staatliche Stelle. Nach Art. 51 Abs. 1 der Verordnung (EU) Nr. 2016/679 ist Aufsichtsbehörde eine oder sind Aufsichtsbehörden mehrere unabhängige Behörden. Das Recht auf Beschwerde ist damit abhängig von der Einrichtung bzw. Zuständigkeit einer staatlichen Aufsichtsbehörde, die aber nach Art. 85 Abs. 2 ausgeschlossen werden darf, weil von Kapitel VI (Art. 51 ff. der Verordnung (EU) Nr. 2016/679) Ausnahmen vorgesehen werden dürfen, die mit § 10 HPresseG-E umgesetzt werden.

Art. 78 der Verordnung (EU) Nr. 2016/679 entfällt aus den gleichen Gründen. Es kann keine Rechtsbehelfe gegen eine Aufsichtsbehörde geben, wenn eine solche für den Bereich der Presse nicht existiert. Art. 79 der Verordnung (EU) Nr. 2016/679 bedarf keiner Erwähnung, weil er nach den im deutschen Rechtssystem zur Verfügung stehenden gerichtlichen Rechtsbehelfen (Unterlassungsklage, Schadensersatzanspruch und Anspruch auf Berichtigung) als erfüllt ange-

sehen werden kann. Art. 81 der Verordnung (EU) Nr. 2016/679 ist nicht anwendbar, weil er sich auf Verfahren gegen die Entscheidung einer Aufsichtsbehörde bezieht (vgl. Erwägungsgrund Nr. 144 der Verordnung (EU) Nr. 2016/679), die es aber bei den Unternehmen und Hilfsunternehmen der Presse nicht gibt, wenn sie personenbezogene Daten zu journalistischen oder literarischen Zwecken verarbeiten. Infolgedessen kommt auch eine Beschwerde von Einrichtungen, Organisationen oder Vereinigungen in Vertretung für betroffene Personen nach Art. 80 der Verordnung (EU) Nr. 2016/679 bei einer Aufsichtsbehörde bzw. gegen eine Aufsichtsbehörde nicht in Betracht. Ebenso wenig bedarf es einer Regelung zur Anwendbarkeit des Art. 80 der Verordnung (EU) Nr. 2016/679 für die Geltendmachung von Ansprüchen nach Art. 82 der Verordnung (EU) Nr. 2016/679 für die betroffene Person durch die genannten Stellen, weil nach dem Erwägungsgrund Nr. 142 der Verordnung (EU) Nr. 2016/679 dies nicht zwingend umzusetzen ist und im Pressebereich wesensfremd wäre. Die Anwendbarkeit des Art. 84 der Verordnung (EU) Nr. 2016/679 bedarf ebenfalls nicht der Erwähnung in § 10 HPresseG-E., weil für bestimmte Handlungen, durch welche der Schutz personenbezogener Daten verletzt wird, im Strafgesetzbuch Sanktionen geregelt sind.

Durch § 10 HPresseG-E wird für das Presseprivileg an einer normativen Säule festgehalten, die durch die Säule der sogenannten freiwilligen Selbstkontrolle ergänzt wird. Die freiwillige Selbstkontrolle der Presse hat sich mit den Regelungen über den Redaktionsdatenschutz im Pressekodex des Deutschen Presserats seit 2001 bewährt. Bei Verstößen gegen die Grundsätze zum Redaktionsdatenschutz werden nach der Beschwerdeordnung des Deutschen Presserates Sanktionen ausgesprochen. Die freiwillige Selbstkontrolle der Presse ist ein wesentliches Instrument zur Gewährleistung der Pressefreiheit. Sie ist neben den in § 10 HPresseG-E vorgesehenen Maßnahmen geeignet, den Schutz des Persönlichkeitsrechts des Einzelnen bzw. das Recht auf den Schutz personenbezogener Daten mit der Pressefreiheit in Einklang zu bringen und zugleich eine unabhängige und kritische Berichterstattung zu ermöglichen. Die Sanktionierung der Pflicht zur Einhaltung des Datenschutzes im Wege gerichtlich einklagbarer Unterlassungs- und Schadensersatzansprüche, ergänzt um die Beschwerdemöglichkeit beim Deutschen Presserat als Redaktionsdatenschutzselbstkontrolle, ist angemessen und erforderlich, um die Freiheit der Presse von datenschutzbehördlicher Aufsicht zu sichern.

Zu Art. 15 (Änderung des Hessischen Ausführungsgesetzes zum Kreislaufwirtschaftsgesetz)

Zu Nr. 1

Die Streichung der Absatzbezeichnung ist eine Folgeänderung der Aufhebung von Abs. 2.

Zu Nr. 2
Die Bezugnahme in § 17 Abs. 1 Satz 4 HAKrWG auf den bisherigen § 13 Abs. 2 HDSG ist zu streichen. Nach § 1 Abs. 2 Satz 1 HDSIG-E ist ein Vorrang bereichsspezifischer Ausnahmen in anderen Gesetzen weiterhin möglich. Insofern ist eine Bezugnahme auf die im Datenschutz- und Informationsfreiheitsgesetz geregelten Ausnahmetatbestände verzichtbar. Die bestehende Regelung einer abfallrechtlichen bereichsspezifischen Ausnahme für die Anforderungen an eine Zweckänderung ist weiterhin zulässig und sachgerecht. In Art. 6 und dem 50. Erwägungsgrund der Verordnung (EU) Nr. 2016/679 wird ausdrücklich festgelegt, dass durch nationale Gesetze weiterhin Zwecke bestimmt werden können, für die eine Verarbeitung von personenbezogenen Daten zu einem anderen Zweck als zu denjenigen, zu denen diese erhoben wurden, zulässig ist, wenn die Verarbeitung für die Wahrnehmung einer Aufgabe erforderlich ist, die im öffentlichen Interesse liegt. Eine solche Regelung ist erforderlich, da es zum Beispiel für die Abfallbehörden bei der Prüfung der Zulässigkeit der Entsorgung von gefährlichen Abfällen im Rahmen des abfallrechtlichen Nachweisverfahrens möglich sein muss, einen Abgleich mit Daten aus dem Genehmigungsverfahren von Abfallentsorgungsanlagen vorzunehmen.

Zu Nr. 3
Abs. 2 ist aufzuheben, da dieser Regelungsgehalt ausdrücklich durch § 1 Abs. 2 Satz 2 des HDSIG-E normiert wird.

Zu Art. 16 (Änderung des Hessischen Beamtengesetzes)

Zu Nr. 1 (Inhaltsübersicht)
Die Überschrift zu §§ 86, 89, 90 und 93 des Hessischen Beamtengesetzes (HBG) ist infolge der Änderung in Nr. 3, 4, 5 und 6 anzupassen.

Zu Nr. 2 (§ 80)
Abs. 6 Satz 1 stellt eine Rechtsgrundlage für die Beihilfebearbeitung im Auftrag dar. Die Vorgaben für die Auftragsdatenverarbeitung sind nunmehr in den Art. 28 und 29 der Verordnung (EU) Nr. 2016/679 abschließend geregelt. Dies wird mit der neuen Formulierung in Satz 1 zum

Ausdruck gebracht und der bisherige Verweis in Satz 3, zweiter Halbsatz auf § 4 HDSG ist zu streichen.

Zu Nr. 3 (§ 86)
Die Überschrift zu § 86 wird zum besseren Verständnis des Regelungsgehalts erweitert.

§ 86 Abs. 1 bis 5 HBG enthalten Rechtsgrundlagen für die Verarbeitung von Personalakten im Sinne des Art. 6 Abs. 1 Buchst. c bzw. Buchst. e der Verordnung (EU) Nr. 2016/679.

In Abs. 3 Satz 1 und 2 werden daher die Begrifflichkeiten an die Begriffsbestimmungen in Art. 4 Nr. 2 der Verordnung (EU) Nr. 2016/679 angepasst.

Abs. 3 Satz 4 stellt eine Rechtsgrundlage für die Auftragsdatenverarbeitung dar. Der Verweis im zweiten Halbsatz auf den bisherigen § 4 HDSG wird geändert in einen Verweis auf die Art. 28 und 29 der Verordnung (EU) Nr. 2016/679, da die Vorgaben für die Auftragsdatenverarbeitung dort nunmehr abschließend geregelt sind.

Zu Nr. 4 (§ 89)
Die Überschrift zu § 89 wird begrifflich an die Regelung in Art. 4, 15 der Verordnung (EU) Nr. 2016/679 angepasst.

Abs. 1 stellt nach Art. 6 Abs. 1 Buchst. c bzw. Buchst. e der Verordnung (EU) Nr. 2016/679 die Rechtsgrundlage für das Einsichts- und Auskunftsrecht der Beamtinnen und Beamten - auch nach Beendigung des Beamtenverhältnisses - in ihre Personalakte dar. Die Einsichtnahme wird dabei neben der Auskunft nach Art. 15 der Verordnung (EU) Nr. 2016/679 zugelassen und die personalaktenführende Behörde bestimmt, wo die Einsicht gewährt wird. Hierbei handelt es sich um eine zulässige Spezifizierung nach Art. 88 Abs. 1 der Verordnung (EU) Nr. 2016/679 im Beschäftigungskontext, da das Einsichts- und Auskunftsrecht in § 89 HBG in erster Linie auf dem unmittelbaren Persönlichkeitsrecht beruht und die Beamtinnen und Beamten besser in die Lage versetzen soll, ihre Belange gegenüber dem Dienstherrn geltend zu machen (Art. 19 Abs. 4 Satz 1 GG, Art. 2 Abs. 3 HV). Es ist dem entsprechend auch Ausdruck der Fürsorgepflicht. Da das Einsichtsrecht somit nicht nur auf dem Recht auf informationelle Selbstbestimmung beruht und es sich daher nicht nur um ein Betroffenenrecht nach Art. 12 ff. der Verordnung (EU) Nr. 2016/679 handelt, muss es neben dem datenschutzrechtlichen Auskunftsrecht nach Art. 15 der Verordnung (EU) Nr. 2016/679 bestehen bleiben.

Abs. 3 schränkt das Auskunfts- und Einsichtsrecht der betroffenen Person in Bezug auf Kopien sowie Informationen in einem gängigen elektronischen Format nach Art. 15 Abs. 3 der Verordnung (EU) Nr. 2016/679 ein. Diese Beschränkung erfolgt auf der Grundlage des Art. 15 Abs. 4 und Art. 23 Abs. 1 Buchst. a bis Buchst. i der Verordnung (EU) Nr. 2016/679.

Abs. 3 gilt auch für Personen nach Abs. 2. Bevollmächtigten, Hinterbliebenen und deren Bevollmächtigten werden nach Art. 88 Abs. 1 der Verordnung (EU) Nr. 2016/679 über Art. 15 hinaus ein Recht auf Einsichtnahme/Auskunft eingeräumt sowie auf Verlangen Kopien sowie Informationen in einem gängigen elektronischen Format zur Verfügung gestellt. Diese Rechte leiten sich zwar vom Einsichtsrecht der Beamtin oder des Beamten selbst ab, stellen aber auch eigenständige Rechte dar, die nicht auf Datenschutzrecht beruhen, sondern bezüglich der Bevollmächtigten auf § 14 HVwVfG und § 67 VwGO und bei den Hinterbliebenen der Rechtswahrung dienen und daher beizubehalten sind.

Zu Nr. 5 (§ 90)
Die Überschrift und die Begrifflichkeiten werden an die Begriffsbestimmungen in Art. 4 Nr. 2 der Verordnung (EU) Nr. 2016/679 angepasst.

In Abs. 2 Satz 1 wird darüber hinaus klargestellt, dass es sich um Auskünfte über den Inhalt der Personalakte handelt.

Zu Nr. 6 (§ 93)
Die Überschrift und die Begrifflichkeiten werden an die Begriffsbestimmungen in Art. 4 Nr. 2 der Verordnung (EU) Nr. 2016/679 angepasst.

Abs. 4 wird gestrichen, da es sich um eine nicht erforderliche Wiederholung der bereits in Art 22 Abs. 1 der Verordnung (EU) Nr. 2016/679 enthaltenen Regelung handelt.

Zu Nr. 7 (§ 96)
In § 96 Abs. 2 Satz 2 wird die Begrifflichkeit "automatisiert verarbeitet" an die Begriffsbestimmungen in Art. 4 Nr. 2 der Verordnung (EU) Nr. 2016/679 angepasst.

Abs. 3 stellt eine Rechtsgrundlage für die Auftragsdatenverarbeitung dar. Der Verweis im zweiten Halbsatz auf den bisherigen § 4 HDSG wird geändert in einen Verweis auf die Art. 28 und

29 der Verordnung (EU) Nr. 2016/679, da die Vorgaben für die Auftragsdatenverarbeitung dort nunmehr abschließend geregelt sind.

Zu Art. 17 (Änderung des Gesetzes über den Einheitlichen Ansprechpartner Hessen)

Der bisherige Verweis auf das hessische Datenschutzgesetz ist anzupassen, allgemein zu formulieren und um den Hinweis auf das EU-Recht zu ergänzen.

Zu Art. 18 (Änderung des Hessischen Gesetzes über die öffentliche Sicherheit und Ordnung)

Allgemeines

Die dem Entwurf des Hessischen Gesetzes über die öffentliche Sicherheit und Ordnung zugrunde liegenden Änderungen dienen der Umsetzung der EU-Datenschutzreform mit deren beiden EU-Rechtsakten der Richtlinie (EU) Nr. 2016/680 und der Verordnung (EU) Nr. 2016/679 im bereichsspezifischen Datenschutzrecht des HSOG, der teilweisen Umsetzung der sich für das HSOG ergebenden Maßgaben aus dem zum Bundeskriminalamtgesetz ergangenen bundesverfassungsgerichtlichen Urteil vom 20. April 2016 sowie der Anpassung bestehender Befugnisnormen zur gefahrenabwehr- und polizeibehördlichen Aufgabenerfüllung.

Sowohl das Erfordernis zur Umsetzung der Richtlinie (EU) Nr. 2016/680 bis zum 6. Mai 2018 als auch die ab dem 25. Mai 2018 unmittelbare Geltung beanspruchende Verordnung (EU) Nr. 2016/679 lösen aufgrund der zahlreichen bereichsspezifischen datenschutzrechtlichen Regelungen im HSOG einen bedeutenden Anpassungs- und Umsetzungsbedarf aus. Hierbei ist zu berücksichtigen, dass sich die beiden EU-Rechtsakte ausgehend von Art. 2 Abs. 1 der Richtlinie (EU) Nr. 2016/680 insoweit voneinander abgrenzen, dass die Richtlinie Anwendung findet bei der Verarbeitung personenbezogener Daten zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung, einschließlich des Schutzes vor und der Abwehr von Gefahren für die öffentliche Sicherheit, und Art. 2 Buchst. d der Verordnung (EU) Nr. 2016/679 dies aufgreifend die Verordnung für die Verarbeitung personenbezogener Daten zu den vorgenannten Zwecken der Richtlinie für nicht anwendbar erklärt. In diesem Zusammenhang ist die landesrechtliche Konturierung des Anwendungsbereichs der Richtlinie in § 40 HDSIG-E von besonderer Bedeutung. Vor dem Hintergrund, dass die zur Aufgabenerfüllung erfolgende Verarbeitung personenbezogener Daten durch die Gefahrenabwehr- und Polizeibehörden nicht ausschließlich dem Anwendungsbereich der Richtlinie (EU) Nr. 2016/680 unterfällt, sind neben den erforderlichen Arbeiten zur Umsetzung der vorgenannten Richtlinie in dem vorliegenden Entwurf sowie dem subsidiär zur Anwendung kommenden HDSIG-E auch die Maßgaben der Verordnung (EU) Nr. 2016/679 und die deren Durchführung dienenden Vorschriften des HDSIG-E in Ansatz zu bringen. Weitere Regelungskomplexe des Entwurfs stellen die Vorschriften zur Übermittlung personenbezogener Daten sowie die Ausgestaltung der datenschutzrechtlichen Betroffenenrechte dar.

Die Änderungen im HSOG dienen zum anderen der teilweisen Umsetzung der Vorgaben des Bundesverfassungsgerichts in seinem Urteil vom 20. April 2016 - 1 BvR 966/09 u.a. - (BVerfG, NJW 2016, 1781 ff.), welche das Bundesverfassungsgericht im Zusammenhang mit der Prüfung bestimmter Normen des Bundeskriminalamtgesetzes (BKAG) gemacht hat. Das Bundesverfassungsgericht hat in seiner Entscheidung u.a. Ausführungen zu Kernbereichsregelungen, Berichtspflichten gegenüber Parlament und Öffentlichkeit, besonderen datenschutzaufsichtlichen Kontrollen bei eingriffsintensiven und verdeckten Maßnahmen und Datenübermittlungen im internationalen Bereich gemacht sowie das von ihm geprägte Kriterium der hypothetischen Datenneuerhebung für eingriffsintensive Maßnahmen weiter konturiert und als allgemeinen datenschutzrechtlichen Grundsatz geprägt. Zwar beschäftigt sich das Urteil des Bundesverfassungsgerichts mit spezifischen Normen des BKAG, jedoch sind die Ausführungen im Urteil an vielen Stellen auch für das polizeiliche Gefahrenabwehrrecht in den Ländern von grundsätzlicher und allgemeingültiger Bedeutung und müssen daher auch im HSOG nachvollzogen werden.

Im Einzelnen

Zu Nr. 1 (Übersicht)
Als Folge der Änderung bzw. Neufassung von Überschriften (§§ 20, 21 bis 23, 27, 28, 29 und 115 HSOG-E) und der Einfügung neuer Paragrafen (§§ 17a, 20a, 20b, 27a und 29a HSOG-E) werden die Angaben der Übersicht angepasst.

Zu Nr. 2 (§ 1)
Es handelt sich um eine Folgeänderung aufgrund des neuen § 29a HSOG-E.

Zu Nr. 3 (§ 3)
Das HSOG verfügt bisher über keine Vorschrift, die regelt, inwieweit die Bestimmungen des allgemeinen Datenschutzrechts auch im Polizeirecht Anwendung finden. Dem wird in § 3 Abs.

4 HSOG-E Rechnung getragen. Anknüpfend an § 1 Abs. 2 HDSIG-E erklärt Satz 1 die Vorschriften des HDSIG-E für subsidiär anwendbar, soweit im HSOG-E keine abschließenden Regelungen getroffen sind. In Satz 2 wird auf die unmittelbare Geltung beanspruchende Verordnung (EU) Nr. 2016/679 Bezug genommen. Neben den der Umsetzung der Richtlinie (EU) Nr. 2016/680 dienenden Vorschriften im HSOG-E und dem insoweit subsidiär zur Anwendung kommenden Dritten Teil des HDSIG-E fallen auch Datenverarbeitungsvorgänge der Gefahrenabwehr- und Polizeibehörden im Rahmen ihrer Aufgabenerfüllung unter den Anwendungsbereich der Verordnung (EU) Nr. 2016/679 und die ihrer Durchführung dienenden Vorschriften des Zweiten Teils des HDSIG-E. Hierbei handelt es sich beispielsweise um Datenverarbeitungsvorgänge der Gefahrenabwehr- und Polizeibehörden im Zusammenhang mit dem Schutz privater Rechte oder Störer- oder Gefahrenlagen ohne jeglichen Straftaten- oder Ordnungswidrigkeitenbezug. Hinsichtlich der vorgenannten gefahrenabwehr- oder polizeibehördlichen Aufgaben ist der Anwendungsbereich der Richtlinie (EU) Nr. 2016/680 nicht eröffnet, sodass auch die deren Umsetzung dienenden Vorschriften des Dritten Teils des HDSIG-E keine Anwendung finden.

Vorbemerkung zu Nr. 4 ff. (§§ 13 ff.)
Das HSOG-E führt, wie von der Richtlinie (EU) Nr. 2016/680 gefordert, den neuen einheitlichen Begriff der Verarbeitung personenbezogener Daten ein. Aus rechtssystematischen Gründen und aufgrund der weiteren europarechtlichen Vorgaben kann der einheitliche Begriff der Verarbeitung im HSOG-E allerdings nicht für die Datenerhebung, die Datenübermittlung, die Einschränkung der Datenverarbeitung und das Löschen der Daten Anwendung finden. Die übrigen Aspekte der Verarbeitung wie die Organisation, das Ordnen, die Speicherung, die Anpassung oder Veränderung, das Auslesen, das Abfragen, die Verwendung, der Abgleich oder die Verknüpfung bezeichnet das HSOG-E, dem Vorbild des Gesetzes zur Neuregelung des Bundeskriminalamtes vom 1. Juni 2017 (BGBl. I S. 1354) (im Folgenden BKAG-neu) folgend zusammenfassend als "Weiterverarbeitung".

Zu Nr. 4 (§ 13)

Zu Abs. 1
Abs. 1 übernimmt in teilweise modifizierter Form die Regelung des bisherigen § 13 Abs. 1 betreffend die Erhebung personenbezogener Daten durch die Gefahrenabwehr- und Polizeibehörden zur Erfüllung ihrer Aufgaben.

§ 13 Abs. 1 Nr. 1, welcher bislang die tatsächliche oder mutmaßliche Einwilligung als Zulässigkeitsgrund für die Erhebung personenbezogener Daten normiert, bedarf aufgrund der Maßgaben der Verordnung (EU) Nr. 2016/679 und der Richtlinie (EU) Nr. 2016/680 einer Regelungsanpassung. Im Anwendungsbereich der Richtlinie (EU) Nr. 2016/680 führt deren Erwägungsgrund 35 zur Frage der Zulässigkeit einer Einwilligung in die Verarbeitung personenbezogener Daten aus, dass die für die Zwecke der Richtlinie zuständigen Behörden bei Wahrnehmung ihrer übertragenen Aufgaben, natürliche Personen auffordern oder anweisen können, ihren Anordnungen nachzukommen. In einem solchen Fall soll die Einwilligung der betroffenen Person im Sinne des Art. 7 der Verordnung (EU) Nr. 2016/679 keine Rechtsgrundlage für die Verarbeitung personenbezogener Daten durch die zuständigen Behörden darstellen. Wird die betroffene Person aufgefordert, einer rechtlichen Verpflichtung nachzukommen, so hat sie keine echte Wahlfreiheit, weshalb ihre Reaktion nicht als freiwillig abgegebene Willensbekundung betrachtet werden kann. Dies soll die Mitgliedstaaten aber nicht daran hindern, durch Rechtsvorschriften vorzusehen, dass die betroffene Person der Verarbeitung ihrer personenbezogenen Daten für die Zwecke dieser Richtlinie zustimmen kann. Beispiele hierfür sind im HSOG die Vorschriften der §§ 13a, 13b. Überdies besteht angesichts der Vielgestaltigkeit der zu bewertenden Sachverhalte das Erfordernis für die Schaffung einer allgemeinen Rechtsvorschrift zur Erhebung personenbezogener Daten aufgrund einer Einwilligung. Daher werden, soweit eine Erhebung personenbezogener Daten zu Zwecken des § 40 HDSIG-E in Rede steht, hinsichtlich der Variante einer tatsächlichen Einwilligung nach § 13 Abs. 1 Nr. 1 die Voraussetzungen des § 13 Abs. 9 HSOG-E in Verbindung mit § 46 HDSIG-E zugrunde gelegt und die bisher in Abs. 1 Nr. 1 zu findende, weitere Variante der mutmaßlichen Einwilligung gestrichen. Hierbei wird in § 13 Abs. 1 Nr. 1 im Zusammenspiel mit § 13 Abs. 9 und § 46 HDSIG-E eine Rechtsgrundlage im Sinne des Art. 8, auch in Verbindung mit Art. 10 der Richtlinie (EU) Nr. 2016/680, geschaffen. Soweit eine Erhebung personenbezogener Daten der Gefahrenabwehr- oder Polizeibehörden zu Zwecken der Verordnung (EU) Nr. 2016/679 in Rede stehen sollte, ist die Zulässigkeit der Datenerhebung zur Aufgabenerfüllung aufgrund einer Einwilligung an dem Maßstab des Art. 6 Abs. 1 Buchst. a i.V.m. Art. 7, auch in Verbindung mit Art. 8 der Verordnung (EU) Nr. 2016/679, zu überprüfen. Die Zulässigkeit einer Erhebung besonderer Kategorien personenbezogener Daten zur Aufgabenerfüllung aufgrund einer Einwilligung ergibt sich im Anwendungsbereich der Verordnung (EU) Nr. 2016/679 aus deren Art. 9 Abs. 2 Buchst. a.

Abs. 1 Nr. 2 wird um die Variante der Erhebung personenbezogener Daten, welche die betroffene Person offensichtlich öffentlich gemacht hat, ergänzt. Soweit sich dies auf die Erhebung personenbezogener Daten im Anwendungsbereich des § 40 HDSIG-E bezieht, handelt es sich um eine Rechtsgrundlage zur rechtmäßigen Verarbeitung personenbezogener Daten im Sinne

des Art. 8 der Richtlinie (EU) Nr. 2016/680, auch in Verbindung mit Art. 10 Buchst. c der Richtlinie (EU) Nr. 2016/680, soweit sich die Verarbeitung auf besondere Kategorien personenbezogener Daten im Sinne des § 41 Nr. 15 HDSIG-E bezieht. Soweit eine Erhebung personenbezogener Daten durch die Gefahrenabwehr- oder Polizeibehörden in Rede steht, welche zu Zwecken außerhalb des § 40 HDSIG-E und damit im Anwendungsbereich der Verordnung (EU) Nr. 2016/679 erfolgt, handelt es sich bei § 13 Abs. 1 Nr. 2 Variante 2 um eine mitgliedstaatliche Rechtsgrundlage für die Erhebung personenbezogener Daten nach Art. 6 Abs. 1 Buchst. e i.V.m. Art. 6 Abs. 3 Satz 1 der Verordnung (EU) Nr. 2016/679. Die Zulässigkeit der Erhebung besonderer Kategorien personenbezogener Daten, welche die betroffene Person offensichtlich öffentlich gemacht hat, ergibt sich aus Art. 6 Abs. 1 Buchst. e i.V.m. Art. 9 Abs. 2 Buchst. e der Verordnung (EU) Nr. 2016/679.

Die Bestimmung in Abs. 1 Nr. 3 wird unverändert übernommen.

Zu Abs. 2
Über § 13 Abs. 1 hinaus gestattet Abs. 2 den Polizeibehörden die Erhebung personenbezogener Daten zu den dort genannten Zwecken. Die Anpassungen in Abs. 2 Nr. 1 bis Nr. 4 dienen der Umsetzung des Art. 6 der Richtlinie (EU) Nr. 2016/680; hiernach ist in der Phase der Datenerhebung zwischen den verschiedenen Kategorien betroffener Personen zu unterscheiden. Eine entsprechende Regelung findet sich in § 67 HDSIG-E. Die erfolgende tatbestandliche Konturierung der in Nr. 2 zu findenden Personengruppe, welche als Kontakt- und Begleit-/Verbindungspersonen umschrieben werden können, dient auch der Umsetzung der dem Urteil des Bundesverfassungsgerichts vom 20. April 2016 hierzu zugrunde gelegten Maßgaben (Rn. 167 ff.). Die in Nr. 3 und Nr. 4 neu aufgenommenen Personenkategorien dienen der Umsetzung des Art. 6 Buchst. c und d der Richtlinie (EU) Nr. 2016/680. Unberührt von § 13 Abs. 2 Nr. 1 bis 5 bleiben die speziellen Vorschriften des § 15 Abs. 2 zur Erhebung personenbezogener Daten der dort zu findenden Personenkreise.

Zu Abs. 5
Der bisherige Abs. 5 Satz 1 wird gestrichen, da sich diese Regelung nunmehr als allgemeine Bestimmung zur Zulässigkeit der Verarbeitung personenbezogener Daten in § 42 Nr. 2 HDSIG-E findet, welche Art. 4 Abs. 1 Buchst. b der Richtlinie (EU) Nr. 2016/680 umsetzt. Für die Datenerhebung der Gefahrenabwehr- und Polizeibehörden im Anwendungsbereich der Verordnung (EU) Nr. 2016/679 bestimmt Art. 5 Abs. 1 Buchst. b inhaltlich dasselbe. Der neue Satz 1 des Abs. 5 übernimmt im Wesentlichen die Regelung des bisherigen § 13 Abs. 5 Satz 2 HSOG zur Erhebung nicht gefahren- oder tatbezogener Merkmale. Der neue Satz 2 regelt die Datenerhebung nach Satz 1 bei besonderen Kategorien personenbezogener Daten und fordert in Umsetzung des Art. 10 der Richtlinie (EU) Nr. 2016/680 als Prüfungsmaßstab für deren Erhebung eine unbedingte Erforderlichkeit. Eine unbedingte Erforderlichkeit ist anzunehmen, wenn keine zumutbaren Alternativ- und Ausgleichsmaßnahmen zur Verfügung stehen, um ein legitimes Ziel zu erreichen. Eine Definition des Begriffs der besonderen Kategorien personenbezogener Daten findet sich in § 41 Nr. 15 HDSIG-E in Umsetzung des Art. 3 Nr. 12 bis Nr. 14 der Richtlinie (EU) Nr. 2016/680 sowie für den Anwendungsbereich der Verordnung (EU) Nr. 2016/679 in Art. 9 Abs. 1.

Zu Abs. 6
Der bisherige Abs. 6 Satz 1 wird auf den Anwendungsbereich der Richtlinie (EU) Nr. 2016/680 und damit auf die Erhebung personenbezogener Daten zu Zwecken des § 40 HDSIG-E beschränkt, da sich der Grundsatz der Direkterhebung von personenbezogenen Daten bei der betroffenen Person in der unmittelbare Geltung beanspruchenden Verordnung (EU) Nr. 2016/679 nicht findet. Es handelt sich bei der Aufrechterhaltung des Grundsatzes der Direkterhebung im Anwendungsbereich der Richtlinie (EU) Nr. 2016/680 insoweit um eine zulässige, strengere mitgliedstaatliche Garantie im Sinne deren Art. 1 Abs. 3. Auch in § 9 Abs. 2 Satz 2 BKAG-neu findet sich weiterhin der Grundsatz der Direkterhebung. Die Regelung des bisherigen Abs. 6 Satz 2 wird in Folge dessen ebenfalls auf den Anwendungsbereich der Richtlinie (EU) Nr. 2016/680 beschränkt und damit bei Erhebungen personenbezogener Daten zu Zwecken des § 40 HDSIG-E aufrechterhalten.

Zu Abs. 8
Da die Bestimmungen zu Informationspflichten der Gefahrenabwehr- und Polizeibehörden über die Verarbeitung personenbezogener Daten gegenüber der betroffenen Person nun in der Vorschrift des § 29 Abs. 1 und Abs. 2 HSOG-E zusammengeführt werden, wird die Regelung in Abs. 8 Satz 2 gestrichen. Abs. 8 Satz 3 wird - unter Streichung der Variante des Unterbleibens einer Mitteilung über die Erhebung personenbezogener Daten aus vorgenannten Gründen - bezogen auf das Unterbleiben eines Hinweises nach Abs. 8 Satz 1 aufrechterhalten.

Zu Abs. 9
In Abs. 9 Satz 1 wird nunmehr die in Abs. 1 Nr. 1 vorgesehene zulässige Datenerhebung aufgrund einer tatsächlichen Einwilligung konkretisiert und unbeschadet spezieller Rechtsvorschriften eine Rechtsgrundlage für die Erhebung personenbezogener Daten aufgrund einer tatsächli-

chen Einwilligung geschaffen. Maßstab für die Zulässigkeit sind im Anwendungsbereich der Richtlinie (EU) Nr. 2016/680 die in § 46 HDSIG-E in allgemeiner Weise formulierten Voraussetzungen. Darüber hinaus muss es sich bei der Datenerhebung der Gefahrenabwehr- oder Polizeibehörden nach Abs. 9 Satz 1 um einen Fall echter Wahlfreiheit im Sinne des Erwägungsgrundes 35 der Richtlinie (EU) Nr. 2016/680 handeln. Abs. 9 Satz 1 dient insoweit der Umsetzung von Art. 8, auch in Verbindung mit Art. 10 der Richtlinie (EU) Nr. 2016/680, und lässt spezielle Datenerhebungsvorschriften aufgrund einer tatsächlichen Einwilligung unberührt. Abs. 9 Satz 2 erfüllt für den Bereich der Verordnung (EU) Nr. 2016/679 eine klarstellende Funktion, da die Erhebung personenbezogener Daten aufgrund einer tatsächlichen Einwilligung in Art. 6 Abs. 1 Buchst. a in Verbindung mit Art. 7 und Art. 8 sowie bezogen auf die Verarbeitung besonderer Kategorien personenbezogener Daten in Art. 9 Abs. 2 Buchst. a der Verordnung (EU) Nr. 2016/679 bereits vorgesehen ist.

Zu Nr. 5 (§ 13a)

Zu Abs. 2
Es handelt sich um eine redaktionelle Anpassung aufgrund der Neufassung des HDSIG-E.

Zu Abs. 3
Es handelt sich um eine redaktionelle Anpassung aufgrund der Neufassung des HDSIG-E.

Zu Abs. 4
Es handelt sich um Folgeänderungen aufgrund der Ergänzung des Satz 3 in Abs. 1.

Zu Abs. 5
Abs. 5 wird in Satz 2 um die Regelung ergänzt, dass die Unterlagen auch verarbeitet werden dürfen, wenn die betroffene Person aus einem anderen Anlass erneut einer Zuverlässigkeitsüberprüfung unterzogen wird. Damit soll die Verwendung der gespeicherten Daten auch für weitere Zuverlässigkeitsprüfungen der betroffenen Person zu anderen Zwecken ohne erneute Datenerhebung ermöglicht werden.

Zu Nr. 6 (§ 13b)

Zu Abs. 2
In Abs. 2 Satz 1 wird der Verweis auf § 13a Abs. 4 ergänzt. Der weitere Verweis in Abs. 2 Satz 1 auf die geänderte Vorschrift des § 58 HDSIG-E zu den gemeinsamen Verfahren, gemeinsam Verantwortlichen stellt eine redaktionelle Anpassung dar.

Zu Nr. 7 (§ 14)
Hierbei handelt es sich um redaktionelle Anpassungen aufgrund der Neufassung des § 20 und der neuen Regelungssystematik von HDSIG-E und HSOG-E(vgl. § 1 Abs. 2 HDSIG-E und § 3 Abs. 4 HSOG-E).

Zu Nr. 8 (§ 15)

Zu Abs. 2
Es handelt sich um eine Folgeänderung aufgrund der Anpassungen in § 13 Abs. 2.

Zu Abs. 6
Es handelt sich um eine Folgeänderung aufgrund der Regelung der hypothetischen Datenneuerhebung in der Neufassung des § 20.

Zu Abs. 9
Die bisher in Abs. 9 zu findende Regelung wird in § 17a überführt, sodass der Absatz gestrichen werden kann.

Zu Nr. 9 (§ 15a)

Zu Abs. 2
Die Änderung in Satz 1 und die Bezugnahme in Abs. 2 Satz 6 auf § 29 Abs. 5 bis 7 HSOG-E stellen redaktionelle Anpassungen dar.

Zu Abs. 6
Die bisherige Regelung des Abs. 6 wird gestrichen und der Inhalt des bisherigen Abs. 5a in diesen überführt. Der bisherige Abs. 6 ist überflüssig geworden, da die zweckkonforme und zweckändernde Weiterverarbeitung von Daten unter Beachtung des Grundsatzes der hypothetischen Datenneuerhebung nunmehr einheitlich in § 20 geregelt ist.

Zu Abs. 7
Es handelt sich um eine redaktionelle Anpassung.

Zu Nr. 10 (§ 17)
Der Verweis in § 17 Abs. 2 auf die in § 12 Abs. 2 HSOG-E geregelte Einschränkung der Auskunftspflicht dient der Berücksichtigung des Schutzes zeugnisverweigerungsberechtigter Personen aufgrund des Urteils des Bundesverfassungsgerichts vom 20. April 2016 (Rn. 256 ff.)

Zu Nr. 11 (§ 17a)
Die Vorschrift des neu aufgenommenen § 17a trägt der Forderung des Urteils des Bundverfassungsgerichts vom 20. April 2016 (Rn. 142, 143, 268, 340, 354) Rechnung, dass es zur Transparenz und zur Kontrolle verdeckter Überwachungsmaßnahmen sowie von Datenübermittlungen im internationalen Bereich regelmäßiger Berichtspflichten gegenüber Parlament und Öffentlichkeit bedarf. Zudem wird die bisher in § 15 Abs. 9 HSOG zu findende Regelung in § 17a überführt, um die Berichtspflichten in einer Vorschrift zu regeln.

Zu Nr. 12 (§ 19)
Abs. 6 wird neu in die Vorschrift des § 19 aufgenommen. Hierdurch wird klargestellt, dass für den Fall, dass sich erkennungsdienstliche Maßnahmen nach Abs. 1 bis 5 auf besondere Kategorien personenbezogener Daten beziehen und die Maßnahme zu Zwecken des § 40 HDSIG-E erfolgt § 43 HDSIG-E zu beachten ist, und bei Zwecken außerhalb des § 40 HDSIG-E § 20 HDSIG-E und Art. 9 der Verordnung (EU) Nr. 2016/679.

Zu Nr. 13 (§ 20)

Zu Abs. 1 bis 5
Die bisherigen Abs. 1 bis 3 zur Speicherung und Verarbeitung personenbezogener Daten sowie zur strengen Zweckbindung und zweckändernden Verarbeitung werden gestrichen. Die aktuelle Regelung in Abs. 2 zur Verwendung von Protokollen findet sich nunmehr in veränderter Form in § 71 HDSIG-E und wurde entsprechend der Vorgaben aus Art. 25 der Richtlinie (EU) Nr. 2016/680 ausgestaltet. Der aktuelle Abs. 4 findet sich nunmehr mit einigen Änderungen in Abs. 6.

Die neuen Absätze 1 bis 5 setzen das vom Bundesverfassungsgericht in seinem Urteil vom 20. April 2016 konkretisierte und geprägte Kriterium der hypothetischen Datenneuerhebung im HSOG um. Die Änderungen im HSOG orientieren sich - mit einigen dem HSOG als landesrechtlichem Gesetz über die öffentliche Sicherheit und Ordnung spezifischen Anpassungen - an den Formulierungen in § 12 BKAG-neu. Obgleich Gegenstand des bundesverfassungsgerichtlichen Urteils die eingriffsintensiven und besonders eingriffsintensiven und verdeckten Maßnahmen des BKAG waren, wird das Kriterium der hypothetischen Datenneuerhebung wie in § 12 BKAG-neu auch im HSOG als allgemeiner Grundsatz ausgestaltet, der bei jeder Datenweiterverarbeitung durch die Polizei- und Gefahrenabwehrbehörden zu beachten ist. Dadurch soll ein Gleichlauf mit § 12 BKAG-neu hergestellt werden, der über § 29 Abs. 4 BKAG-neu auch für den polizeilichen Informationsverbund gilt, an dem gemäß § 29 Abs. 3 BKAG-neu u.a. die Polizeibehörden der Länder teilnehmen. Allerdings wird der Grundsatz der hypothetischen Datenneuerhebung im Unterschied zu § 12 BKAG-neu im HSOG nicht auf die Weiterverarbeitung zur Strafverfolgung erstreckt, da nach Art. 74 Abs. 1 Nr. 1 GG der Bundesgesetzgeber die konkurrierende Gesetzgebung in Bezug auf das Strafverfahren innehat und als Annex hierzu auch das jeweilige Datenschutzrecht umfasst ist. Der Bundesgesetzgeber hat insoweit etwa in § 100e Abs. 6 Nr. 3 und § 161 Abs. 2 StPO Regelungen zur Verwendung von personenbezogenen Daten aus verdeckten und eingriffsintensiven polizeirechtlichen Maßnahmen (bspw. die akustische Wohnraumüberwachung, die Online-Durchsuchung und die Überwachung der Telekommunikation) zur Strafverfolgung bzw. in Strafverfahren getroffen. Für (ggf. weitergehende) Regelungen im Landespolizeigesetz zur hypothetischen Datenneuerhebung im Zusammenhang mit der Weiterverarbeitung von auf Grundlage entsprechender polizeirechtlicher Maßnahmen erhobenen personenbezogenen Daten zur Strafverfolgung ist daher kein Raum.

Das Bundesverfassungsgericht hat in seinem Urteil festgestellt, dass sich die Anforderungen an die Nutzung und Übermittlung staatlich erhobener Daten nach den Grundsätzen der Zweckbindung und Zweckänderung und sich die Reichweite der Zweckbindung nach der jeweiligen Ermächtigung für die Datenerhebung richten. Das Bundesverfassungsgericht führt weiter aus (Rn. 286 und 287), dass sich die Verhältnismäßigkeitsanforderungen für eine zweckändernde Nutzung insbesondere von Daten, die aus besonders eingriffsintensiven Maßnahmen stammen, am Grundsatz der hypothetischen Datenneuerhebung orientieren: "Die Ermächtigung zu einer Zweckänderung ist dabei am Verhältnismäßigkeitsgrundsatz zu messen. Hierbei orientiert sich das Gewicht, das einer solchen Regelung im Rahmen der Abwägung zukommt, am Gewicht des Eingriffs der Datenerhebung. Informationen, die durch besonders eingriffsintensive Maßnahmen erlangt wurden, können auch nur zu besonders gewichtigen Zwecken benutzt werden (vgl. BVerfGE 100, 313 <394>; 109, 279 <377>; 133, 277<372 f. Rn. 225> m.w.N.). [....] Für Daten aus eingriffsintensiven Überwachungs- und Ermittlungsmaßnahmen wie denen des vorliegenden Verfahrens kommt es danach darauf an, ob die entsprechenden Daten nach verfassungsrechtlichen Maßstäben neu auch für den geänderten Zweck mit vergleichbar schwerwiegenden Mitteln erhoben werden dürften".

Zu Abs. 1
Satz 1 sieht vor, dass die Weiterverarbeitung von personenbezogenen Daten zur Erfüllung derselben Aufgabe und zum Schutz derselben Rechtsgüter oder sonstigen Rechte oder zur Verhütung derselben Straftaten oder Ordnungswidrigkeiten durch die Gefahrenabwehr- und Polizeibehörden, die die Daten selbst erhoben haben, nicht den verfassungsrechtlichen Anforderungen an eine Zweckänderung unterliegt. Die Weiterverarbeitung meint in diesem Zusammenhang die zweckkonforme Verarbeitung, die keine zweckändernde Verarbeitung bzw. Weiterverarbeitung darstellt.

Das Bundesverfassungsgericht führt hierzu in seinem Urteil aus (Rn. 278 f., 282): "Der Gesetzgeber kann eine Datennutzung über das für die Datenerhebung maßgebende Verfahren hinaus als weitere Nutzung im Rahmen der ursprünglichen Zwecke dieser Daten erlauben. Er kann sich insoweit auf die der Datenerhebung zugrundeliegenden Rechtfertigungsgründe stützen und unterliegt damit nicht den verfassungsrechtlichen Anforderungen an eine Zweckänderung. a) Die zulässige Reichweite solcher Nutzungen richtet sich nach der Ermächtigung für die Datenerhebung. Die jeweilige Eingriffsgrundlage bestimmt Behörde, Zweck und Bedingungen der Datenerhebung und definiert damit die erlaubte Verwendung. Die Zweckbindung der auf ihrer Grundlage gewonnenen Informationen beschränkt sich folglich nicht allein auf eine Bindung an bestimmte, abstrakt definierte Behördenaufgaben, sondern bestimmt sich nach der Reichweite der Erhebungszwecke in der für die jeweilige Datenerhebung maßgeblichen Ermächtigungsgrundlage. Eine weitere Nutzung innerhalb der ursprünglichen Zwecksetzung kommt damit nur seitens derselben Behörde im Rahmen derselben Aufgabe und für den Schutz derselben Rechtsgüter in Betracht wie für die Datenerhebung maßgeblich: Ist diese nur zum Schutz bestimmter Rechtsgüter oder zur Verhütung bestimmter Straftaten erlaubt, so begrenzt dies deren unmittelbare sowie weitere Verwendung auch in derselben Behörde, soweit keine gesetzliche Grundlage für eine zulässige Zweckänderung eine weitergehende Nutzung erlaubt. [....] Für die Wahrung der Zweckbindung kommt es demnach darauf an, dass die erhebungsberechtigte Behörde die Daten im selben Aufgabenkreis zum Schutz derselben Rechtsgüter und zur Verfolgung oder Verhütung derselben Straftaten nutzt, wie es die jeweilige Datenerhebungsvorschrift erlaubt."

Als landespolizeigesetzliche Ausgestaltung im Hinblick auf die Aufgaben der Gefahrenabwehr- und Polizeibehörden werden die Begriffe "sonstigen Rechte" und "Ordnungswidrigkeiten" ergänzt. Klarstellend wird zudem die Formulierung "unter Berücksichtigung der jeweiligen Datenerhebungsvorschrift" aufgenommen, um zu verdeutlichen, dass eine Bestimmung derselben Aufgabe und derselben Rechtsgüter, Rechte, Straftaten oder Ordnungswidrigkeiten anhand der Reichweite der Erhebungszwecke in der maßgeblichen Ermächtigungsgrundlage vorzunehmen ist.

Satz 2 regelt die entsprechende Anwendung von Satz 1 für personenbezogene Daten, denen keine Erhebung vorausgegangen ist - dazu gehören beispielsweise auch unaufgefordert durch Dritte erlangte Daten. Danach soll Satz 1 mit der Maßgabe gelten, dass aufgrund der fehlenden Datenerhebungsvorschrift für die Bestimmung derselben Aufgabe und derselben Rechtsgüter etc. der Zweck der Speicherung heranzuziehen ist. Diese Systematik folgt dem bisherigen Verständnis bei der Behandlung solcher Daten, vgl. etwa § 14 Abs. 1 Satz 1 Bundesdatenschutzgesetz.

Satz 3 trägt den besonderen Anforderungen des Bundesverfassungsgerichts an die Zweckbindung für Daten aus Maßnahmen durch den Einsatz technischer Mittel in oder aus Wohnungen Rechnung. Aufgrund des besonderen Eingriffsgewichts solcher Datenerhebungen gilt hier eine besonders enge Bindung der weiteren Nutzung der bei diesen Maßnahmen gewonnenen Daten an die Voraussetzungen und Zwecke der Datenerhebung. Das Bundesverfassungsgericht führt hierzu aus (Rn. 283): "Weiter reicht die Zweckbindung allerdings für Daten aus Wohnraumüberwachungen und Online-Durchsuchungen: Hier ist jede weitere Nutzung der Daten nur dann zweckentsprechend, wenn sie auch aufgrund einer den Erhebungsvoraussetzungen entsprechenden dringenden Gefahr (vgl. BVerfGE 109, 279 <377, 379>) oder im Einzelfall drohenden Gefahr (vgl. BVerfGE 120, 274 <326, 328 f.>) erforderlich ist. Das außerordentliche Eingriffsgewicht solcher Datenerhebungen spiegelt sich hier auch in einer besonders engen Bindung jeder weiteren Nutzung der gewonnenen Daten an die Voraussetzungen und damit Zwecke der Datenerhebung. Eine Nutzung der Erkenntnisse als bloßer Spuren- oder Ermittlungsansatz unabhängig von einer dringenden oder im Einzelfall drohenden Gefahr kommt hier nicht in Betracht."

Für die Verarbeitung von personenbezogenen Daten, die aus Maßnahmen durch den Einsatz technischer Mittel in oder aus Wohnungen nach § 15 Abs. 4 erlangt wurden, sieht Satz 3 daher vor, dass eine Gefahr im Sinne der Vorschrift vorliegen muss.

Zu Abs. 2

Satz 1 setzt die Vorgaben des Bundesverfassungsgerichts an die zweckändernde Verarbeitung von personenbezogenen Daten um und führt den Grundsatz der hypothetischen Datenneuerhebung als allgemeinen Grundsatz in das HSOG ein. Das Bundesverfassungsgericht (Rn. 288 bis 290) hat zum Grundsatz der hypothetischen Datenneuerhebung ausgeführt: "Voraussetzung für eine Zweckänderung ist danach aber jedenfalls, dass die neue Nutzung der Daten dem Schutz von Rechtsgütern oder der Aufdeckung von Straftaten eines solchen Gewichts dient, die verfas-

sungsrechtlich ihre Neuerhebung mit vergleichbar schwerwiegenden Mitteln rechtfertigen könnten (vgl. BVerfGE 100, 313 <389 f.>; 109, 279 <377>; 110, 33 <73>; 120, 351 <369>; 130, 1 <34>). Nicht in jedem Fall identisch sind die Voraussetzungen einer Zweckänderung mit denen einer Datenerhebung hingegen hinsichtlich des erforderlichen Konkretisierungsgrades der Gefahrenlage oder des Tatverdachts. Die diesbezüglichen Anforderungen bestimmen unter Verhältnismäßigkeitsgesichtspunkten primär den Anlass nur unmittelbar für die Datenerhebung selbst, nicht aber auch für die weitere Nutzung der erhobenen Daten. Als neu zu rechtfertigender Eingriff bedarf aber auch die Ermächtigung zu einer Nutzung für andere Zwecke eines eigenen, hinreichend spezifischen Anlasses. Verfassungsrechtlich geboten, aber regelmäßig auch ausreichend, ist insoweit, dass sich aus den Daten - sei es aus ihnen selbst, sei es in Verbindung mit weiteren Kenntnissen der Behörde - ein konkreter Ermittlungsansatz ergibt. Der Gesetzgeber kann danach - bezogen auf die Datennutzung von Sicherheitsbehörden - eine Zweckänderung von Daten grundsätzlich dann erlauben, wenn es sich um Informationen handelt, aus denen sich im Einzelfall konkrete Ermittlungsansätze zur Aufdeckung von vergleichbar gewichtigen Straftaten oder zur Abwehr von zumindest auf mittlere Sicht drohenden Gefahren für vergleichbar gewichtige Rechtsgüter wie die ergeben, zu deren Schutz die entsprechende Datenerhebung zulässig ist."

Satz 1 Nr. 1 und 2 erfüllen diese verfassungsrechtlichen Anforderungen und lassen die Weiterverarbeitung personenbezogener Daten zur Erfüllung der Aufgaben der Gefahrenabwehr- und Polizeibehörden zu anderen Zwecken als denjenigen, zu denen sie erhoben worden sind, nur zu, wenn mindestens vergleichbar gewichtige Straftaten oder Ordnungswidrigkeiten verhütet oder mindestens vergleichbar gewichtige Rechtsgüter oder sonstige Rechte geschützt werden sollen und sich im Einzelfall konkrete Ermittlungsansätze zur Verhütung solcher Straftaten ergeben oder zur Abwehr von in einem übersehbaren Zeitraum drohenden Gefahren für solche Rechtsgüter oder sonstigen Rechte erkennen lassen, zu deren Schutz die entsprechende Datenerhebung verfassungsrechtlich zulässig wäre. Im Vergleich zu § 12 Abs. 2 BKAG-neu werden jedoch landesrechtlich notwendige Ergänzungen im Hinblick auf die Aufgaben der Gefahrenabwehr- und Polizeibehörden vorgenommen und die Begriffe "sonstige Rechte" und "Ordnungswidrigkeiten" eingefügt.

Klarstellend wird - wie schon bei Abs. 1 - die Formulierung "unter Berücksichtigung der jeweiligen Datenerhebungsvorschrift" aufgenommen, um zu verdeutlichen, dass hier eine Bestimmung der vergleichbar bedeutsamen Rechtsgüter (Individual- und Universalrechtsgüter) oder sonstigen Rechte oder vergleichbar schwerwiegenden Straftaten oder Ordnungswidrigkeiten nicht anhand einer objektivierten Vergleichbarkeit, sondern anhand der Erhebungsschwellen in den jeweiligen maßgeblichen Ermächtigungsgrundlagen vorzunehmen ist. Mit der Formulierung "vergleichbar schwerwiegend" werden keine gleichgewichtigen Zwecke vorausgesetzt, sondern die "Vergleichbarkeit" folgt aus den jeweiligen Erhebungsschwellen. Wenn etwa bei einer Telekommunikationsüberwachung, die zur Abwehr einer Lebensgefahr erfolgt, Zufallserkenntnisse zu einem anderen Lebenssachverhalt mit Anhaltspunkten für eine Freiheitsgefahr anfallen, kann auch diese andere Gefahr mit diesem Spurenansatz weiter erforscht werden. Die Abwehr der Freiheitsgefahr erscheint zwar gegenüber der Abwehr der Lebensgefahr auf den ersten Blick nicht gleichgewichtig, sie ist jedoch im Hinblick auf die Erhebungsschwelle vergleichbar gewichtig. Insbesondere bei offenen Maßnahmen ist eine solche Betrachtungsweise unumgänglich, da hier aufgrund der regelmäßig niedrigen Erhebungsschwellen kein Grund besteht, die Verwendung von etwa zum Schutz eines bedeutsamen bzw. hochwertigen Rechtsguts (z.B. Leib oder Leben) durch eine offene Maßnahme erhobenen Daten auch für ein weniger bedeutsames Rechtsgut (z.B. Eigentum) auszuschließen. Unter Berücksichtigung der jeweiligen Datenerhebungsvorschrift ist beispielsweise bei einer Befugnisnorm zur offenen Datenerhebung, die keine Beschränkung auf bestimmte Rechtsgüter enthält, jedes Rechtsgut vergleichbar bedeutsam, sodass entsprechend erhobene Daten beim Vorliegen der übrigen Voraussetzungen des Satz 1 weiterverarbeitet werden können.

Die in Abs. 2 Satz 1 Nr. 2 Buchst. b verwendete Formulierung "in einem übersehbaren Zeitraum drohenden Gefahren für mindestens vergleichbar bedeutsame Rechtsgüter" erfordert, dass sich etwa eine Gefahr für mindestens vergleichbar bedeutsame Rechtsgüter oder sonstige Rechte, zu deren Schutz die ursprüngliche Datenerhebung vorgenommen wurde, nicht nur abstrakt, sondern vielmehr als eine in ersten Umrissen absehbare und konkretisierte Möglichkeit eines Schadenseintrittes für ein solches Rechtsgut oder sonstiges Recht darstellt.

Satz 2 sieht vor, dass die strengen Vorgaben der Zweckbindung und der Grundsatz der hypothetischen Datenneuerhebung nicht gelten, wenn die vorhandenen zur Identifizierung dienenden Daten einer Person (Grunddaten) zu Identifizierungszwecken - nicht aber Identitätsfeststellungen aufgrund spezialgesetzlicher Befugnisnormen - verwendet werden sollen. Die zweifelsfreie Klärung der Identität einer Person ist notwendig, um Identitätsverwechslungen auszuschließen und damit zu verhindern, dass Eingriffe in die Grundrechte von unbeteiligten Personen stattfinden. Aufgrund der in doppelter Weise eng begrenzten Datenverwendung ist das Eingriffsgewicht dieser Maßnahme folglich mit der Rechtsprechung des Bundesverfassungsgerichts zu vereinbaren.

Satz 3 regelt, dass der Grundsatz der hypothetischen Datenneuerhebung die Nutzung personenbezogener Daten etwa zu Zwecken der wissenschaftlichen Forschung, der Aus- und Fortbildung und zur Vorgangsbearbeitung nicht ausschließt und auch besondere Verwendungsregelungen und -beschränkungen weiterhin möglich sind.

Satz 4 regelt die entsprechende Anwendung von Satz 1 bis 3 für personenbezogene Daten, denen keine Erhebung vorausgegangen ist, wozu auch unaufgefordert durch Dritte erlangte Daten gehören. Wie schon bei Abs. 1 soll aufgrund der fehlenden Datenerhebungsvorschrift hier für die Bestimmung der Vergleichbarkeit der Rechtsgüter etc. der Zweck der Speicherung herangezogen werden.

Zu Abs. 3
Satz 1 trägt den besonderen Anforderungen des Bundesverfassungsgerichts (Rn. 291) an die zweckändernde Nutzung von Daten aus Maßnahmen durch den Einsatz technischer Mittel in oder aus Wohnungen Rechnung. Ihre Verwendung zu einem geänderten Zweck ist im Falle des Vorliegens einer Gefahr nur möglich, wenn eine im einzelnen Fall bestehende Gefahr (§ 11 HSOG) im Sinne des § 15 Abs. 4 vorliegt.

Satz 2 untersagt, dass Erkenntnisse aus optischen Wohnraumüberwachungen zu Strafverfolgungszwecken verwendet werden dürfen und dient damit der Umsetzung der besonderen Vorgaben des Bundesverfassungsgerichts zum Verbot der Verwendung von personenbezogenen Daten aus der optischen Wohnraumüberwachung für die Strafverfolgung (Rn. 317). Diese Regelung im HSOG ist notwendig, um Art. 13 Abs. 3 GG gerecht zu werden, der für die Strafverfolgung nur den Einsatz der akustischen Wohnraumüberwachung vorsieht und dies nach Auffassung des Bundesverfassungsgerichts durch eine Übermittlung von Daten aus einer präventiv angeordneten optischen Wohnraumüberwachung nicht unterlaufen werden darf.

Zu Abs. 4
In Abs. 4 wird neu die Verpflichtung zur Sicherstellung der Beachtung der Abs. 1 bis 3 durch organisatorische und technische Maßnahmen nach dem Vorbild des § 12 Abs. 5 BKAG-neu normiert, um insbesondere die Einhaltung der Grundsätze der hypothetischen Datenneuerhebung in polizeilichen Informationssystemen zu gewährleisten. Diese Verpflichtung ist beispielsweise näher in der speziellen Regelung zur Kennzeichnung in § 20a HSOG-E ausgestaltet.

Zu Abs. 5
Der neue Abs. 5 soll aufgrund des Wegfalls des bisherigen § 20 Abs. 1 und 3 HSOG unter Verweis auf § 20 Abs. 1 bis 4 HSOG-E klarstellen, dass eine Weiterverarbeitung stets an die Erforderlichkeit der Aufgabenerfüllung geknüpft und an die Vorgaben der neuen Abs. 1 bis 4 gebunden ist, soweit dieses oder ein anderes Gesetz keine besonderen Regelungen und Weiterverarbeitungserfordernisse vorsieht. Von der Regelung werden sowohl die zweckkonforme als auch die zweckändernde Weiterverarbeitung umfasst, wobei stets der Grundsatz der hypothetischen Datenneuerhebung zu beachten ist.

Zu Abs. 6
Die bisherigen Sätze des Abs. 6 werden gestrichen. Die Regelung in Abs. 6 Satz 2 zur Kennzeichnung findet sich nunmehr in einer neuen Regelung in § 20a HSOG-E.

Der bisherige Abs. 4 wird Abs. 6. Die Änderung in Satz 1 ist redaktioneller Art, während durch die Änderung in Satz 2 im Zusammenhang mit Satz 1 geregelt werden soll, dass Abs. 6 künftig für jegliche Form der Weiterverarbeitung - auch der automatisierten - von personenbezogenen Daten aus der Strafverfolgung zur Abwehr einer Gefahr und zur vorbeugenden Bekämpfung von Straftaten anwendbar sein soll. Damit gilt auch die Verdachtsregelung des Satz 2 für alle Formen der Weiterverarbeitung und nicht nur in automatisierten Verfahren.

Diese Änderung ist u.a. notwendig, um die rechtlichen Grundlagen für mögliche künftige Entwicklungen bspw. im Bereich der Digitalisierung von Kriminalakten zu schaffen.

Zu Abs. 7
Der bisherige Abs. 5 wird Abs. 7 und vor dem Hintergrund des Wegfalls des bisherigen § 20 Abs. 1 und 3 HSOG geändert und ergänzt, um eine Rechtsgrundlage für jegliche Form der Weiterverarbeitung - auch der automatisierten - von personenbezogenen Daten zu Personen nach § 13 Abs. 2 Nr. 1 bis 5 HSOG-E zur vorbeugenden Bekämpfung von Straftaten zu schaffen.

Zu Abs. 8
Der bisherige Abs. 7 wird Abs. 8. Bei den Änderungen in Satz 1 handelt es sich zum einen um eine Anpassung an die mit Änderungsgesetz vom 14. Dezember 2010 (GVBl. I S. 536) im Verwaltungsfachhochschulgesetz eingeführte Bezeichnung der Verwaltungsfachhochschule und um eine redaktionelle Änderung. Zum anderen wird hier auch die Weiterverarbeitung von Daten zur effektiven Wirksamkeitskontrolle, d.h. zu Evaluierungszwecken, aufgenommen, um

auch diese im erforderlichen Maße von den strengen Vorgaben der allgemeinen Datenweiterverarbeitungsregelungen auszunehmen.

Durch die Änderungen in Satz 3 und 4 wird geregelt, dass die Weiterverarbeitung personenbezogener Daten aus besonders eingriffsintensiven Maßnahmen nicht zulässig ist, außer die Weiterverarbeitung ist zu Zwecken des Satz 1 unerlässlich. Damit wird dem Grundsatz der hypothetischen Datenneuerhebung in ausreichendem Maße Rechnung getragen.

Zu Abs. 9
Der bisherige Abs. 8 wird Abs. 9. Im Rahmen der Zuverlässigkeitsüberprüfung nach den §§ 13a und 13b HSOG-E kann es notwendig sein, auch auf die Daten der polizeilichen Vorgangsverwaltung zugreifen zu können. Damit soll sichergestellt werden, dass das Datenmaterial, auf das zurückgegriffen wird, auch die aktuellen Daten erhält, die im Rahmen der Vorgangsverwaltung eingegeben werden und aufgrund ihrer Aktualität noch keinen Eingang in weitere polizeiliche Systeme gefunden haben. Dies wird durch die Ergänzung in Satz 1 sichergestellt. Bei den weiteren Änderungen in Satz 1 und 2 handelt es sich um redaktionelle Anpassungen.

Zu Abs. 10

Die aktuelle Regelung des Abs. 10 findet sich nunmehr in § 29 Abs. 4 HSOG-E. Damit werden die Benachrichtigungs- und Unterrichtungspflichten, auch bei der Weiterverarbeitung personenbezogener Daten von Kindern in einer Vorschrift zusammengefasst.

Der bisherige Abs. 9 wird Abs. 10 und redaktionell angepasst.

Zu Abs. 11
Bei der Änderung in Abs. 11 handelt es sich um eine redaktionelle Anpassung.

Zu Abs. 12
Der bisherigen Regelung wird ein neuer Abs. 12 angefügt.

In Satz 1 wird die neue Regelung zur Einwilligung in § 13 Abs. 9 HSOG-E auch bei der Weiterverarbeitung personenbezogener Daten für entsprechend anwendbar erklärt.

In Satz 2 wird klarstellend auf den neuen § 68 HDSIG-E hingewiesen, der die bisherige Regelung aus Abs. 6 Satz 1 zu Bewertungen ersetzt.

Schließlich wird in Satz 3 in Anlehnung an § 16 Abs. 6 BKAG-neu die Weiterverarbeitung personengebundener und ermittlungsunterstützender Hinweise, die auf Grundlage von objektiven Erkenntnissen und möglichst umfassenden Informationen zur betreffenden Person gewonnen werden, geregelt.

Zu Nr. 14 (§§ 20a, 20b)

Zu § 20a
Der Grundsatz der hypothetischen Datenneuerhebung lässt sich in den polizeilichen Informationssystemen nur umsetzen, wenn die darin gespeicherten personenbezogenen Daten mit den notwendigen Zusatzinformationen versehen sind - mithin gekennzeichnet sind. Hierzu wird in Anlehnung an die Vorschrift des § 14 BKAG-neu die Regelung des § 20a neu in das HSOG-E aufgenommen.

Zu Abs. 1
Satz 1 sieht vor, dass personenbezogene Daten bei der Speicherung in polizeilichen Informationssystemen, zu denen Systeme gehören sollen, die dem polizeilichen Informationsaustausch und der Auskunft dienen und nicht etwa der Vorgangsverwaltung, zu kennzeichnen sind. Diese Kennzeichnungspflicht erfolgt durch Angabe des Mittels der Erhebung der Daten einschließlich der Angabe, ob die Daten offen oder verdeckt erhoben wurden (Nr. 1), bei Personen, zu denen Grunddaten angelegt wurden, durch die Angabe der Kategorie der betroffenen Person (Nr. 2), durch die Angabe der Rechtsgüter oder sonstigen Rechte, deren Schutz die Erhebung dient oder der Straftaten oder Ordnungswidrigkeiten, deren Verfolgung oder Verhütung die Erhebung dient (Nr. 3), und durch die Angabe der Stelle, die sie erhoben hat (Nr. 4). Die Kennzeichnungspflicht schafft die Voraussetzung für eine umfassende Anwendung des Grundsatzes der hypothetischen Datenneuerhebung.

Nach Satz 2 kann die Kennzeichnung auch durch eine Angabe der Rechtsgrundlage der der Erhebung zugrundeliegenden Mittel ergänzt werden.

In Satz 3 wird geregelt, dass personenbezogene Daten, denen keine Erhebung vorausgegangen ist, soweit möglich, nach Satz 1 zu kennzeichnen sowie die erste datenverarbeitende Stelle und, soweit möglich, der Dritte, von dem die Daten erlangt wurden, anzugeben sind.

Zu Abs. 2
Zur Vermeidung einer Weiterverarbeitung von Daten, die nicht den Vorgaben der hypothetischen Datenneuerhebung entspricht, bestimmt Abs. 2, dass personenbezogene Daten, die nicht den Anforderungen des Abs. 1 entsprechend gekennzeichnet sind, solange nicht weiterverarbeitet werden dürfen, bis eine entsprechende Kennzeichnung erfolgt ist.

Zu Abs. 3
Damit gewährleistet ist, dass der Grundsatz der hypothetischen Datenneuerhebung auch bei der Weiterverarbeitung von Daten bei anderen Stellen beachtet werden kann, regelt Abs. 3, dass die nach Abs. 1 vorzunehmende Kennzeichnung im Falle der Übermittlung der Daten durch die empfangende Stelle aufrechtzuerhalten ist.

Zu Abs. 4
Abs. 4 regelt verschiedene notwendige Ausnahmen zur Kennzeichnungspflicht. In Satz 1 handelt es sich um die tatsächliche Unmöglichkeit einer Kennzeichnung - etwa, wenn nicht bekannt oder feststellbar ist, wer die Daten erhoben hat oder zu welchem Zweck sie ursprünglich erhoben wurden. In Satz 2 werden die Fälle der technischen Unmöglichkeit und des unverhältnismäßigen Aufwands einer Kennzeichnung geregelt. Satz 2 soll jedoch in Verbindung mit § 115 HSOG-E nur mit einer Befristung Anwendung finden.

Zu § 20b
In § 20b wird eine Vorschrift zur Weiterverarbeitung personenbezogener Daten für die wissenschaftliche Forschung in das HSOG-E aufgenommen.

Zu Abs. 1
Abs. 1 stellt klar, dass abweichend von §§ 24 und 45 HDSIG-E die Weiterverarbeitung und Übermittlung personenbezogener Daten, die aus in § 20 Abs. 3 (verdeckter Einsatz technischer Mittel in oder aus Wohnungen nach § 15 Abs. 4) genannten Maßnahmen erlangt wurden, nicht zulässig ist, außer die Weiterverarbeitung ist für die polizeiliche Eigenforschung und eine effektive Wirksamkeitskontrolle, d.h. Evaluierung, unerlässlich. Damit trägt die Regelung dem Grundsatz der hypothetischen Datenneuerhebung in ausreichendem Maße Rechnung. Hierbei handelt es sich im Zusammenhang mit § 24 HDSIG-E um eine mitgliedstaatliche Bestimmung im Sinne des Art. 6 Abs. 3 in Verbindung mit Art. 6 Abs. 1 Buchst. e der Verordnung (EU) Nr. 2016/679.

Zu Abs. 2
In Abs. 2 wird die Übermittlung personenbezogener Daten im Anwendungsbereich des HSOG-E auf Amtsträger oder für den öffentlichen Dienst besonders Verpflichtete oder zur Geheimhaltung Verpflichtete beschränkt.

Zu Abs. 3
Durch Abs. 3 soll gewährleistet werden, dass die Daten gegen unbefugte Kenntnisnahme geschützt sind und die hierfür notwendigen technischen und organisatorischen Maßnahmen getroffen werden.

Zu Nr. 15 (§ 21)

Zu Abs. 1
Die Änderung in Abs. 1 Satz 1 dient u.a. der Umsetzung der vom Bundesverfassungsgericht in seinem Urteil vom 20. April 2016 aufgestellten Anforderungen des Grundsatzes der hypothetischen Datenneuerhebung zur Zweckbindung und Zweckänderung im Hinblick auf die Datenübermittlung (Rn. 307 ff.). Die Übermittlungsbeschränkungen betreffend Bewertungen, welche bisher in Abs. 3 Satz 1 und 2 geregelt sind, werden in Abs. 1 Satz 3 und 4 aufgenommen.

Zu Abs. 2
In Abs. 2 wird die bisherige Vorschrift des § 21 Abs. 2 gestrichen und stattdessen ein Übermittlungsverbot nach Vorbild des § 28 Abs. 1 BKAG-neu eingefügt. Das hier statuierte Verbot bezieht sich auf sämtliche Datenübermittlungsvorschriften und gilt demnach für Übermittlungen im Inland, an Stellen in Mitgliedstaaten der Europäischen Union und an das internationale Ausland.

Zu Abs. 3
Die bisherige Regelung des Abs. 3 Satz 1 und 2 wird in Abs. 1 Satz 3 und 4 neu aufgenommen. Die bisherige Regelung des Abs. 3 Satz 3 wird durch die Einführung des Grundsatzes der hypothetischen Datenneuerhebung in § 20 und die Vorschrift des § 20a zur Kennzeichnung personenbezogener Daten ersetzt.

Neu aufgenommen werden in Abs. 3 besondere Übermittlungsverbote bei Datenübermittlungen nach den Vorschriften der §§ 22 Abs. 5 und 23. Die in Abs. 3 genannten Gründe sind als Prüfungsmaßstab für Datenübermittlungen an Stellen in Mitgliedstaaten der Europäischen Union und an Stellen im internationalen Ausland zugrunde zu legen. Um den Anforderungen des Bun-

desverfassungsgerichts in seinem Urteil vom 20. April 2016 (Rn. 328) gerecht zu werden, wird die Besorgnis einer Verletzung von elementaren Rechtsgrundsätzen und Menschenrechten als Beispiel in Abs. 3 Nr. 4 aufgenommen.

Zu Abs. 4
Die bisherige Regelung des § 21 Abs. 4 wird in Anlehnung an § 25 Abs. 5 BKAG-neu um die Verweise auf die Stellen nach § 61 des Bundeszentralregistergesetzes sowie auf die Verwertungsverbote nach § 52 und § 63 des Bundeszentralregistergesetzes erweitert.

Zu Abs. 5
Abs. 5 entspricht der bisherigen Regelung des § 21 Abs. 5.

Zu Abs. 6
Abs. 6 Satz 1 zur zweckkonformen Verarbeitung übermittelter personenbezogener Daten entspricht unter Ersetzung des Begriffspaars "die Empfängerin oder der Empfänger" durch die "empfangende Stelle" dem bisherigen Abs. 6. Die Regelung wird in Satz 2 erweitert um die Variante der zweckändernden Verarbeitung und dient der Umsetzung der vom Bundesverfassungsgericht in seinem Urteil vom 20. April 2016 aufgestellten Anforderungen des Grundsatzes der hypothetischen Datenneuerhebung an die weitere Verarbeitung der Daten durch die empfangende Stelle. Auch die empfangende Stelle hat künftig die Voraussetzungen des Grundsatzes der hypothetischen Datenneuerhebung zu berücksichtigen, wenn sie die übermittelten Daten zu anderen Zwecken, als zu denen die Daten übermittelt wurden, verarbeiten will. Abs. 6 Satz 2, 2. Halbsatz macht die zweckändernde Verarbeitung von personenbezogenen Daten, welche nach § 22 Abs. 3 an eine nicht öffentliche Stelle übermittelt worden sind, einschränkend von der Zustimmung der übermittelnden Gefahrenabwehr- oder Polizeibehörde abhängig. In Abs. 6 Satz 3 wird die bisherige Regelung des § 22 Abs. 3 Satz 3 HSOG aufgenommen, die empfangende Stelle ist auf die ihr obliegende Pflicht zur zweckkonformen Verarbeitung der übermittelten Daten hinzuweisen. Abs. 6 Satz 4 übernimmt für den Anwendungsbereich des § 22 Abs. 5 HSOG-E in Anlehnung an die Regelung des bisherigen § 23 Abs. 3 HSOG und unter Verweis auf Satz 2 und 3 die dort geregelten Bestimmungen zur Zulässigkeit einer zweckändernden Weiterverarbeitung übermittelter Daten und Hinweispflichten.

Zu Abs. 7
In Abs. 7 wird in Anlehnung an § 25 Abs. 9 BKAG-neu eine Regelung zur Übermittlung von in Akten verbundenen personenbezogenen Daten in das HSOG-E für den Fall eingeführt, dass eine Trennung derjenigen personenbezogenen Daten, die übermittelt werden dürfen, von den weiteren personenbezogenen Daten der betroffenen Person oder eines Dritten nicht oder nur mit unverhältnismäßigem Aufwand möglich ist, soweit nicht berechtigte Interessen der betroffenen Person oder eines Dritten an der Geheimhaltung offensichtlich überwiegen; Abs. 8, 2. Halbsatz schließt eine Verwendung dieser mitübermittelten Daten aus.

Zu Abs. 8
Der neue Abs. 8 enthält unverändert die bisherige Regelung des § 21 Abs. 7.

Zu Nr. 16 (§ 22)
Die Vorschrift regelt die Datenübermittlung im innerstaatlichen Bereich sowie im Bereich der Europäischen Union und deren Mitgliedstaaten.

Zu Abs. 1
Abs. 1 entspricht weitgehend der Regelung des bisherigen § 22 Abs. 1. Abs. 1 Satz 2 wird allerdings dahin gehend geändert, dass die Regelung auf die Datenübermittlung zwischen Polizeibehörden im innerstaatlichen Bereich beschränkt wird. Vorschriften zur Übermittlung personenbezogener Daten an Stellen in Mitgliedstaaten der Europäischen Union oder deren Mitgliedstaaten sowie der am Schengen-Besitzstand teilhabenden assoziierten Staaten werden in Abs. 5 zusammengeführt. Die Regelung des bisherigen Abs. 1 Satz 4 wird aufgrund der Einführung des Grundsatzes der hypothetischen Datenneuerhebung gestrichen, sodass der bisherige Satz 5 nunmehr Satz 4 wird. Bei der Änderung in Satz 4 handelt es sich um eine redaktionelle Anpassung.

Zu Abs. 2
Abs. 2 übernimmt weitgehend die Regelung des bisherigen § 22 Abs. 2. Unter Beachtung des § 20 Abs. 2 und 3, welcher über die Vorschrift des § 21 Abs. 1 HSOG-E vorliegend zur Anwendung kommt, wird der Grundsatz der hypothetischen Datenneuerhebung für die Übermittlungen an öffentliche Stellen, die keine polizeilichen Aufgaben wahrnehmen, umgesetzt. In seinem Urteil vom 20. April 2016 führt das Bundesverfassungsgericht (Rn. 287) aus, dass, "die Tatsache, dass die Zielbehörde bestimmte Datenerhebungen, zu denen die Ausgangsbehörde berechtigt ist, ihrerseits wegen ihres Aufgabenspektrums nicht vornehmen darf, einem Datenaustausch nicht prinzipiell" entgegensteht. In Abs. 2 Satz 2 wird im Sinne der rechtssprachlichen Einheitlichkeit der Begriff "benachrichtigen" anstelle "unterrichten" zugrunde gelegt.

Zu Abs. 3
Die bisher in § 22 Abs. 3 zu findende Regelung zur Übermittlung personenbezogener Daten an ausländische öffentliche Stellen und an über- und zwischenstaatliche Stellen wird nunmehr in § 22 Abs. 5 verortet. Der neu formulierte Abs. 3 regelt die Voraussetzungen für eine Übermittlung personenbezogener Daten an nicht öffentliche Stellen. Unter Beachtung des § 20 Abs. 2 und 3, welcher über die Vorschrift des § 21 Abs. 1 HSOG-E vorliegend zur Anwendung kommt, wird der Grundsatz der hypothetischen Datenneuerhebung für die Übermittlungen an nicht öffentliche Stellen umgesetzt. Abs. 3 Satz 3 und 4 überführen unter Erweiterung des Wortlauts und redaktionellen Änderungen die Regelung des bisherigen § 23 Abs. 4 Satz 1 und 2. Satz 5 und 6 führen in Anlehnung an § 25 Abs. 3 und 4 BKAG-neu eine Regelung zum Unterbleiben der Löschung oder Vernichtung des Nachweises und zu einem Zustimmungserfordernis zu Datenübermittlungen an nicht öffentliche Stellen ein.

Zu Abs. 4
Abs. 4 übernimmt unter redaktioneller Anpassung den Wortlaut des bisherigen § 22 Abs. 4.

Zu Abs. 5
In Abs. 5 wird eine neue Regelung zur Übermittlung personenbezogener Daten an öffentliche und nicht öffentliche Stellen in Mitgliedstaaten der Europäischen Union geschaffen. Hierbei finden die Abs. 1 bis 4 des § 22 entsprechende Anwendung. Abs. 5 Satz 2, welcher die bisherige Regelung des § 22 Abs. 2 a. E. ablöst, eröffnet die Möglichkeit der Datenübermittlung an Polizeibehörden oder sonstige für die Zwecke des § 40 HDSIG-E zuständige öffentliche Stellen der am Schengen-Besitzstand teilhabenden assoziierten Staaten.

Zu Abs. 6
Der neue Abs. 6 übernimmt die Regelung des bisherigen § 22 Abs. 5.

Zu Nr. 17 (§ 23)
§ 23 regelt die Voraussetzungen für die Übermittlung personenbezogener Daten an Stellen in Drittländern oder an andere als die in § 22 Abs. 5 genannten über- und zwischenstaatlichen Stellen. Die in die Vorschrift des § 23 HSOG-E neu aufgenommenen Regelungen hinsichtlich Datenübermittlungen zu Zwecken des § 40 HDSIG-E sind in Verbindung mit den Vorschriften der §§ 73 bis 76 HDSIG-E, bei Übermittlungen zu Zwecken außerhalb des § 40 HDSIG-E in Verbindung mit Art. 44 bis 49 der Verordnung (EU) Nr. 2016/679 zu lesen.

Zu Abs. 1
Abs. 1 findet Anwendung bei Datenübermittlungen der Gefahrenabwehr- und Polizeibehörden an zu Zwecken des § 40 HDSIG-E zuständige öffentliche Stellen in Drittländern und an über- und zwischenstaatliche Stellen in Drittländern, die zu den vorgenannten Zwecken tätig sind. Hierbei sind stets ergänzend die Vorschriften der §§ 73 bis 75 HDSIG-E zu beachten. Unter Beachtung des § 20 Abs. 2 und 3, welcher über die Vorschrift des § 21 Abs. 1 Satz 1 HSOG-E vorliegend zur Anwendung kommt, wird der Grundsatz der hypothetischen Datenneuerhebung für die Datenübermittlungen nach Abs. 1 umgesetzt. Voraussetzung für eine solche Datenübermittlung ist - wie bereits in der bisherigen Regelung des § 22 Abs. 3 HSOG geregelt -, dass diese erforderlich ist zur Erfüllung einer Aufgabe der übermittelnden Gefahrenabwehr- oder Polizeibehörde (Nr. 1) oder zur Abwehr einer erheblichen Gefahr durch die empfangende Stelle (Nr. 2).

Zu Abs. 2
Abs. 2 ermöglicht über die Regelung des Abs. 1 hinaus die Datenübermittlung zu Zwecken des § 40 HDSIG-E an sonstige Empfänger in Drittländern, welche selbst nicht mit Aufgaben nach § 40 HDSIG-E befasst sind. Hierbei ist die Vorschrift des § 76 HDSIG-E ergänzend zu beachten, sodass das Vorliegen der dort genannten strengen Voraussetzungen stets zu prüfen ist. Der Kreis der möglichen Empfänger wird über die in Abs. 1 genannten Stellen auf sonstige (öffentliche) Stellen oder Einrichtungen und Private in Drittländern ausgeweitet. Der Grundsatz der hypothetischen Datenneuerhebung, welcher über die Vorschrift des § 21 Abs. 1 Satz 1 HSOG-E vorliegend zur Anwendung kommt, wird auf diese Weise für die Datenübermittlung im Sinne des Abs. 2 Satz 1 umgesetzt. Abs. 2 Satz 2 lässt unter den Voraussetzungen des Abs. 1 Satz 1 Nr. 1 oder Nr. 2 (Nr. 1 Erfüllung einer Aufgabe der übermittelnden Gefahrenabwehr- oder Polizeibehörde, Nr. 2 Abwehr einer erheblichen Gefahr durch die empfangende Stelle) oder des Abs. 1 Satz 2 darüber hinaus die Datenübermittlung an zwischen- und überstaatliche Organisationen zu, welche nicht mit Aufgaben nach § 40 HDSIG-E betraut sind. Auch insoweit sind die Vorschrift des § 76 HDSIG-E ergänzend zu beachten und der Grundsatz der hypothetischen Datenneuerhebung über die Vorschrift des § 21 Abs. 1 Satz 1 HSOG-E in Ansatz zu bringen.

Zu Abs. 3
Abs. 3 enthält ergänzende Regelungen zu Art. 44 bis 49 der Verordnung (EU) Nr. 2016/679 und damit zu den Übermittlungen personenbezogener Daten außerhalb der Zwecke des § 40 HDSIG-E an öffentliche Stellen in Drittländern oder an andere über- und zwischenstaatliche Stellen als die in § 22 Abs. 5 genannten.

Zu Abs. 4
Der neue Abs. 4 trägt den vom Bundesverfassungsgericht in seinem Urteil vom 20. April 2016 (Rn. 339) aufgestellten Anforderungen an die Vergewisserung - in Form einer fortlaufend aktualisierten Aufstellung - über das Vorhandensein eines datenschutzrechtlich angemessenen und mit elementaren Menschenrechtsgewährleistungen vereinbaren Umgangs mit den übermittelten Daten im Empfängerstaat und Art. 38 der Richtlinie (EU) Nr. 2016/680 Rechnung. Der Bundesgesetzgeber hat in § 28 Abs. 3 BKAG-neu eine entsprechende Regelung aufgenommen. Die seitens des Bundeskriminalamts zu führende Aufstellung über die Einhaltung elementarer rechtsstaatlicher Grundsätze und Menschenrechtsstandards sowie das Datenschutzniveau in den jeweiligen Drittländern bildet eine solche Erkenntnisquelle, die von den hessischen Behörden für eine fortlaufend aktualisierte Aufstellung herangezogen werden kann.

Zu Nr. 18 (§ 24)
Die Änderung in Abs. 1 Satz 2 Nr. 2 resultiert aus der Anpassung an die mit Änderungsgesetz vom 14. Dezember 2010 (GVBl. I S. 536) im Verwaltungsfachhochschulgesetz eingeführte Bezeichnung der Verwaltungsfachhochschule. Der Wortlaut des Abs. 1 Satz 2 Nr. 4 wird um "sonstige öffentliche Stellen" ergänzt, um den bestehenden Anforderungen in Zuverlässigkeitsüberprüfungsverfahren insbesondere auf Grundlage von bereichsspezifischen Vorschriften gerecht zu werden. Der bisherige Abs. 2 zur schriftlichen Festlegung der nach § 10 HDSG erforderlichen technischen und organisatorischen Maßnahmen wird ersetzt durch die in § 59 HDSIG-E zu findende Regelung. Der bisherige Abs. 3 wird in Abs. 1 Satz 4 überführt.

Zu Nr. 19 (§ 26)

Zu Abs. 3
Die in Abs. 3 Satz 2 und 3 erfolgenden Ergänzungen orientieren sich an der Vorschrift des § 48 Abs. 3 BKAG-neu. Die Streichung des bisherigen letzten Halbsatzes des Abs. 3 Satz 3 dient der Umsetzung des Urteils des Bundesverfassungsgerichts vom 20. April 2016 (Rn. 205) zur Aufbewahrungsfrist der Löschungsprotokolle zwecks effektiver Ausübung der Betroffenenrechte und einer wirksamen Kontrolle durch die oder den Hessischen Datenschutzbeauftragten. Der neu aufgenommene Satz 4 wird im Einklang mit § 48 Abs. 3 Satz 4 und 5 BKAG-neu ausgestaltet.

Zu Abs. 5
Die Regelung findet sich jetzt in § 29 Abs. 5 bis 7 HSOG-E und ist zusammengeführt mit den weiteren Regelungen zur Benachrichtigung.

Vorbemerkung zu Nr. 20 und 21 (§§ 27, 27a)
In den §§ 27, 27a HSOG-E finden sich Bestimmungen zu Berichtigung, Löschung und Einschränkung der Verarbeitung personenbezogener Daten. Während § 27 für die Verarbeitung personenbezogener Daten zu Zwecken des § 40 HDSIG-E Anwendung findet, trifft § 27a Regelungen für Verarbeitungen außerhalb des § 40 HDSIG-E. Ausgangspunkt ist für die Bestimmung der Anwendbarkeit der jeweiligen Vorschrift der Zweck, für welchen die personenbezogenen Daten verarbeitet werden, da die gefahrenabwehr- und polizeibehördliche Aufgabenerfüllung nicht in Gänze unter den Anwendungsbereich des § 40 HDSIG-E und die Zwecke des Art. 1 Abs. 1 der Richtlinie (EU) Nr. 2016/680 fällt. Werden Gefahrenabwehr- oder Polizeibehörden zu Zwecken außerhalb des § 40 HDSIG-E tätig, unterfällt die Verarbeitung personenbezogener Daten insoweit der Verordnung (EU) Nr. 2016/679 und dem Ersten und Zweiten Teil des HDSIG-E. Um diese datenschutzrechtliche Zweiteilung bei gefahrenabwehr- und polizeibehördlicher Aufgabenerfüllung auch im Bereich der Berichtigung, Löschung und Einschränkung der Verarbeitung personenbezogener Daten herauszustellen, werden für die beiden Anwendungsbereiche innerhalb und außerhalb der Zwecke des § 40 HDSIG-E eigenständige Vorschriften geschaffen. Mit den Vorschriften der §§ 27, 27a HDSIG-E und der dort erfolgenden Bezugnahme auf § 40 HDSIG-E ist keine Kompetenz- oder Aufgabenerweiterung der Gefahrenabwehr- oder Polizeibehörden verbunden.

Ziel der §§ 27, 27a ist es, für die gefahrenabwehr- und polizeibehördliche Aufgabenerfüllung - unabhängig von der Eröffnung des Anwendungsbereichs des § 40 HDSIG-E - im Bereich der Bestimmungen zu Berichtigung, Löschung und Einschränkung der Verarbeitung personenbezogener Daten einen weitgehenden Gleichlauf herbeizuführen.

Zu Nr. 20 (§ 27)

Zu Abs. 1
In Abs. 1 wird für die Berichtigung, Löschung und Einschränkung der Verarbeitung personenbezogener Daten zu Zwecken des § 40 HDSIG-E auf die grundsätzliche Geltung der §§ 53 und 70 des HDSIG-E verwiesen, soweit keine besonderen Regelungen getroffen werden. Während § 53 HDSIG-E Regelungen zur Löschung, Berichtigung und Einschränkung der Verarbeitung personenbezogener Daten als Betroffenenrechte trifft, finden sich in § 70 HDSIG-E Bestimmungen zur Löschung, Berichtigung und Einschränkung der Verarbeitung personenbezogener Daten von Amts wegen. Dieses System wird in das HSOG-E überführt. Hierbei werden sämtliche in Art.

16 der Richtlinie (EU) Nr. 2016/680 geregelte Rechte umgesetzt. Soweit im bisherigen § 27 HSOG der Begriff der Sperrung der Daten verwendet wird, findet sich nunmehr der in der Richtlinie (EU) Nr. 2016/680 und Verordnung (EU) Nr. 2016/679 verwendete Begriff der Einschränkung der Verarbeitung in den Bestimmungen.

Die bisherige Regelung in § 27 Abs. 1 Satz 2 zu Daten in Akten findet sich nunmehr in Abs. 3. In den Abs. 2 bis 6 finden sich ergänzende oder abweichende Regelungen zu den §§ 53 und 70 des HDSIG-E, die für die Datenverarbeitung im Rahmen des HSOG-E notwendig sind.

Zu Abs. 2
Abs. 2 sieht Ergänzungen zu den §§ 53 Abs. 2 und 70 Abs. 2 HDSIG-E in der Variante der Löschung im Anwendungsbereich des HSOG-E bei Datenverarbeitungen zu Zwecken des § 40 HDSIG-E vor.

In Satz 1 werden in Umsetzung des Art. 16 Abs. 2 der Richtlinie (EU) Nr. 2016/680 die Regelungen aus dem aktuellen § 27 Abs. 2 HSOG überwiegend übernommen und in das neue System eingepasst. Die Regelung des bisherigen § 27 Abs. 2 Nr. 1 (unzulässige Speicherung) findet sich nunmehr sowohl in der Form des Betroffenenrechts als auch in der unmittelbar bestehenden Pflicht des Verantwortlichen in §§ 53 Abs. 2 und 70 Abs. 2 HDSIG-E, weshalb eine ausdrückliche Regelung in Abs. 2 Nr. 1 nicht mehr erforderlich ist. Die bisherigen Nr. 2 und Nr. 3 des § 27 Abs. 2 Satz 1 werden daher mit redaktionellen Anpassungen zu Nr. 1 und Nr. 2 des neuen § 27 Abs. 2 Satz 1, wobei diese Anwendungsfälle eine Konkretisierung der §§ 53 Abs. 2 und 70 Abs. 2 HDSIG-E darstellen.

Der bisherige Abs. 2 Satz 2 zu Daten aus dem Kernbereich privater Lebensgestaltung und anderen Verwertungsverboten sowie die sich bisher in Abs. 2 Satz 3 bis 5 anschließenden Regelungen werden in modifizierter Form in den neu gestalteten Abs. 5 überführt. Der bisherige Abs. 2 Satz 6 wird ersatzlos gestrichen, da der Fall der Einschränkung der Verarbeitung statt Löschung bei Unmöglichkeit oder unverhältnismäßig hohem Aufwand nunmehr neben weiteren Fallgestaltungen, die teilweise denjenigen in § 27 Abs. 6 HSOG entsprechen, in § 53 Abs. 3 HDSIG-E zu finden ist.

Im neuen Satz 2 des Abs. 2 wird abweichend von § 53 Abs. 3 Nr. 1 HDSIG-E die Pflicht begründet, im Fall der verdeckten Datenerhebung nach Abs. 2 Satz 1 Nr. 2 die Verarbeitung der Daten einzuschränken, wenn die betroffene Person über eine verdeckte Datenerhebung noch nicht benachrichtigt worden ist. Folgerichtig wird in dem neuen Satz 3 die bisherige Regelung des § 27 Abs. 7 Satz 2 HSOG zur Verwendung der eingeschränkten Daten zur Benachrichtigung der betroffenen Person sowie zur Ermöglichung der Prüfung der Rechtmäßigkeit der Maßnahme sinngemäß übernommen.

Zu Abs. 3
In Abs. 3 finden sich die besonderen Regelungen zur Berichtigung, Löschung (Vernichtung) und Einschränkung personenbezogener Daten in Akten. Eine Akte ist dabei jede der Aufgabenerfüllung dienende Unterlage, die nicht Teil der automatisierten Datenverarbeitung ist. Die Bestimmung des Begriffs der Akte, die sich im aktuellen § 2 Abs. 7 HDSG findet, soll auch künftig zur Anwendung kommen, obgleich diese Definition im neuen HDSIG-E nicht mehr enthalten ist.

In Satz 1 wird die bisherige Regelung des § 27 Abs. 1 Satz 2 HSOG aufgenommen, wonach die Berichtigung in Akten durch einen Vermerk in der Akte stattfindet oder dies auf sonstige Weise festgehalten wird. Der bisherige Abs. 3 Satz 1, 2. Halbsatz betreffend Daten aus dem Kernbereich privater Lebensgestaltung wird durch die neue Regelung in § 27 Abs. 5 Satz 7 ersetzt. Satz 2 trifft eine der Vorschrift des § 78 Abs. 1 Satz 2 BKAG-neu vergleichbare Regelung im Falle des Bestreitens der Richtigkeit von Daten, bei denen weder die Richtigkeit noch die Unrichtigkeit festgestellt werden kann, und bestimmt die entsprechende Kennzeichnung der Daten, um eine Einschränkung der Verarbeitung nach § 53 Abs. 1 Satz 3 HDSIG-E zu ermöglichen.

Satz 3 greift die Bestimmung des bisherigen § 27 Abs. 3 Satz 1 HSOG sinngemäß auf und regelt unter Orientierung an § 78 BKAG-neu für den Fall der Unzulässigkeit der Verarbeitung sowie für den Fall des Abs. 2 Satz 1 Nr. 1, dass bei der nach bestimmten Fristen vorzunehmenden Überprüfung oder aus Anlass einer Einzelfallbearbeitung festgestellt wird, dass die Kenntnis der personenbezogenen Daten für die speichernde Stelle zur Erfüllung der in ihrer Zuständigkeit liegenden Aufgaben nicht mehr erforderlich ist, die Einschränkung der Verarbeitung in Akten. Satz 4 bestimmt sodann, dass bei der Einschränkung der Verarbeitung nach Satz 3 und den sonstigen Fällen der Einschränkung der Verarbeitung nach §§ 53 Abs. 3, 70 Abs. 3 HDSIG-E diese durch Anbringung eines entsprechenden Vermerks vorzunehmen ist.

Satz 5 greift die Regelung des bisherigen § 27 Abs. 3 Satz 2 HSOG auf und sieht nunmehr unter Orientierung an § 78 Abs. 2 Satz 2 BKAG-neu grundsätzlich die Vernichtung der Akte vor, wenn die gesamte Akte zur Erfüllung der in der Zuständigkeit der speichernden Stelle liegenden Aufgaben nicht mehr erforderlich ist.

Satz 6 greift die bisherige Regelung des § 27 Abs. 3 Satz 3 HSOG zu in Akten gespeicherten personenbezogenen Daten über eine verdeckte Datenerhebung auf und bestimmt, dass diese nach Maßgabe des Abs. 2 Satz 1 Nr. 2 zu vernichten sind. Zudem wird in Satz 7 die entsprechende Geltung von Abs. 2 geregelt, um so die Streichung des bisherigen § 27 Abs. 6 HSOG auch im Hinblick auf Akten zu kompensieren. Bei personenbezogenen Daten in Akten über eine verdeckte Datenerhebung gilt daher - wie bisher - auch, dass die Einschränkung der Verarbeitung statt Vernichtung nur erfolgt, wenn die betroffene Person über die verdeckte Datenerhebung noch nicht unterrichtet worden ist. Die Verwendungsbeschränkung dieser Daten für die Rechtmäßigkeitskontrolle und die Zwecke der Benachrichtigung wird folgerichtig auch bei Akten bestimmt.

Zu Abs. 4
Abs. 4 Satz 1 und 2 übernehmen mit einigen redaktionellen Änderungen die Regelung des bisherigen § 27 Abs. 4 Satz 1 und 2 HSOG zur Ermächtigung zum Erlass einer Rechtsverordnung zur Regelung von Prüffristen, die auch in § 70 Abs. 4 HDSIG-E gefordert werden. In Abs. 4 Satz 5 wird eine Prüffrist für die nach § 20 Abs. 7 gespeicherten Daten über die in § 13 Abs. 2 Nr. 2 bis Nr. 5 genannten Personen normiert, welche eine Dauer von drei Jahren nicht überschreiten darf. Über das Erfordernis einer weiteren Speicherung entscheidet die Behördenleitung oder eine von dieser beauftragte Bedienstete oder ein beauftragter Bediensteter.

Zu Abs. 5
Der bisherige § 27 Abs. 5 Satz 1 HSOG zur Mitteilungspflicht der Berichtigung, Löschung oder Einschränkung der Verarbeitung an den Empfänger bei Übermittlung von Daten findet sich nunmehr in den §§ 53 Abs. 5 und 70 Abs. 3 HDSIG-E wieder. Demgegenüber wird der bisherige § 27 Abs. 5 Satz 2 HSOG zum Unterbleiben einer Mitteilung bei unverhältnismäßigem Aufwand ersatzlos gestrichen, da Art. 16 Abs. 5 und 6 der Richtlinie (EU) Nr. 2016/680 eine solche Ausnahme nicht kennen.

In Abs. 5 wird eine Regelung zu personenbezogenen Daten, welche dem Kernbereich privater Lebensgestaltung oder im Falle der Unzulässigkeit der Speicherung sowie in sonstigen Fällen des Abs. 2 Satz 1 einem Verwertungsverbot unterliegen, aufgenommen und die bisher in Abs. 2 Satz 2 zu findende Regelung überführt. Neu aufgenommen wird als zweiter Halbsatz die Bestimmung, dass § 53 Abs. 3 HDSIG-E zur möglichen Einschränkung der Verarbeitung statt einer Löschung dieser Kernbereichsdaten nicht in Frage kommt. Das Regelungssystem "Einschränkung der Verarbeitung statt Löschung" kommt insoweit aufgrund des besonderen Kernbereichsschutzes nicht zur Anwendung. Als Satz 2 wird in Umsetzung des Urteils des Bundesverfassungsgerichts vom 20. April 2016 die Klarstellung aufgenommen, dass Daten, die den Kernbereich privater Lebensgestaltung betreffen, unverzüglich zu löschen sind.

Die Sätze 3 bis 6 übernehmen überwiegend die bisherige Regelung zur Dokumentation an dieser Stelle, ergänzt um die klarstellende Nennung der Daten aus dem Kernbereich. Die bisherige Regelung zur Löschung der Dokumentation wird abgelöst durch eine neue Regelung, die sich an der vergleichbaren Vorschrift des § 45 Abs. 7 Satz 9 BKAG-neu orientiert und in das Regelungsgefüge des HSOG eingepasst wird. Danach orientiert sich die Löschung nicht mehr ausschließlich an den Zwecken der Datenschutzkontrolle, die nunmehr in § 29a HSOG-E eine ausdrückliche Regelung erfährt, sondern bezieht für die zeitliche Bestimmung auch die Benachrichtigungspflicht nach § 29 HSOG-E mit ein. Die verfahrensrechtlichen Absicherungen in Form des Verwertungs- und Löschungsgebots unterstützen dabei den Kernbereichsschutz. Satz 7 erklärt das vorstehende Verfahren für in Akten befindliche Daten aus dem Kernbereich privater Lebensgestaltung für entsprechend anwendbar.

Zu Abs. 6
Der bisherige § 27 Abs. 6 kann entfallen, da sich die Regelungen zur Einschränkung der Verarbeitung (Sperrung) statt Löschung und Vernichtung personenbezogener Daten überwiegend im neuen Abs. 2 und in den §§ 53 Abs. 3 und 70 Abs. 3 HDSIG-E finden.

Abs. 6 übernimmt daher mit redaktionellen Änderungen die bisherige Regelung des § 27 Abs. 8 HSOG zur Abgabe von Datenträgern an ein öffentliches Archiv.

Zu Abs. 7
Der bisherige § 27 Abs. 7 kann entfallen, da sich die Regelungen zur Einschränkung der Verarbeitung (Sperrung) statt Löschung und Vernichtung personenbezogener Daten überwiegend im neuen Abs. 2 und in den §§ 53 Abs. 3 und 70 Abs. 3 HDSIG-E finden.

Zu Nr. 21 (§ 27a)
Die Vorschrift schafft eine Regelung zu Berichtigung, Löschung und Einschränkung der Verarbeitung personenbezogener Daten, welche durch die Gefahrenabwehr- oder Polizeibehörden zu Zwecken außerhalb des § 40 HDSIG-E erhoben und weiterverarbeitet worden sind.

Zu Abs. 1
Abs. 1 gestaltet die im Anwendungsbereich der Verordnung (EU) Nr. 2016/679 in Art. 16 und 18 zu findenden Betroffenenrechte zur Berichtigung unrichtiger Daten und zur Einschränkung

der Verarbeitung personenbezogener Daten näher aus. Eine entsprechende Regelung für die Verarbeitung personenbezogener Daten zu Zwecken des § 40 HDSIG-E und deren Berichtigung oder Einschränkung deren Verarbeitung findet sich in §§ 53, 70 HDSIG-E.

Abs. 1 Satz 1 gestaltet im Sinne des Art. 6 Abs. 2 und 3 der Verordnung (EU) Nr. 2016/679 die Regelung des Art. 18 Abs. 1 Buchst. a der Verordnung (EU) Nr. 2016/679 zur Einschränkung der Verarbeitung personenbezogener Daten aus. Nach Art. 18 Abs. 1 Buchst. a der Verordnung (EU) Nr. 2016/679 hat die betroffene Person das Recht, von dem Verantwortlichen die Einschränkung der Verarbeitung personenbezogener Daten zu verlangen, wenn die Richtigkeit der personenbezogenen Daten von der betroffenen Person bestritten wird, und zwar für die Dauer, die es dem Verantwortlichen ermöglicht, die Richtigkeit der personenbezogenen Daten zu überprüfen. Hierzu trifft Abs. 1 Satz 1 eine für die gefahrenabwehr- und polizeibehördliche Aufgabenerfüllung ergänzende landesrechtliche Regelung in Bezug auf Zeugenaussagen und fachliche Bewertungen. Bezugspunkt des Rechts auf Einschränkung der Verarbeitung personenbezogener Daten und damit auch der Frage nach der Richtigkeit oder Unrichtigkeit personenbezogener Daten sind hiernach diejenigen Tatsachen, die die betroffene Person berühren, und nicht etwa der Inhalt einer Zeugenaussage oder einer dem Sachverhalt zugrunde gelegten behördlichen Bewertung.

Abs. 1 Satz 2 erklärt für den Fall, dass nach Bestreiten der Richtigkeit der Daten deren Richtigkeit oder Unrichtigkeit nicht festgestellt werden kann, das Recht auf Berichtigung personenbezogener Daten für nicht anwendbar und lässt an dessen Stelle das Recht auf Einschränkung der Verarbeitung der in Rede stehenden personenbezogenen Daten treten.

Abs. 1 Satz 3 bis 7 enthalten ergänzende Bestimmungen zu dem zur Anwendung kommenden Verfahren, wenn die oder der Verantwortliche dem Verlangen nach Berichtigung personenbezogener Daten nicht oder nur eingeschränkt nachkommt. Satz 3 verpflichtet im Gleichlauf mit § 53 Abs. 6 HDSIG-E den Verantwortlichen, die betroffene Person, welche ihr Recht auf Berichtigung unrichtiger personenbezogener Daten geltend gemacht hat, über die an die Stelle der Berichtigung tretende Einschränkung der Verarbeitung zu unterrichten. Diese Unterrichtung unterbleibt nach Satz 4 außerhalb des § 40 HDSIG-E, welcher § 53 Abs. 6 Satz 2 HDSIG-E nachgebildet ist, soweit bereits diese eine Gefährdung im Sinne des § 32 Abs. 1 HDSIG-E mit sich bringen würde.

Satz 5 stellt im Gleichlauf mit § 53 Abs. 6 Satz 3 HDSIG-E ein Begründungserfordernis für die Unterrichtung auf, welches ausnahmsweise nicht besteht, wenn die Mitteilung der Gründe den mit dem Absehen von der Unterrichtung verfolgten Zweck gefährden würde. Satz 6 erklärt anstelle des § 52 Abs. 7 in Verbindung mit § 53 Abs. 7 HDSIG-E die Bestimmung des § 33 Abs. 3 HDSIG-E für entsprechend anwendbar, welcher außerhalb des Anwendungsbereichs des § 40 HDSIG-E Regelungen zur Geltendmachung von Betroffenenrechten durch die Hessische Datenschutzbeauftragte oder den Hessischen Datenschutzbeauftragten trifft. Satz 7 verpflichtet die oder den Verantwortlichen - im Gleichlauf mit § 52 Abs. 8 HDSIG-E in Verbindung mit § 53 Abs. 7 HDSIG-E - dazu, die sachlichen und rechtlichen Gründe für die Entscheidung, von der Unterrichtung der betroffenen Personen abzusehen, zu dokumentieren.

Zu Abs. 2
Abs. 2 übernimmt im Gleichlauf mit § 27 Abs. 3 HSOG-E die Regelung des § 27 Abs. 1 Satz 2 HSOG teilweise und regelt die Pflicht zur Berichtigung in Akten zu findender, unrichtiger personenbezogener Daten. Die Vorschrift gestaltet im Sinne des Art. 6 Abs. 2 und 3 der Verordnung (EU) Nr. 2016/679 die sich aus Art. 16 der Verordnung (EU) Nr. 2016/679 ergebende Berichtigungspflicht für den Fall der nicht automatisierten Datenverarbeitung näher aus. Wird nach Abs. 2 Satz 1 die Unrichtigkeit personenbezogener Daten in Akten festgestellt, ist der bestehenden Pflicht zur Berichtigung der unrichtigen Daten dadurch Rechnung zu tragen, dass dies in der Akte vermerkt oder auf sonstige Weise festgehalten wird. Abs. 2 Satz 2 bestimmt im Gleichlauf mit Abs. 1 Satz 2 für den Fall, dass nach Bestreiten der Richtigkeit der in Akten zu findenden Daten deren Richtigkeit oder Unrichtigkeit nicht festgestellt werden kann, dass das Recht auf Berichtigung personenbezogener Daten keine Anwendung findet und lässt an dessen Stelle das Recht auf Einschränkung der Verarbeitung der in Rede stehenden personenbezogenen Daten treten. Die von der Einschränkung der Verarbeitung betroffenen personenbezogenen Daten sind in der Akte zu kennzeichnen.

Zu Abs. 3
Abs. 3 erklärt für Datenverarbeitungen außerhalb des Anwendungsbereichs des § 40 HDSIG-E in Ergänzung der sich unmittelbar aus Art. 17 Abs. 1 der Verordnung (EU) Nr. 2016/679 ergebenden Löschungsgründe die Regelung des § 27 Abs. 2 Satz 1 und Abs. 5 HSOG-E für entsprechend anwendbar, um insoweit einen Gleichlauf mit der Regelung zur Löschung personenbezogener Daten im Anwendungsbereich des § 40 HDSIG-E herbeizuführen. Zudem wird bei personenbezogenen Daten in Akten geregelt, dass an die Stelle der Löschung nach Art. 17 Abs. 1 der Verordnung (EU) Nr. 2016/679 die Einschränkung der Verarbeitung nach Art. 18 der Verordnung (EU) Nr. 2016/679 tritt und folgerichtig § 27 Abs. 3 Satz 3 bis 6 HSOG-E entsprechend gilt. Hierbei

handelt es sich um landesrechtliche Regelungen im Sinne des Art. 6 Abs. 2 und 3 der Verordnung (EU) Nr. 2016/679. Auf die Begründung zu § 27 HSOG-E wird Bezug genommen.

Zu Abs. 4
Abs. 4 trifft mit Blick auf die gefahrenabwehr- und polizeibehördliche Aufgabenerfüllung außerhalb des Anwendungsbereichs des § 40 HDSIG-E von der Bestimmung des § 34 Abs. 1 und 2 HDSIG-E abweichende Regelungen. Entgegen § 34 Abs. 1 HDSIG-E, welcher auf Fälle der nicht automatisierten Datenverarbeitung beschränkt ist, findet § 27a Abs. 4 bei allen Arten der Datenverarbeitung Anwendung.

Satz 1 schafft hinsichtlich Nr. 1 bis Nr. 3 einen Gleichlauf mit § 53 Abs. 3 HDSIG-E sowie hinsichtlich Nr. 4 mit § 27 Abs. 2 Satz 2 HSOG-E und damit im Sinne des Art. 6 Abs. 2 und 3 der Verordnung (EU) Nr. 2016/679 spezifische Bestimmungen, welche dazu führen, dass anstelle einer Löschung personenbezogener Daten die Einschränkung deren Verarbeitung tritt. Durch die parallele Ausgestaltung der Vorschriften innerhalb und außerhalb des Anwendungsbereichs des § 40 HDSIG-E wird erreicht, dass im Rahmen gefahrenabwehr- und polizeibehördlicher Aufgabenerfüllung weitgehend einheitliche Bestimmungen zugrunde gelegt werden können. Sie dienen der ordnungsgemäßen Aufgabenerfüllung der Gefahrenabwehr- und Polizeibehörden und gestalten in verhältnismäßiger Weise die Rechte der Betroffenen europarechtskonform aus (Art. 6, 23 der Verordnung (EU) Nr. 2016/679). Satz 2 bestimmt, dass in den Fällen des Abs. 4 Satz 1 an die Stelle einer Löschung der betroffenen personenbezogenen Daten die Einschränkung deren Verarbeitung tritt.

Satz 3 regelt, dass bei personenbezogenen Daten in Akten Satz 2 mit der Maßgabe gilt, dass an Stelle der Vernichtung die Verarbeitung personenbezogener Daten in Akten durch Anbringung eines entsprechenden Vermerks einzuschränken ist.

Satz 4 übernimmt den Regelungsgehalt des § 27 Abs. 7 Satz 1 HSOG, Satz 5 übernimmt den Regelungsgehalt des § 27 Abs. 7 Satz 2 HSOG.

Zu Abs. 5
Abs. 5 macht von Art. 23 Abs. 1 und Abs. 2 der Verordnung (EU) Nr. 2016/679 Gebrauch und regelt das zur Anwendung kommende Verfahren, wenn von der Unterrichtung der betroffenen Person über die vorgenommene Einschränkung der Verarbeitung der personenbezogenen Daten abgesehen wird. Dabei werden Regelungsinhalt und Systematik aus § 27a Abs. 1 Satz 3 bis 7 HSOG-E übernommen.

Zu Abs. 6
Abs. 6 erklärt außerhalb des Anwendungsbereichs des § 40 HDSIG-E die Vorschriften der §§ 53 Abs. 4 und 70 Abs. 4 HDSIG-E und § 27 Abs. 4 und 6 HSOG-E zur Ermächtigung zum Erlass einer Rechtsverordnung zur Regelung von Prüffristen und zur Abgabe von Datenträgern an ein öffentliches Archiv für entsprechend anwendbar.

Zu Nr. 22 (§§ 28 und 29)

Zu § 28
Der in § 28 HSOG-E neu aufgenommene Regelungsinhalt setzt die Anforderungen aus dem Urteil des Bundesverfassungsgerichts vom 20. April 2016 zum Bundeskriminalamtgesetz an eine vollständige Protokollierungspflicht bei verdeckten und sonstigen eingriffsintensiven Maßnahmen (Rn. 141) im HSOG-E um und verortet bereits bestehende Protokollierungsvorschriften, etwa aus § 15b Abs. 3, an einer Stelle. Damit wird eine eigenständige Vorschrift zur Protokollierung gegenüber der in § 71 HDSIG-E enthaltenen Regelung geschaffen, die sich an § 82 BKAG-neu orientiert. Die bisherige Regelung des § 28 zu Verfahrensverzeichnissen wird aufgehoben. Das datenschutzrechtliche Instrument des Verfahrensverzeichnisses findet in der Verordnung (EU) Nr. 2016/679 und der Richtlinie (EU) Nr. 2016/680 keine Grundlage.

Zu Abs. 1
Abs. 1 gestaltet in Umsetzung des Urteils des Bundesverfassungsgerichts vom 20. April 2016 die Pflicht zur vollständigen Protokollierung bei verdeckten und eingriffsintensiven Maßnahmen nach den §§ 15 bis 17, 26 HSOG aus. Abs. 1 sieht dabei eine bisher bereits vergleichbar in § 15b Abs. 3 HSOG enthaltene Aufzählung der Inhalte der Protokollierung bei verdeckten und eingriffsintensiven Maßnahmen vor und orientiert sich dafür am Wortlaut des § 82 Abs. 1 BKAG-neu.

Zu Abs. 2
Abs. 2 regelt nach dem Vorbild des § 82 Abs. 2 BKAG-neu, dass zusätzlich zu Abs. 1 die zu den verschiedenen Maßnahmen jeweils aufgezählten Personen und Inhalte zu protokollieren sind.

Zu Abs. 3
In Abs. 3 Satz 1 wird geregelt, dass Nachforschungen zur Feststellung der Identität der in Abs. 2 bezeichneten Personen nur vorzunehmen sind, wenn dies unter Abwägung der Eingriffsinten-

sität der Maßnahme, des Aufwands für die Identitätsfeststellung und der daraus folgenden Beeinträchtigungen für die betroffenen Personen geboten ist. Durch die in Satz 2 geforderte Protokollierung der Anzahl der Personen, deren Protokollierung unterblieben ist, soll dem Erfordernis der umfassenden Protokollierung der in Rede stehenden Maßnahmen Genüge getan werden.

Zu Abs. 4
Abs. 4 Satz 1 enthält eine Nutzungsbeschränkung der Protokolldaten für Benachrichtigungszwecke sowie Zwecke der Datenschutz- und Rechtmäßigkeitskontrolle.

Zu § 29

Zu Abs. 1
Die Vorschrift enthält datenschutzrechtliche Regelungen zu den Rechten betroffener Personen auf Auskunft, Information und Benachrichtigung. Abs. 1 verweist mit Blick auf die gefahrenabwehr- und polizeibehördliche Aufgabenerfüllung hinsichtlich der Verarbeitung personenbezogener Daten zu Zwecken des § 40 HDSIG-E auf die §§ 50 bis 52 HDSIG-E und auf Art. 13 bis 15 der Verordnung (EU) Nr. 2016/679 sowie die zu deren Durchführung in das HDSIG-E aufgenommenen Vorschriften der §§ 31 bis 33, soweit die Verarbeitung personenbezogener Daten durch Gefahrenabwehr- oder Polizeibehörden zu Zwecken außerhalb des § 40 HDSIG-E stattfindet. Die vorgenannten Vorschriften finden Anwendung, soweit in § 29 HSOG-E nichts Abweichendes bestimmt ist. Der bisher verwendete Begriff der "Unterrichtung" wird der Regelung des § 29 HSOG-E als Recht der betroffenen Person nun im Sinne der rechtssprachlichen Einheitlichkeit als "Benachrichtigung" zugrunde gelegt.

Die bisher in § 29 Abs. 1 zu findende Regelung zur Erteilung von Auskunft wird durch § 52 HDSIG-E abgelöst, soweit eine Verarbeitung personenbezogener Daten zu Zwecken des § 40 HDSIG-E in Rede steht, sowie durch Art. 15 der Verordnung (EU) Nr. 2016/679 bei einer Auskunft über die gefahrenabwehr- oder polizeibehördliche Verarbeitung personenbezogener Daten zur Aufgabenerfüllung außerhalb des Anwendungsbereichs des § 40 HDSIG-E. Der bereits in § 29 Abs. 1 normierte Grundsatz der Gebührenfreiheit für die Gewährung einer Auskunft über die stattgefundene Verarbeitung personenbezogener Daten ergibt sich nun aus § 54 Abs. 3 HDSIG-E sowie mit Blick auf die Verordnung (EU) Nr. 2016/679 aus Art. 12 Abs. 5 der vorgenannten Verordnung.

Zu Abs. 2
Abs. 2 enthält von den Vorschriften der §§ 31, 32 HDSIG-E abweichende Bestimmungen im Sinne des § 3 Abs. 4 HSOG-E i.V.m. § 1 Abs. 2 HDSIG-E. Die §§ 31, 32 HDSIG-E finden vorbehaltlich des § 29 Abs. 2 HSOG-E Anwendung, soweit die Gefahrenabwehr- oder Polizeibehörden personenbezogene Daten zu Zwecken außerhalb des § 40 HDSIG-E verarbeiten. Hierbei dienen die §§ 31, 32 HDSIG-E im allgemeinen Datenschutzrecht der Durchführung der in Art. 13, 14 der Verordnung (EU) Nr. 2016/679 vorgesehenen Informationspflichten der oder des Verantwortlichen einer Verarbeitung personenbezogener Daten. Die Anwendungsbereiche des Art. 13 der Verordnung (EU) Nr. 2016/679 und § 31 HDSIG-E einerseits sowie des Art. 14 der Verordnung (EU) Nr. 2016/679 und § 32 HDSIG-E andererseits unterscheiden sich dahin gehend, ob die personenbezogenen Daten bei der betroffenen Person erhoben worden sind (Art. 13 der Verordnung (EU) Nr. 2016/679 und § 31 HDSIG-E) oder bei Dritten erhoben worden sind (Art. 14 der Verordnung (EU) Nr. 2016/679 und § 32 HDSIG-E).

Abs. 2 Satz 1 greift die Vorschrift des § 31 Abs. 1 HDSIG-E betreffend die Informationspflicht bei der Verarbeitung von personenbezogenen Daten, die bei der betroffenen Person erhoben wurden, auf. Während § 31 Abs. 1 HDSIG-E für die in Art. 13 Abs. 3 der Verordnung (EU) Nr. 2016/679 vorgesehene Fallgruppe gilt, dass der Verantwortliche beabsichtigt, die personenbezogenen Daten für einen anderen Zweck weiterzuverarbeiten als für denjenigen, für den die Daten bei der betroffenen Person erhoben wurden, und hierzu Ausnahmen von der Informationspflicht formuliert, erstreckt § 29 Abs. 2 Satz 1 HSOG-E den Anwendungsbereich des § 31 Abs. 1 HDSIG-E über Art. 13 Abs. 3 hinaus auch auf die Fallgestaltungen der Informationspflichten nach Art. 13 Abs. 1 und 2 der Verordnung (EU) Nr. 2016/679 und sieht neben der Nichterteilung einer Information auch vor, dass eine Information aufgeschoben oder eingeschränkt erteilt wird.

§ 29 Abs. 2 Satz 1 HSOG-E schafft eine Rechtsgrundlage dafür, die Erteilung der Information soweit und solange aufzuschieben, einzuschränken oder zu unterlassen, wie andernfalls die Erteilung der Information die Voraussetzungen des § 31 Abs. 1 HDSIG-E erfüllt. Auch die einschränkende Voraussetzung zu § 31 Abs. 1 Nr. 2 Buchst. a bis e HDSIG-E, dass die Interessen des Verantwortlichen an der Nichterteilung, Einschränkung oder dem Aufschub der Information die Interessen der betroffenen Person überwiegen, sowie die Regelung des § 31 Abs. 1 Satz 2 HDSIG-E sind zu beachten. Abs. 2 Satz 2 erklärt § 31 Abs. 3 HDSIG-E für nicht anwendbar, da sich das Verfahren bei einem Unterbleiben der Information wegen eines vorübergehenden Hinderungsgrundes aus § 29 Abs. 2 Satz 4 HSOG-E i.V.m. § 33 Abs. 3 HDSIG-E ergibt.

Abs. 2 Satz 3 enthält abweichende Bestimmungen von der in § 32 HDSIG-E und Art. 14 der Verordnung (EU) Nr. 2016/679 geregelten Informationspflicht über die Verarbeitung personenbezogener Daten, welche nicht bei der betroffenen Person erhoben worden sind, sondern aus einer anderen Quelle erlangt wurden. Voraussetzung ist wie im Fall des § 29 Abs. 2 Satz 1 HSOG-E, dass die Gefahrenabwehr- oder Polizeibehörden personenbezogene Daten zu Zwecken außerhalb des § 40 HDSIG-E verarbeiten. Abs. 2 Satz 3 weicht von der Vorschrift des § 32 Abs. 1 HDSIG-E dahin gehend ab, dass die Pflicht der oder des Verantwortlichen, die Information nach Art. 14 Abs. 1, 2 und 4 der Verordnung (EU) Nr. 2016/679 zu erteilen, neben der Nichterteilung auch aufgeschoben oder eingeschränkt werden kann, wie andernfalls die Erteilung der Information die Voraussetzungen des § 32 Abs. 1 HDSIG-E erfüllt. Die einschränkende Voraussetzung des § 32 Abs. 1 a. E. HDSIG-E, dass die Interessen des Verantwortlichen an der Nichterteilung, Einschränkung oder dem Aufschub der Information die Interessen der betroffenen Person überwiegen, sowie § 32 Abs. 1 Satz 2 HDSIG-E sind überdies zu beachten.

Abs. 2 Satz 4 erklärt im Fall der Einschränkung der Information nach § 29 Abs. 2 Satz 1 oder Satz 3 HSOG-E die Vorschrift des § 33 Abs. 3 HDSIG-E für entsprechend anwendbar, welche die Möglichkeit zugunsten der betroffenen Person aufzeigt, das Recht auf Information durch die oder den Hessischen Datenschutzbeauftragten auszuüben. Dies dient dem Schutz der Rechte und Freiheiten der betroffenen Person im Sinne des Art. 23 Abs. 2 Buchst. c, d, g und h der Verordnung (EU) Nr. 2016/679.

Zu Abs. 3
Abs. 3 enthält ergänzende Regelungen zu dem nach § 33 HDSIG-E bestehenden Auskunftsrecht einer betroffenen Person bei gefahrenabwehr- oder polizeibehördlichen Datenverarbeitungen außerhalb der Zwecke des § 40 HDSIG-E. Nach Art. 15 Abs. 1 der Verordnung (EU) Nr. 2016/679 hat die betroffene Person das Recht, von dem Verantwortlichen eine Bestätigung darüber zu verlangen, ob sie betreffende personenbezogene Daten verarbeitet werden; ist dies der Fall, so hat sie das Recht auf Auskunft über diese personenbezogenen Daten und auf die in Art. 15 Abs. 1 Buchst. a bis h der Verordnung (EU) Nr. 2016/679 genannten Informationen.

Abs. 3 Satz 1 ergänzt die Regelung des § 33 Abs. 1 HDSIG-E dahin gehend, dass die Auskunftserteilung über die personenbezogenen Daten, die Gegenstand der Verarbeitung sind, und zu Informationen nach Art. 15 Abs. 1 Buchst. a bis h der Verordnung (EU) Nr. 2016/679 auch teilweise oder vollständig eingeschränkt werden kann. Abs. 3 Satz 2 erklärt die in § 33 Abs. 2 HDSIG-E geregelten Beschränkungen sowie Dokumentations- und Begründungspflichten für nicht anwendbar, weil insoweit hierzu flankierend in Abs. 3 Satz 3 bis Satz 6 das zur Anwendung kommende Verfahren für den Fall des Absehens von oder der Einschränkung einer Auskunft - im Gleichlauf mit der Vorschrift des § 52 Abs. 6 und Abs. 8 HDSIG-E - geregelt wird. Dies dient zum einen dem Schutz der öffentlichen Sicherheit (Art. 23 Abs. 1 Buchst. c der Verordnung (EU) Nr. 2016/679) und den in Art. 23 Abs. 1 Buchst. d der Verordnung (EU) Nr. 2016/679 genannten Zwecken sowie andererseits dem Schutz der Rechte und Freiheiten der betroffenen Person im Sinne des Art. 23 Abs. 2 Buchst. c, d, g und h der Verordnung (EU) Nr. 2016/679. Nach Abs. 3 Satz 3 hat der Verantwortliche die betroffene Person über das Absehen von oder die Einschränkung der Auskunft unverzüglich schriftlich zu unterrichten. Dies gilt nach Abs. 3 Satz 4 nicht, soweit bereits die Erteilung dieser Informationen eine Gefährdung im Sinne des § 32 Abs. 1 HDSIG-E mit sich bringen würde. Abs. 3 Satz 5 formuliert eine Begründungspflicht für die Entscheidung, von einer Auskunft abzusehen oder diese eingeschränkt zu erteilen, welche ausnahmsweise nicht besteht, wenn die Mitteilung der Gründe den verfolgten Zweck gefährden würde.

Abs. 3 Satz 6 statuiert eine Dokumentationspflicht. Abs. 3 Satz 7 erklärt auch im Falle der Einschränkung der Auskunftserteilung das in § 33 Abs. 3 HDSIG-E geregelte Verfahren für entsprechend anwendbar, welches die Möglichkeit zugunsten der betroffenen Person aufzeigt, das Auskunftsrecht durch die oder den Hessischen Datenschutzbeauftragten auszuüben. Dies dient dem Schutz der Rechte und Freiheiten der betroffenen Person im Sinne des Art. 23 Abs. 2 Buchst. c, d, g und h der Verordnung (EU) Nr. 2016/679.

Zu Abs. 4
Abs. 4 übernimmt die Regelung des bisherigen § 20 Abs. 10 HSOG. Die Änderung des Begriffs "unterrichten" hin zu "benachrichtigen" erfolgt im Sinne der rechtssprachlichen Einheitlichkeit.

Zu Abs. 5 bis 7
Abs. 5 bis 7 übernehmen in modifizierter Form die Regelung des § 29 Abs. 6 HSOG und ergänzen diese.

Abs. 5 Satz 1 regelt die Pflicht zur Benachrichtigung betroffener Personen im Fall einer Erhebung personenbezogener Daten durch verdeckte und eingriffsintensive Maßnahmen nach § 28 Abs. 2 HSOG-E in Erweiterung des bisherigen § 29 Abs. 6 Satz 2 HSOG und in Anlehnung an den Kreis der Personen in § 74 Abs. 1 Satz 1 BKAG-neu. Die Maßgaben des Abs. 5 Satz 1 werden im Gleichlauf mit den Protokollierungspflichten des § 28 Abs. 2 HSOG-E ausgestaltet.

Der Inhalt der Benachrichtigung ergibt sich aus § 51 HDSIG-E. Abs. 5 Satz 2 äußert sich in Anlehnung an die Wortlaute des § 29 Abs. 6 Satz 3 HSOG und § 74 Abs. 1 Satz 4 BKAG-neu dazu, unter welchen Voraussetzungen seitens des der oder Verantwortlichen Nachforschungen zur Feststellung der Identität einer Person oder deren Anschrift vorzunehmen sind.

In Abs. 6 Satz 1 wird die Zurückstellung der Benachrichtigung nach Abs. 5 geregelt und dafür der Regelungsgehalt des aktuellen § 29 Abs. 6 Satz 4 HSOG überführt und in Anlehnung an § 74 Abs. 2 Satz 1 BKAG-neu um die Merkmale des Bestands des Staates und der Sachen von bedeutendem Wert, deren Erhaltung im öffentlichen Interesse geboten ist, erweitert. Abs. 6 Satz 2 enthält eine Regelung zur Benachrichtigung betroffener Personen im Fall von Maßnahmen nach § 16. Nach Abs. 6 Satz 3 obliegt - wie bereits bisher nach § 29 Abs. 6 Satz 5 HSOG - die jeweilige Entscheidung über das Unterbleiben einer Benachrichtigung der Behördenleitung oder einer hierzu beauftragten Bediensteten und eines hierzu beauftragten Bediensteten. Abs. 6 Satz 4 statuiert eine Dokumentationspflicht über die Gründe, welche der Entscheidung zur Zurückstellung der Benachrichtigung zugrunde liegen. Abs. 6 Satz 5 übernimmt die Regelung des § 29 Abs. 6 Satz 6 HSOG.

Abs. 7 bestimmt in Satz 1 unter Übernahme des bisherigen § 29 Abs. 6 Satz 3 HSOG und in Anlehnung an § 74 Abs. 1 Satz 2 BKAG-neu, dass eine Benachrichtigung unterbleibt, soweit dies im überwiegenden Interesse einer betroffenen Person liegt.
Abs. 7 Satz 2 bestimmt die Voraussetzungen, welche vorliegen müssen, damit im Falle einer Maßnahme nach § 28 Abs. 2 Nr. 4 und. 5 eine Benachrichtigung derjenigen Personen, gegen die sich die Maßnahme nicht gerichtet hat, unterbleiben kann. Nach Abs. 7 Satz 3 obliegt die jeweilige Entscheidung über das Unterbleiben einer Benachrichtigung der Behördenleitung oder einer hierzu beauftragten Bediensteten und eines hierzu beauftragten Bediensteten.

Zu Abs. 8

Abs. 7 wird zu Abs. 8 und übernimmt mit Anpassungen die Regelung des bisherigen § 29 Abs. 7 HSOG.

Zu Nr. 23 (§ 29a)
Neu aufgenommen wird die Regelung des § 29a zur Datenschutzkontrolle. Die Vorschrift dient der Umsetzung der Anforderungen des Urteils des Bundesverfassungsgerichts vom 20. April 2016 (Rn. 140 f., 266, 340 und 354) im Hinblick auf die datenschutzaufsichtliche Kontrolle der Wahrnehmung der polizeibehördlichen Datenverarbeitungsbefugnisse im Bereich der verdeckten und eingriffsintensiven Maßnahmen sowie bei der Datenübermittlung im internationalen Bereich nach § 23 HSOG-E. Diese Kontrolle soll in Umsetzung des vorgenannten Urteils (Rn. 141) in angemessenen Abständen - mindestens alle zwei Jahre im Stichprobenverfahren - stattfinden. Ausdrücklich unberührt von der Regelung des § 29a bleiben die weiteren Aufgaben und Kontrollen der oder des Hessischen Datenschutzbeauftragten.

Zu Nr. 24 (§ 115)
Die Vorschrift regelt eine angemessene Befristung der Regelung des § 20a Abs. 4 Satz 2 HSOG-E, um die technische Unmöglichkeit und den unverhältnismäßigen Aufwand einer Kennzeichnung nicht unbefristet zu dulden.

Zu Art. 19 (Änderung des Hessischen Brand- und Katastrophenschutzgesetzes)

Die Änderung des § 55 des Hessischen Gesetzes über den Brandschutz, die Allgemeine Hilfe und den Katastrophenschutz (HBKG) ist erforderlich, weil die Verordnung (EU) Nr. 2016/679 ab dem 25. Mai 2018 als unmittelbar anwendbares Recht gelten wird und durch die dort eingeräumten Öffnungsklauseln Regelungen in den datenschutzrechtlichen Bestimmungen der Länder zulässig sind. Zudem wird die Verweisung auf das HDSIG-E beibehalten.

Zu Art. 20 (Änderung des Hessischen Spielhallengesetzes)

§ 12 Abs. 1 Nr. 16 des Hessischen Spielhallengesetzes (HessSpielhG) ist im Hinblick auf die Umsetzung der Verordnung (EU) Nr. 2016/679 anzupassen.

§ 12 HessSpielhG regelt den Ordnungswidrigkeitstatbestand. § 12 Abs. 1 Nr. 16 HessSpielhG stellt sich hinsichtlich des Passus "Löschung" mit Art. 83 der Verordnung (EU) Nr. 2016/679 als unvereinbar dar. Jener entfällt künftig; er erschöpft sich in der Wiederholung einer in Art. 83 genannten, unmittelbar aus der Verordnung (EU) Nr. 2016/679 resultierenden Ordnungswidrigkeit bei Verstoß gegen die Pflicht zur Löschung. Die Speicherpflicht ist fachrechtlich begründet, die Löschpflicht hingegen datenschutzrechtlich.

Zu Art. 21 (Änderung des Hessischen Disziplinargesetzes)

Die Begrifflichkeiten in § 33 des Hessischen Disziplinargesetzes (HDG) werden an die Begriffsbestimmungen in Art. 4 Nr. 2 der Verordnung (EU) Nr. 2016/679 angepasst.

Zu Art. 22 (Änderung des Hessischen Personalvertretungsgesetzes)

Die Begrifflichkeiten in § 62 des Hessischen Personalvertretungsgesetzes (HPVG) werden an die Begriffsbestimmungen in Art. 4 Nr. 2 der Verordnung (EU) Nr. 2016/679 angepasst.

Zu Art. 23 (Änderung des Heilberufsgesetzes)

Zu Nr. 1 (§ 2 Abs. 3 Satz 4)
In § 2 Abs. 3 Satz 4 war der Verweis auf die unmittelbar geltende Verordnung (EU) Nr. 2016/679 aufzunehmen.

Zu Nr. 2 (§ 9 Abs. 6)
Die Richtlinie 95/46/EG wird durch die Verordnung (EU) Nr. 679/2016 aufgehoben, daher ist der Verweis in § 9 Satz 6 auf die Richtlinie 95/46/EG durch einen Verweis auf die Verordnung (EU) Nr. 2016/679 zu ersetzen.

Zu Art. 24 (Änderung des Hessischen Gesetzes über den öffentlichen Gesundheitsdienst)

Der Verweis auf das ebenfalls durch dieses Gesetz neugefasste Hessische Datenschutz- und Informationsfreiheitsgesetz ist zu aktualisieren und es ist ein Verweis auf die unmittelbar geltende Verordnung (EU) Nr. 2016/679 aufzunehmen.

Zu Art. 25 (Änderung des Hessischen Krankenhausgesetzes 2011)

Zu Nr. 1 (§ 12 Abs. 1)
In § 12 Abs. 1 des Zweiten Gesetzes zur Weiterentwicklung des Krankenhauswesens in Hessen (HKHG 2011) wird der Verweis auf die unmittelbar geltende Verordnung (EU) Nr. 2016/679 eingefügt.

Zu Nr. 2 (§ 12 Abs. 3)
Aufgrund der Novellierung des Hessischen Datenschutzgesetzes wird der Verweis auf dieses Gesetz entsprechend angepasst.

Zu Art. 26 (Änderung des Patientenmobilitätsgesetzes)

Die Richtlinie 95/46/EG wird durch die Verordnung (EU) Nr. 2016/679 aufgehoben, daher ist der Verweis auf die Richtlinie 95/46/EG durch einen Verweis auf die Verordnung (EU) Nr. 2016/679 zu ersetzen.

Zu Art. 27 (Änderung des Maßregelvollzugsgesetzes)

Auf den Maßregelvollzug findet ebenso wie auf den Strafvollzug grundsätzlich die Richtlinie (EU) Nr. 2016/680 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zweck der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung sowie zum freien Datenverkehr und zur Aufhebung des Rahmenbeschlusses 2008/977/J1 des Rats Anwendung.

Entsprechend wird das Strafvollzugsgesetz, auf das das Maßregelvollzugsgesetz insbesondere in Bezug auf den Datenschutz verweist, an die Vorgaben aus der Richtlinie (EU) Nr. 2016/680 angepasst. Diese Gesetzesänderungen im Strafvollzugsgesetz werden für das Maßregelvollzugsgesetz nachvollzogen, wobei die Besonderheiten des Maßregelvollzugs in Abgrenzung zum Strafvollzug Berücksichtigung finden.

Zu Nr. 1 (§ 5a Satz 2)
Es handelt sich hier um redaktionelle Änderungen in Form von Aktualisierungen der Gesetzeszitate.

Zu Nr. 2 (§ 7 Abs. 1 Satz 1)
Es handelt sich hier um eine redaktionelle Änderung in Form einer Aktualisierung des Gesetzeszitates.

Zu Nr. 3 (§ 19 Abs. 1)
§ 19 regelt die Überwachung von Besuchen im Maßregelvollzug. Die Bestimmungen zu Besuchen im Strafvollzug sehen mit der Novellierung in § 34 Abs. 5 HStVollzG-E auch eine Überwachung der Besuche durch optisch-elektronische Einrichtungen, also durch Videoüberwachung vor und schränkt gleichzeitig die Aufzeichnung von Daten auf den Fall unbedingter Erforderlichkeit ein. Dies trägt der sicheren Umsetzung der Richtlinie (EU) Nr. 2016/680 entsprechend Art. 10 bzw. § 43 Abs. 1 HDSIG-E Rechnung.

Zu Nr. 4 (§ 31 Satz 4)
Die Regelung erübrigt sich an dieser Stelle durch den Verweis in § 36 Abs. 1 auf die Neufassung von § 59 HStVollzG-E.

Zu Nr. 5 (§ 32)
Hier handelt es sich um eine redaktionelle Änderung.

Zu Nr. 6 (§ 36 Abs. 1)
Wegen der Parallelen des Maßregelvollzugs zum Strafvollzug wird in Abs. 1 auch weiterhin in weiten Teilen auf den Dreizehnten Titel des Hessischen Strafvollzugsgesetzes verwiesen.

Wie bisher wird jedoch den Besonderheiten des Maßregelvollzugs Rechnung getragen. Insofern wird zum Einen nicht umfänglich auf den Dreizehnten Titel des Hessischen Strafvollzugsgesetzes verwiesen und werden zum Anderen in den Maßgaben des Abs. 1 sowie den folgenden Absätzen gesonderte Regelungen getroffen. Dies hat seinen Grund insbesondere darin, dass die Aufgabe im Maßregelvollzug in der Besserung und Sicherung der untergebrachten Person liegt, dass therapeutische Behandlung also im Vordergrund der Unterbringung steht. Unterschiede zu den datenschutzrechtlichen Bestimmungen im Strafvollzugsgesetz haben ihren Kern darin, dass es sich beim Maßregelvollzug nicht um eine Justizvollzugsanstalt, sondern um ein Krankenhaus handelt. Die Besonderheiten, die das Arzt-Patientenverhältnis betreffen, und die Besonderheiten, die darin beruhen, dass Unterbringung und Behandlung untrennbar miteinander verwoben sind, werden in den Maßgaben in Abs. 1 sowie in den folgenden Absätzen gesondert geregelt.

Inhaltlich neu aufgenommen sind die Verweise auf § 58 Abs. 5 und 6 HStVollzG, die mit der Novellierung des Strafvollzugsgesetzes im Jahr 2013 neu gefasst wurden und die Feststellung der Identität von Besuchern und die Überwachung der Außenbereiche einer Anlage regeln. Wegen der Parallelen im Maßregelvollzug wird auf diese Normen verwiesen.

Ebenso wird auf den neu gefassten § 59 HStVollzG-E und die hierin getroffenen Regelungen zum Auslesen von Datenspeichern verwiesen. Da § 59 HStVollzG-E hier die weitergehenden Regelungsinhalte trifft, ist § 31 Satz 4 MVollzG obsolet geworden.

Neu gefasst wird ferner die Maßgabe nach Abs. 1 Nr. 3. Hiernach ist nun auch eine Übermittlung von Daten der untergebrachten Person an die forensisch psychiatrischen Ambulanzen, die nach § 2 Abs. 2 verpflichtend zu betreiben sind, um Nachsorgemaßnahmen zu vermitteln oder durchzuführen, zulässig. Nur so kann eine Behandlung im Rahmen von Weisungen nach § 68 b Abs. 2 StGB sichergestellt werden.

Die Befugnis der Fachaufsichtsbehörde, von den Einrichtungen des Maßregelvollzugs neben der Übersendung der Personalakte auch solche Daten zu erhalten, die dem § 203 StGB unterliegen, wird klarstellend in Abs. 1 Nr. 6 aufgenommen. Die Übermittlung der Daten ist zur Erfüllung der Aufgaben der Fachaufsicht unter anderem aus § 7a Abs. 5 und § 35 Satz 1 erforderlich.

Mit Abs. 1 Nr. 7 wird neu die Maßgabe aufgenommen, dass die Personal- und Krankenakten 30 Jahre aufbewahrt werden können. Dies hat seinen Grund darin, dass die Hauptaufgabe des Maßregelvollzugs in der Besserung der untergebrachten Person, d.h. in ihrer ärztlichen und therapeutischen Behandlung besteht. Bis zu 30 Jahre nach der Behandlung können deliktische Schadensersatzansprüche aufgrund ärztlicher Fehler geltend gemacht werden. Schäden, die auf einer Verletzung des Lebens, des Körpers oder der Gesundheit oder der Freiheit beruhen, verjähren nach § 199 Abs. 2 BGB erst nach 30 Jahren. Bis dahin muss es daher möglich sein, die Tatbestände aus den Akten nachvollziehen zu können.

Zu Art. 28 (Änderung des Hessischen Ausführungsgesetzes zum Therapieunterbringungsgesetz)

Die Verweisung in § 7 Abs. 1 auf die Bestimmungen des Hessischen Sicherungsverwahrungsvollzugsgesetzes wurde in eine dynamische Verweisung geändert; darüber hinaus wurde in Abs. 1 und Abs. 2 die Änderung durch das vorliegende Gesetz aufgenommen.

Zu Art. 29 (Änderung des Hessischen Vermessungs- und Geoinformationsgesetzes)

Aufgrund Art. 23 Abs. 1 Buchst. e der Verordnung (EU) Nr. 2016/679 werden das Recht auf Berichtigung nach Art. 16, das Recht auf Einschränkung der Verarbeitung nach Art. 18 und das Widerspruchsrecht nach Art. 21 der Verordnung (EU) Nr. 2016/679 insoweit eingeschränkt, wie sich diese Rechte auf Informationsinhalte beziehen, die im Liegenschaftskataster lediglich nachrichtlich in Übereinstimmung mit dem Grundbuch geführt werden. Die Betroffenenrechte bleiben aber weiterhin grundsätzlich erhalten, da sie vorbehaltlich abweichender bereichsspezifischer Regelungen bei dem für die Führung der Eigentumsangaben originär zuständigen Grundbuchamt geltend gemacht werden können.

Die Einschränkung der Betroffenenrechte soll aber dann nicht gelten, wenn die betroffene Person geltend macht, dass die im Liegenschaftskataster nachrichtlich geführten Eigentumsangaben nicht mit der Originalquelle, dem Grundbuch übereinstimmen.

Die Bestimmungen des geltenden § 9 Abs. 5 Satz 4 HVGG können entfallen. Entsprechende Regelungen finden sich bereits in Art. 14 Abs. 5 Buchst. c der Verordnung (EU) Nr. 2016/679.

Zu Art. 30 (Aufhebung bisherigen Rechts)

Die Vorschrift regelt die Aufhebung des bisherigen Hessischen Datenschutzgesetzes.

Zu Art. 31 (Inkrafttreten)
Die Vorschrift regelt das Inkrafttreten des Gesetzes.

Wiesbaden, 5. Dezember 2017

Für die Fraktion
der CDU
Der Fraktionsvorsitzende:
Boddenberg

Für die Fraktion
BÜNDNIS 90/DIE GRÜNEN
Der Fraktionsvorsitzende:
Wagner (Taunus)