21. Wahlperiode

Drucksache **21/3019**

HESSISCHER LANDTAG

07. 11. 2025
DDA

Stellungnahme
Landesregierung
zu Dreiundfünfzigster Tätigkeitsbericht zum Datenschutz und Siebter Bericht zur Informationsfreiheit

des Hessischen Beauftragten für Datenschutz und Informationsfreiheit

Drucksache 21/1516

Eingegangen am 7. November 2025 Ausgegeben am 7. November 2025
Herstellung: Kanzlei des Hessischen Landtags · Postfach 3240 · 65022 Wiesbaden · www.Hessischer-Landtag.de

Inhaltsverzeichnis

Zweiter Teil – 7. Tätigkeitsbericht zur Informationsfreiheit

Erster Teil – 53. Tätigkeitsbericht zum Datenschutz

1. Neue Aufgaben und Rahmenbedingungen

Zu 1.1 Vorsitz in der Datenschutzkonferenz

Die Landesregierung nimmt den Bericht des Hessischen Beauftragten für Datenschutz und Informationsfreiheit zur Kenntnis.

Zu 1.2 Mitwirkung in europäischen Datenschutzgremien

Die Landesregierung nimmt den Bericht des Hessischen Beauftragten für Datenschutz und Informationsfreiheit zur Kenntnis.

Zu 1.3 Rechtsprechung des Europäischen Gerichtshofs zur Aufsichtstätigkeit

Die Landesregierung nimmt den Bericht des Hessischen Beauftragten für Datenschutz und Informationsfreiheit zur Kenntnis.

Zu 1.4 Rechtsprechung des Europäischen Gerichtshofs zur Anonymität

Die Landesregierung nimmt den Bericht des Hessischen Beauftragten für Datenschutz und Informationsfreiheit zur Kenntnis.

Zu 1.5 Settlement-Verfahren

Die Landesregierung nimmt den Bericht des Hessischen Beauftragten für Datenschutz und Informationsfreiheit zur Kenntnis.

Zu 1.7 Gespräche mit Microsoft

Die Landesregierung nimmt den Bericht des Hessischen Beauftragten für Datenschutz und Informationsfreiheit zur Kenntnis.

Das vom Hessischen Beauftragten für Datenschutz und Informationsfreiheit entwickelte normative Konzept beruht darauf, dass seitens der hessischen Landesverwaltung datenschutzrechtliche Defizite des Dienstangebots durch eigene Anstrengungen ausgeglichen werden müssen, z.B. durch Erstellung der notwendigen Dokumentationen oder Ergreifung der technischen und organisatorischen Maßnahmen, die für einen datenschutzkonformen Betrieb notwendig sind. Wie eine praktische Umsetzung im Detail aussehen könnte, bedarf daher noch einer tiefergehenden Betrachtung.

Zu 1.8 Landesbeauftragte für den Datenschutz in Sachsen-Anhalt

Die Landesregierung nimmt den Bericht des Hessischen Beauftragten für Datenschutz und Informationsfreiheit zur Kenntnis.

2. Europäische und internationale Zusammenarbeit

Zu 2.1 Einheitliche Bewertung großer Sprachmodelle der Künstlichen Intelligenz

Die Landesregierung nimmt den Bericht des Hessischen Beauftragten für Datenschutz und Informationsfreiheit zur Kenntnis.

3. Verfahren vor Gerichten und zur Verhängung von Geldbußen

Zu 3.1 Gerichtsverfahren

Die Landesregierung nimmt den Bericht des Hessischen Beauftragten für Datenschutz und Informationsfreiheit zur Kenntnis.

Zu 3.2 Verfahren über die Verhängung von Geldbußen

Die Landesregierung nimmt den Bericht des Hessischen Beauftragten für Datenschutz und Informationsfreiheit zur Kenntnis.

Verstöße im Gesundheitswesen

Der Hessische Beauftragte für Datenschutz und Informationsfreiheit hat die Hessische Landesärztekammer (LAEKH) auf Google-Rezensionen einer Praxis hingewiesen. Infolgedessen hat die LAEKH Kontakt mit der betroffenen Praxis aufgenommen, um die Rezensionen in enger Zusammenarbeit mit dem Datenschutzbeauftragten anzupassen. Als Maßnahme wurde eine Sensibilisierung durchgeführt, sodass von weitergehenden berufsrechtlichen Konsequenzen abgesehen wurde. Ein Fall zur unsachgemäßen Aufbewahrung von Patientenakten wurde der LAEKH bisher noch nicht gemeldet. Daher beabsichtigt die LAEKH, beim Hessischen Beauftragten für Datenschutz und Informationsfreiheit nachzufragen.

4. Polizei, Verfassungsschutz und Justiz

Zu 4.1 Aktuelle Entwicklungen im Sicherheitsbereich

Erweiterung um sog. Angsträume

Der Hessische Beauftragte für Datenschutz und Informationsfreiheit kritisiert das Fehlen einer gesetzlich vorgeschriebenen Kriminalitätsanalyse zur Feststellung eines Kriminalitätsschwerpunktes für die Videoüberwachung von Angsträumen und verweist auf die Möglichkeit von zunächst weniger invasiven Maßnahmen wie baulichen Veränderungen und die Schaffung von Lichtquellen. Weiterhin merkt der Hessische Beauftragte für Datenschutz und Informationsfreiheit an, dass der präventive Zweck einer Videoüberwachung zur Gefahrenabwehr nur erfüllt

werden könne, wenn ausreichend Personal zur Verfügung stehe, das die Bildübertragung konsequent im Auge behalte und entsprechend reagieren könne. Nach Auffassung des Hessischen Beauftragten für Datenschutz und Informationsfreiheit sei es fraglich, ob eine derartige, in das Recht auf informationelle Selbstbestimmung eingreifende, Maßnahme lediglich auf eine individuell empfundene Stärkung des Sicherheitsgefühls gestützt werden könne. Die Stärkung des Sicherheitsgefühls, der die Regelung laut Gesetzesbegründung dienen soll, zählt nach Auffassung des Hessischen Beauftragten für Datenschutz und Informationsfreiheit – auch in Verbindung mit Tatgelegenheitsstrukturen wie Lage, Einsehbarkeit und Frequentierung – nicht zu den Schutzgütern des Gefahrenabwehrrechts.

Die Landesregierung teilt diese Bedenken nicht.
Die Prüfung, ob mit weniger eingriffsintensiven Maßnahmen Abhilfe geschaffen werden kann, ist bereits Bestandteil der zwingend durchzuführenden Verhältnismäßigkeitsprüfung im Rahmen des § 14 Abs. 3 HSOG. Voraussetzung für die Installation einer Videoüberwachungsanlage ist nämlich die Durchführung einer ortsbezogenen Lagebeurteilung unter besonderer Berücksichtigung der Verhältnismäßigkeit. In dieser Prüfung werden auch anderweitige und grundrechtsschonendere Maßnahmen einbezogen, die ebenfalls für die Gefahrenabwehr geeignet sind. Dazu gehören auch Maßnahmen oder Handlungen wie z.B. die Installation von Lichtquellen.

Die Erweiterung der Videoüberwachung bietet mehrere Vorteile, die zur Eindämmung von Kriminalität beitragen. Die Präsenz von Überwachungskameras hat eine abschreckende Wirkung auf potenzielle Straftäter. Erfahrungen mit den bislang eingesetzten Kameras zeigen, dass sichtbar platzierte Kameras das Risiko krimineller Aktivitäten senken und zugleich das Sicherheitsgefühl der Bevölkerung stärken. Es geht daher nicht lediglich um die Stärkung des Sicherheitsgefühls der Bevölkerung, sondern vielmehr darum zu verhindern, dass diese Orte zukünftig zu Kriminalitätsschwerpunkten werden. Dies wiederum ist nach einer ortsbezogenen Lagebeurteilung zu ermitteln. Vor diesem Hintergrund scheint es unverhältnismäßig, trotz Kenntnis von begünstigenden Tatgelegenheitsstrukturen an bestimmten öffentlichen Orten erst Straftaten hinnehmen zu müssen, bevor dort präventiv Abhilfe geschaffen werden kann. Damit ist der Eingriff in das informationelle Selbstbestimmungsrecht gerechtfertigt.

Klarstellend wurde außerdem § 1 HSOG um folgenden Absatz 7 ergänzt, der die Aufgaben der Gefahrenabwehr- und Polizeibehörden präzisiert:

> *„Im Rahmen der Aufgabenwahrnehmung der Gefahrenabwehrbehörden und der Polizeibehörden kommen der Kriminalprävention, der Demokratieförderung, der Extremis-*

musprävention und insbesondere auch der Stärkung des Sicherheitsgefühls der Bevölkerung besondere Bedeutung zu."

Unmittelbarer Nahbereich von Flughäfen

Hinsichtlich der Erweiterung der Vermutungsregelung des neuen § 14 Abs. 3a Satz 2 HSOG um den unmittelbaren Nahbereich von Flughäfen kritisiert der Hessische Beauftragte für Datenschutz und Informationsfreiheit den Begriff des „öffentlich zugänglichen Bereichs" im Zusammenhang mit dem Flughafengelände als zu unbestimmt.

Die Landesregierung teilt diese Bedenken nicht.
Gesetzliche Regelungen sind stets abstrakt gefasst, damit der Anwendungsbereich nicht übermäßig eingeschränkt werden muss. bei der Normanwendung ist der Verhältnismäßigkeitsgrundsatz im Sinne von § 4 HSOG zu berücksichtigen.

Problematisch ist nach Auffassung des Hessischen Beauftragten für Datenschutz und Informationsfreiheit darüber hinaus, dass durch den Verweis in Absatz 3a auf die Voraussetzungen in Absatz 3 Satz 1 für eine Videoüberwachung an öffentlich zugänglichen Bereichen in unmittelbarer Nähe von Flughäfen – als Vermutungsregelung/Beweislastumkehr mit kursorischer Prüfung – ebenfalls ein Kriminalitätsschwerpunkt oder eine konkrete Gefahr vorausgesetzt wird, was regelmäßig schwer zu begründen sein dürfte.

Die Landesregierung teilt diese Bedenken nicht.
Laut der Gesetzesbegründung zu § 14 Abs. 3a HSOG (LT-Drs. 20/10821) ist eine Videoüberwachung an den aufgeführten Örtlichkeiten nur dann unzulässig, wenn nachweislich keine tatsächlichen Anhaltspunkte die Annahme rechtfertigen, dass Straftaten drohen. Dort heißt es auch „sofern danach allerdings nicht zur Überzeugung des Gerichts feststeht, dass es an den Voraussetzungen des § 14 Abs. 3 Satz 1 fehlt, wird es von ihrem Vorliegen ausgehen" (a.a.O. S. 41).

Erweiterung um besonders gefährdete Religionsstätten

Der Hessische Beauftragte für Datenschutz und Informationsfreiheit sieht in Bezug auf die Erweiterung des § 14 Abs. 4 HSOG um „besonders gefährdete Religionsstätten" und im Zusammenhang mit der Religionsausübung besondere Kategorien personenbezogener Daten i. S. d. § 41 Nr. 15 Buchst. a) HDSIG betroffen, bei denen spezifische Vorgaben für die Datenverarbeitung zu beachten sind.

Die Landesregierung teilt diese Bedenken nicht.

Der Staat hat nach Art. 2 Abs. 2 Satz 1 GG den Auftrag, das Leben und die körperliche Unversehrtheit der Bürger zu schützen. Zudem dient die Videoüberwachung von „besonders gefährdeten Religionsstätten" gerade dazu, die Ausübung der Religionsfreiheit der Besucher von Religionsstätten nach Art. 4 Abs. 1 und 2 GG zu gewährleisten. Aufgrund der jüngsten Anschläge besteht ein hohes Risiko, dass sich z.B. im Umfeld von Synagogen gemeingefährliche Straftaten ereignen.

Die religiöse Überzeugung ist zwar eine besondere Kategorie personenbezogener Daten i. S. d. § 41 Nr. 15 a) HDSIG. Es ist jedoch zu prüfen, ob durch das offene Beobachten und Aufzeichnen mittels Bildübertragung nach § 14 Abs. 4 HSOG tatsächlich entsprechende Daten erhoben werden oder ob dies ausgeschlossen werden kann. Falls entsprechende Daten (mit)erhoben werden, sind die genannten Garantien tatsächlich erforderlich.
Ungeachtet dessen sieht § 14 Abs. 4 Satz 3 HSOG bereits die entsprechende Anwendung von § 14 Abs. 1 Satz 2 und 3 und Abs. 3 Satz 2 und 3 HSOG vor. Damit werden besondere Vorkehrungen im Hinblick auf die spezifischen Anforderungen an die Datensicherheit und die Speicherdauer getroffen, die auch den Anforderungen des § 43 HDSIG entsprechen.

Einsatz von Bodycams in Wohnungen, Absatz 6

Die neue Regelung in § 14 Abs. 6 Satz 3 HSOG, die den Einsatz von Bodycams nun auch in Wohnungen ermöglicht, ist nach der Auffassung des Hessischen Beauftragten für Datenschutz und Informationsfreiheit mit erheblichen verfassungsrechtlichen Risiken verbunden, da umstritten ist, ob ein solcher Eingriff in die Unverletzlichkeit der Wohnung überhaupt gerechtfertigt werden kann (Problematik der Anwendbarkeit von Art. 13 Abs. 4 und 5 oder Abs. 7 GG), zumal der Einsatz von Bodycams in Wohnungen aktuell Gegenstand anhängiger Verfassungsklagen vor dem Bundesverfassungsgericht in Karlsruhe sowie dem Bayerischen Verfassungsgerichtshof sind.

Auch wenn es umstritten ist, welche Schrankenregelung des Art. 13 GG im Zusammenhang mit Bodycams Anwendung finden soll, spricht für Art. 13 Abs. 7 GG nach Auffassung der Landesregierung, dass Art. 13 Abs. 4 GG insbesondere nach Sinn und Zweck nur für verdeckte Maßnahmen gilt (vgl. Schenke, VerwArchiv 2019, 436, 456 ff.). So auch das OLG Karlsruhe im Beschluss vom 26.4.2023 (Az. 14 W 15/23 (Wx), NJW 2023, 2888 Rn. 18):

> *„Nach zutreffender Ansicht sind die speziellen, für verdeckte Maßnahmen geltenden Voraussetzungen der Absätze 3 bis 5 des Art. 13 GG nicht heranzuziehen."*

Der Hessische Beauftragte für Datenschutz und Informationsfreiheit hat im Hinblick darauf die Aufnahme einer Evaluierungsregelung angeregt.

Die Landesregierung teilt diese Auffassung nicht.
Es sprechen gewichtige Argumente für die Anwendbarkeit der Regelung aus Art. 13 Abs. 7 GG. Zudem ist der Regelungsvorschlag bereits so wenig eingriffsintensiv wie möglich ausgestaltet.

Mustererkennung und biometrische Echtzeit-Fernidentifizierung bei Überwachungsmaßnahmen

Durch die in § 14 HSOG neu eingefügten Abs. 8 bis 11 wurde eine Grundlage für den Einsatz intelligenter Videoanalyse und biometrischer Echtzeit-Fernidentifizierung geschaffen. Diese Erweiterung des Einsatzes von Videoschutzanlagen erstreckt sich auf die Anwendungsalternativen in § 14 Abs. 1, 3, 3a und 4 HSOG, was durch den Hessischen Beauftragten für Datenschutz und Informationsfreiheit kritisiert wird.

Die Landesregierung stimmt dieser Kritik nicht zu.
Die nach diesen § 14 Abs. 1, 3, 3a und 4 HSOG zugelassenen Bildaufzeichnungen ermöglichen die Sicherung von Bildmaterial sowie eine offene Beobachtung von Brennpunktbereichen. Eine vollständige und ausreichend schnelle Auswertung des gesicherten Bildmaterials ist jedoch aufgrund des erheblichen personellen und zeitlichen Aufwands nicht möglich. Dieser Umstand soll durch den Einsatz von entsprechender Bildanalysesoftware auf Grundlage künstlicher Intelligenz (KI) umgekehrt werden. Der Einsatz intelligenter Bildanalysesoftware wird im Rahmen aller Anwendungsalternativen ermöglicht, um Gefahren in all diesen Anwendungsalternativen frühzeitig zu erkennen und hierdurch möglichst umfassend die Begehung von Straftaten zu verhindern oder die weitere Tatausführung zu unterbinden sowie um Opfer zu schützen. Dabei ist zu beachten, dass die vorgeschalteten Maßnahmen nach § 14 Abs. 1, 3, 3a und 4 HSOG nicht anlasslos, sondern unter variierenden, engen räumlichen und inhaltlichen Voraussetzungen eingesetzt werden und zudem vor dem Einsatz intelligenter Analysesoftware nach § 14 Abs. 8 und 9 HSOG stets eine Verhältnismäßigkeitsüberprüfung im Sinne von § 4 HSOG erfolgt.

§ 14 Abs. 8 Satz 1 Nr. 1 HSOG eröffnet die Möglichkeit des Einsatzes von Bildanalysesoftware, welche automatisiert bestimmte Muster von Bewegungen, die auf die Begehung einer Straftat hindeuten, erkennt und auswertet. Nach § 14 Abs. 8 Satz 1 Nr. 2 ist der Einsatz einer Bildanalysesoftware zur Erkennung von Mustern bezogen auf Waffen im Sinne des § 1 Abs. 2 des Waffengesetzes, Messer und gefährliche Gegenstände möglich. Vom Hessischen Beauftragten für Datenschutz und Informationsfreiheit wird insoweit problematisiert, dass die Norm keine

Regelungen dazu enthält, welche konkreten Bewegungs- oder Verhaltensmuster der automatisierten Auswertung und dem zum Einsatz kommenden Algorithmus zugrunde gelegt werden.

Nach Auffassung der Landesregierung muss dies jedoch nicht durch Gesetz geregelt werden. Vielmehr sind gesetzliche Regelungen stets abstrakt gefasst. Bei der Normanwendung ist unter Berücksichtigung des Verhältnismäßigkeitsgrundsatzes im Sinne von § 4 HSOG zu entscheiden, welche konkreten Bewegungs- oder Verhaltensmuster der automatisierten Auswertung und dem zum Einsatz kommenden Algorithmus zugrunde gelegt werden. Zu betonen ist zudem, dass die Auswertung nicht anhand personenbezogener Merkmale erfolgt, sodass von den Personen, die sich im Aufnahmebereich befinden, grundsätzlich nicht mehr Daten erfasst werden als in den Fällen des § 14 Abs. 1, 3, 3a und 4.

Durch § 14 Abs. 8 Satz 4 sowie Abs. 9 HSOG wird der Einsatz biometrischer Echtzeit-Fernidentifizierung zur Nachverfolgung (§ 14 Abs. 8 S. 4 HSOG) bzw. zur gezielten Suche (§ 14 Abs. 9 HSOG) möglich. Die biometrische Echtzeit-Fernidentifizierung zur gezielten Suche ist nach § 14 Abs. 9 Satz 3 HSOG auf das zeitlich und örtlich unbedingt erforderliche Maß zu beschränken. Insoweit führt der Hessische Beauftragte für Datenschutz und Informationsfreiheit an, dass es an einer Definition der zeitlichen und örtlichen Begrenzung fehlt.

Die Landesregierung teilt diese Bedenken nicht.
Die zeitliche und örtliche Begrenzung auf das unbedingt erforderliche Maß hängt stets vom konkreten Einzelfall ab und lässt sich nicht allgemeingültig festlegen.

Der Hessische Beauftragte für Datenschutz und Informationsfreiheit führt weiterhin an, dass in § 14 Abs. 8 bis 11 HSOG keine spezifischen Löschfristen oder Vorgaben dafür enthalten sind, dass ein Mensch vor Ergreifen von Folgemaßnahmen die gewonnenen Ergebnisse noch einmal prüft und bewertet. Letzteres ergibt sich jedoch bereits unmittelbar aus der Verordnung (EU) 2024/1689 des Europäischen Parlaments und des Rates vom 13. Juni 2024 – Verordnung über künstliche Intelligenz (KI-VO). Nach Art. 5 Abs. 3 UAbs. 2 S. 3 KI-VO darf eine Entscheidung, aus der sich eine nachteilige Rechtsfolge für eine Person ergibt, nicht ausschließlich auf der Grundlage der Ausgabe des biometrischen Echtzeit-Fernidentifizierungssystems getroffen werden. Hinsichtlich der Löschfristen gelten die allgemeinen Vorgaben, es bedurfte insofern keiner spezifischen Regelung.

Nach Auffassung des Hessischen Beauftragten für Datenschutz und Informationsfreiheit ergibt sich vor dem Hintergrund der Wesentlichkeitstheorie die Problematik, inwieweit wesentliche Entscheidungen an die Exekutive delegiert werden können. Nach der Rechtsprechung des

Bundesverfassungsgerichts (Urteil vom 16. Februar 2023 (1 BvR 1547/19 und 1 BvR 2634/20) muss der Gesetzgeber die wesentlichen Grundlagen zur Begrenzung von Art und Umfang der Daten und der Verarbeitungsmethoden selbst durch Gesetz vorgeben. Soweit eine tiefergehende gesetzliche Normierung nicht praktikabel erscheint, kann er jedoch die Verwaltung zur näheren Regelung organisatorischer und technischer Einzelheiten ermächtigen. Dabei muss sichergestellt sein, dass im Zusammenwirken der gesetzlichen Vorgaben mit den Regelungsermächtigungen und -verpflichtungen der Verwaltung Art und Umfang der Daten und die Verarbeitungsmethoden insgesamt inhaltlich ausreichend, normenklar und transparent begrenzt sind. Sowohl § 14 Abs. 8 HSOG als auch § 14 Abs. 9 HSOG erfüllen diese Anforderungen, da aus den Regelungen jeweils hervorgeht, welche Daten in welchem Umfang verarbeitet werden und nach § 14 Abs. 10 Satz 3 HSOG nur die Einzelheiten des notwendigen Inhalts der Begründung und nach § 14 Abs. 11 Satz 9 HSOG nur das Nähere zum technischen Verfahren in Verwaltungsvorschriften geregelt wird.

Der Hessische Beauftragte für Datenschutz und Informationsfreiheit wirft außerdem die Frage auf, ob § 14 Abs. 8 bis 11 HSOG die von der KI-VO geforderten notwendigen und verhältnismäßigen Schutzvorkehrungen und Bedingungen für die Verwendung biometrischer Echtzeit-Fernidentifizierungssysteme in ausreichendem Maße aufgreifen.

Nach Auffassung der Landesregierung ist das der Fall. Insbesondere ist der Einsatz biometrischer Echtzeit-Fernidentifizierung nach § 14 Abs. 8 bis 11 HSOG nur in den in Art. 5 Abs.1 UAbs. 1 lit. h, Abs. 2, Abs. 3 KI-VO aufgeführten Grenzen und unter den dort genannten Bedingungen möglich.

Automatisierte Anwendung zur Datenanalyse, § 25a HSOG

Der Hessische Beauftragte für Datenschutz und Informationsfreiheit führt in Bezug auf die Änderung des § 25a HSOG an, dass weder der Begriff der KI oder des KI-Systems erwähnt wird, noch sich besondere verfahrensrechtliche Vorkehrungen oder schützende Regelungen in der Norm finden. Es sei daher fraglich, ob die Maßgaben des Bundesverfassungsgerichts (Urteil vom 16. Februar 2023 (1 BvR 1547/19 und 1 BvR 2634/20)) zum Einsatz von KI-Systemen im Zusammenhang mit der automatisierten Anwendung zur Datenanalyse auf der Ebene eines förmlichen Gesetzes umgesetzt werden.

Die Landesregierung teilt diese Bedenken nicht.

In § 25a Abs. 1 Satz 5 HSOG wurde die Einschränkung, dass eine regelbasierte und von Menschen definierte Abfolge von Analyse- und Verarbeitungsschritten erforderlich ist, gestrichen. Diese Änderung ermöglicht, dass künftig KI zur automatisierten Datenanalyse eingesetzt

werden kann. Dies ist aufgrund der voranschreitenden technologischen Entwicklung erforderlich, um Gefahrenabwehr auch künftig effizient betreiben zu können. Dabei wurde der Begriff der KI oder des KI-Systems nicht ausdrücklich erwähnt, da hierfür keinerlei Bedürfnis besteht und andere Technologien nicht ausgeschlossen werden sollten. Auch weiterhin ist die automatisierte Anwendung zur Datenanalyse jedoch von Menschen zu veranlassen und manuell auszulösen (vgl. § 25a Abs. 1 S. 5 HSOG).

Der Einsatz von KI ist in der KI-VO geregelt, die unmittelbar gilt. In § 25a HSOG sind darüber hinaus schützende verfahrensrechtliche Vorkehrungen, wie beispielsweise Regelungen zur Zugriffskontrolle und Begründungspflicht in § 25a Abs. 4 HSOG enthalten. Der neue § 25a Abs. 6 HSOG hebt zudem hervor, dass die Polizeibehörden sicherzustellen haben, dass diskriminierende Algorithmen weder herausgebildet noch verwendet werden. Die Maßgaben des Bundesverfassungsgerichts (Urteil vom 16. Februar 2023 (1 BvR 1547/19 und 1 BvR 2634/20)) zum Einsatz von KI-Systemen im Zusammenhang mit der automatisierten Anwendung zur Datenanalyse sind mithin hinreichend umgesetzt.

Überdies wurden im Rahmen der Novellierung in § 25a Abs. 2 Satz 4 HSOG auch Telekommunikationsdaten bei Maßnahmen nach § 25a Abs. 2 Satz 1 Nr. 3 HSOG zur Senkung des Eingriffsgewichts ausgeschlossen.

Elektronische Aufenthaltsüberwachung

Der Hessische Beauftragte für Datenschutz und Informationsfreiheit weist im Zusammenhang mit der Neufassung des § 31a Abs. 5 HSOG, der nunmehr die Verbindung der erhobenen Daten zu einem Bewegungsbild aufgrund richterlicher Anordnung ermöglicht, darauf hin, dass dessen Erstellung allein von dem Erfordernis der Erfüllung des Überwachungszwecks abhängig gemacht werde und die Norm selbst keine konkreten Vorgaben enthalte, an denen sich die Behörde im Zusammenhang mit der Bewertung der Verhältnismäßigkeit der Maßnahme orientieren könne.

Die Landesregierung stimmt dieser Ansicht nicht zu.

Die Neuregelung des § 31a Abs. 5 HSOG bestimmt die Reichweite der zu erhebenden Informationen beim Einsatz einer elektronischen Aufenthaltsüberwachung (EAÜ). Während § 31a Abs. 5 Satz 1 HSOG eine gängige Regelung enthält, wonach der Aufenthaltsort und etwaige Beeinträchtigungen der Datenerhebung verarbeitet werden dürfen, ist es nach § 31a Abs. 5 Satz 2 HSOG nunmehr möglich, dass aus den erhobenen Daten Bewegungsbilder erstellt werden, soweit dies zur Erfüllung des Überwachungszwecks erforderlich ist. Dabei sind die

der Regelung des § 31a Abs. 5 Satz 2 HSOG unterfallenden Fälle zu unterscheiden von inhaltlich noch weitergehenden, weil zusätzliche Informationen verarbeitenden Persönlichkeitsprofilen, die stets unzulässig sind (vgl. BVerfG, Urteil vom 20.4.2016 – 1 BvR 966/09, 1 BvR 1140/09, Rn. 130; Beschluss vom 11. 5. 2007 – 2 BvR 543/06, Rn. 59, beck-online).

Gegenüber der reinen EAÜ ist das in Rede stehende Vorgehen dennoch von besonderer Eingriffsintensität (allgemeines Persönlichkeitsrecht und Recht auf informationelle Selbstbestimmung, Art. 2 Abs. 1 i. V. m. Art. 1 Abs. 1 GG) und muss mit Blick auf die grundrechtlichen Garantien nicht nur einfachgesetzlich zulässig, sondern darüber hinaus stets nach dem Grundsatz der Verhältnismäßigkeit gerechtfertigt sein. Ergibt sich somit auf der auf Grundlage von Tatsachen anzustellenden Gefährdungsprognose, dass von der betroffenen Person in absehbarer Zeit eine hinreichend konkretisierte Gefahr für die von § 31a HSOG geschützten, bedeutenden Rechtsgüter ausgeht, kann dieser Gefahr zu Abwehrzwecken durch die befristete Anordnung der EAÜ nebst Genehmigung der Erstellung eines Bewegungsbildes begegnet werden, sofern die Schwere des damit verbundenen Eingriffs in die grundrechtlich geschützte Lebenssphäre der betroffenen Person in angemessenem Verhältnis zum Anlass steht. Die jeweils maßgeblichen und im Rahmen der Verhältnismäßigkeitsprüfung zu berücksichtigen Aspekte hängen dabei vom konkreten Einzelfall ab.

Vorweggenommen werden kann dabei, dass die Neureglung dem besonderen Wohnraumschutz nach Art. 13 GG Rechnung trägt. Nach § 31a Abs. 5 Satz 5 HSOG ist im Rahmen des technisch Möglichen sicherzustellen, dass innerhalb der Wohnung der betroffenen Person keine über den Umstand ihrer Anwesenheit hinausgehende Aufenthaltsdaten erhoben werden. Mit ihr ist mithin kein Eingriff in die Garantie der Unverletzlichkeit der Wohnung als grundrechtlich geschützte Lebenssphäre der betroffenen Person verbunden.

Darüber hinaus ist neben dem bereits in § 31a Abs. 3 Satz 1 HSOG vorgesehenen Richtervorbehalt für die Anordnung der EAÜ (sowie deren Verlängerung) auch die Befugnis zur Erstellung eines Bewegungsbildes unter Richtervorbehalt gestellt (§ 31a Abs. 5 Satz 2 HSOG). Damit trägt der Gesetzgeber der Tatsache Rechnung, dass die Erstellung eines Bewegungsbildes durch eine EAÜ einen nochmals tieferen Grundrechtseingriff bedeutet und diese Maßnahme daher aus den Gedanken des Rechtsstaatsprinzips und der Gewaltenkontrolle einem gesonderten ausdrücklichen Richtervorbehalt unterworfen wird.

Zu 4.2 Entscheidung des BVerfG zum Hessischen Verfassungsschutzgesetz

Der Hessische Beauftragte für Datenschutz und Informationsfreiheit berichtet in seinem Tätigkeitsbericht zutreffend, dass der Erste Senat des Bundesverfassungsgerichts (BVerfG) mit

Beschluss vom 17. Juli 2024 (Az. 1 BvR 2133/22) einzelne Vorschriften des Hessischen Verfassungsschutzgesetzes (HVSG) wegen Verstoßes gegen das Recht auf informationelle Selbstbestimmung (Art. 2 Abs. 1 i. V. m. Art. 1 Abs. 1 GG) für verfassungswidrig erklärt hat. Bis zu einer Neuregelung, längstens bis zum 31. Dezember 2025, gelten die mit dem Grundgesetz unvereinbaren Vorschriften mit bestimmten Maßgaben fort. Die betroffenen Vorschriften werden im Rahmen eines aktuellen Gesetzgebungsverfahrens derzeit entsprechend der Vorgaben geändert.

Vor dem zweiten Kabinettdurchgang des Änderungsgesetzes sind u. a. die Ressortbeteiligung sowie die Verbändeanhörung durchgeführt worden, in deren Rahmen der Hessische Beauftragte für Datenschutz und Informationsfreiheit jeweils zu den beabsichtigten Änderungen beteiligt wurde. Im Zuge der Ressortbeteiligung gab der Hessische Beauftragte für Datenschutz und Informationsfreiheit eine umfangreiche Stellungnahme ab, die zu teilweisen Änderungen des Gesetzesentwurfs führte, u.a. die stellenweise ausführlichere Fassung der Gesetzesbegründung und die Vereinheitlichung von Begrifflichkeiten. Auch wurde dem Hessischen Beauftragten für Datenschutz und Informationsfreiheit im Rahmen eines umfangreichen Antwortschreibens dargelegt, weshalb einzelne Änderungsvorschläge übernommen bzw. nicht übernommen wurden. In der darauffolgenden Verbändeanhörung gab der Hessische Beauftragte für Datenschutz und Informationsfreiheit erneut eine Stellungnahme ab, die zur Anpassung einer Verweisnorm führte. Zudem gab der Hessische Beauftragte für Datenschutz und Informationsfreiheit im Rahmen der Sachverständigenanhörung durch den Hessischen Landtag zu den geplanten Änderungen eine Stellungnahme ab.

Ortung von Mobilfunkendgeräten, § 9 HVSG

Die niedrige Eingriffsschwelle des Abs. 1 für den punktuellen Einsatz der technischen Mittel hat das BVerfG in Fortschreibung seiner Rechtsprechung noch einmal ausdrücklich als verfassungskonform bestätigt (BVerfG, 1 BvR 2133/22, Rn. 129 f.). Zusätzlich hat das BVerfG das Erfordernis des Vorliegens tatsächlicher Anhaltspunkte als Einschränkung der Zweckbestimmung festgestellt (BVerfG, a. a. O., Rn. 139). Ergänzend zu § 5 Abs. 1 HVSG wird dieses daher noch einmal allgemein in die Eingriffsschwelle des § 9 Abs. 1 HVSG aufgenommen.
Mithin soll nunmehr abstrakt an die Eignung der erhobenen Daten angeknüpft werden.
Die nach dem Beschluss des BVerfG dafür relevanten Kriterien einer Erfassung der Persönlichkeit sollen dazu unmittelbar im Gesetz geregelt werden.

Einsatz von verdeckten Mitarbeiterinnen und Mitarbeitern, § 12 HVSG

Der Kritik des BVerfG soll durch eine ersatzlose Streichung des fraglichen Kriteriums begegnet werden, so dass jedweder Einsatz Verdeckter Mitarbeiterinnen und Mitarbeiter den erhöhten

Eingriffsvoraussetzungen unterliegen würde. Darüber hinaus soll das durch das BVerfG ausdrücklich aufgestellte Erfordernis tatsächlicher Anhaltspunkte (BVerfG, a. a. O. Rn. 189) sowohl für die Annahme einer beobachtungsbedürftigen Bestrebung als auch für das Gebotensein der Aufklärung ergänzt werden.

Informationsübermittlung durch das Landesamt an Strafverfolgungsbehörden, § 20a HVSG

Das BVerfG stellt fest, dass zusätzlich zum Strafrahmen und an die Begehung im Zusammenhang mit der Beteiligung an einer beobachtungsbedürftigen Bestrebung oder Tätigkeit erforderlich sei, „dass sich insbesondere eine bestimmte Begehungsform im Tatbestand selbst niederschlägt und zugleich das besonders schwere Unrecht der Tat begründet" (BVerfG, a. a. O., Rn. 207, vgl. auch Rn. 214). Erforderlich ist demnach, im Bereich der Straftaten mit einer Höchststrafdrohung von fünf Jahren Freiheitsstrafe eine Kombination aus dem Strafrahmen, der spezifischen Begehungsmodalität des Beteiligungszusammenhangs sowie einer im Tatbestand selbst zum Ausdruck kommenden verfassungsschutzspezifischen Schwere vorauszusetzen. Dabei verlangt das BVerfG die Erstellung eines spezifischen Katalogs oder die Inbezugnahme eines bestehenden (BVerfG, a. a. O., Rn. 206).
Mangels Existenz eines bestehenden Straftatenkatalogs soll entsprechend den Vorgaben des BVerfG ein solcher Katalog erstellt werden. Die zugrundeliegenden Kriterien der Erstellung lassen sich der Gesetzesbegründung entnehmen.

Informationsübermittlung an sonstige inländische öffentliche Stellen, § 20b HVSG

Das BVerfG hat klargestellt, dass es für das Erfordernis der hohen Schwelle der mindestens konkretisierten Gefahr allein darauf ankommt, dass die empfangenden öffentlichen Stellen über operative Anschlussbefugnisse verfügen und nicht darauf, ob und inwieweit die Datenübermittlung im Einzelfall deren Einsatz nach sich ziehen soll. Entsprechend soll in § 20b Abs. 2 HVSG ein neuer Satz 2 eingefügt werden, der bei Vorliegen operativer Anschlussbefugnisse der empfangenden Stelle dieses Erfordernis abbildet. In Satz 3 soll klarstellend die Definition der operativen Befugnis des BVerfG legaldefiniert werden. Hierbei soll es auf das Vorliegen einer entsprechenden operativen Zwangsbefugnis der fraglichen Behörde und nicht auf die Möglichkeit einer etwaigen Erzwingung von Handlungen oder Duldungen im Verwaltungsvollstreckungsverfahren ankommen.

Zu 4.3 Datenschutzkontrollen bei einer Staatsanwaltschaft

Die Landesregierung stimmt den Ausführungen des Hessischen Beauftragten für Datenschutz und Informationsfreiheit zu.

Zu 4.4 Offenlegung personenbezogener Daten im staatsanwaltschaftlichen Einstellungsbescheid

Die Landesregierung stimmt den Ausführungen des Hessischen Beauftragten für Datenschutz und Informationsfreiheit zu.

Zu 4.5 Datenschutzkontrollen bei Polizeibehörden und Verfassungsschutz

Kontrolle der Antiterrordatei (ATD)

Der Hessische Beauftragte für Datenschutz und Informationsfreiheit hat die ATD am 11. Dezember 2024 turnusmäßig nach § 10 Abs. 2 Antiterrordateigesetz im Hessischen Landeskriminalamt (HLKA) geprüft. Ein Abschlussergebnis der Datenschutzkontrolle liegt dem HLKA noch nicht vor. Über das abschließende Ergebnis der Kontrolle wird der HBDI im nächsten Tätigkeitsbericht informieren. Eine Stellungnahme ist deshalb noch nicht möglich.

Datenschutzkontrolle von verdeckten Maßnahmen

Gemäß der gesetzlichen Vorgabe des § 29a HSOG hat der Hessische Beauftragte für Datenschutz und Informationsfreiheit im Berichtszeitraum mit der Datenschutzkontrolle von verdeckten Maßnahmen – konkret die Anordnungen des Einsatzes verdeckter Ermittler (VE) oder verdeckt ermittelnder Personen (VP) – der Hessischen Polizei begonnen. Über die noch nicht abgeschlossene Kontrolle wird der Hessische Beauftragte für Datenschutz und Informationsfreiheit in seinem nächsten Tätigkeitsbericht berichten. Eine Stellungnahme ist deshalb noch nicht möglich.

Datenschutzkontrolle polizeilich vergebener personengebundener Hinweise

Die vom Hessischen Beauftragten für Datenschutz und Informationsfreiheit im HLKA im Jahr 2023 begonnene Prüfung der polizeilich vergebenen personengebundenen Hinweise (PHW) wurde abgeschlossen. Sie umfasste im Konkreten eine Stichprobenkontrolle der durch die Polizeipräsidien Mittelhessen und Osthessen vergebenen PHW Betäubungsmittelkonsument (PHW BTMK).

Aufgrund des im Tätigkeitsbericht aufgezeigten Prüfungsergebnisses wurden im Rahmen der 36. und 37. Arbeitstagungen (Mai und November 2024) der Z1-Leitungen Hessen und des HLKA, HSG 25, die retrograde Überprüfung und, falls notwendig, die Bereinigung aller vor dem 19. Oktober 2012 gespeicherten PHW BTMK durch die datenbesitzenden Dienststellen festgelegt und im Nachgang die Umsetzung veranlasst.

In Zusammenhang mit den Feststellungen des Hessischen Beauftragten für Datenschutz und Informationsfreiheit zur unterschiedlichen Dokumentation sowie zum Zeitpunkt der Erfassung

wurden im Rahmen der Überarbeitung der Analyserichtlinien Vorgaben zur einheitlichen Verfahrensweise für die Dokumentation sowie den Zeitpunkt der Vergabe von PHW ergänzt.

Prüfung zum Zeugenschutz im Bundeszentralregister (BZR)

Im Jahr 2024 konnte die Datenschutzkontrolle zum Zeugenschutz im BZR gemäß § 44a Bundeszentralregistergesetz beendet werden. Hinsichtlich des vorgesehenen Prüfungsgegenstandes kam lediglich ein relevanter Fall des PP Südosthessen (PP SOH) in Betracht.
Neben grundsätzlichen Ausführungen der Leitung von OE20 und der zuständigen Sachbearbeitung des PP SOH zur Arbeit der Zeugenschutzdienststellen nahm der Hessische Beauftragte für Datenschutz und Informationsfreiheit unmittelbar Einsicht in die entsprechende Fallakte des PP SOH. Verstöße gegen Datenschutzvorschriften wurden vom Hessischen Beauftragten für Datenschutz und Informationsfreiheit nicht festgestellt. Vielmehr konnte er sich im Rahmen der Prüfung von der dokumentierten und strukturierten Arbeitsweise der Zeugenschutzstellen in Hessen überzeugen.

Zu 4.6 Typosquatting bei der Hessischen Polizei

Die Landesregierung stimmt den Ausführungen des Hessischen Beauftragten für Datenschutz und Informationsfreiheit zu.

Ergänzend wird darauf hingewiesen, dass sich nach Einbeziehung des HLKA und Initiierung weiterer Prüfungen keine konkreten Hinweise auf einen gezielten Datenmissbrauch ergeben haben und keine Ermittlungsverfahren einzuleiten waren.

5. Allgemeine Verwaltung, Kommunen

Zu 5.1 Datenschutz als Vertrauensbasis für Künstliche Intelligenz in der Verwaltung

Die Landesregierung stimmt den Ausführungen des Hessischen Beauftragten für Datenschutz und Informationsfreiheit zur datenschutzrechtlichen Dimension des Einsatzes von Systemen Künstlicher Intelligenz (KI) in der Verwaltung zu. Wie dieser sieht sie große Potentiale und eine hohe Bandbreite an Einsatzmöglichkeiten für KI in der Verwaltung.

Der Hessische Beauftragte für Datenschutz und Informationsfreiheit weist zu Recht darauf hin, dass die Datenschutz-Grundverordnung (DS-GVO) auch für KI-Systeme Anwendung findet, sofern personenbezogene Daten verarbeitet werden. Aus Sicht der Landesregierung stellt dieser Umstand die verantwortlichen Stellen vor besondere Herausforderungen, da die DS-GVO auf einem traditionell deterministischen IT-Verständnis basiert, das sich nicht ohne Weiteres

auf KI-Systeme übertragen lässt. So können beispielsweise die Betroffenenrechte auf Auskunft, Berichtigung und Löschung in KI-basierten Systemen nur eingeschränkt oder mit erheblichem Aufwand umgesetzt werden, insbesondere wenn keine eindeutig zuordenbaren Datensätze existieren. Umso wichtiger ist es, diese Rechte frühzeitig in der Planung und vor dem Einsatz von KI-Systemen zu berücksichtigen und mögliche Methoden zu identifizieren, die ihre Umsetzung rechtskonform ermöglichen.

Die Landesregierung begrüßt ausdrücklich, dass der Hessische Beauftragte für Datenschutz und Informationsfreiheit insbesondere für die kommunale Ebene Fortbildungsangebote für den Einsatz von KI anbieten will. Solche Maßnahmen ermöglichen es, Risiken und Nutzungsmöglichkeiten aufzuzeigen. Dies ist ein Ansatz, den die Landesregierung selbst verfolgt, indem das Thema bereits durch erste Regelungswerke und Informationsbroschüren aufgearbeitet wurde, um eine Sensibilisierung hierfür herbeizuführen; bei zukünftigen Aktualisierungen im weiteren Ausbau des Dialogs mit dem Hessischen Beauftragten für Datenschutz und Informationsfreiheit.

Zugleich ist festzuhalten, dass sich die Potenziale von KI in der öffentlichen Verwaltung nicht ausschließlich im Zusammenhang mit personenbezogenen Daten erschließen. Vielmehr bestehen vielfältige Einsatzmöglichkeiten von KI auch dort, wo keine oder nur rein technische bzw. aggregierte Daten verarbeitet werden. In diesen Fällen stehen Effizienz, Qualität und Modernisierung des Verwaltungshandelns im Zentrum.

Die neue EU-KI-Verordnung bietet einen regulatorischen Rahmen, der auch diese Anwendungsbereiche berücksichtigt – differenziert und risikoorientiert. Nicht jede Technologie mit dem Label „KI" stellt automatisch ein datenschutzrechtlich sensibles System dar. Die im Tätigkeitsbericht genannten Beispiele sind gute Beispiele für die Verarbeitung von aggregierten Daten und zeigen wie wertvoll der KI-Einsatz für eine effiziente Verwaltung sein kann.

Zu 5.2 Rechtsgrundlagen für Datenverarbeitungen in Kommunen

Die Landesregierung stimmt den Ausführungen des Hessischen Beauftragten für Datenschutz und Informationsfreiheit zu.

Zu 5.3 Fragebogen zu kommunalen Datenschutzbeauftragten

Die Landesregierung nimmt den Bericht des Hessischen Beauftragten für Datenschutz und Informationsfreiheit zur Kenntnis.

Zu 5.4 Datenschutz bei politischen Informationssystemen

Die Landesregierung stimmt den Ausführungen des Hessischen Beauftragten für Datenschutz und Informationsfreiheit zu.

Zu 5.5 Bundesweites Projekt zum Datenschutz in der Rehabilitation und Teilhabe (SGB IX)

Die Landesregierung nimmt den Bericht des Hessischen Beauftragten für Daten-schutz und Informationsfreiheit zur Kenntnis.

Die Einbindung des Hessischen Beauftragten für Datenschutz und Informationsfreiheit in das bundesweite Projekt zum Datenschutz in der Rehabilitation und Teilhabe (SGB IX) wird von der Landesregierung ausdrücklich begrüßt und unterstützt. Die in der Arbeitsgruppe gelebte konstruktive Zusammenarbeit sowie die mehrfach erreichten praxisrelevanten Arbeitsergebnisse sind besonders hervorzuheben. Sie sind von spürbarem Nutzen für alle Beteiligten in diesem anspruchsvollen Aufgabenfeld. Die weitere Begleitung der Arbeitsgruppe durch den Hessischen Beauftragten für Datenschutz und Informationsfreiheit wird als wichtig und zielführend eingeschätzt.

6. Schulen und Hochschulen

Zu 6.1 Datenschutzrechtliches Verhältnis zwischen Schulen und Schulträgern

Die Landesregierung stimmt den Ausführungen des Hessischen Beauftragten für Datenschutz und Informationsfreiheit zum Verlauf und den Ergebnissen der Gespräche zu.
Die in den Gesprächen entwickelten Mustervorlagen für Schulen stellen keine Vorgaben der Landesregierung gegenüber den Schulträgern zu den Zuständigkeiten im Bereich des Datenschutzes dar. Sie sind als gemeinsam erarbeitetes Angebot zu verstehen, das bei Erfüllung der sich unmittelbar aus der DS-GVO ergebenden datenschutzrechtlichen Pflichten, dienen kann. Die Landesregierung beabsichtigt, den Dialog in Abstimmung mit dem Hessische Beauftragte für Datenschutz und Informationsfreiheit fortzusetzen.

Zu 6.2 Messenger-Dienste für Elternbeiräte

Die Landesregierung stimmt den Ausführungen des Hessischen Beauftragten für Datenschutz und Informationsfreiheit grundsätzlich zu.

Klarstellend wird darauf hingewiesen, dass der Einsatz datenschutzrechtlich unbedenklicher Messenger-Dienste auf solche Tätigkeiten der Elternbeiräte begrenzt ist, für die rechtlich keine besondere Form vorgegeben wird. Für Tätigkeiten, die nach dem Gesetz einer besonderen Form unterliegen, stellen sie kein geeignetes Kommunikationsmittel dar. So regelt § 2 Abs. 2 Satz 1 der Verordnung für die Wahl zu den Elternvertretungen und die Entschädigung der

Mitglieder des Landeselternbeirats und der vom Landeselternbeirat gebildeten Ausschüsse, dass zu allen Wahlen schriftlich eingeladen werden muss. In der Regel erfolgt die Wahl der Elternbeiräte beim ersten Elternabend der jeweiligen Klasse oder Jahrgangsstufe bzw. in der ersten Sitzung des jeweiligen Gremiums am Beginn des Schuljahrs. Eine Einladung zu einem Elternabend über Messenger-Dienste per Textform erfüllt damit die Voraussetzungen einer ordnungsgemäßen Ladung nicht. Gleiches gilt für Einladungen zu Wahlen in den Elternbeiräten (Schulelternbeiräte, Stadt- und Kreiselternbeiräte, Landeselternbeirat).

7. Beschäftigungsverhältnisse

Zu 7.2 Mündliche Datenverarbeitungen im Beschäftigungsverhältnis

Die Landesregierung nimmt den Bericht des Hessischen Beauftragten für Daten-schutz und Informationsfreiheit zur Kenntnis.

Zu 7.3 Keine Ermittlungen ins Blaue hinein

Die Landesregierung nimmt den Bericht des Hessischen Beauftragten für Datenschutz und Informationsfreiheit zur Kenntnis.

Zu 7.4 Keine anlass- und lückenlose Totalüberwachung der Korrespondenz von Beschäftigten

Die Landesregierung nimmt den Bericht des Hessischen Beauftragten für Datenschutz und Informationsfreiheit zur Kenntnis.

Zu 7.5 Personalausweis und Führerscheinkontrollen durch Arbeitgeber

Die Landesregierung stimmt den Ausführungen des Hessischen Beauftragten für Datenschutz und Informationsfreiheit zu.

Der Schutz personenbezogener Daten im Beschäftigungsverhältnis ist ein besonders sensibler Bereich, der einer sorgfältigen Abwägung von berechtigtem Interesse des Arbeitgebers und dem Recht auf informationelle Selbstbestimmung bedarf. Gleichzeitig ist festzuhalten, dass es im Rahmen dienstlicher Anforderungen – etwa bei der Überlassung von Dienstfahrzeugen oder beim Zugang zu sicherheitsrelevanten Bereichen – zu legitimen Kontrollbedarfen kommen kann. So verpflichtet § 21 Abs. 1 Nr. 2 Straßenverkehrsgesetz (StVG) Fahrzeughalter – und damit auch öffentliche Arbeitgeber – sicherzustellen, dass nur Personen mit gültiger Fahrerlaubnis ein Fahrzeug führen. Die Verletzung dieser Pflicht kann bereits bei Fahrlässigkeit strafrechtliche Konsequenzen nach sich ziehen. In solchen Fällen sind datenschutzfreundliche Lösungen, wie z. B. dokumentierte Sichtkontrollen ohne Speicherung oder Kopie von Ausweisdokumenten, zu bevorzugen. Diese Vorgehensweise ist z.B. im Ministerium des Innern, für

Sicherheit und Heimatschutz geübte Praxis.

8. Internet und Medien

Zu 8.1 Datenschutz und KI – Aktuelle Entwicklungen

Die Landesregierung stimmt den Ausführungen des Hessischen Beauftragten für Datenschutz und Informationsfreiheit zu.

Es wird darauf hingewiesen, dass die vom Hessischen Beauftragten für Datenschutz und Informationsfreiheit angeführten Argumente und Bewertungen auch für SLM (Small Language Models; Kleine Sprachmodelle) gelten.

Zu 8.2 Nicht überall nur Einwilligungen!

Die Landesregierung nimmt den Bericht des Hessischen Beauftragten für Datenschutz und Informationsfreiheit zur Kenntnis.

Zu 8.3 Die Beitreibung des Rundfunkbeitrags

Die Landesregierung stimmt den Ausführungen des Hessischen Beauftragten für Datenschutz und Informationsfreiheit zu.

9. Werbung und Adresshandel

Zu 9.3 Die Beschwerde bei der Aufsichtsbehörde – ein Recht für betroffene Personen

Die Landesregierung nimmt den Bericht des Hessischen Beauftragten für Datenschutz und Informationsfreiheit zur Kenntnis.

11. Wirtschaft

Zu 11.5 Ausweiskopien in Hotels

Die Landesregierung stimmt den Ausführungen des Hessischen Beauftragten für Datenschutz und Informationsfreiheit zu den Rechtsgrundlagen im Bundesmeldegesetz und Personalausweisgesetz zu.

12. Gesundheitsbereich

Zu 12.1 Recht des Patienten auf kostenlose Kopie der Patientenakte

Landesärztekammer Hessen

Die LAEKH hat das Urteil des Europäischen Gerichtshofs bereits in ihrer Delegiertenversammlung am 23. November 2024 umgesetzt. § 10 Abs. 2 der Berufsordnung für Ärztinnen und Ärzte in Hessen wurde zum 1. Januar 2025 wie folgt geändert:

„(2) Ärztinnen und Ärzte haben Patientinnen und Patienten auf deren Verlangen in die sie betreffende Dokumentation Einsicht zu gewähren, soweit der Einsichtnahme nicht erhebliche therapeutische Gründe oder erhebliche Rechte der Ärztin, des Arztes oder Dritter entgegenstehen. Auf Verlangen sind der Patientin oder dem Patienten Kopien der Unterlagen ~~gegen Erstattung der Kosten~~ herauszugeben."

Die Umsetzung des EUGH-Urteils in der (Muster-)Berufsordnung der Bundesärztekammer wird für den Deutschen Ärztetag 2026 in Hannover erwartet. Diese Information wurde bereits am 8. August dem Hessischen Beauftragten für Datenschutz und Informationsfreiheit mitgeteilt.

Psychotherapeutenkammer Hessen (PTK)

Auch die PTK steht in engem Austausch mit dem Hessischen Beauftragten für Datenschutz und Informationsfreiheit zu diesem Thema. Der letzte Austausch fand im Juli statt, wobei die PTK eine bundeseinheitliche Regelung befürwortet, die durch eine Änderung der Muster-Berufsordnung erreicht werden soll. In ihren Newslettern weist die PTK regelmäßig auf die aktuelle Rechtslage sowie die hierzu ergangene Rechtsprechung hin. Am 4. Juli informierte die PTK den Hessischen Beauftragten für Datenschutz und Informationsfreiheit darüber, dass sie weiterhin öffentlichkeitswirksam auf das Thema aufmerksam machen wird.

Landeszahnärztekammer Hessen (LZKH

Nach Auffassung der LZKH ist die erste Kopie der Patientenakte der Patientin oder dem Patienten kostenlos zur Verfügung zu stellen. Für zusätzliche Kopien darf lediglich ein angemessenes Entgelt verlangt werden. Die LZKH hat hierzu entsprechende Informationsmaterialien für Praxen sowie für Patientinnen und Patienten erstellt. Die Berufsordnung für Zahnärztinnen und Zahnärzte in Hessen wurde bereits durch Beschluss der Delegiertenversammlung der LZKH angepasst. Sobald die neue Berufsordnung offiziell bekanntgegeben wird, wird die aktualisierte Version umgehend auf der Homepage des Ministeriums für Familie, Senioren, Sport, Gesundheit und Pflege veröffentlicht.

Zu 12.2 Krankenhausschließungen in Hessen

Für den Bereich der Krankenhäuser wurde durch die Novellierung des Hessischen Krankenhausgesetzes (HKHG) im Jahr 2022 – wie im Bericht des Hessischen Beauftragten für Datenschutz und Informationsfreiheit angeführt – in § 12 Abs. 5 HKHG eine Regelung getroffen, die den Schutz für Patientendaten im Falle einer Klinikschließung gewährleistet:

„Der Krankenhausträger hat Maßnahmen zu treffen, die sicherstellen, dass im Falle der Schließung eines Krankenhauses, insbesondere aufgrund einer drohenden Zahlungsunfähigkeit, oder einer Betriebsstätte eines Krankenhauses die dort geführten Patientenunterlagen entsprechend ihrer individuellen Aufbewahrungsdauer unter Beachtung der datenschutzrechtlichen Vorgaben, insbesondere zur Gewährleistung von Vertraulichkeit, Integrität und Verfügbarkeit aufbewahrt werden können, und dass Ansprüche der Patientinnen und Patienten auf jederzeitige Durchsetzung ihrer Rechte nach der Verordnung (EU) 2016/679 sowie ihrer Rechte nach dem Bürgerlichen Gesetzbuch nicht beeinträchtigt werden. Maßnahmen im Sinne des Satz 1 sind insbesondere Sicherungsmaßnahmen, die einen Zugang zu, einen Zugriff auf und die Kenntnisnahme von Patientenunterlagen durch unbefugte Personen verhindern sowie die in regelmäßigen Abständen durchgeführte Prüfung, ob Patientenunterlagen vernichtet werden können. Der Krankenhausträger weist die getroffenen Sicherungsmaßnahmen entsprechend der individuellen Aufbewahrungsdauer ab dem 1. Mai 2022 und sodann alle zwei Jahre gegenüber dem für das Krankenhauswesen zuständigen Ministerium nach."

Reha-Kliniken sind jedoch – anders als Krankenhäuser – gesetzlich nicht auf Landesebene verankert, daher hat das Ministerium für Familie, Senioren, Sport, Gesundheit und Pflege weder eine Planungs- noch eine Aufsichtsfunktion über sie. Die rechtliche Beziehung verläuft ausschließlich auf Vertragsebene zwischen der jeweiligen Reha-Klinik und den Krankenkassen als Kostenträgern. Das Ministerium hat sich dennoch mit den Kostenträgern in Verbindung gesetzt. Darüber wurde der Hessische Beauftragte für Datenschutz und Informationsfreiheit in einem Schreiben der Ministerin vom 30. September 2024 informiert.

Grundlage der Zusammenarbeit mit Reha-Kliniken bzw. für die Leistungserbringung von Reha-Leistungen sind im Rahmen des SGB V die Versorgungsverträge nach §§ 111 und 111a SGB V für die stationäre bzw. § 111c SGB V für die ambulante Rehabilitation. Regelungen zum Datenschutz sind dort ebenfalls enthalten. Sofern Kliniken schließen oder ihren Betrieb einstellen, enden diese Versorgungsverträge regelhaft und damit auch die rechtlichen Möglichkeiten der Verbände der Krankenkassen in Hessen als Vertragspartei im Rahmen des Versorgungsvertrags auf die Kliniken einzuwirken.
Die grundsätzlichen Regelungen zum Datenschutz, wie zum Beispiel die Datenschutz-Grundverordnung, sind jedoch immer gültig und von allen Beteiligten zu beachten und umzusetzen.

Zu 12.3 Letztverantwortung für die Aufbewahrung von Patientenakten

Im Rahmen der Evaluierung des Hessischen Gesetzes über das Berufsrecht und die Kammern

der Heilberufe (Heilberufsgesetz) wurde die Anregung des Hessischen Beauftragten für Datenschutz und Informationsfreiheit aufgenommen. Die Letztverantwortung für die Aufbewahrung von Patientenakten, sofern dies nicht durch den dafür zuständigen Kammerangehörigen oder dessen Rechtsnachfolger sichergestellt wird, soll künftig als Teil der Selbstverwaltungsaufgaben der Kammern verankert werden. Der Entwurf befindet sich derzeit in der rechtlichen Prüfung.

Zu 12.4 Cyberangriff auf das Universitätsklinikum Frankfurt am Main

Die Landesregierung stimmt den Ausführungen des Hessischen Beauftragten für Datenschutz und Informationsfreiheit zu.

Die Digitalisierung schreitet im Gesundheitssektor immer weiter voran und eröffnet die Möglichkeit, die Gesundheitsversorgung noch wirksamer und effizienter zu gestalten. Allgemein besteht auch ein hohes Potential in der Digitalisierung des Gesundheitssektors. Aber auch Risiken sind damit verbunden. Die Landesregierung stimmt der Einschätzung des Hessischen Beauftragten für Datenschutz und Informationsfreiheit zu, dass Cyberangriffe auf Einrichtungen des Gesundheitswesens zunehmen und enorme Folgen haben können. Vom Ausfall der Homepage bis hin zur vollständigen Lahmlegung der Gesundheitseinrichtung ist alles möglich. Auch sensible Daten sowohl von Mitarbeiterinnen und Mitarbeitern von Gesundheitseinrichtungen als auch von Patientinnen und Patienten können von einem Angriff betroffen sein. Die Steigerung der Resilienz vor Cyberangriffen im Gesundheitswesen ist daher elementare Grundlage für die Sicherheit aller.
Dieser Gefährdungslage soll u.a. mit dem branchenspezifischen Sicherheitsstandard „Medizinische Versorgung" begegnet werden.

Die Landesregierung teilt die positive Bewertung des Hessischen Beauftragten für Datenschutz und Informationsfreiheit zum Umgang des Universitätsklinikums mit dem Cyberangriff. Im vorliegenden Fall wurde das Ministerium für Familie, Senioren, Sport, Gesundheit und Pflege zeitnah über den Vorfall des Cyberangriffs auf die Uniklinik Frankfurt am Main unterrichtet und wurde auch in der anschließenden Analyse der Klinik über den Prozess der Verbesserung der Datensicherheit informiert.

Zu 12.5 Handvenenscanner in einer Blutspendeeinrichtung

Die Landesregierung stimmt dem Bericht des Hessische Beauftragte für Datenschutz und Informationsfreiheit zu.

Wie im Tätigkeitsbericht zutreffend ausgeführt, ist das Verfahren der Handvenenerkennung

mit dem Prinzip der Fingerabdruckerkennung vergleichbar. Von Mensch zu Mensch kann zwischen einem individuellen Venenmuster und der Position der Venen unterschieden werden. Beides bleibt zeitlebens unverändert und eignet sich daher für ein Identifikationsverfahren.

Die Argumentation des Hessischen Beauftragten für Datenschutz können ist nachvollziehbar. Dem Spender oder der Spenderin muss ein Verfahren für die Feststellung der Identität angeboten werden, mit dem die betroffene Person einverstanden ist. Entsprechend der Richtlinie zur Gewinnung von Blut- und Blutbestandteilen der Bundesärztekammer unter Punkt 2.2.4.1 ist für die Feststellung der Spenderidentität ein gültiges amtliches Personaldokument ausreichend. Dahingehend ist eine Identifizierung per Handvenenerkennung für die Erbringung einer Blut-/Plasmaspende nicht zwingend erforderlich.

Es ist zu vermuten, dass das betroffene Unternehmen das Verfahren der Handvenenerkennung aus Personalgründen bevorzugt hat. Während die Identität über den Venenscan schnell erfasst werden kann, braucht es für eine Identifizierung mittels Lichtbildausweis zusätzliches Personal.

Zu 12.6 Datenerhebungen im Rahmen von Schuleingangsuntersuchungen

Die Landesregierung nimmt den Bericht des Hessischen Beauftragten für Datenschutz und Informationsfreiheit zur Kenntnis.

Die maßgebliche Verordnung über die Zulassung und die Ausgestaltung von Untersuchungen und Maßnahmen der Schulgesundheitspflege wurde vom Minister für Soziales und Integration im Einvernehmen mit dem Kultusminister verordnet.
Die fachliche Zuständigkeit liegt beim Hessischen Ministerium für Familie, Senioren, Sport, Gesundheit und Pflege.

13. Wissenschaft und Forschung

Zu 13.1 Der Begriff der wissenschaftlichen Forschung

Die Landesregierung nimmt den Bericht des Hessischen Beauftragten für Datenschutz und Informationsfreiheit zur Kenntnis.

Zu 13.2 Änderung des Hessischen Landesstatistikgesetzes

Die Landesregierung stimmt den Ausführungen des Hessischen Beauftragten für Datenschutz und Informationsfreiheit zu.

Im Rahmen der Evaluierung des HLStatG wurden sowohl das HSL als auch der Hessische

Beauftragte für Datenschutz und Informationsfreiheit beteiligt. Für das HSL waren insbesondere die Möglichkeit der Einschränkung des Auskunftsrechts und die Schaffung einer Rechtsgrundlage für das „Webscraping" von Bedeutung. Diese Anliegen wurden vom Hessischen Beauftragten für Datenschutz und Informationsfreiheit unterstützt sowie im Fall des Auskunftsrechts entsprechend in der Begründung ergänzt.

14 Technik und Organisation

Zu 14.1 Software und IT-Dienste als Beratungsgegenstand

Die Landesregierung nimmt den Bericht des Hessischen Beauftragten für Datenschutz und Informationsfreiheit zur Kenntnis.

Zu 14.2 Angemessene technische und organisatorische Maßnahmen

Die Landesregierung nimmt den Bericht des Hessischen Beauftragten für Datenschutz und Informationsfreiheit zur Kenntnis.

Zu 14.3 Löschen und Vernichten

Die Landesregierung nimmt den Bericht des Hessischen Beauftragten für Datenschutz und Informationsfreiheit zur Kenntnis.

Zu 14.4 Software-gestützte Schwärzung von PDF-Dateien

Die Landesregierung nimmt den Bericht des Hessischen Beauftragten für Datenschutz und Informationsfreiheit zur Kenntnis.

Zu 14.5 Einsatz neuer Prüftools zur technischen Prüfung von Websites

Die Landesregierung nimmt den Bericht des Hessischen Beauftragten für Datenschutz und Informationsfreiheit zur Kenntnis.

Zu 14.6 Prüfung des Software-Einsatzes bei hessischen Gesundheitsämtern

Die Landesregierung nimmt den Bericht des Hessischen Beauftragten für Datenschutz und Informationsfreiheit zur Kenntnis.

Das Hessische Landesamt für Gesundheit und Pflege ist – entgegen der Darstellung im Tätigkeitsbericht – nicht von dem Projekt „Einheitlichen Software für die hessischen Gesundheitsämter (DigiLGL)" betroffen, da das Landesamt aufgrund der sich von den Gesundheitsämtern unterscheidenden Aufgaben andere Fachanwendungen einsetzt.

Zu 14.7 Datenschutzverletzungen

Die Landesregierung nimmt den Bericht des Hessischen Beauftragten für Datenschutz und Informationsfreiheit zur Kenntnis und unterstreicht seine Ausführungen, wonach oftmals eine Konnexität zwischen Cyberangriffen und Datenschutzverletzungen besteht. Vor diesem Hintergrund hat die Landesregierung Awareness-Formate innerhalb der Landesverwaltungen sowie für Kommunen und KMU zur Meldepflicht gem. Art. 33 DS-GVO durchgeführt.

Zu 14.8 Unangemessene und nicht notwendige Berechtigungen bei Android-Apps

Die Landesregierung stimmt den Ausführungen des Hessischen Beauftragten für Datenschutz und Informationsfreiheit zu.

Ergänzend wird darauf aufmerksam gemacht, dass Berichte nahelegen, dass auch iOS-Apps unangemessene und nicht notwendige Berechtigungen einfordern. Beispielhaft seien Taschenlampen-Apps, die Standortberechtigungen fordern und Spiele, die auf Kontakte zugreifen möchten, genannt. Weiterhin berichtet ein Artikel auf der Plattform heise.de, dass eine im iOS APP Store und Google Play Store angebotene App unter einem fingierten Vorwand Zugriff auf Fotomediatheken erlangte, um unbemerkt Fotos und Screenshots nach Passphrasen für Krypto-Wallets zu scannen und zu exfiltrieren.

Zu 14.9 Fehladressierung von E-Mails aus der Hessischen Landesverwaltung

Die Landesregierung stimmt den Ausführungen des Hessischen Beauftragten für Datenschutz und Informationsfreiheit, wonach Sensibilisierungsmaßnahmen sowie digitale Tools (z.B. digitale Adressbücher) dazu beitragen können, Fälle von Fehladressierung von E-Mails aus der Landesverwaltung zu reduzieren. Ebenso nimmt sie das sog. „Typosquatting" als veritable Sicherheitsbedrohung wahr. In den Awareness-Formaten hat die Landesregierung daher schon jetzt zahlreiche Beschäftigte der Landesverwaltung, von Kommunen und KMU zu den Themen Typosquatting und Fehladressierung sensibilisiert.

15. Öffentlichkeitsarbeit

Zu 15.1 Veranstaltungen

Die Landesregierung nimmt den Bericht des Hessischen Beauftragten für Datenschutz und Informationsfreiheit zur Kenntnis.

Zu 15.2 Schulungen

Die Landesregierung nimmt den Bericht des Hessischen Beauftragten für Datenschutz und Informationsfreiheit zur Kenntnis.

Zu 15.3 Vorträge und Podiumsdiskussionen

Die Landesregierung nimmt den Bericht des Hessischen Beauftragten für Datenschutz und Informationsfreiheit zur Kenntnis.

Zu 15.4 Publikationen

Die Landesregierung nimmt den Bericht des Hessischen Beauftragten für Datenschutz und Informationsfreiheit zur Kenntnis.

Zu 15.5 Elektronische Medien

Die Landesregierung nimmt den Bericht des Hessischen Beauftragten für Datenschutz und Informationsfreiheit zur Kenntnis.

Zu 15.6 Presseanfragen und Pressemitteilungen

Die Landesregierung nimmt den Bericht des Hessischen Beauftragten für Datenschutz und Informationsfreiheit zur Kenntnis.

16. Arbeitsstatistik

Zu 16.1 Zahlen und Fakten

Die Landesregierung nimmt den Bericht des Hessischen Beauftragten für Datenschutz und Informationsfreiheit zur Kenntnis.

Zu 16.2 Ergänzende Angaben

Die Landesregierung nimmt den Bericht des Hessischen Beauftragten für Datenschutz und Informationsfreiheit zur Kenntnis.

Hinweis der Landesregierung betreffend Bericht des Hessischen Beauftragten für Datenschutz und Informationsfreiheit als Aufsichtsbehörde nach § 40 Bundesdatenschutzgesetz

Die Landesregierung nimmt den Bericht des Hessischen Beauftragten für Datenschutz und Informationsfreiheit zum Datenschutz im nichtöffentlichen Bereich – Aufsichtsbehörde nach § 40 Bundesdatenschutzgesetz – zur Kenntnis.

Nach § 15 Abs. 4 HDSIG ist die Landesregierung nicht verpflichtet, zur Tätigkeit des Hessischen Beauftragten für Datenschutz und Informationsfreiheit als Aufsichtsbehörde nach § 40 BDSG Stellung zu nehmen. Bei den entsprechenden Textziffern (7.1, 9.1, 9.2, 10.1, 10.2, 11.1

bis 11.4,) entfällt deshalb die Stellungnahme der Landesregierung.

Unabhängig von dieser gesetzlichen Regelung hat die Landesregierung zu Textziffern des Tätigkeitsberichts dennoch Stellung genommen, wenn darin Sachverhalte mit einem konkreten Bezug zum Datenschutz im öffentlichen Bereich und den Aufgaben der Landesregierung angesprochen wurden.

Zweiter Teil – 7. Tätigkeitsbericht zur Informationsfreiheit

Zu 1. Entwicklung der Informationsfreiheit

Die Landesregierung den Bericht des Hessischen Beauftragten für Datenschutz und Informationsfreiheit zur Kenntnis.

Zu 2. (Kein) Informationszugang zu privatrechtlich organisierten kommunalen Stellen

Die Landesregierung stimmt den Ausführungen des Hessischen Beauftragten für Datenschutz und Informationsfreiheit zu.

Zu 3. Informationsfreiheitsrecht: Jeder ist nicht „Jeder"

Die Landesregierung stimmt den Ausführungen des Hessischen Beauftragten für Datenschutz und Informationsfreiheit zu.

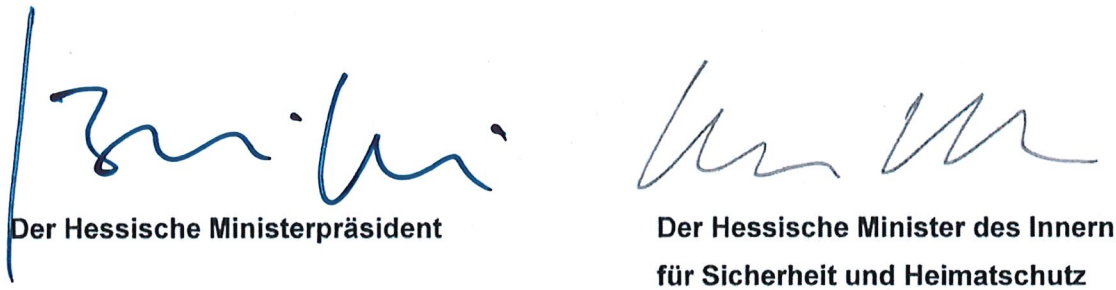
Zu 4. Was sind öffentlich-rechtliche Verwaltungsaufgaben?

Die Landesregierung stimmt den Ausführungen des Hessischen Beauftragten für Datenschutz und Informationsfreiheit zu.

Zu 5. Arbeitsstatistik Informationsfreiheit

Die Landesregierung den Bericht des Hessischen Beauftragten für Datenschutz und Informationsfreiheit zur Kenntnis.

Wiesbaden, den 31. Oktober 2025



Der Hessische Ministerpräsident

Der Hessische Minister des Innern, für Sicherheit und Heimatschutz