



Gesetz- und Verordnungsblatt

für das Land Hessen

2025

Wiesbaden, den 12. Dezember 2025

Nr. 97

Der Landtag hat das folgende Gesetz beschlossen:

**Gesetz
zur Neufassung des Hessischen Verfassungsschutzgesetzes und
zur Änderung weiterer Vorschriften**

Vom 10. Dezember 2025

Artikel 1¹⁾

Hessisches Verfassungsschutzgesetz (HVSG)

INHALTSÜBERSICHT

ERSTER TEIL

Organisation und Aufgaben des Landesamts

- § 1 Organisation des Landesamts
- § 2 Aufgaben des Landesamts
- § 3 Begriffsbestimmungen

ZWEITER TEIL

Befugnisse des Landesamts

- § 4 Informationserhebung
- § 5 Informationserhebung mit nachrichtendienstlichen Mitteln
- § 5a Gerichtliche Kontrolle
- § 6 Überwachung des Brief-, Post- und Fernmeldeverkehrs und der Telekommunikation
- § 7 Verdeckter Einsatz technischer Mittel zur Wohnraumüberwachung
- § 7a Verdeckter Zugriff auf informationstechnische Systeme
- § 8 Verfahren bei Maßnahmen nach den §§ 7 und 7a
- § 9 Ortung von Mobilfunkendgeräten
- § 10 Besondere Auskunftsersuchen
- § 11 Observation
- § 12 Verdeckte Mitarbeiterinnen und Verdeckte Mitarbeiter
- § 13 Vertrauensleute

¹⁾ FFN 18-9

§ 14 Schranken nachrichtendienstlicher Mittel

DRITTER TEIL

Verarbeitung personenbezogener Daten

- § 15 Geltung datenschutzrechtlicher Vorschriften
- § 16 Speicherung, Berichtigung, Löschung und Verarbeitungseinschränkung
- § 17 Zweckbindung
- § 18 Informationsübermittlung durch öffentliche Stellen an das Landesamt
- § 19 Informationsübermittlung durch das Landesamt an übergeordnete Behörden und Aufklärung der Öffentlichkeit
- § 19a Übermittlung personenbezogener Daten durch das Landesamt an andere Stellen
- § 20 Informationsübermittlung durch das Landesamt an Polizeibehörden
- § 20a Informationsübermittlung durch das Landesamt an Strafverfolgungsbehörden
- § 20b Informationsübermittlung durch das Landesamt an sonstige inländische öffentliche Stellen
- § 20c Informationsübermittlung durch das Landesamt an öffentliche Stellen zu arbeits- und dienstrechtlichen Zwecken
- § 21 Informationsübermittlung durch das Landesamt an ausländische öffentliche Stellen
- § 22 Informationsübermittlung durch das Landesamt an Stellen außerhalb des öffentlichen Bereichs
- § 23 Übermittlungsverbote
- § 24 Minderjährigenschutz
- § 25 Nachberichtspflicht
- § 26 Auskunft
- § 27 Dateianordnungen

VIERTER TEIL

Schlussvorschriften

- § 28 Einschränkung von Grundrechten
- § 29 Inkrafttreten

PRÄAMBEL

Der Verfassungsschutz dient dem Schutz der freiheitlichen demokratischen Grundordnung. Er ist Dienstleister der Demokratie und hält insbesondere die analytischen Kompetenzen zur Beurteilung jener Gefahren vor, die Demokratie und Menschenrechte durch extremistische Bestrebungen drohen. Er tauscht sich mit Wissenschaft und Gesellschaft aus. Hierzu gehört auch der öffentliche Diskurs. Er berücksichtigt gesellschaftliche Vielfalt und gesellschaftliche Entwicklungen.

ERSTER TEIL

Organisation und Aufgaben des Landesamts

§ 1

Organisation des Landesamts

(1) Das Landesamt für Verfassungsschutz (Landesamt) untersteht als obere Landesbehörde dem für den Verfassungsschutz zuständigen Ministerium. Es darf mit Polizeidienststellen organisatorisch nicht verbunden werden.

(2) Verfassungsschutzbehörden anderer Länder dürfen in Hessen nur im Einvernehmen, das Bundesamt für Verfassungsschutz nur im Benehmen mit dem Landesamt tätig werden. Das Landesamt darf in anderen Ländern nur tätig werden, soweit die Rechtsvorschriften der anderen Länder dies zulassen.

§ 2

Aufgaben des Landesamts

(1) Das Landesamt ist zuständig für die Zusammenarbeit Hessens mit dem Bund und den anderen Ländern in Angelegenheiten des Verfassungsschutzes. Aufgabe des Landesamts ist es, es den zuständigen Stellen zu ermöglichen, rechtzeitig die erforderlichen Maßnahmen zur Abwehr von Gefahren für die freiheitliche demokratische Grundordnung, den Bestand und die Sicherheit des Bundes und der Länder zu treffen. Das Landesamt hat auch die Aufgabe, den in Abs. 2 genannten Bestrebungen und Tätigkeiten durch Information, Aufklärung und Beratung entgegenzuwirken und vorzubeugen (Prävention).

(2) Aufgabe des Landesamts ist die Sammlung und Auswertung von Informationen, insbesondere von sach- und personenbezogenen Auskünften, Nachrichten und Unterlagen, über

1. Bestrebungen, die gegen die freiheitliche demokratische Grundordnung, den Bestand oder die Sicherheit des Bundes oder eines Landes gerichtet sind oder die eine ungesetzliche Beeinträchtigung der Amtsführung der Verfassungsorgane des Bundes oder eines Landes oder ihrer Mitglieder zum Ziel haben,
2. sicherheitsgefährdende oder geheimdienstliche Tätigkeiten im Geltungsbereich des Grundgesetzes für eine fremde Macht,
3. Bestrebungen im Geltungsbereich des Grundgesetzes, die durch Anwendung von Gewalt oder darauf gerichtete Vorbereitungshandlungen auswärtige Belange der Bundesrepublik Deutschland gefährden,
4. Bestrebungen im Geltungsbereich des Grundgesetzes, die gegen den Gedanken der Völkerverständigung (Art. 9 Abs. 2 des Grundgesetzes), insbesondere gegen das friedliche Zusammenleben der Völker (Art. 26 Abs. 1 des Grundgesetzes), gerichtet sind,
5. Bestrebungen und Tätigkeiten der Organisierten Kriminalität im Geltungsbereich des Grundgesetzes.

(3) Das Landesamt wirkt mit bei Sicherheitsüberprüfungen und Überprüfungen nach § 3 Abs. 2 Satz 1 des Bundesverfassungsschutzgesetzes vom 20. Dezember 1990 (BGBl. I S. 2954, 2970), zuletzt geändert durch Gesetz vom 25. Oktober 2024 (BGBl. 2024 I Nr. 332).

(4) Das Landesamt ist zuständig für Sicherheitsüberprüfungen nach § 2 Abs. 2 Satz 1 Nr. 2 des Artikel 10-Gesetzes vom 26. Juni 2001 (BGBl. I S. 1254, 2998, 2017 I S. 154), zuletzt geändert durch Gesetz vom 22. Dezember 2023 (BGBl. I Nr. 413).

§ 3

Begriffsbestimmungen

(1) Die Begriffsbestimmungen des § 4 Abs. 1 Satz 1 bis 4 sowie Abs. 2 des Bundesverfassungsschutzgesetzes finden Anwendung.

(2) Erheblich beobachtungsbedürftig sind Tätigkeiten nach § 2 Abs. 2 Nr. 2, Bestrebungen, die zur Zielverfolgung Straftaten begehen oder darauf gerichtet sind, sowie solche Bestrebungen, die allgemein, insbesondere nach Verhaltens- oder Wirkungsweise, geeignet sind, die freiheitliche demokratische Grundordnung, den Bestand oder die Sicherheit des Bundes oder eines Landes erheblich zu beeinträchtigen. Dies ist insbesondere der Fall, wenn die Bestrebungen

1. zur Zielverfolgung
 - a) Gewalt anwenden, androhen, fördern oder befürworten oder
 - b) zu Hass oder Willkürmaßnahmen anstacheln,
2. verdeckt vorgehen, insbesondere Ziele, Organisation, Finanzierung, Beteiligte, Zusammenarbeit oder Aktionen in wesentlichem Umfang verschleiern,
3. erhebliche gesellschaftliche Bedeutung besitzen, insbesondere unter Berücksichtigung der Anzahl der Beteiligten, deren Mobilisierungsfähigkeit, der Finanzkraft sowie der Aktionsfähigkeit oder
4. zur Zielverfolgung in erheblichem Umfang gesellschaftlichen Einfluss auszuüben suchen, insbesondere durch
 - a) Vertretung in Ämtern und Mandaten,
 - b) wirkungsbreite Publikationen, Bündnisse, Unterstützerstrukturen,
 - c) systematische Desinformationen in öffentlichen Prozessen politischer Willensbildung oder zur Verächtlichmachung der freiheitlichen demokratischen Grundordnung, auch durch systematische Verunglimpfung ihrer Institutionen und Repräsentanten, oder
 - d) Herbeiführung einer Atmosphäre der Angst oder Bedrohung,

und hinreichend konkrete und gewichtige Anhaltspunkte dafür bestehen, dass das entsprechende Agieren der Bestrebung erfolgreich sein kann.

(3) Voraussetzung für die Einstufung gemäß Abs. 2 ist, dass hinreichende tatsächliche Anhaltspunkte für die Sachverhalte nach Abs. 2 Satz 1 vorliegen. Die Beobachtungsbedürftigkeit ist jährlich zu überprüfen. Die Einstufung der Beobachtungsbedürftigkeit nach Abs. 2 Satz 1 entfällt in der Regel, wenn nach fünf Jahren kein die Einstufung nach Abs. 2 Satz 2 begründender Sachverhalt hinreichend festgestellt ist oder eine fünf Jahre zurückliegende Feststellung sich zwischenzeitlich nicht neuerlich bestätigt hat. Wird im Rahmen der Überprüfung nach Satz 2 festgestellt, dass ein Sachverhalt nach Abs. 2 Satz 1, der einer bereits richterlich angeordneten Maßnahme zugrunde liegt, zwischenzeitlich entfallen ist, so ist die betreffende Maßnahme zu beenden, auch wenn die Frist der richterlichen Anordnung noch nicht abgelaufen ist.

(4) Organisierte Kriminalität im Sinne dieses Gesetzes ist die von Gewinn- oder Machtstreben bestimmte planmäßige Begehung von Straftaten, die einzeln oder in ihrer Gesamtheit von erheblicher Bedeutung für die Rechtsordnung sind, durch mehr als zwei Beteiligte, die auf längere oder unbestimmte Dauer arbeitsteilig tätig werden

1. unter Verwendung gewerblicher oder geschäftsähnlicher Strukturen,

2. unter Anwendung von Gewalt oder durch entsprechende Drohung oder
3. unter Einflussnahme auf Politik, Verwaltung, Justiz, Medien oder Wirtschaft.

ZWEITER TEIL

Befugnisse des Landesamts

§ 4

Informationserhebung

(1) Das Landesamt darf die zur Erfüllung seiner Aufgaben nach § 2 Abs. 1 und 2 erforderlichen Informationen erheben und verarbeiten. Einzelheiten zum Umgang mit den erhobenen Informationen regelt eine von dem für den Verfassungsschutz zuständigen Ministerium zu erlassende Dienstvorschrift.

(2) Das Landesamt darf personenbezogene Daten aus allgemein zugänglichen Quellen erheben und verarbeiten, um zu prüfen, ob tatsächliche Anhaltspunkte für Bestrebungen oder Tätigkeiten nach § 2 Abs. 2 vorliegen.

(3) Liegen bei der betroffenen Person tatsächliche Anhaltspunkte für Bestrebungen oder Tätigkeiten nach § 2 Abs. 2 vor oder wird das Landesamt nach § 2 Abs. 3 oder 4 tätig, darf es Auskünfte bei öffentlichen Stellen oder Dritten einholen, wenn die Daten

1. nicht aus allgemein zugänglichen Quellen,
2. nur mit übermäßigem Aufwand oder
3. nur durch eine die betroffene Person stärker belastende Maßnahme

erhoben werden können. Würde durch die Erhebung von Auskünften nach Satz 1 der Zweck der Maßnahme gefährdet oder die betroffene Person unverhältnismäßig beeinträchtigt, darf das Landesamt Akten und Register öffentlicher Stellen einsehen. Im Übrigen gilt § 18 Abs. 4.

(4) Das Landesamt muss Ersuchen auf Auskunft oder Einsicht nicht begründen, soweit dies dem Schutz der betroffenen Person dient oder eine Begründung den Zweck der Maßnahme gefährden würde. Es hat die Ersuchen aktenkundig zu machen. Über die Einsichtnahme nach Abs. 3 Satz 2 hat das Landesamt einen Nachweis zu führen, aus dem der Zweck, die ersuchte Behörde und die Aktenfundstelle hervorgehen. Der Nachweis ist gesondert aufzubewahren, gegen unberechtigten Zugriff zu sichern und am Ende des Kalenderjahres, das dem Jahr seiner Erstellung folgt, zu vernichten.

(5) Zur Beantwortung von Übermittlungsersuchen nach § 20b Abs. 1 darf das Landesamt personenbezogene Daten nur erheben, soweit dies zur Überprüfung der dem Landesamt bereits vorliegenden Informationen erforderlich ist. Abs. 3 bleibt unberührt.

(6) Werden Daten bei der betroffenen Person oder bei Dritten außerhalb des öffentlichen Bereichs offen erhoben, so sind die Befragten auf die Freiwilligkeit ihrer Angaben hinzuweisen. Gegenüber der betroffenen Person ist der Erhebungszweck anzugeben. Die Befragten sind bei einer Sicherheitsüberprüfung nach § 2 Abs. 3 oder 4 auf eine dienst-, arbeitsrechtliche oder sonstige vertragliche Mitwirkungspflicht hinzuweisen.

(7) Ein Ersuchen des Landesamts um Übermittlung personenbezogener Daten darf nur diejenigen personenbezogenen Daten enthalten, die für die Erteilung der Auskunft unerlässlich sind. Schutzwürdige Interessen der betroffenen Person dürfen nur in unvermeidbarem Umfang beeinträchtigt werden.

(8) Zur Aufgabenerfüllung nach § 2 dürfen personenbezogene Daten von Personen, bei denen keine tatsächlichen Anhaltspunkte dafür vorliegen, dass sie selbst Bestrebungen oder Tätigkeiten im Sinne des § 2 Abs. 2 nachgehen (Unbeteiligte), nur erhoben, verarbeitet oder genutzt werden, wenn

1. dies für die Erforschung von Bestrebungen oder Tätigkeiten nach § 2 Abs. 2 vorübergehend erforderlich ist,
2. die Erforschung des Sachverhalts auf andere Weise aussichtslos oder wesentlich erschwert wäre und
3. überwiegende schutzwürdige Belange der betroffenen Personen nicht entgegenstehen.

Personenbezogene Daten Unbeteiligter dürfen auch erhoben werden, wenn sie mit zur Aufgabenerfüllung erforderlichen Informationen untrennbar verbunden sind.

(9) Daten, die für das Verständnis der zu speichernden Informationen nicht erforderlich sind, sind unverzüglich zu löschen. Dies gilt nicht, wenn die Löschung nicht oder nur mit unvertretbarem Aufwand möglich ist; in diesem Fall dürfen die Daten nicht verwertet werden.

§ 5

Informationserhebung mit nachrichtendienstlichen Mitteln

(1) Das Landesamt darf Informationen mit nachrichtendienstlichen Mitteln erheben. Für personenbezogene Daten gilt dies nur, wenn

1. bei der betroffenen Person tatsächliche Anhaltspunkte für Bestrebungen oder Tätigkeiten nach § 2 Abs. 2 vorliegen und anzunehmen ist, dass auf diese Weise zusätzliche Erkenntnisse erlangt werden können,
2. tatsächliche Anhaltspunkte dafür vorliegen, dass auf diese Weise die zur Erforschung von Bestrebungen und Tätigkeiten nach § 2 Abs. 2 erforderlichen Quellen gewonnen werden können,
3. dies zum Schutz der Mitarbeiterinnen und Mitarbeiter, Einrichtungen, Gegenstände und Informationsquellen des Landesamts gegen sicherheitsgefährdende oder geheimdienstliche Tätigkeiten erforderlich ist oder
4. dies zur Überprüfung der Nachrichtenehrlichkeit und der Eignung von Vertrauensleuten erforderlich ist.

(2) Nachrichtendienstliche Mittel sind Mittel und Methoden, die mittelbar oder unmittelbar dem von der betroffenen oder außenstehenden Person nicht erkennbaren Erheben von Daten dienen. Als nachrichtendienstliche Mittel darf das Landesamt einsetzen:

1. Überwachung des Brief-, Post- und Fernmeldeverkehrs im Sinne des Art. 10 des Grundgesetzes einschließlich notwendiger Begleitmaßnahmen nach § 6,
2. technische Mittel zur Wohnraumüberwachung nach § 7,
3. verdeckter Zugriff auf informationstechnische Systeme nach § 7a,
4. technische Mittel zur Ortung von Mobilfunkendgeräten nach § 9,
5. besondere Auskunftsersuchen nach § 10 zu
 - a) den Umständen des Postverkehrs bei Unternehmen, die geschäftsmäßig Postdienstleistungen erbringen oder daran mitwirken,

b) Telekommunikationsverbindungs- und Teledienstenutzungsdaten bei Unternehmen, die geschäftsmäßig Telekommunikationsdienste und Teledienste erbringen oder daran mitwirken,

c) Daten bei Verkehrsunternehmen, Betreibern von Computerreservierungssystemen und globalen Distributionssystemen sowie bei Kreditinstituten, Finanzdienstleistungsinstituten und Finanzunternehmen,

6. Observation nach § 11,

7. Verdeckte Mitarbeiterinnen, Verdeckte Mitarbeiter und Vertrauensleute nach den §§ 12 und 13,

8. verdeckte Ermittlungen und Befragungen,

9. Ton- und Bildaufzeichnungen außerhalb der Schutzbereiche der Art. 10 und 13 des Grundgesetzes mit und ohne Inanspruchnahme technischer Mittel,

10. Tarnmittel,

11. Funkbeobachtungen,

12. Beobachtung des Internets; dies beinhaltet auch die verdeckte Teilnahme an der im Internet geführten Kommunikation, insbesondere in Foren und elektronischen Kommunikationsplattformen.

(3) Nachrichtendienstliche Mittel dürfen auch angewendet werden, wenn Dritte hierdurch unvermeidbar betroffen werden. Sofern dieses Gesetz keine strengeren Anforderungen vorsieht, dürfen Personen, die nicht selbst an einer Bestrebung oder Tätigkeit gemäß § 2 Abs. 2 beteiligt sind (Unbeteiligte), nur in eine Überwachungsmaßnahme einbezogen werden, wenn die Überwachung gerade dieser Personen zur Aufklärung einer Bestrebung oder Tätigkeit gemäß § 2 Abs. 2 im Einzelfall geboten ist. Eine Überwachung Unbeteiligter ist dabei so zu begrenzen, dass deren Grundrechtsbeeinträchtigungen in angemessenem Verhältnis zu dem im Einzelfall erwartbaren Aufklärungsbeitrag stehen.

(4) Einzelheiten regelt das für den Verfassungsschutz zuständige Ministerium durch Dienstvorschrift, insbesondere die organisatorische Zuständigkeit für die Anordnung von Informationserhebungen mit nachrichtendienstlichen Mitteln. Die Dienstvorschrift ist der Parlamentarischen Kontrollkommission nach § 1 des Verfassungsschutzkontrollgesetzes vom 25. Juni 2018 (GVBl. S. 302, 317), zuletzt geändert durch Gesetz vom 10. Dezember 2025 (GVBl. 2025 Nr. 97), zu übersenden.

(5) Gemeinden, Gemeindeverbände und die sonstigen der Aufsicht des Landes unterstehenden Körperschaften, Anstalten und Stiftungen des öffentlichen Rechts sowie die Gerichte und Staatsanwaltschaften und das Landesamt leisten sich gegenseitig Amts- und Rechtshilfe. Dies gilt insbesondere für die technische Hilfe bei Tarnmaßnahmen. Polizeiliche Befugnisse oder Weisungsbefugnisse stehen dem Landesamt nicht zu. Das Landesamt darf auch nicht im Wege der Amtshilfe Polizeibehörden um Maßnahmen ersuchen, zu denen es selbst nicht befugt ist.

(6) Zur Erfüllung von Aufgaben aufgrund eines Gesetzes nach Art. 73 Abs. 1 Nr. 10 Buchst. b und c des Grundgesetzes stehen dem Landesamt die Befugnisse zu, die es zur Erfüllung der entsprechenden Aufgaben nach diesem Gesetz hat.

§ 5a

Gerichtliche Kontrolle

(1) Wird der Einsatz nachrichtendienstlicher Mittel durch dieses Gesetz unter den Vorbehalt richterlicher Anordnung gestellt, liegt die Zuständigkeit für die richterlichen Entscheidungen beim

Amtsgericht am Sitz des Landesamts; über Beschwerden entscheidet das in § 120 Abs. 4 Satz 2 des Gerichtsverfassungsgesetzes in der Fassung der Bekanntmachung vom 9. Mai 1975 (BGBl. I S. 1077), zuletzt geändert durch Gesetz vom 27. Dezember 2024 (BGBl. 2024 I Nr. 438), bezeichnete Gericht.

(2) Für das Verfahren gelten die Vorschriften des Gesetzes über das Verfahren in Familiensachen und in den Angelegenheiten der freiwilligen Gerichtsbarkeit vom 17. Dezember 2008 (BGBl. I S. 2586, 2587), zuletzt geändert durch Gesetz vom 7. April 2025 (BGBl. 2025 I Nr. 109), entsprechend mit der Maßgabe, dass eine Anhörung oder Unterrichtung der Betroffenen durch das Gericht unterbleibt. Die Rechtsbeschwerde ist ausgeschlossen.

(3) Der Antrag ist hinreichend substantiiert zu begründen; insbesondere sind dem Gericht alle beurteilungsrelevanten Tatsachen mitzuteilen. Im Antrag sind anzugeben:

1. bei gezielt gegen bestimmte Personen gerichteten Maßnahmen die Person, gegen die sich die Maßnahme richtet, soweit möglich, mit Name und Anschrift,
2. bei Maßnahmen nach § 7 Abs. 1 die zu überwachende Wohnung oder die zu überwachten Wohnräume,
3. bei Maßnahmen nach § 7a Abs. 1 die vom Zugriff betroffenen informationstechnischen Systeme,
4. Art, Umfang und Dauer der Maßnahme,
5. der Sachverhalt sowie
6. eine Begründung.

(4) Das Gericht prüft, ob die beantragte Maßnahme den gesetzlichen Voraussetzungen entspricht. Die Anordnung ergeht schriftlich gegenüber der beantragenden Stelle. In der Anordnung sind anzugeben:

1. bei gezielt gegen bestimmte Personen gerichteten Maßnahmen die Person, gegen die sich die Maßnahme richtet, soweit möglich, mit Name und Anschrift,
2. bei Maßnahmen nach § 7 Abs. 1 die zu überwachende Wohnung oder die zu überwachten Wohnräume,
3. Art, Umfang und Dauer der Maßnahme sowie
4. die wesentlichen Gründe.

(5) Bei Maßnahmen gemäß §§ 12 und 13 gelten Abs. 3 und 4 mit der Maßgabe, dass Gegenstand von Antrag und Anordnung der Einsatz der verdeckten Mittel zur Aufklärung einer bestimmten nachrichtendienstlich beobachtungsbedürftigen Bestrebung oder Tätigkeit ist, ohne dabei konkrete Verdeckte Mitarbeiterinnen oder Mitarbeiter oder Vertrauenspersonen zu benennen. Sollen im Rahmen der Maßnahme gemäß § 12 oder § 13 konkrete Einzelpersonen nicht nur punktuell durch die Maßnahme betroffen, sondern dauerhaft Ziel eines personenbezogenen Aufklärungsansatzes sein, so sind sie mit in die gerichtliche Entscheidung aufzunehmen.

(6) Bei Gefahr im Verzug kann die Behördenleitung oder ihre Vertretung die Anordnung treffen; eine richterliche Entscheidung ist unverzüglich nachzuholen.

§ 6

Überwachung des Brief-, Post- und Fernmeldeverkehrs und der Telekommunikation

Die Überwachung des Brief-, Post- und Fernmeldeverkehrs im Sinne des Art. 10 des Grundgesetzes richtet sich nach dem Artikel 10-Gesetz mit den in Satz 2 bis 4 bestimmten Maßgaben und dem Hessischen Ausführungsgesetz zum Artikel 10-Gesetz vom 16. Dezember 1969 (GVBl. I S. 303), zuletzt geändert durch Gesetz vom 12. Dezember 2023 (GVBl. S. 798), in der jeweils geltenden Fassung. Ist eine laufende Kontrolle nach § 4 Abs. 1 Satz 2 des Hessischen Ausführungsgesetzes zum Artikel 10-Gesetz durch die G 10-Kommission noch nicht beendet, ist die Dokumentation nach § 3a Abs. 1 Satz 10 des Artikel 10 Gesetzes bis zum Abschluss der laufenden Kontrolle aufzubewahren. § 4 Abs. 1 Satz 5 des Artikel 10-Gesetzes ist mit der Maßgabe anzuwenden, dass die Protokolldaten sechs Monate nach der Mitteilung oder nach der Feststellung der endgültigen Nichtmitteilung nach § 12 Abs. 1 Satz 1 oder 5 des Artikel 10-Gesetzes zu löschen sind. § 4 Abs. 1 Satz 6 des Artikel 10-Gesetzes ist mit der Maßgabe anzuwenden, dass die Löschung der Daten auch unterbleibt, soweit die Daten für eine Nachprüfung der Rechtmäßigkeit der Beschränkungsmaßnahme nach § 4 Abs. 1 Satz 2 des Hessischen Ausführungsgesetzes zum Artikel 10-Gesetz durch die G 10-Kommission von Bedeutung sein können.

§ 7

Verdeckter Einsatz technischer Mittel zur Wohnraumüberwachung

(1) Das Landesamt darf bei Vorliegen einer dringenden Gefahr für

1. den Bestand oder die Sicherheit des Bundes oder eines Landes,
2. Leib, Leben oder Freiheit einer Person oder
3. solche Güter der Allgemeinheit, deren Bedrohung die Grundlagen oder den Bestand des Bundes oder eines Landes oder die Grundlagen der Existenz der Menschen berührt,

zu deren Abwehr in einer Wohnung verdeckt technische Mittel einsetzen, um das nicht-öffentliche gesprochene Wort abzuhören und aufzuzeichnen sowie Bildaufnahmen und Bildaufzeichnungen herzustellen. Zur Vorbereitung und Durchführung der Maßnahme darf die Wohnung auch ohne Wissen der Inhaberin oder des Inhabers und der Bewohnerin oder des Bewohners betreten werden, wenn dies ausdrücklich angeordnet wurde.

(2) Die Anordnung einer Wohnraumüberwachung ist nur zulässig, wenn die Erforschung des Sachverhalts auf andere Weise aussichtslos oder wesentlich erschwert wäre und geeignete polizeiliche Hilfe für das betroffene Rechtsgut nicht rechtzeitig erlangt werden kann. Die Maßnahme darf sich nur gegen eine Person richten, von der aufgrund tatsächlicher Anhaltspunkte anzunehmen ist, dass sie für die Gefahr verantwortlich ist (Zielperson), und nur in deren Wohnung durchgeführt werden. In der Wohnung einer anderen Person ist die Maßnahme nur zulässig, wenn tatsächliche Anhaltspunkte bestehen, dass sich die Zielperson dort zur Zeit der Maßnahme aufhält, sich dort für die Erforschung des Sachverhalts relevante Informationen ergeben werden und der Zweck der Maßnahme nicht allein unter Beschränkung auf die Wohnung der Zielperson zu erreichen ist.

(3) Werden in Privaträumen Gespräche mit Personen des persönlichen Vertrauens geführt, ist die Anwendung von Mitteln nach Abs. 1 unzulässig. Dies gilt nicht, wenn tatsächliche Anhaltspunkte die Annahme rechtfertigen, dass

1. den Gesprächen insgesamt ein höchstvertraulicher Charakter fehlen wird oder
2. die Gespräche unmittelbar die Besprechung oder Planung von Straftaten, die sich gegen die in Abs. 1 genannten Rechtsgüter richten, zum Gegenstand haben werden.

(4) Die Maßnahme ist im Übrigen unzulässig, soweit tatsächliche Anhaltspunkte dafür vorliegen, dass durch sie allein Erkenntnisse gewonnen werden würden

1. aus dem Kernbereich privater Lebensgestaltung oder
2. bei einer Rechtsanwältin, einem Rechtsanwalt, einem Kammerrechtsbeistand, einer der in § 53 Abs. 1 Satz 1 Nr. 1, 2 oder 4 der Strafprozeßordnung in der Fassung der Bekanntmachung vom 7. April 1987 (BGBl. I S. 1074, 1319), zuletzt geändert durch Gesetz vom 17. Juli 2025 (BGBl. 2025 I Nr. 163), genannten Person oder einer diesen nach § 53a Abs. 1 Satz 1 der Strafprozeßordnung gleichstehenden Person, über die der Berufsgeheimnisträger das Zeugnis verweigern dürfte.

Erfolgen Maßnahmen bei einem der im Übrigen in § 53 Abs. 1 Satz 1 Nr. 3 bis 3b oder 5 der Strafprozeßordnung genannten Berufsgeheimnisträger oder einer diesen nach § 53a Abs. 1 Satz 1 der Strafprozeßordnung gleichstehenden Person, sind das öffentliche Interesse an den von dem Berufsgeheimnisträger wahrgenommenen Aufgaben und das Interesse an der Geheimhaltung der diesem anvertrauten oder bekannt gewordenen Tatsachen besonders zu berücksichtigen. Satz 1 Nr. 2 und Satz 2 gelten nicht bei Maßnahmen zur Aufklärung von eigenen Bestrebungen oder Tätigkeiten der genannten zeugnisverweigerungsberechtigten Personen.

(5) Ergeben sich während der Überwachung tatsächliche Anhaltspunkte im Sinne von Abs. 4 Satz 1, ist die Maßnahme unverzüglich zu unterbrechen, sobald dies ohne Gefährdung von Leib oder Leben eingesetzter Personen möglich ist. Bestehen insoweit Zweifel, darf nur eine automatische Aufzeichnung fortgesetzt werden. Unterbleibt ein Abbruch aufgrund einer Gefährdung nach Satz 1, sind die Tatsache des Eindringens in den Kernbereich privater Lebensgestaltung und die Umstände des Fortsetzens der Maßnahme zu dokumentieren. Sind das Abhören und Beobachten nach Satz 1 unterbrochen worden, so darf die Maßnahme fortgeführt werden, wenn keine Anhaltspunkte nach Abs. 4 Satz 1 vorliegen. Daten, die durch eine Maßnahme nach Abs. 1 erlangt worden sind, sind dem für die Anordnung zuständigen Gericht unverzüglich vorzulegen. Dieses entscheidet unverzüglich über die Verwendbarkeit oder Löschung der Daten. Soweit Erkenntnisse im Sinne von Abs. 4 Satz 1 durch eine Maßnahme nach Abs. 1 erlangt worden sind, dürfen sie nicht verwendet werden und sind unverzüglich zu löschen. Die Tatsachen der Erfassung der Daten und der Löschung sind zu dokumentieren. Die Dokumentation darf ausschließlich für Zwecke der Datenschutzkontrolle verwendet werden. Die Dokumentation ist sechs Monate nach der Mitteilung oder nach Erteilung der gerichtlichen Zustimmung zur Feststellung der endgültigen Nichtmitteilung nach § 8 Abs. 4 zu löschen.

(6) Bei Gefahr im Verzug können die Erkenntnisse, die durch eine Maßnahme nach Abs. 1 erlangt worden sind, unter Aufsicht einer oder eines Bediensteten, die oder der die Befähigung zum Richteramt hat, gesichtet werden. Die oder der Bedienstete entscheidet im Benehmen mit der oder dem Datenschutzbeauftragten des Landesamts über eine vorläufige Verwertung der Erkenntnisse. Die Bediensteten sind zur Verschwiegenheit über die ihnen bekannt gewordenen Erkenntnisse, die nicht verwertet werden dürfen, verpflichtet. Die gerichtliche Entscheidung nach Abs. 5 Satz 5 und 6 ist unverzüglich nachzuholen.

§ 7a

Verdeckter Zugriff auf informationstechnische Systeme

(1) Das Landesamt darf unter den Voraussetzungen des § 7 Abs. 1 Satz 1 und Abs. 2 Satz 1 und 2 erster Halbsatz mit der Maßgabe, dass eine konkretisierte Gefahr für ein dort genanntes Rechtsgut vorliegt, zur Abwehr dieser Gefahr mit technischen Mitteln verdeckt auf informationstechnische Systeme, welche die Zielperson in der berechtigten Erwartung von Vertraulichkeit als eigene nutzt und die ihrer selbstbestimmten Verfügung unterliegen, nur zugreifen, um

1. Zugangsdaten und verarbeitete Daten zu erheben oder
2. zur Vorbereitung einer Maßnahme nach Nr. 1 spezifische Kennungen sowie den Standort eines informationstechnischen Systems zu ermitteln.

Die erhobenen Daten dürfen über den Anlass und Zweck hinaus, zu dem sie erhoben wurden, nur zur Abwehr einer Gefahr im Sinne des Satz 1 oder zur Verfolgung einer Straftat, auf Grund derer eine entsprechende Maßnahme nach § 100b der Strafprozeßordnung angeordnet werden könnte, weiterverarbeitet werden.

(2) Durch technische Maßnahmen ist sicherzustellen, dass

1. an dem informationstechnischen System nur Veränderungen vorgenommen werden, die für die Datenerhebung unerlässlich sind, und
2. die vorgenommenen Veränderungen bei Beendigung der Maßnahme soweit technisch möglich automatisiert rückgängig gemacht werden.

Das eingesetzte Mittel ist nach dem Stand der Technik gegen unbefugte Nutzung zu schützen. Erhobene Daten sind nach dem Stand der Technik gegen Veränderung, unbefugte Löschung und unbefugte Kenntnisnahme zu schützen.

(3) § 7 Abs. 1 Satz 2, Abs. 4, Abs. 5 Satz 5 bis 10 und Abs. 6 findet entsprechende Anwendung. Soweit wie informationstechnisch und ermittlungstechnisch möglich, hat die Erhebung von Erkenntnissen im Sinne des § 7 Abs. 4 Satz 1 zu unterbleiben. Der Zugriff auf informationstechnische Systeme anderer ist zulässig, wenn tatsächliche Anhaltspunkte vorliegen, dass

1. die Zielperson deren informationstechnisches System benutzt oder benutzt hat,
2. sich dadurch für die Abwehr der Gefahr relevante Informationen ergeben werden und
3. ein Zugriff auf das informationstechnische System der Zielperson allein nicht zur Erforschung des Sachverhalts ausreicht.

§ 8

Verfahren bei Maßnahmen nach den §§ 7 und 7a

(1) Der Einsatz technischer Mittel nach den §§ 7 und 7a bedarf einer richterlichen Anordnung. Die Anordnung ist auf höchstens einen Monat zu befristen. Verlängerungen um jeweils nicht mehr als einen weiteren Monat sind zulässig, soweit die Voraussetzungen der Anordnung fortbestehen. Bei der Prüfung der Verhältnismäßigkeit der Verlängerung ist die Gesamtdauer der Maßnahme zu berücksichtigen.

(2) Das Landesamt prüft unverzüglich und sodann in Abständen von höchstens sechs Monaten, ob die erhobenen personenbezogenen Daten für Zwecke nach Abs. 6 erforderlich sind. Soweit dies nicht der Fall ist, sind sie unverzüglich unter Aufsicht einer oder eines Bediensteten, die oder der die Befähigung zum Richteramt hat, zu löschen. Die Löschung ist zu protokollieren. Die Protokolldaten dürfen ausschließlich zur Durchführung der Datenschutzkontrolle verwendet werden. Die Protokolldaten sind sechs Monate nach der Mitteilung oder nach Erteilung der gerichtlichen Zustimmung zur Feststellung der endgültigen Nichtmitteilung nach Abs. 4 zu löschen. Die Löschung der Daten unterbleibt, soweit die Daten für eine Mitteilung nach Abs. 4 oder für eine gerichtliche Überprüfung der Rechtmäßigkeit der Maßnahme von Bedeutung sein können. In diesem Fall sind die Daten in der Verarbeitung einzuschränken; sie dürfen nur zu diesen Zwecken verwendet werden.

(3) Die verbleibenden Daten sind zu kennzeichnen. Die Behördenleitung oder ihre Stellvertretung kann anordnen, dass bei der Übermittlung auf die Kennzeichnung verzichtet wird, wenn dies unerlässlich ist, um die Geheimhaltung einer Maßnahme nicht zu gefährden, und das für die Anordnung zuständige Gericht zugestimmt hat. Bei Gefahr im Verzug kann die Anordnung bereits vor der Zustimmung getroffen werden. Wird die Zustimmung versagt, ist die Kennzeichnung durch den Übermittlungsempfänger unverzüglich nachzuholen; die übermittelnde Behörde hat ihn hiervon zu unterrichten. Nach einer Übermittlung ist die Kennzeichnung durch den Empfänger aufrechtzuerhalten.

(4) Eine Maßnahme nach § 7 oder § 7a ist der betroffenen Person nach ihrer Einstellung mitzuteilen. Die Mitteilung unterbleibt, solange eine Gefährdung des Zwecks der Beschränkung nicht ausgeschlossen werden kann oder solange der Eintritt übergreifender Nachteile für das Wohl des Bundes oder eines Landes absehbar ist. Erfolgt die nach Satz 2 zurückgestellte Mitteilung nicht binnen zwölf Monaten nach Beendigung der Maßnahme, bedarf die weitere Zurückstellung der Zustimmung des für die Anordnung zuständigen Gerichts. Das Gericht bestimmt die Dauer der weiteren Zurückstellung. Einer Mitteilung bedarf es nicht, wenn das Gericht festgestellt hat, dass

1. eine der Voraussetzungen in Satz 2 auch nach fünf Jahren nach Beendigung der Maßnahme noch vorliegt,
2. sie mit an Sicherheit grenzender Wahrscheinlichkeit auch in Zukunft vorliegt und
3. die Voraussetzungen für eine Löschung sowohl beim Landesamt als auch beim Empfänger vorliegen.

Eine Mitteilung kann auch auf Dauer unterbleiben, wenn überwiegende Interessen einer betroffenen Person entgegenstehen oder wenn die Identität oder der Aufenthaltsort einer betroffenen Person nur mit unverhältnismäßigem Aufwand zu ermitteln ist. Die Mitteilung obliegt dem Landesamt. Wurden personenbezogene Daten übermittelt, erfolgt die Mitteilung im Benehmen mit dem Empfänger.

(5) Die aus der Anordnung sich ergebenden Maßnahmen sind unter Verantwortung des Landesamts und unter Aufsicht einer oder eines Bediensteten vorzunehmen, die oder der die Befähigung zum Richteramt hat. Die Maßnahmen sind unverzüglich zu beenden, wenn sie nicht mehr erforderlich sind oder die Voraussetzungen der Anordnung nicht mehr vorliegen. Die Beendigung ist dem für die Anordnung zuständigen Gericht anzugeben.

(6) Personenbezogene Daten, die durch eine Maßnahme der optischen Wohnraumüberwachung erlangt wurden, dürfen nur weiterverarbeitet und an andere Stellen übermittelt werden, soweit dies zur Abwehr einer dringenden Gefahr im Sinne des § 7 Abs. 1 erforderlich ist. Personenbezogene Daten aus einer Maßnahme der akustischen Wohnraumüberwachung dürfen darüber hinaus zur Strafverfolgung übermittelt werden, wenn bestimmte Tatsachen den Verdacht begründen, dass jemand eine besonders schwere Straftat im Sinne der § 100c Abs. 1, § 100b Abs. 2 der Strafprozeßordnung begangen hat.

(7) Dient der Einsatz technischer Mittel nach § 7 ausschließlich dem Schutz der für den Verfassungsschutz bei einem Einsatz in Wohnungen tätigen Personen, erfolgt die Anordnung abweichend von Abs. 1 durch die Behördenleitung oder ihre Vertretung. Eine anderweitige Verwendung der hierbei erlangten Erkenntnisse ist nur zulässig, wenn zuvor richterlich festgestellt wurde, dass die Maßnahme rechtmäßig ist und die Voraussetzungen des § 7 Abs. 1 vorliegen; Abs. 1 Satz 3 gilt entsprechend. Im Übrigen sind die Daten unverzüglich zu löschen.

(8) Dient der Zugriff auf ein informationstechnisches System nach § 7a ausschließlich der Aufklärung eines gegenwärtigen elektronischen Angriffs, bei dem hinreichende tatsächliche Anhaltspunkte dafür bestehen, dass er durch, im Auftrag oder zur Unterstützung einer fremden Macht durchgeführt wird, bedarf es abweichend von § 7 Abs. 5 Satz 5 und 6 keiner richterlichen Entscheidung über die Verwendbarkeit, sofern die Weiterverarbeitung der Daten darauf beschränkt bleibt,

1. Informationen über den Einsatz von Schadprogrammen oder andere Angriffsmethoden zu sammeln und auszuwerten oder
2. Ziele des Angriffs zu informieren.

Eine anderweitige Verwendung der erhobenen Daten ist nur nach richterlicher Entscheidung zulässig. Liegen die Voraussetzungen nach Satz 1 oder 2 nicht vor, sind die erhobenen Daten unverzüglich ohne inhaltliche Kenntnisnahme unter Aufsicht einer Bediensteten oder eines

Bediensteten, die oder der die Befähigung zum Richteramt hat, zu löschen; § 4 Abs. 1 Satz 3 bis 7 des Artikel 10-Gesetzes ist entsprechend anzuwenden.

§ 9

Ortung von Mobilfunkendgeräten

(1) Das Landesamt darf im Einzelfall, soweit dies aufgrund tatsächlicher Anhaltspunkte zur Erfüllung seiner Aufgaben nach § 2 erforderlich ist, technische Mittel einsetzen

1. zur Ermittlung der Geräte- oder Kartennummer und
2. zur Ermittlung des Standorts eines aktiv geschalteten Mobilfunkendgeräts.

(2) Werden technische Mittel nach Abs. 1 Nr. 2 wiederholt über einen längeren Zeitraum oder in so enger zeitlicher Taktung eingesetzt, dass die dadurch ermöglichte Nachverfolgung der Bewegung des Mobilfunkendgeräts im Raum potentiell Rückschlüsse auf Verhaltensweisen, Routinen, persönliche Neigungen oder Vorlieben der betroffenen Person zulässt, so ist dies nur zulässig, soweit es zur Aufklärung einer erheblich beobachtungsbedürftigen Bestrebung oder Tätigkeit nach § 3 Abs. 2 im Einzelfall geboten ist.

(3) § 3 Abs. 2 Satz 1 und 2 und die §§ 9 und 10 Abs. 2 und 3 des Artikel 10-Gesetzes gelten entsprechend. Maßnahmen nach Abs. 2 bedürfen einer richterlichen Anordnung. Die Anordnung ist auf höchstens sechs Monate zu befristen. Verlängerungen um jeweils nicht mehr als sechs weitere Monate sind zulässig, soweit die Voraussetzungen der Anordnung fortbestehen. Bei der Prüfung der Verhältnismäßigkeit der Verlängerung ist die Gesamtdauer der Maßnahme zu berücksichtigen.

§ 10

Besondere Auskunftsersuchen

(1) Das Landesamt darf im Einzelfall, soweit dies aufgrund tatsächlicher Anhaltspunkte zur Erfüllung seiner Aufgaben nach § 2 erforderlich ist, bei denjenigen, die geschäftsmäßig Postdienstleistungen erbringen oder Telemedien anbieten oder daran mitwirken, Auskünfte über Daten, die für die Begründung, inhaltliche Ausgestaltung, Änderung oder Beendigung eines Vertragsverhältnisses über Postdienstleistungen oder Telemedien gespeichert worden sind, einholen.

(2) Das Landesamt darf, sofern tatsächliche Anhaltspunkte dafür vorliegen, dass dies im Einzelfall zur Aufklärung von Bestrebungen oder Tätigkeiten nach § 2 Abs. 2 geboten ist, bei

1. Verkehrsunternehmen sowie Betreibern von Computerreservierungssystemen und Globalen Distributionssystemen für Flüge zu Namen und Anschriften von Kunden sowie zu Inanspruchnahme und Umständen von Transportleistungen, insbesondere zum Zeitpunkt von Abfertigung und Abflug und zum Buchungsweg,
2. Kreditinstituten, Finanzdienstleistungsinstituten und Finanzunternehmen zu Konten, Konteninhabern und sonstigen Berechtigten sowie weiteren am Zahlungsverkehr Beteiligten und über Geldbewegungen und Geldanlagen, insbesondere über Kontostand und Zahlungsein- und -ausgänge,

Auskünfte einholen. Im Fall von Bestrebungen nach § 2 Abs. 2 Nr. 1, 3, 4 oder 5 gilt dies nur, wenn diese allgemein, insbesondere nach Verhaltens- oder Wirkungsweise, geeignet sind, die freiheitliche demokratische Grundordnung, den Bestand oder die Sicherheit des Bundes oder eines Landes nicht nur unerheblich zu beeinträchtigen. In jedem Fall müssen hinreichende Anhaltspunkte vorliegen, die es zumindest möglich erscheinen lassen, dass in § 20 genannte Rechtsgüter konkret bedroht sind und das gegen sie gerichtete Handeln erfolgreich sein kann. Für die Zwecke von Ersuchen nach Satz 1 Nr. 2 darf das Landesamt das Bundeszentralamt für Steuern ersuchen, bei den Kreditinstituten die in § 93b Abs. 1 der Abgabenordnung in der

Fassung der Bekanntmachung vom 23. Januar 2025 (BGBl. 2025 I Nr. 24) bezeichneten Daten abzurufen, wenn dies zur Aufklärung von Bestrebungen und Tätigkeiten nach § 2 Abs. 2 im Einzelfall geboten ist.

(3) Das Landesamt darf im Einzelfall, soweit dies aufgrund tatsächlicher Anhaltspunkte zur Aufklärung von Bestrebungen oder Tätigkeiten nach § 2 Abs. 2 erforderlich ist, von denjenigen, die geschäftsmäßig Telekommunikationsdienste erbringen oder daran mitwirken, Auskünfte über die nach den § 3 Nr. 6 und § 172 des Telekommunikationsgesetzes vom 23. Juni 2021 (BGBl. I S. 1858), zuletzt geändert durch Gesetz vom 24. Juli 2025 (BGBl. 2025 I Nr. 181), erhobenen Daten verlangen (§ 174 Abs. 1 Satz 1 des Telekommunikationsgesetzes). Dies gilt auch für Daten, mittels derer der Zugriff auf Endgeräte oder auf Speichereinrichtungen, die in diesen Endgeräten oder hiervon räumlich getrennt eingesetzt werden, geschützt wird (§ 174 Abs. 1 Satz 2 des Telekommunikationsgesetzes). Die Auskunft darf auch anhand einer zu einem bestimmten Zeitpunkt zugewiesenen Internetprotokoll-Adresse verlangt werden (§ 174 Abs. 1 Satz 3 des Telekommunikationsgesetzes); diese Rechtsgrundlage und die tatsächlichen Anhaltspunkte, die dieses Auskunftsverlangen veranlassen, sind aktenkundig zu machen. Die Auskunft darf nur verlangt werden, wenn die gesetzlichen Voraussetzungen für das Nutzen der Daten vorliegen.

(4) Das Landesamt darf im Einzelfall zur Erfüllung seiner Aufgaben nach § 2 unter den Voraussetzungen des § 3 Abs. 1 des Artikel 10-Gesetzes bei Personen und Unternehmen, die geschäftsmäßig

1. Postdienstleistungen erbringen oder daran mitwirken, Auskünfte zu den sonstigen Umständen des Postverkehrs,
2. Telekommunikationsdienste erbringen oder daran mitwirken, Auskünfte zu Verkehrsdaten nach § 9 Abs. 1 Satz 1 Nr. 1 bis 5 des Telekommunikation-Digitale-Dienste-Datenschutz-Gesetz vom 23. Juni 2021 (BGBl. I S. 1982, 2022 I S. 1045), zuletzt geändert durch Gesetz vom 12. Juli 2024 (BGBl. 2024 I Nr. 234),
3. Telemedien anbieten oder daran mitwirken, Auskünfte über
 - a) Merkmale zur Identifikation des Nutzers von Telemedien,
 - b) Beginn und Ende sowie über den Umfang der jeweiligen Nutzung und
 - c) die vom Nutzer in Anspruch genommenen Telemedien

einholen.

(5) Auskünfte nach Abs. 3, soweit Daten nach § 174 Abs. 1 Satz 2 und 3 des Telekommunikationsgesetzes betroffen sind, und Auskünfte nach Abs. 4 dürfen nur auf Anordnung des für den Verfassungsschutz zuständigen Ministeriums eingeholt werden. Die Anordnung ist durch die Behördenleitung schriftlich zu beantragen. Der Antrag ist zu begründen. Das Ministerium unterrichtet unverzüglich die G 10-Kommission nach § 2 Abs. 1 des Hessischen Ausführungsgesetzes zum Artikel 10-Gesetz über die Anordnung vor deren Vollzug und holt deren Zustimmung ein. Bei Gefahr im Verzug kann das Ministerium den Vollzug der Anordnung auch bereits vor Unterrichtung der G 10-Kommission anordnen. Die G 10-Kommission prüft von Amts wegen oder aufgrund von Beschwerden die Zulässigkeit und Notwendigkeit der Einholung von Auskünften. § 15 Abs. 5 des Artikel 10-Gesetzes ist entsprechend anzuwenden. Anordnungen, welche die G 10-Kommission für unzulässig erklärt, hat das Ministerium unverzüglich aufzuheben. § 12 Abs. 1 und 3 des Artikel 10-Gesetzes findet entsprechende Anwendung.

(6) Bei Maßnahmen nach Abs. 2 und 4 ist § 4 des Artikel 10-Gesetzes, für Maßnahmen nach Abs. 2 mit Ausnahme des § 4 Abs. 2 Satz 3 und 4 des Artikel 10-Gesetzes, mit der Maßgabe nach § 6 Satz 3 und 4 dieses Gesetzes anzuwenden, die §§ 9, 10 Abs. 2 und 3, § 11 Abs. 1 und 2, § 12 Abs. 1 und 3, § 17 Abs. 3 des Artikel 10-Gesetzes sowie § 2 des Hessischen Ausführungsgesetzes zum Artikel 10-Gesetz sind entsprechend anzuwenden. Abweichend von § 10 Abs. 3 des Artikel 10-Gesetzes genügt eine räumlich und zeitlich hinreichende Bezeichnung der

Telekommunikation, sofern anderenfalls die Erreichung des Zwecks der Maßnahme aussichtslos oder wesentlich erschwert wäre. Soweit dem Verpflichteten keine Entschädigung nach besonderen Bestimmungen zusteht, findet § 20 des Artikel 10-Gesetzes entsprechende Anwendung. Im Übrigen hat der Verpflichtete die Auskunft unentgeltlich zu erteilen.

(7) Die zur Erteilung der Auskunft erforderlichen Daten müssen unverzüglich, vollständig und richtig übermittelt werden. Das Auskunftsersuchen und die übermittelten Daten dürfen der betroffenen Person oder Dritten vom Verpflichteten nicht mitgeteilt werden.

(8) Auf Auskünfte nach Abs. 4 Nr. 2 sind die Vorgaben des § 8b Abs. 8 Satz 4 und 5 des Bundesverfassungsschutzgesetzes anzuwenden. Für die Erteilung von Auskünften nach Abs. 1, 2 und 4 Nr. 3 gilt die Nachrichtendienste-Übermittlungsverordnung vom 11. Oktober 2012 (BGBl. I S. 2117), zuletzt geändert durch Gesetz vom 12. Mai 2021 (BGBl. I S. 990).

(9) Dem Verpflichteten ist es verboten, allein aufgrund eines Auskunftsersuchens einseitige Handlungen vorzunehmen, die für die betroffene Person nachteilig sind und die über die Erteilung der Auskunft hinausgehen, insbesondere bestehende Verträge oder Geschäftsverbindungen zu beenden, ihren Umfang zu beschränken oder ein Entgelt zu erheben oder zu erhöhen. Die Anordnung ist mit dem ausdrücklichen Hinweis auf dieses Verbot und darauf zu verbinden, dass das Auskunftsersuchen nicht die Aussage beinhaltet, dass sich die betroffene Person rechtswidrig verhalten hat oder ein darauf gerichteter Verdacht bestehen müsse.

(10) Auskunft nach Abs. 1 bis 4 darf bei Unternehmen eingeholt werden, die in Deutschland

1. eine Niederlassung haben oder
2. Leistungen erbringen oder hieran mitwirken.

§ 11

Observation

(1) Das Landesamt darf außerhalb der Schutzbereiche der Art. 10 und 13 des Grundgesetzes Personen verdeckt mit oder ohne Inanspruchnahme technischer Mittel planmäßig observieren, insbesondere das nichtöffentlich gesprochene Wort mithören, abhören und aufzeichnen sowie Bildaufnahmen und Bildaufzeichnungen anfertigen, sofern dies aufgrund tatsächlicher Anhaltspunkte zur Aufklärung von Bestrebungen oder Tätigkeiten nach § 2 Abs. 2 im Einzelfall geboten ist.

(2) Die Maßnahme ist im Einzelfall länger als 48 Stunden oder an mehr als drei Tagen innerhalb einer Woche (langfristige Observation) nur zulässig, wenn dies zur Aufklärung einer erheblich beobachtungsbedürftigen Bestrebung oder Tätigkeit nach § 3 Abs. 2 im Einzelfall geboten ist.

(3) Eine Maßnahme nach Abs. 2 darf sich gezielt nur gegen eine Person richten, von der auf Grund tatsächlicher Anhaltspunkte anzunehmen ist, dass sie entweder

1. an der Bestrebung oder Tätigkeit beteiligt ist oder
2. mit einer Person nach Nr. 1 in Kontakt steht und
 - a) von der Bestrebung oder Tätigkeit Kenntnis hat oder
 - b) die Person nach Nr. 1 sich ihrer zur Förderung der Bestrebung oder Tätigkeit bedient

und eine Maßnahme gegen die Person nach Nr. 1 allein nicht zur Erforschung des Sachverhalts ausreicht.

(4) Maßnahmen der langfristigen Observation nach Abs. 2 bedürfen einer richterlichen Anordnung. Die Anordnung ist auf höchstens drei Monate zu befristen. Verlängerungen um jeweils nicht mehr als drei weitere Monate sind zulässig, soweit die Voraussetzungen der Anordnung fortbestehen. Bei der Prüfung der Verhältnismäßigkeit der Verlängerung ist die Gesamtdauer der Maßnahme zu berücksichtigen.

(5) Die Maßnahme ist unzulässig, soweit tatsächliche Anhaltspunkte dafür vorliegen, dass durch sie allein Erkenntnisse gewonnen werden würden

1. aus dem Kernbereich privater Lebensgestaltung oder
2. bei einer Rechtsanwältin, einem Rechtsanwalt, einem Kammerrechtsbeistand, einer der in § 53 Abs. 1 Satz 1 Nr. 1, 2 oder 4 der Strafprozeßordnung genannten Person oder einer diesen nach § 53a Abs. 1 Satz 1 der Strafprozeßordnung gleichstehenden Person, über die der Berufsgeheimnisträger das Zeugnis verweigern dürfte.

Erfolgen Maßnahmen bei einem der im Übrigen in § 53 Abs. 1 Satz 1 Nr. 3 bis 3b oder 5 der Strafprozeßordnung genannten Berufsgeheimnisträger oder einer diesen nach § 53a Abs. 1 Satz 1 der Strafprozeßordnung gleichstehenden Person, sind das öffentliche Interesse an den von dem Berufsgeheimnisträger wahrgenommenen Aufgaben und das Interesse an der Geheimhaltung der diesem anvertrauten oder bekannt gewordenen Tatsachen besonders zu berücksichtigen. Satz 1 Nr. 2 und Satz 2 gelten nicht bei Maßnahmen zur Aufklärung von eigenen Bestrebungen oder Tätigkeiten der genannten zeugnisverweigerungsberechtigten Personen.

(6) Erfolgt während der Maßnahme eine unmittelbare Kenntnisnahme und ergeben sich tatsächliche Anhaltspunkte im Sinne von Abs. 5 Satz 1, ist die Maßnahme unverzüglich zu unterbrechen, sobald dies ohne Gefährdung von Leib oder Leben eingesetzter Personen möglich ist. Unterbleibt ein Abbruch aufgrund einer Gefährdung nach Satz 1, sind die Tatsache des Eindringens in den Kernbereich privater Lebensgestaltung und die Umstände des Fortsetzens der Maßnahme zu dokumentieren. Vor der Weitergabe von Informationen hat die eingesetzte Mitarbeiterin oder der eingesetzte Mitarbeiter zu prüfen, ob durch die Informationen oder die Art und Weise, in der sie erlangt wurden, Erkenntnisse im Sinne von Abs. 5 Satz 1 berührt sind. Entsprechende Erkenntnisse dürfen nicht zur Verwertung weitergegeben werden. Sind das Abhören und Beobachten nach Satz 1 unterbrochen worden, so darf die Maßnahme fortgeführt werden, wenn keine Anhaltspunkte nach Abs. 5 Satz 1 vorliegen. Soweit Erkenntnisse im Sinne von Abs. 5 Satz 1 durch die Maßnahme erlangt worden sind, dürfen sie nicht verwendet werden und sind unverzüglich zu löschen. Die Tatsachen der Erfassung der Daten und der Löschung sind zu dokumentieren. Die Dokumentation darf ausschließlich für Zwecke der Datenschutzkontrolle verwendet werden. Die Dokumentation ist sechs Monate nach der Mitteilung oder nach Zustimmung der Behördenleitung zur endgültigen Nichtmitteilung nach Abs. 8 zu löschen.

(7) Bestehen Zweifel, ob oder wie lange die Voraussetzungen nach Abs. 6 Satz 1 vorliegen, darf die Maßnahme ausschließlich als automatische Aufzeichnung fortgeführt werden. Diese ist unverzüglich dem für die Anordnung zuständigen Gericht vorzulegen. Dieses entscheidet unverzüglich über die Verwendbarkeit oder Löschung der Daten. Bei Gefahr im Verzug können Aufzeichnungen nach Satz 1 unter Aufsicht einer oder eines Bediensteten, die oder der die Befähigung zum Richteramt hat, gesichtet werden. Die oder der Bedienstete entscheidet im Benehmen mit der oder dem Datenschutzbeauftragten des Landesamts vorläufig über eine Verwendung der Erkenntnisse. Die Bediensteten sind zur Verschwiegenheit über die ihnen bekannt gewordenen Erkenntnisse, die nicht verwendet werden dürfen, verpflichtet. Die gerichtliche Entscheidung nach Satz 2 und 3 ist unverzüglich nachzuholen.

(8) Dauert eine langfristige Observation nach Abs. 2 durchgehend länger als eine Woche oder findet sie an mehr als 14 Tagen innerhalb eines Monats statt, ist die Maßnahme der betroffenen Person nach ihrer Einstellung mitzuteilen. Die Mitteilung unterbleibt, solange eine Gefährdung des Zwecks der Beschränkung nicht ausgeschlossen werden kann oder solange der Eintritt übergreifender Nachteile für das Wohl des Bundes oder eines Landes absehbar ist. Erfolgt die nach Satz 2 zurückgestellte Mitteilung nicht binnen zwölf Monaten nach Beendigung der Maßnahme,

bedarf die weitere Zurückstellung der Zustimmung der Behördenleitung. Die Behördenleitung bestimmt die Dauer der weiteren Zurückstellung. Einer Mitteilung bedarf es nicht, wenn

1. eine der Voraussetzungen in Satz 2 auch nach fünf Jahren nach Beendigung der Maßnahme noch vorliegt,
2. sie mit an Sicherheit grenzender Wahrscheinlichkeit auch in Zukunft vorliegt und
3. die Voraussetzungen für eine Löschung vorliegen.

Eine Mitteilung kann auch auf Dauer unterbleiben, wenn überwiegende Interessen einer betroffenen Person entgegenstehen oder wenn die Identität oder der Aufenthaltsort einer betroffenen Person nur mit unverhältnismäßigem Aufwand zu ermitteln ist. Die Mitteilung obliegt dem Landesamt.

§ 12

Verdeckte Mitarbeiterinnen und Verdeckte Mitarbeiter

(1) Das Landesamt darf eigene Mitarbeiterinnen und Mitarbeiter unter einer ihnen verliehenen und auf Dauer angelegten Legende (Verdeckte Mitarbeiterinnen und Verdeckte Mitarbeiter) einsetzen, wenn dies aufgrund tatsächlicher Anhaltspunkte zur Aufklärung einer erheblich beobachtungsbedürftigen Bestrebung oder Tätigkeit nach § 3 Abs. 2 unerlässlich ist.

(2) Eine Maßnahme nach Abs. 1 darf sich gezielt nur gegen eine Person richten, von der auf Grund tatsächlicher Anhaltspunkte anzunehmen ist, dass sie entweder

1. an der Bestrebung oder Tätigkeit beteiligt ist oder
2. mit einer Person nach Nr. 1 in Kontakt steht und
 - a) von der Bestrebung oder Tätigkeit Kenntnis hat oder
 - b) die Person nach Nr. 1 sich ihrer zur Förderung der Bestrebung oder Tätigkeit bedient

und eine Maßnahme gegen die Person nach Nr. 1 allein nicht zur Erforschung des Sachverhalts ausreicht.

(3) Maßnahmen nach Abs. 1 bedürfen einer richterlichen Anordnung. Die Anordnung ist auf höchstens zwölf Monate zu befristen. Verlängerungen um jeweils nicht mehr als zwölf weitere Monate sind zulässig, soweit die Voraussetzungen der Anordnung fortbestehen. Bei der Prüfung der Verhältnismäßigkeit der Verlängerung ist die Gesamtdauer der Maßnahme zu berücksichtigen.

(4) Bei der Planung von Einsatzumständen sollen nach Möglichkeit Situationen vermieden werden, bei denen regelmäßig Erkenntnisse gewonnen werden würden

1. aus dem Kernbereich privater Lebensgestaltung oder
2. bei einer Rechtsanwältin, einem Rechtsanwalt, einem Kammerrechtsbeistand, einer der in § 53 Abs. 1 Satz 1 Nr. 1, 2 oder 4 der Strafprozeßordnung genannten Person oder einer diesen nach § 53a Abs. 1 Satz 1 der Strafprozeßordnung gleichstehenden Person, über die der Berufsgeheimnisträger das Zeugnis verweigern dürfte.

Bei einem gegen eine Person gerichteten Einsatz darf unter keinen Umständen der Kernbereich zum Ziel staatlicher Ermittlungen gemacht werden. Insbesondere dürfen zum Aufbau oder zum Erhalt eines Vertrauensverhältnisses keine intimen Beziehungen oder vergleichbar engste persönliche Bindungen begründet oder fortgeführt werden. Entstehen solche Bindungen, ist der Einsatz gegen diese Person abzubrechen.

(5) Erfolgt während der Maßnahme eine unmittelbare Kenntnisnahme und ergeben sich tatsächliche Anhaltspunkte im Sinne von Abs. 4 Satz 1, ist die Maßnahme unverzüglich zu unterbrechen, sobald dies ohne Gefährdung von Leib oder Leben oder Enttarnung eingesetzter Personen möglich ist. Unterbleibt ein Abbruch aufgrund einer Gefährdung nach Satz 1, sind die Tatsache des Eindringens in den Kernbereich privater Lebensgestaltung und die Umstände des Fortsetzens der Maßnahme zu dokumentieren. Die Maßnahme darf fortgeführt werden, wenn keine Anhaltspunkte nach Abs. 4 Satz 1 mehr vorliegen. Soweit Erkenntnisse im Sinne von Abs. 4 Satz 1 durch eine Maßnahme erlangt worden sind, dürfen sie nicht verwendet werden und sind unverzüglich zu löschen. Die Tatsachen der Erfassung der Daten und der Löschung sind zu dokumentieren. Die Dokumentation darf ausschließlich für Zwecke der Datenschutzkontrolle verwendet werden. Die Dokumentation ist am Ende des Kalenderjahres, das der Protokollierung folgt, zu löschen.

(6) Vor der Weitergabe von Informationen hat die Verdeckte Mitarbeiterin oder der Verdeckte Mitarbeiter zu prüfen, ob durch die Informationen oder die Art und Weise, in der sie erlangt wurden, Erkenntnisse im Sinne von Abs. 4 Satz 1 berührt sind. Entsprechende Erkenntnisse dürfen nicht zur Verwertung weitergegeben werden.

(7) Bestehen Zweifel, ob bei einer Maßnahme Erkenntnisse im Sinne von Abs. 4 Satz 1 gewonnen worden sind, entscheidet der behördliche Datenschutzbeauftragte. Dieser entscheidet unverzüglich über die Verwendbarkeit und Löschung der Daten.

(8) Verdeckte Mitarbeiterinnen und Verdeckte Mitarbeiter dürfen weder zur Gründung von Bestrebungen nach § 2 Abs. 2 noch zur steuernden Einflussnahme auf derartige Bestrebungen eingesetzt werden. Sie dürfen in Personenzusammenschlüssen oder für diese tätig werden, auch wenn dadurch ein Straftatbestand verwirklicht wird. Im Übrigen dürfen Verdeckte Mitarbeiterinnen und Verdeckte Mitarbeiter im Einsatz bei der Beteiligung an Bestrebungen solche Handlungen vornehmen, die

1. nicht in Individualrechte eingreifen,
2. von den an den Bestrebungen Beteiligten derart erwartet werden, dass sie zur Gewinnung und Sicherung der Informationszugänge unumgänglich sind, und
3. nicht außer Verhältnis zur Bedeutung des aufzuklärenden Sachverhalts stehen.

Sofern zureichende tatsächliche Anhaltspunkte dafür bestehen, dass eine Verdeckte Mitarbeiterin oder ein Verdeckter Mitarbeiter rechtswidrig einen Straftatbestand von erheblicher Bedeutung verwirklicht hat, wird ihr oder sein Einsatz unverzüglich beendet und die Strafverfolgungsbehörde unterrichtet. Über Ausnahmen von Satz 4 entscheidet die Behördenleitung oder ihre Vertretung.

(9) Bei Einsätzen zur Erfüllung der Aufgabe nach § 2 Abs. 2 Nr. 5 gilt § 9a Abs. 3 des Bundesverfassungsschutzgesetzes entsprechend.

(10) Für Mitarbeiterinnen und Mitarbeiter, die verdeckt Informationen in sozialen Netzwerken und sonstigen Kommunikationsplattformen im Internet erheben, gelten Abs. 8 und 9 sowie § 9a Abs. 3 des Bundesverfassungsschutzgesetzes entsprechend, auch wenn sie nicht unter einer auf Dauer angelegten Legende tätig werden.

§ 13

Vertrauensleute

(1) Für den Einsatz von Privatpersonen, deren planmäßige, dauerhafte Zusammenarbeit mit dem Landesamt Dritten nicht bekannt ist (Vertrauensleute), gilt § 12 Abs. 1 bis 9 entsprechend. Vor der Weitergabe von Informationen an die VP-Führung haben Vertrauensleute selbst zu prüfen, ob durch die Informationen oder die Art und Weise, in der sie erlangt wurden, Erkenntnisse im Sinne von § 12 Abs. 4 Satz 1 berührt sind. Die VP-Führung hat die gewonnenen Informationen

auf Erkenntnisse im Sinne von § 12 Abs. 4 Satz 1 überprüfen, bevor sie zur Verwertung weitergegeben werden.

(2) Über die Verpflichtung von Vertrauensleuten entscheidet die Behördenleitung oder ihre Vertretung. Vertrauensleute müssen nach ihren persönlichen und charakterlichen Voraussetzungen für die Zusammenarbeit mit dem Verfassungsschutz geeignet sein. Diese Eignung ist fortlaufend durch das Landesamt zu überprüfen. Als Vertrauensleute dürfen Personen nicht angeworben und eingesetzt werden, die

1. nicht voll geschäftsfähig, insbesondere minderjährig sind,
2. von den Geld- oder Sachzuwendungen für die Tätigkeit auf Dauer als alleinige Lebensgrundlage abhängen würden,
3. an einem Aussteigerprogramm teilnehmen,
4. Mitglied des Europäischen Parlaments, des Deutschen Bundestages, eines Landesparlaments oder Mitarbeiterin oder Mitarbeiter eines solchen Mitglieds sind oder
5. im Bundeszentralregister mit einer Verurteilung wegen eines Verbrechens oder zu einer Freiheitsstrafe, deren Vollstreckung nicht zur Bewährung ausgesetzt worden ist, eingetragen sind.

Die Behördenleitung oder ihre Vertretung kann eine Ausnahme von Satz 4 Nr. 5 zulassen, wenn die Verurteilung nicht als Täter eines Totschlags (§§ 212, 213 des Strafgesetzbuchs in der Fassung der Bekanntmachung vom 13. November 1998 (BGBl. I S. 3322), zuletzt geändert durch Gesetz vom 7. November 2024 (BGBl. 2024 I Nr. 351), oder einer allein mit lebenslanger Haft bedrohten Straftat erfolgt ist und der Einsatz zur Aufklärung von Bestrebungen unerlässlich ist, die auf die Begehung von in § 3 Abs. 1 des Artikel 10-Gesetzes oder § 100b Abs. 2 der Strafprozeßordnung bezeichneten Straftaten gerichtet sind. Im Falle einer Ausnahme nach Satz 5 ist der Einsatz nach höchstens sechs Monaten zu beenden, wenn er zur Erforschung der in Satz 5 genannten Bestrebungen nicht zureichend gewichtig beigetragen hat. Auch im Weiteren ist die Qualität der gelieferten Informationen fortlaufend zu bewerten.

§ 14

Schranken nachrichtendienstlicher Mittel

(1) Von mehreren möglichen und geeigneten Maßnahmen hat das Landesamt diejenige zu treffen, die den Einzelnen und die Allgemeinheit am wenigsten beeinträchtigt.

(2) Eine Maßnahme darf nicht zu einem Nachteil führen, der zu dem erstrebten Erfolg erkennbar außer Verhältnis steht.

(3) Eine Maßnahme ist nur zulässig, bis ihr Zweck erreicht ist oder sich zeigt, dass er nicht erreicht werden kann.

(4) Eine Maßnahme ist unzulässig, soweit tatsächliche Anhaltspunkte dafür vorliegen, dass durch sie allein Erkenntnisse gewonnen werden würden

1. aus dem Kernbereich privater Lebensgestaltung oder
2. bei einer Rechtsanwältin, einem Rechtsanwalt, einem Kammerrechtsbeistand, einer der in § 53 Abs. 1 Satz 1 Nr. 1, 2 oder 4 der Strafprozeßordnung genannten Person oder einer diesen nach § 53a Abs. 1 Satz 1 der Strafprozeßordnung gleichstehenden Person, über die der Berufsgeheimnisträger das Zeugnis verweigern dürfte.

Erfolgen Maßnahmen bei einem der im Übrigen in § 53 Abs. 1 Satz 1 Nr. 3 bis 3b oder 5 der Strafprozeßordnung genannten Berufsgeheimnisträger oder einer diesen nach § 53a Abs. 1 Satz 1 der Strafprozeßordnung gleichstehenden Person, sind das öffentliche Interesse an den

von dem Berufsgeheimnisträger wahrgenommenen Aufgaben und das Interesse an der Geheimhaltung der diesem anvertrauten oder bekannt gewordenen Tatsachen besonders zu berücksichtigen. Satz 1 Nr. 2 und Satz 2 gelten nicht bei Maßnahmen zur Aufklärung von eigenen Bestrebungen oder Tätigkeiten der genannten zeugnisverweigerungsberechtigten Personen.

(5) Erfolgt während der Maßnahme eine unmittelbare Kenntnisnahme und ergeben sich tatsächliche Anhaltspunkte im Sinne von Abs. 4 Satz 1, ist die Maßnahme unverzüglich zu unterbrechen, sobald dies ohne Gefährdung von Leib oder Leben oder Enttarnung eingesetzter Personen möglich ist. Unterbleibt ein Abbruch aufgrund einer Gefährdung nach Satz 1, sind die Tatsache des Eindringens in den Kernbereich privater Lebensgestaltung und die Umstände des Fortsetzens der Maßnahme zu dokumentieren. Die Dokumentation ist dem behördlichen Datenschutzbeauftragten zur unverzüglichen Entscheidung über die Verwertbarkeit und Löschung der Datenerhebung vorzulegen. Die Maßnahme darf fortgeführt werden, wenn keine Anhaltspunkte nach Abs. 4 Satz 1 mehr vorliegen. Soweit Erkenntnisse im Sinne von Abs. 4 Satz 1 durch eine Maßnahme erlangt worden sind, dürfen sie nicht verwendet werden und sind unverzüglich zu löschen. Die Tatsachen der Erfassung der Daten und der Löschung sind zu dokumentieren. Die Dokumentation darf ausschließlich für Zwecke der Datenschutzkontrolle verwendet werden. Die Dokumentation ist am Ende des Kalenderjahres, das der Protokollierung folgt, zu löschen.

DRITTER TEIL

Verarbeitung personenbezogener Daten

§ 15

Geltung datenschutzrechtlicher Vorschriften

Bei der Erfüllung der Aufgaben nach § 2 durch das Landesamt findet das Hessische Datenschutz- und Informationsfreiheitsgesetz vom 3. Mai 2018 (GVBl. S. 82), zuletzt geändert durch Gesetz vom 15. November 2021 (GVBl. S. 718), wie folgt Anwendung:

1. § 1 Abs. 8, die §§ 4, 14 Abs. 1 und 3, § 19 sowie der Zweite Teil finden keine Anwendung,
2. die §§ 41, 46 Abs. 1 bis 4 und die §§ 47 bis 49, 57, 59, 78 und 79 sind entsprechend anzuwenden.

§ 16

Speicherung, Berichtigung, Löschung und Verarbeitungseinschränkung

(1) Das Landesamt darf zur Erfüllung seiner Aufgaben personenbezogene Daten in Dateien speichern, verändern und nutzen, wenn

1. tatsächliche Anhaltspunkte für Bestrebungen oder Tätigkeiten nach § 2 Abs. 2 vorliegen,
2. dies für die Erforschung und Bewertung von Bestrebungen oder Tätigkeiten nach § 2 Abs. 2 erforderlich ist oder
3. das Landesamt nach § 2 Abs. 3 tätig wird.

Unterlagen, die nach Satz 1 gespeicherte Angaben belegen, dürfen auch gespeichert werden, wenn in ihnen weitere personenbezogene Daten Dritter enthalten sind. Eine Abfrage von Daten Dritter ist unzulässig.

(2) Umfang und Dauer der Speicherung personenbezogener Daten sind auf das für die Aufgabenerfüllung des Landesamts erforderliche Maß zu beschränken.

(3) Das Landesamt darf Daten über eine minderjährige Person unter 14 Jahren in Dateien und zu ihrer Person geführten Akten nur speichern, wenn tatsächliche Anhaltspunkte dafür bestehen,

dass sie eine der in § 3 Abs. 1 und 1a des Artikel 10-Gesetzes genannten Straftaten plant, begeht oder begangen hat.

(4) In Dateien oder zu ihrer Person geführten Akten gespeicherte Daten über eine minderjährige Person sind nach zwei Jahren auf die Erforderlichkeit der Speicherung zu überprüfen und spätestens nach fünf Jahren zu löschen, es sei denn, dass nach Eintritt der Volljährigkeit weitere Erkenntnisse angefallen sind, die eine Fortdauer der Speicherung rechtfertigen, oder die Behördenleitung im Einzelfall aufgrund tatsächlicher Anhaltspunkte für das Erfordernis einer Fortdauer der Speicherung ausnahmsweise eine andere Entscheidung trifft. Nicht erforderliche Daten sind zu löschen.

(5) Personenbezogene Daten, die erhoben worden sind, um zu prüfen, ob Bestrebungen oder Tätigkeiten nach § 2 Abs. 2 vorliegen, dürfen in Dateien erst gespeichert werden, wenn sich tatsächliche Anhaltspunkte für derartige Bestrebungen oder Tätigkeiten ergeben haben. Bis zu diesem Zeitpunkt dürfen auch keine zur Person geführten Akten angelegt werden.

(6) Unrichtige personenbezogene Daten sind zu berichtigen. Wird bei personenbezogenen Daten in Akten festgestellt, dass sie unrichtig sind, oder wird ihre Richtigkeit von der betroffenen Person bestritten, so ist dies zu vermerken oder auf sonstige Weise festzuhalten.

(7) Das Landesamt prüft bei der Einzelfallbearbeitung und im Übrigen nach von ihm festgesetzten angemessenen Fristen, spätestens jedoch nach fünf Jahren, ob gespeicherte personenbezogene Daten zur Aufgabenerfüllung noch erforderlich sind; wenn tatsächliche Anhaltspunkte dafür bestehen, dass eine Person eine der in § 3 Abs. 1 und 1a des Artikel 10-Gesetzes genannten Straftaten plant, begeht oder begangen hat, erfolgt die Prüfung in der Regel erst nach zehn Jahren. Gespeicherte personenbezogene Daten über Bestrebungen nach § 2 Abs. 2 Nr. 1 und 3 bis 5 sind spätestens 15 Jahre nach dem Zeitpunkt der letzten gespeicherten relevanten Information zu löschen, es sei denn, die Behördenleitung trifft im Einzelfall aufgrund tatsächlicher Anhaltspunkte für das Erfordernis einer Fortdauer der Speicherung ausnahmsweise eine andere Entscheidung. Enthalten Sachakten oder Akten zu anderen Personen personenbezogene Daten, die nach Satz 2 zu löschen sind, dürfen sie nicht mehr verwendet werden. Soweit Daten automatisiert verarbeitet oder Akten automatisiert erschlossen werden, ist auf den Ablauf der Fristen nach Satz 1 und 2 hinzuweisen. Nicht erforderliche Daten sind zu löschen.

(8) Personenbezogene Daten sind nicht zu löschen, sondern nur in der Verarbeitung einzuschränken, wenn

1. Grund zu der Annahme besteht, dass schutzwürdige Belange der betroffenen Person beeinträchtigt würden,
2. die Daten zur Behebung einer bestehenden Beweisnot unerlässlich sind oder
3. die Verwendung der Daten zu wissenschaftlichen Zwecken erforderlich ist.

In den Fällen des Satz 1 Nr. 3 sind die Daten zum frühestmöglichen Zeitpunkt zu anonymisieren.

(9) Die Verpflichtung nach § 4 Abs. 1 und 2 des Hessischen Archivgesetzes vom 13. Oktober 2022 (GVBl. S. 493) bleibt unberührt.

(10) Akten oder Auszüge aus Akten dürfen auch in elektronischer Form geführt werden. Insoweit kommen die Regelungen zu personenbezogenen Daten in Akten zur Anwendung. Eine Abfrage personenbezogener Daten mittels automatisierter Verarbeitung ist insoweit nur zulässig, wenn die Voraussetzungen des Abs. 1 Satz 1 Nr. 1 oder 2 vorliegen. Der automatisierte Abgleich dieser personenbezogenen Daten ist nur beschränkt auf Akten eng umgrenzter Anwendungsgebiete zulässig. Bei jeder Abfrage sind für Zwecke der Datenschutzkontrolle der Zeitpunkt, die Angaben, die die Feststellung der abgefragten Daten ermöglichen, sowie Angaben zur Feststellung des Abfragenden zu protokollieren. Die protokollierten Daten dürfen nur für Zwecke der Datenschutzkontrolle, der Datensicherung oder zur Sicherstellung eines ordnungsgemäßen Betriebs der

Datenverarbeitungsanlage verwendet werden. Die Protokolldaten sind am Ende des Kalenderjahres, das der Protokollierung folgt, zu löschen.

(11) Zum Zweck der gegenseitigen Information über den Einsatz von Vertrauenspersonen darf das Landesamt zusammen mit den Verfassungsschutzbehörden des Bundes und der anderen Länder eine Übersicht als gemeinsame Datei führen. Die Übersicht kann Angaben über wesentliche Eigenschaften der Vertrauenspersonen und deren Einsatzbereiche enthalten. Das Landesamt und das Hessische Landeskriminalamt koordinieren den jeweiligen Einsatz von Vertrauenspersonen; Näheres regeln gemeinsame Richtlinien.

§ 17

Zweckbindung

(1) Das Landesamt darf personenbezogene Daten auch über den für die Datenerhebung maßgebenden Anlass hinaus zum Zweck der Aufgabenerfüllung des Verfassungsschutzes im Sinne des § 2 nutzen. Die Übermittlung personenbezogener Daten an eine andere Stelle stellt eine Nutzung für andere Zwecke dar und ist nur nach Maßgabe der §§ 20 bis 24 zulässig.

(2) Personenbezogene Daten dürfen auch zur Ausübung von Aufsichts- und Kontrollbefugnissen übermittelt und in dem dafür erforderlichen Umfang verwendet werden.

§ 18

Informationsübermittlung durch öffentliche Stellen an das Landesamt

(1) Die Behörden, Gerichte hinsichtlich der dort geführten Register, sonstigen öffentlichen Stellen des Landes Hessen sowie die Gemeinden, Gemeindeverbände und sonstigen der Aufsicht des Landes Hessen unterstehenden juristischen Personen des öffentlichen Rechts haben dem Landesamt die ihnen bei Erfüllung ihrer Aufgaben bekanntgewordenen Informationen einschließlich personenbezogener Daten auch ohne vorheriges Ersuchen des Landesamts zu übermitteln, wenn tatsächliche Anhaltspunkte dafür bestehen, dass die Informationen für die Erfüllung der Aufgaben des Landesamts erforderlich sein können. § 18 Abs. 1a und 1b des Bundesverfassungsschutzgesetzes bleibt unberührt. Die Übermittlung kann auch durch Einsichtnahme des Landesamts in Akten und Dateien der jeweiligen öffentlichen Stelle erfolgen, soweit die Übermittlung in sonstiger Weise den Zweck der Maßnahme gefährden oder einen übermäßigen Aufwand erfordern würde. Über die Einsichtnahme in amtlich geführte Dateien führt das Landesamt einen Nachweis, aus dem der Zweck und die eingesehene Datei hervorgehen; die Nachweise sind gesondert aufzubewahren, gegen unberechtigten Zugriff zu sichern und am Ende des Kalenderjahres, das dem Jahr ihrer Erstellung folgt, zu löschen. Unter den Voraussetzungen von Satz 1 übermitteln die Staatsanwaltschaften außerdem Anklageschriften und Urteile.

(2) Das Landesamt überprüft die übermittelten Informationen nach ihrem Eingang unverzüglich darauf, ob sie für die Erfüllung seiner Aufgaben erforderlich sind. Ergibt die Prüfung, dass die Informationen nicht erforderlich sind, werden sie unverzüglich gelöscht. Die Löschung kann unterbleiben, wenn die Trennung von anderen Informationen, die zur Erfüllung der Aufgaben erforderlich sind, nicht oder nur mit unvertretbarem Aufwand erfolgen kann; in diesem Fall dürfen die nicht erforderlichen Informationen nicht verwendet werden.

(3) Die Übermittlung personenbezogener Daten nach Abs. 1, die aufgrund einer Maßnahme nach § 100a der Strafprozeßordnung bekannt geworden sind, ist nur zulässig, wenn tatsächliche Anhaltspunkte dafür bestehen, dass jemand eine der in § 3 Abs. 1 und 1a des Artikel 10-Gesetzes genannten Straftaten plant, begeht oder begangen hat. Auf die dem Landesamt nach Satz 1 übermittelten Kenntnisse und Unterlagen findet § 4 Abs. 1 und 4 bis 6 des Artikel 10-Gesetzes entsprechende Anwendung.

(4) Die in Abs. 1 genannten Stellen sind zur Übermittlung verpflichtet, wenn im Einzelfall ein Ersuchen des Landesamts nach § 4 Abs. 3 vorliegt. Hält die ersuchte Stelle das Verlangen nach Auskunft oder Einsichtnahme nach § 4 Abs. 3 nicht für rechtmäßig, so teilt sie dies dem

Landesamt mit. Besteht dieses auf dem Verlangen nach Auskunft oder Einsichtnahme, so entscheidet die für die ersuchte Stelle zuständige oberste Aufsichtsbehörde, soweit gesetzlich nichts anderes bestimmt ist.

§ 19

Informationsübermittlung durch das Landesamt an übergeordnete Behörden und Aufklärung der Öffentlichkeit

(1) Das Landesamt unterrichtet die Ministerien und die Staatskanzlei über Bestrebungen und Tätigkeiten nach § 2 Abs. 2 oder tatsächliche Anhaltspunkte hierfür, die für deren Zuständigkeitsbereich von Bedeutung sind. Dabei dürfen auch personenbezogene Daten übermittelt werden.

(2) Das für den Verfassungsschutz zuständige Ministerium und das Landesamt informieren die Öffentlichkeit zum Zweck der Aufklärung über Bestrebungen und Tätigkeiten nach § 2 Abs. 2, soweit hinreichend gewichtige tatsächliche Anhaltspunkte hierfür vorliegen. Dabei dürfen auch personenbezogene Daten bekanntgegeben werden, wenn die Bekanntgabe für das Verständnis des Zusammenhangs oder der Darstellung von Organisationen erforderlich ist und das Allgemeininteresse das schutzwürdige Interesse der betroffenen Person überwiegt.

(3) Zur Aufklärung der Öffentlichkeit erstellt das Landesamt insbesondere einmal jährlich einen Bericht über Bestrebungen und Tätigkeiten nach § 2 Abs. 2 oder hinreichend gewichtige tatsächliche Anhaltspunkte hierfür. Der Bericht wird von dem für den Verfassungsschutz zuständigen Ministerium herausgegeben und auf der Internetseite des Landesamts für fünf Jahre bereitgestellt.

§ 19a

Übermittlung personenbezogener Daten durch das Landesamt an andere Stellen

(1) Eine Übermittlung personenbezogener Daten durch das Landesamt an eine andere Stelle ist nur zulässig, soweit die Übermittlung der betreffenden Daten zur Erfüllung der Aufgaben der betreffenden Stelle im Einzelfall geboten ist und § 23 nicht entgegensteht.

(2) Die Übermittlung mit nachrichtendienstlichen Mitteln ersterhobener personenbezogener Daten an öffentliche Stellen ist darüber hinaus nur unter den zusätzlichen Voraussetzungen der §§ 20 bis 20c zulässig. Die Übermittlung personenbezogener Daten an ausländische öffentliche Stellen und an Stellen außerhalb des öffentlichen Bereichs ist nur nach Maßgabe der §§ 21 und 22 zulässig.

(3) Soweit personenbezogene Daten übermittelt werden, die mit Maßnahmen nach den §§ 6, 7, 7a oder 8 gewonnen wurden, richtet sich die Übermittlung an andere Stellen nach § 4 Abs. 4 des Artikel 10-Gesetzes bzw. § 8 Abs. 6, wobei eine Übermittlung nach § 4 Abs. 4 Satz 1 Nr. 1 und 2 des Artikel 10-Gesetzes nur zulässig ist, wenn die fraglichen Daten auch nach §§ 20 oder 20a übermittelt werden dürften.

(4) Der Empfänger darf die Informationen nur zu dem Zweck verwenden, zu dem sie ihm übermittelt worden sind. Der Empfänger ist auf die Verwendungsbeschränkung hinzuweisen.

(5) Zur Übermittlung ist auch das für den Verfassungsschutz zuständige Ministerium befugt.

(6) Jede Übermittlung mit nachrichtendienstlichen Mitteln ersterhobener personenbezogener Daten an andere Stellen ist unter Nennung der der Übermittlung zugrunde gelegten Rechtsvorschrift zu protokollieren.

§ 20

Informationsübermittlung durch das Landesamt an Polizeibehörden

Das Landesamt darf mit nachrichtendienstlichen Mitteln ersterhobene personenbezogene Daten an Polizeibehörden übermitteln, soweit dies erforderlich ist zur Abwehr einer wenigstens konkretisierten Gefahr für

1. die freiheitliche demokratische Grundordnung, den Bestand oder die Sicherheit des Bundes oder eines Landes,
2. den Bestand oder die Sicherheit anderer Staaten oder internationaler Organisationen, denen Deutschland angehört, oder das friedliche Zusammenleben der Völker,
3. Menschenwürde, Leib, Leben, Gesundheit, sexuelle Selbstbestimmung oder Freiheit einer Person oder
4. Sachen von bedeutendem Wert, deren Erhaltung im besonderen öffentlichen Interesse geboten ist.

§ 20a

Informationsübermittlung durch das Landesamt an Strafverfolgungsbehörden

(1) Begründen bestimmte Tatsachen den Verdacht, dass jemand eine besonders schwere Straftat begangen (§ 25 des Strafgesetzbuchs), an der Begehung teilgenommen (§§ 26, 27 des Strafgesetzbuchs), oder die Beteiligung versucht (§§ 22, 23, 30 des Strafgesetzbuchs) oder zu einer besonders schweren Straftat öffentlich aufgefordert (§ 111 des Strafgesetzbuchs) hat, darf das Landesamt mit nachrichtendienstlichen Mitteln ersterhobene personenbezogene Daten an die Strafverfolgungsbehörden übermitteln, soweit dies zur Verfolgung der Tat erforderlich ist.

(2) Besonders schwere Straftaten sind solche, die mit einer Höchststrafe von mindestens zehn Jahren Freiheitsstrafe bedroht sind. Besonders schwere Straftaten sind darüber hinaus, wenn sie im Zusammenhang mit der Beteiligung an einer beobachtungsbedürftigen Bestrebung nach § 2 Abs. 2 Nr. 1, 3, 4 oder 5 oder in Ausübung einer beobachtungsbedürftigen Tätigkeit nach § 2 Abs. 2 Nr. 2 begangen werden,

1. Aufstacheln zum Verbrechen der Aggression (§ 80a des Strafgesetzbuchs),
2. Vorbereitung eines hochverräterischen Unternehmens (§ 83 Abs. 2 des Strafgesetzbuchs),
3. Fortführung einer für verfassungswidrig erklärten Partei (§ 84 Abs. 1 bis 3 des Strafgesetzbuchs),
4. Verstoß gegen ein Vereinigungsverbot (§ 85 Abs. 1 des Strafgesetzbuchs),
5. Agententätigkeit zu Sabotagezwecken (§ 87 Abs. 1 des Strafgesetzbuchs),
6. Verfassungsfeindliche Sabotage (§ 88 des Strafgesetzbuchs),
7. Verfassungsfeindliche Einwirkung auf Bundeswehr und öffentliche Sicherheitsorgane (§ 89 Abs. 1 und 2 des Strafgesetzbuchs),
8. Terrorismusfinanzierung (§ 89c Abs. 5 des Strafgesetzbuchs),
9. Landesverräterische Agententätigkeit (§ 98 Abs. 1 Satz 1 des Strafgesetzbuchs),
10. Geheimdienstliche Agententätigkeit (§ 99 Abs. 1 des Strafgesetzbuchs),

11. Landesverräterische Fälschung (§ 100a Abs. 1 bis 3 des Strafgesetzbuchs),
12. Störpropaganda gegen die Bundeswehr (§ 109d des Strafgesetzbuchs),
13. Sabotagehandlungen an Verteidigungsmitteln (§ 109e Abs. 1 bis 3 und Abs. 5 erster Halbsatz des Strafgesetzbuchs),
14. Sicherheitsgefährdender Nachrichtendienst (§ 109f des Strafgesetzbuchs),
15. Sicherheitsgefährdendes Abbilden (§ 109g Abs. 1 und 3 des Strafgesetzbuchs),
16. Tätlicher Angriff auf Vollstreckungsbeamte (§ 114 Abs. 1 und 2 des Strafgesetzbuchs), auch in Verbindung mit § 115 des Strafgesetzbuchs,
17. Bildung krimineller Vereinigungen (§ 129 Abs. 5 Satz 1 und 2 des Strafgesetzbuchs), auch in Verbindung mit § 129b des Strafgesetzbuchs,
18. Bildung einer terroristischen Vereinigung (§ 129a Abs. 3 und 5 des Strafgesetzbuchs), auch in Verbindung mit § 129b des Strafgesetzbuchs,
19. Volksverhetzung (§ 130 Abs. 1 und 3 des Strafgesetzbuchs),
20. Nichtanzeige geplanter Straftaten (§ 138 Abs. 1 Nr. 5 und Abs. 2 des Strafgesetzbuchs),
21. Mittelbare Falschbeurkundung (§ 271 Abs. 3 und 4 des Strafgesetzbuchs),
22. Vorbereitung der Fälschung von amtlichen Ausweisen (§ 275 Abs. 2 erste Alternative des Strafgesetzbuchs), auch in Verbindung mit § 276a des Strafgesetzbuchs,
23. Verschaffen von falschen amtlichen Ausweisen (§ 276 Abs. 2 des Strafgesetzbuchs), auch in Verbindung mit § 276a des Strafgesetzbuchs,
24. Missbrauch ionisierender Strahlen (§ 309 Abs. 6 des Strafgesetzbuchs),
25. Vorbereitung eines Explosions- oder Strahlungsverbrechens (§ 310 Abs. 1 Nr. 2 und 3 sowie Abs. 3 erste Alternative des Strafgesetzbuchs),
26. Gefährliche Eingriffe in den Bahn-, Schiffs- und Luftverkehr (§ 315 Abs. 4 und 5 des Strafgesetzbuchs),
27. Gefährliche Eingriffe in den Straßenverkehr (§ 315b Abs. 1 und 2 des Strafgesetzbuchs),
28. Störung öffentlicher Betriebe (§ 316b Abs. 1 und 2 des Strafgesetzbuchs),
29. Angriffe auf den Luft- und Seeverkehr (§ 316c Abs. 4 des Strafgesetzbuchs),
30. Rechtsbeugung (§ 339 des Strafgesetzbuchs),
31. Falschbeurkundung im Amt (§ 348 des Strafgesetzbuchs),
32. Straftaten nach § 51 Abs. 1 des Waffengesetzes vom 11. Oktober 2002 (BGBl. I S. 3970, 4592, 2003 I S. 1957), zuletzt geändert durch Gesetz vom 17. Juli 2025 (BGBl. 2025 I Nr. 171),
33. Straftaten nach § 19 Abs. 1 des Gesetzes über die Kontrolle von Kriegswaffen in der Fassung der Bekanntmachung vom 22. November 1990 (BGBl. I S. 2506), zuletzt geändert durch Verordnung vom 19. Februar 2025 (BGBl. 2025 I Nr. 47),

34. Straftaten nach § 20a Abs. 1, auch in Verbindung mit § 21 des Gesetzes über die Kontrolle von Kriegswaffen,
35. Straftaten nach § 22a Abs. 1 des Gesetzes über die Kontrolle von Kriegswaffen.

§ 20b

Informationsübermittlung an sonstige inländische öffentliche Stellen

(1) Das Landesamt darf mit nachrichtendienstlichen Mitteln ersterhobene personenbezogene Daten an sonstige inländische öffentliche Stellen übermitteln, wenn eine gesetzliche Regelung, die den Schutz eines der in § 20 genannten Rechtsgüter bezweckt, eine Mitwirkung des Landesamts vorsieht und die Datenübermittlung im Einzelfall erforderlich ist

1. zur Überprüfung der Zuverlässigkeit der betroffenen Person
 - a) im Rahmen eines Erlaubniserteilungsverfahrens auf Ersuchen der überprüfenden Stelle oder
 - b) zur Erfüllung einer gesetzlichen Nachberichtspflicht, wenn dem Landesamt im Nachhinein Informationen bekannt werden, die für die Beurteilung der Zuverlässigkeit der betreffenden Person von Bedeutung sind,
2. zur Prüfung der Frage, ob von der betroffenen Person oder Organisation eine Gefährdung der freiheitlichen demokratischen Grundordnung oder der Sicherheit der Bundesrepublik Deutschland ausgeht, oder ob gegen diese Person oder Organisation sonstige Sicherheitsbedenken bestehen,
 - a) auf Ersuchen der überprüfenden Stelle oder
 - b) zur Erfüllung einer gesetzlichen Unterrichtungspflicht, wenn nachträglich sicherheitserhebliche Erkenntnisse über die überprüfte Person bekannt werden.

(2) Das Landesamt darf von sich aus mit nachrichtendienstlichen Mitteln ersterhobene personenbezogene Daten an sonstige inländische öffentliche Stellen zum Schutz eines der in § 20 genannten Rechtsgüter übermitteln, wenn hinreichende tatsächliche Anhaltspunkte dafür vorliegen, dass dies im Einzelfall zur Erfüllung der Aufgaben des Empfängers erforderlich ist. Verfügt die empfangende Stelle bei der Verwendung der Daten über operative Anschlussbefugnisse, ist dies nur zulässig, soweit es zur Abwehr einer wenigstens konkretisierten Gefahr für ein Rechtsgut nach § 20 erforderlich ist. Eine operative Anschlussbefugnis ist die Möglichkeit, gegenüber Einzelnen Maßnahmen erforderlichenfalls auch mit Zwang durchzusetzen.

(3) Das Landesamt darf mit nachrichtendienstlichen Mitteln ersterhobene personenbezogene Daten an Vereinsverbotsbehörden im Sinne des § 3 Abs. 2 des Vereinsgesetzes vom 5. August 1964 (BGBl. I S. 593), zuletzt geändert durch Gesetz vom 30. November 2020 (BGBl. I S. 2600), übermitteln, wenn Tatsachen die Annahme rechtfertigen, dass die Informationsübermittlung zur Vorbereitung oder Durchführung einer Maßnahme nach § 3 Abs. 1 Satz 1 des Vereinsgesetzes im Einzelfall erforderlich ist.

§ 20c

Informationsübermittlung durch das Landesamt an öffentliche Stellen zu arbeits- und dienstrechtlichen Zwecken

(1) Das Landesamt darf mit nachrichtendienstlichen Mitteln ersterhobene personenbezogene Daten für Zwecke dienst- oder arbeitsrechtlicher Maßnahmen an personalführende öffentliche Stellen übermitteln, wenn hinreichende tatsächliche Anhaltspunkte dafür vorliegen, dass die betroffene Person Bestrebungen oder Tätigkeiten nach § 2 Abs. 2 verfolgt oder unterstützt.

(2) Das Landesamt darf darüber hinaus mit nachrichtendienstlichen Mitteln ersterhobene personenbezogene Daten an personalführende öffentliche Stellen übermitteln zum Zwecke der Überprüfung der Verfassungstreue von Personen, die sich um Einstellung in den öffentlichen Dienst bewerben in den Fällen des § 13a Abs. 1 Satz 1 Nr. 1 des Hessischen Gesetzes über die öffentliche Sicherheit und Ordnung in der Fassung der Bekanntmachung vom 14. Januar 2005 (GVBl. I S. 14), zuletzt geändert durch Gesetz vom 10. Dezember 2025 (GVBl. 2025 Nr. 97).

§ 21

Informationsübermittlung durch das Landesamt an ausländische öffentliche Stellen

(1) Das Landesamt darf personenbezogene Daten an ausländische öffentliche Stellen sowie an über- und zwischenstaatliche Stellen übermitteln, wenn die Übermittlung im Einzelfall zur Wahrung erheblicher Sicherheitsinteressen des Empfängers erforderlich ist. Sind die Daten mit nachrichtendienstlichen Mitteln ersterhoben worden, sind die §§ 20 bis 20b entsprechend anzuwenden. Die Übermittlung unterbleibt, wenn erkennbar ist, dass

1. auswärtige Belange der Bundesrepublik Deutschland oder
2. überwiegende schutzwürdige Interessen des Betroffenen entgegenstehen, insbesondere, wenn hierdurch Leib, Leben oder Freiheit einer Person oder sonstige elementare Menschenrechte gefährdet würden oder Verletzungen von elementaren rechtsstaatlichen Grundsätzen drohen oder
3. im Einzelfall ein datenschutzrechtlich angemessener Umgang mit den Daten beim Empfänger nicht hinreichend gesichert ist.

Bei der Prüfung, ob eine Übermittlung zu unterbleiben hat, berücksichtigt das Landesamt insbesondere den bisherigen Umgang des Empfängers mit übermittelten Daten.

(2) Der Empfänger darf die Informationen nur zu dem Zweck verwenden, zu dem sie ihm übermittelt worden sind. Der Empfänger ist auf die Verwendungsbeschränkung und darauf hinzuweisen, dass das Landesamt sich vorbehält, Auskunft über die Verwendung der Daten zu verlangen. Das Landesamt kann bei der Übermittlung ausschließen, dass die übermittelten Informationen für die Anwendung operativer Befugnisse genutzt werden.

§ 22

Informationsübermittlung durch das Landesamt an Stellen außerhalb des öffentlichen Bereichs

(1) Das Landesamt darf personenbezogene Daten an Personen oder Stellen außerhalb des öffentlichen Bereichs nicht übermitteln, es sei denn, dass dies zum Schutz der freiheitlichen demokratischen Grundordnung, des Bestandes oder der Sicherheit des Bundes oder eines Landes oder zur Gewährleistung der Sicherheit von lebens- oder verteidigungswichtigen Einrichtungen im Einzelfall erforderlich ist und das für den Verfassungsschutz zuständige Ministerium im Einzelfall seine Zustimmung erteilt hat. Das Landesamt führt über die Auskunft nach Satz 1 einen Nachweis, aus dem der Zweck der Übermittlung, die Fundstelle und der Empfänger hervorgehen; die Nachweise sind gesondert aufzubewahren, gegen unberechtigten Zugriff zu sichern und am Ende des Kalenderjahres, das dem Jahr seiner Erstellung folgt, zu vernichten. Der Empfänger darf die übermittelten personenbezogenen Daten nur für den Zweck verwenden, zu dem sie ihm übermittelt wurden. Der Empfänger ist auf die Verwendungsbeschränkung und darauf hinzuweisen, dass das Landesamt sich vorbehält, Auskunft über die Verwendung der Daten zu verlangen. Satz 1 bis 4 finden keine Anwendung, wenn personenbezogene Daten zum Zwecke von Datenerhebungen nach § 4 übermittelt werden.

(2) Der Empfänger darf die Informationen nur zu dem Zweck verwenden, zu dem sie ihm übermittelt worden sind. Der Empfänger ist auf die Verwendungsbeschränkung und darauf hinzuweisen, dass das Landesamt sich vorbehält, Auskunft über die Verwendung der Daten zu verlangen.

§ 23

Übermittlungsverbote

Die Übermittlung von Informationen nach diesem Teil unterbleibt, wenn

1. erkennbar ist, dass unter Berücksichtigung der Art der Informationen und ihrer Erhebung die schutzwürdigen Interessen der betroffenen Person das Interesse der Allgemeinheit oder des Empfängers an der Übermittlung überwiegen,
2. überwiegende Sicherheitsinteressen, insbesondere Gründe des Quellenschutzes oder des Schutzes operativer Maßnahmen, dies erfordern oder
3. besondere gesetzliche Regelungen entgegenstehen; die Verpflichtung zur Wahrung gesetzlicher Geheimhaltungspflichten oder von Berufs- oder besonderen Amtsgeheimnissen, die nicht auf gesetzlichen Vorschriften beruhen, bleibt unberührt.

§ 24

Minderjährigenschutz

(1) Personenbezogene Daten minderjähriger Personen dürfen nach den Vorschriften dieses Gesetzes übermittelt werden, solange die Voraussetzungen ihrer Speicherung nach § 16 Abs. 3 erfüllt sind. Liegen diese Voraussetzungen nicht mehr vor, bleibt eine Übermittlung nur zulässig, wenn sie zur Abwehr einer erheblichen Gefahr oder zur Verfolgung einer der in § 100a der Strafprozessordnung genannten Straftaten erforderlich ist.

(2) Personenbezogene Daten minderjähriger Personen dürfen nach den Vorschriften dieses Gesetzes nicht an ausländische oder über- oder zwischenstaatliche Stellen übermittelt werden.

§ 25

Nachberichtspflicht

Erweisen sich personenbezogene Daten nach ihrer Übermittlung nach den Vorschriften dieses Gesetzes als unvollständig oder unrichtig, sind sie unverzüglich gegenüber dem Empfänger zu berichtigen, wenn dies zu einer anderen Bewertung der Daten führen könnte oder zur Wahrung schutzwürdiger Interessen der betroffenen Person erforderlich ist.

§ 26

Auskunft

(1) Das Landesamt erteilt der betroffenen Person über zu ihrer oder seiner Person gespeicherte Daten auf Antrag unentgeltlich Auskunft, soweit die betroffene Person hierzu ein besonderes Interesse an einer Auskunft darlegt. Legt die betroffene Person nach Aufforderung ein besonderes Interesse nicht dar, entscheidet das Landesamt nach pflichtgemäßem Ermessen. Die Auskunft erstreckt sich nicht auf

1. die Herkunft der Daten und die Empfänger von Übermittlungen und
2. Daten, die nicht strukturiert in automatisierten Dateien gespeichert sind, es sei denn, die betroffene Person macht Angaben, die das Auffinden der Daten ermöglichen, und der für die Erteilung der Auskunft erforderliche Aufwand steht nicht außer Verhältnis zu dem von der betroffenen Person dargelegten Auskunftsinteresse.

Das Landesamt bestimmt das Verfahren, insbesondere die Form der Auskunftserteilung, nach pflichtgemäßem Ermessen.

(2) Die Auskunftserteilung unterbleibt, soweit durch sie

1. eine Gefährdung der Erfüllung der Aufgaben zu besorgen ist,
2. Nachrichtenzugänge gefährdet sein können oder die Ausforschung des Erkenntnisstandes oder der Arbeitsweise des Landesamts zu befürchten ist,
3. die öffentliche Sicherheit gefährdet oder sonst dem Wohl des Bundes oder eines Landes ein Nachteil bereitet würde oder
4. Daten oder die Tatsache ihrer Speicherung preisgegeben werden, die nach einer Rechtsvorschrift oder ihrem Wesen nach, insbesondere wegen der überwiegenden berechtigten Interessen eines Dritten, geheim gehalten werden müssen.

Die Entscheidung trifft die Behördenleitung oder eine von ihr besonders beauftragte Mitarbeiterin oder ein von ihr besonders beauftragter Mitarbeiter.

(3) Die Ablehnung der Auskunftserteilung bedarf keiner Begründung. Sie enthält einen Hinweis auf die Rechtsgrundlage für das Fehlen der Begründung und darauf, dass sich die betroffene Person an die Hessische Datenschutzbeauftragte oder den Hessischen Datenschutzbeauftragten wenden kann. Mitteilungen der oder des Hessischen Datenschutzbeauftragten an die betroffene Person dürfen ohne Zustimmung des Landesamts keine Rückschlüsse auf den Kenntnisstand des Landesamts zulassen.

§ 27

Dateianordnungen

(1) Für den erstmaligen Einsatz einer automatisierten Datei nach § 16 trifft das Landesamt in einer Dateianordnung, die der Zustimmung des für den Verfassungsschutz zuständigen Ministeriums bedarf, die in § 14 Abs. 1 Satz 1 des Bundesverfassungsschutzgesetzes genannten Festlegungen. Die oder der Hessische Datenschutzbeauftragte ist vor Erlass einer Dateianordnung anzuhören. Das Gleiche gilt für wesentliche Änderungen von Dateianordnungen. Das Landesamt führt ein Verzeichnis der geltenden Dateianordnungen.

(2) Das Landesamt hat in angemessenen Abständen die Notwendigkeit der Weiterführung oder Änderung der Dateien zu überprüfen.

(3) Ist im Hinblick auf die Dringlichkeit der Aufgabenerfüllung die vorherige Mitwirkung der in Abs. 1 genannten Stellen nicht möglich, so kann das Landesamt eine Sofortanordnung treffen. Das Verfahren nach Abs. 1 ist unverzüglich nachzuholen.

VIERTER TEIL

Schlussvorschriften

§ 28

Einschränkung von Grundrechten

Aufgrund dieses Gesetzes können die Grundrechte auf die Versammlungsfreiheit (Art. 8 Abs. 1 des Grundgesetzes, Art. 14 Abs. 1 der Verfassung des Landes Hessen), das Brief-, Post- und Fernmeldegeheimnis (Art. 10 Abs. 1 des Grundgesetzes, Art. 12 der Verfassung des Landes Hessen), die informationelle Selbstbestimmung und Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme (Art. 12a der Verfassung des Landes Hessen) und die Unverletzlichkeit der Wohnung (Art. 13 Abs. 1 des Grundgesetzes, Art. 8 der Verfassung des Landes Hessen) eingeschränkt werden.

§ 29

Inkrafttreten

Dieses Gesetz tritt am Tag nach der Verkündung in Kraft.

Artikel 2²⁾

Änderung des Verfassungsschutzkontrollgesetzes

Das Verfassungsschutzkontrollgesetz vom 25. Juni 2018 (GVBl. S. 302, 317), geändert durch Gesetz vom 28. Juni 2023 (GVBl. S. 432), wird wie folgt geändert:

1. Dem § 1 Abs. 5 wird folgender Satz angefügt:

„Die Mitglieder der Parlamentarischen Kontrollkommission bleiben nach Ablauf der Wahlperiode oder der Auflösung des Landtags bis zur Wahl einer neuen Parlamentarischen Kontrollkommission im Amt.“

2. § 3 wird wie folgt geändert:

- a) Abs. 3 wird wie folgt geändert:

- aa) In Nr. 1 wird die Angabe „25. Juni 2018 (GVBl. S. 302)“ durch „10. Dezember 2025 (GVBl. 2025 Nr. 97)“ ersetzt.
- bb) In Nr. 2 Buchst. a wird die Angabe „§§ 7, 9“ durch „§§ 7, 7a, 9“ ersetzt.

- b) In Abs. 4 wird die Angabe „19. Dezember 2022 (BGBl. I S. 2632)“ durch „25. Oktober 2024 (BGBl. 2024 I Nr. 332)“ ersetzt.

3. In § 6 Satz 3 wird die Angabe „§§ 7,“ durch „§§ 7, 7a,“ ersetzt.

Artikel 2a³⁾

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 13. Dezember 2024 (GVBl. 2024 Nr. 83), wird wie folgt geändert:

1. In § 10 wird nach der Angabe „Art. 8 der Verfassung des Landes Hessen“ ein Komma und die Angabe „Eigentumsgarantie (Art. 45 Abs. 1 der Verfassung des Landes Hessen)“ eingefügt.

2. § 12a wird wie folgt gefasst:

„§ 12a

Schutz zeugnisverweigerungsberechtigter Berufsgeheimnisträger

(1) Maßnahmen nach § 14 Abs. 6 Satz 3, § 15 Abs. 2 und 4, § 15a Abs. 1, 2, 2a und 3, § 15b Abs. 1, § 15c Abs. 1, § 16 Abs. 1 und 2 sowie § 17 Abs. 1, die sich gegen eine in § 53 Abs. 1 Satz 1 Nr. 1, 2, 3 oder Nr. 4 der Strafprozeßordnung genannte Person richten und voraussichtlich Erkenntnisse erbringen würden, über die diese Person das Zeugnis verweigern dürfte, sind unzulässig. Dennoch erlangte Erkenntnisse dürfen nicht verwertet werden. Aufzeichnungen hierüber sind unverzüglich zu löschen. Die Tatsache ihrer Erlangung und Löschung ist zu dokumentieren. Satz 2 bis 4 gelten entsprechend, wenn durch eine Maßnahme,

²⁾ Ändert FFN 18-8

³⁾ Ändert FFN 310-63

die sich nicht gegen eine in § 53 Abs. 1 Satz 1 Nr. 1, 2, 3 oder Nr. 4 der Strafprozeßordnung genannte Person richtet, von einer dort genannten Person Erkenntnisse erlangt werden, über die sie das Zeugnis verweigern dürfte. Für Personen nach § 53 Abs. 1 Satz 1 Nr. 3 der Strafprozeßordnung gelten Satz 1 bis 5 nur, soweit es sich um Rechtsanwälte oder Kammerrechtsbeistände handelt.

(2) Soweit durch eine Maßnahme nach Abs. 1 Satz 1 eine in § 53 Abs. 1 Satz 1 Nr. 3, 3a, 3b oder 5 der Strafprozeßordnung genannte Person betroffen wäre und dadurch voraussichtlich Erkenntnisse erlangt würden, über die diese Person das Zeugnis verweigern dürfte, ist dies im Rahmen der Prüfung der Verhältnismäßigkeit unter Würdigung des öffentlichen Interesses an den von dieser Person wahrgenommenen Aufgaben und des Interesses an der Geheimhaltung der dieser Person anvertrauten oder bekannt gewordenen Tatsachen besonders zu berücksichtigen. Von einem Überwiegen des Interesses an der Datenerhebung ist in der Regel nicht auszugehen, wenn die Maßnahme nicht der Abwehr einer unmittelbar bevorstehenden Gefahr für Leben, Gesundheit oder Freiheit dient. Soweit hiernach geboten, ist die Maßnahme zu unterlassen oder, soweit dies nach der Art der Maßnahme möglich ist, zu beschränken. Für Personen nach § 53 Abs. 1 Satz 1 Nr. 3 der Strafprozeßordnung gelten Satz 1 und 2 nur, soweit es sich nicht um Rechtsanwälte oder Kammerrechtsbeistände handelt.

(3) Abs. 1 und 2 gelten entsprechend, soweit die in § 53a der Strafprozeßordnung Genannten das Zeugnis verweigern dürften.

(4) Abs. 1 bis 3 gelten nicht, sofern Tatsachen die Annahme rechtfertigen, dass die zeugnisverweigerungsberechtigte Person die Gefahr verursacht hat.“

3. § 13a Abs. 2 Satz 3 wird wie folgt gefasst:

„Im Fall des Abs. 1 Satz 1 Nr. 1 Buchst. a ist eine Überprüfung der betroffenen Personen anhand von Datenbeständen des Landesamts für Verfassungsschutz regelmäßig erforderlich.“

4. § 14 Abs. 3a wird wie folgt gefasst:

„(3a) Es wird vermutet, dass die Voraussetzungen nach Abs. 3 Satz 1 in den öffentlich zugänglichen Bereichen von Flughäfen, Personenbahnhöfen, Sportstätten, Einkaufszentren und Packstationen vorliegen. Diese Vermutung gilt auch für öffentlich zugängliche Bereiche in unmittelbarer Nähe von Flughäfen. Abs. 1 Satz 2 und 3 und Abs. 3 Satz 3 und 4 gelten entsprechend.“

5. § 14a Abs. 1 und 1a wird wie folgt gefasst:

„(1) Die Polizeibehörden können unter den Voraussetzungen des § 18 Abs. 1, Abs. 2 Satz 1 Nr. 1, 3 bis 6 durch den Einsatz technischer Mittel automatisch Bilder von Fahrzeugen aufzeichnen und deren Kennzeichen erfassen. Die Maßnahme ist im Fall des § 18 Abs. 1 nur zulässig

1. zur Abwehr einer Gefahr für den Bestand oder die Sicherheit des Bundes oder eines Landes oder Leib, Leben oder Freiheit einer Person oder Sachen von bedeutendem Wert, deren Erhalt im öffentlichen Interesse geboten ist,
2. wenn gleichgewichtige Schäden für die Umwelt zu erwarten sind oder
3. zur Durchsetzung der Versicherungspflicht.

Die Bildaufzeichnung kann auch erfolgen, wenn die Insassen der Fahrzeuge unvermeidbar betroffen werden. Datenerhebungen nach diesem Absatz dürfen

1. nicht flächendeckend,

2. in den Fällen des § 18 Abs. 1, Abs. 2 Satz 1 Nr. 1, 3 und 4 nicht dauerhaft,
3. in den Fällen des § 18 Abs. 2 Satz 1 Nr. 5 und 6 nicht längerfristig und
4. in den Fällen des § 18 Abs. 2 Satz 1 Nr. 6 bei Straßen nur auf Bundesautobahnen und Europastraßen

durchgeführt werden. Sie sind in geeigneter Weise für Kontrollzwecke zu dokumentieren.

(1a) Es ist, soweit möglich, technisch sicherzustellen, dass von den nach Abs. 1 Satz 1 aufgezeichneten Bildern keine Personen außerhalb der Fahrzeuge erfasst werden. Soweit solche Personen unvermeidbar erfasst werden, sind diese unverzüglich technisch unkenntlich zu machen. Es ist sicherzustellen, dass während und außerhalb des Betriebs des technischen Mittels sowie bei der Übertragung der erlangten Daten kein unbefugter Zugriff auf diese erfolgen kann.“

6. § 14b wird wie folgt gefasst:

„§ 14b

Abschnittskontrolle

Die Ordnungsbehörden und die Polizei dürfen im öffentlichen Verkehrsraum zur Verhütung der Überschreitung der zulässigen Höchstgeschwindigkeit von Kraftfahrzeugen nach Maßgabe des Satz 2 Bildaufzeichnungen offen anfertigen und damit auf einer festgelegten Wegstrecke die Durchschnittsgeschwindigkeit eines Kraftfahrzeugs ermitteln (Abschnittskontrolle). Die Bildaufzeichnungen dürfen nur das Kraftfahrzeugkennzeichen, das Kraftfahrzeug und seine Fahrtrichtung sowie Zeit und Ort erfassen; es ist technisch sicherzustellen, dass Insassen nicht zu sehen sind oder sichtbar gemacht werden können. Bei Kraftfahrzeugen, bei denen nach Feststellung der Durchschnittsgeschwindigkeit keine Überschreitung der zulässigen Höchstgeschwindigkeit vorliegt, sind die nach Satz 2 erhobenen Daten sofort automatisch zu löschen. Die Abschnittskontrolle ist kenntlich zu machen.“

7. § 15a wird wie folgt geändert:

- a) Abs. 2 wird wie folgt geändert:

- aa) In Satz 1 wird die Angabe „Telekommunikation-Telemedien-Datenschutz-Gesetzes vom 23. Juni 2021 (BGBl. I S. 1982), zuletzt geändert durch Gesetz vom 12. August 2021 (BGBl. I S. 3544),“ durch „Telekommunikation-Digitale-Dienste-Datenschutz-Gesetzes vom 23. Juni 2021 (BGBl. I S. 1982, 2022 I S. 1045), zuletzt geändert durch Gesetz vom 12. Juli 2024 (BGBl. 2024 I Nr. 234),“ ersetzt.
- bb) In Satz 3 wird die Angabe „10. September 2021 (BGBl. I S. 4147)“ durch „24. Juli 2025 (BGBl. 2025 I Nr. 181),“ ersetzt.

- b) Abs. 2a wird wie folgt geändert:

- aa) In Satz 1 und 2 werden die Wörter „Telekommunikation-Telemedien-Datenschutz-Gesetzes“ jeweils durch „Telekommunikation-Digitale-Dienste-Datenschutz-Gesetzes“ ersetzt.
- bb) In Satz 3 wird die Angabe „§ 14 Abs. 1 des Telemediengesetzes“ durch „§ 2 Abs. 2 Nr. 2 des Telekommunikation-Digitale-Dienste-Datenschutz-Gesetzes“ ersetzt.

- c) Abs. 3 wird wie folgt gefasst:

„(3) Die Polizeibehörden können unter den Voraussetzungen des Abs. 1 technische Mittel einsetzen, um spezielle Kennungen eines Mobilfunkendgeräts oder sonstigen Endgeräts, spezielle Kennungen der darin verwendeten Karte sowie den Standort zu ermitteln.“

- d) In Abs. 7 wird die Angabe „(BGBl. I S. 1254, 2298), zuletzt geändert durch Gesetz vom 5. Juli 2021 (BGBl. I S. 2274)“ durch „(BGBl. I S. 1254, 2298; 2017 I S. 154), zuletzt geändert durch Gesetz vom 22. Dezember 2023 (BGBl. 2023 I Nr. 413)“ ersetzt.

8. § 16 wird wie folgt geändert:

- a) Die Abs. 3 bis 7 werden wie folgt gefasst:

„(3) Die Datenerhebung durch den Einsatz von V-Personen oder VE-Personen ist nur zulässig, wenn andere Maßnahmen mit Ausnahme der in den §§ 15 bis 15c und 17 genannten erheblich weniger Erfolg versprechen würden oder die polizeiliche Aufgabenerfüllung mit Hilfe anderer Maßnahmen wesentlich erschwert würde. Im Rahmen der Aufgabenerfüllung können personenbezogene Daten auch über dritte Personen erhoben werden, soweit dies unerlässlich ist, um die Datenerhebung nach Abs. 1 und 2 durchführen zu können. Liegen tatsächliche Anhaltspunkte vor, dass durch den Einsatz von V-Personen oder VE-Personen allein Erkenntnisse aus dem Kernbereich privater Lebensgestaltung erlangt würden, ist deren Einsatz unzulässig.“

(4) Bei der Planung des Einsatzes sollen nach Möglichkeit Situationen vermieden werden, bei denen regelmäßig Erkenntnisse aus dem Kernbereich privater Lebensgestaltung gewonnen werden würden. Bei einem gegen eine Person gerichteten Einsatz darf unter keinen Umständen der Kernbereich zum Ziel des Einsatzes gemacht werden. Insbesondere dürfen zum Aufbau oder zum Erhalt eines Vertrauensverhältnisses keine intimen Beziehungen oder vergleichbar engste persönliche Bindungen begründet oder fortgeführt werden. Entstehen solche Bindungen, ist der Einsatz gegen diese Person abzubrechen.

(5) Ergeben sich während der Durchführung des Einsatzes Anhaltspunkte dafür, dass der Kernbereich privater Lebensgestaltung betroffen ist, ist der Einsatz zu unterbrechen, sobald dies ohne Gefährdung für Leib, Leben oder Enttarnung der eingesetzten Personen möglich ist. Unterbleibt ein Abbruch aufgrund einer Gefährdung nach Satz 1, sind die Tatsache des Eindringens in den Kernbereich privater Lebensgestaltung und die Umstände des Fortsetzens der Maßnahme zu dokumentieren. Die Maßnahme darf fortgeführt werden, wenn keine Anhaltspunkte mehr dafür vorliegen, dass der Kernbereich privater Lebensgestaltung betroffen ist. Soweit Erkenntnisse aus dem Kernbereich privater Lebensgestaltung durch eine Maßnahme erlangt worden sind, dürfen sie nicht verwendet werden und sind unverzüglich zu löschen. Die Tatsachen der Erfassung der Daten und der Löschung sind zu dokumentieren. Die Dokumentation darf ausschließlich für Zwecke der Datenschutzkontrolle nach § 29a verwendet werden. Die Dokumentation ist am Ende des Kalenderjahres, das der Protokollierung folgt, zu löschen.

(6) Vor der Weitergabe von Informationen haben die eingesetzten Personen zu prüfen, ob durch die Informationen oder die Art und Weise, in der sie erlangt wurden, Erkenntnisse aus dem Kernbereich privater Lebensgestaltung betroffen sind. Entsprechende Erkenntnisse dürfen nicht zur Verwertung weitergegeben werden.

(7) Bestehen Zweifel, ob bei einer Maßnahme Erkenntnisse aus dem Kernbereich privater Lebensgestaltung gewonnen worden sind, entscheidet die oder der behördliche Datenschutzbeauftragte unverzüglich über die Verwendbarkeit und Löschung der Daten.“

- b) Abs. 8 Satz 1 wird wie folgt gefasst:

„(8) Soweit es für den Aufbau oder zur Aufrechterhaltung der Legende unerlässlich ist, dürfen für den Einsatz von VE-Personen entsprechende Urkunden hergestellt oder verändert werden.“

9. § 16a wird wie folgt gefasst:

„§ 16a

Anerkennung von richterlichen Anordnungen anderer Länder

Richterliche Anordnungen anderer Länder, die die personenbezogene Datenerhebung nach den §§ 14 bis 16 betreffen, werden als nach diesem Gesetz angeordnete Maßnahme anerkannt, wenn auch hiernach der Einsatz derselben Maßnahme hätte angeordnet werden dürfen.“

10. In § 17a Satz 2 wird die Angabe „Satz 4“ durch „Satz 5“ ersetzt.

11. § 20 Abs. 6 wird wie folgt gefasst:

„(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, weiterverarbeiten, soweit dies zur Abwehr einer Gefahr oder zur vorbeugenden Bekämpfung von Straftaten erforderlich ist. Bei den Daten von Personen, die verdächtig sind, eine Straftat begangen zu haben, ist die Weiterverarbeitung nur zulässig, wenn tatsächliche Anhaltspunkte die Annahme rechtfertigen, dass zukünftig Strafverfahren gegen die betroffenen Personen zu führen sein werden; entfällt der Verdacht, sind die Daten zu löschen. Näheres zur Übermittlung von Verfahrensausgängen und Einstellungsbegründungen seitens der Staatsanwaltschaft an die Polizei wird in einer gemeinsamen Verwaltungsvorschrift des Ministeriums des Innern, für Sicherheit und Heimatschutz und des Ministeriums der Justiz und für den Rechtsstaat geregelt.“

12. § 25a Abs. 1 bis 5 wird wie folgt gefasst:

„(1) Die Polizeibehörden dürfen rechtmäßig gespeicherte personenbezogene Daten auf einer Analyseplattform automatisiert zusammenführen. Sie dürfen nach Maßgabe der Sätze 3 bis 6 und der Abs. 2 bis 5 diese zusammengeführten Daten, auch gemeinsam mit weiteren rechtmäßig erhobenen personenbezogenen Daten, verknüpfen, aufbereiten und auswerten sowie für statistische Zwecke anwenden (automatisierte Anwendung zur Datenanalyse). Die automatisierte Anwendung zur Datenanalyse ist ein technisches Hilfsmittel, das es den Polizeibehörden bei der Erfüllung ihrer Aufgaben nach Maßgabe der folgenden Absätze ermöglichen soll, ihre Bewertungen, Prognosen und Entscheidungen auf der Grundlage möglichst verlässlicher Tatsachenfeststellungen zu treffen. Sie erfolgt immer anhand anlassbezogener und zielgerichteter Suchkriterien. Sie wird manuell ausgelöst. Eine direkte Anbindung an Internetdienste ist ausgeschlossen.

(2) Die Polizeibehörden können gespeicherte personenbezogene Daten mittels einer automatisierten Anwendung zur Datenanalyse weiterverarbeiten,

1. wenn dies zur Abwehr einer Gefahr für den Bestand oder die Sicherheit des Bundes oder eines Landes oder Leib, Leben oder Freiheit einer Person oder Sachen von bedeutsamem Wert, deren Erhaltung im öffentlichen Interesse geboten ist, oder wenn gleichgewichtige Schäden für die Umwelt zu erwarten sind, erforderlich ist (Abwehr konkreter Gefahren),
2. wenn tatsächliche Anhaltspunkte die Annahme rechtfertigen, dass innerhalb eines übersehbaren Zeitraumes auf eine zumindest ihrer Art nach konkretisierte Weise Straftaten mit erheblicher Bedeutung begangen werden und dies zur Verhinderung dieser Straftaten erforderlich ist (Abwehr konkretisierter Gefahren),
3. wenn tatsächliche Anhaltspunkte die Annahme rechtfertigen, dass schwere oder besonders schwere Straftaten begangen werden sollen, und die Weiterverarbeitung erforderlich ist, um diese Straftaten zu verhindern (Vorbeugende Bekämpfung von Straftaten).

Zum Zweck der automatisierten Anwendung zur Datenanalyse können Vorgangsdaten, Falldaten, Daten aus den polizeilichen Auskunftssystemen, Verkehrsdaten, Telekommunikationsdaten, Daten aus Asservaten und Daten aus dem polizeilichen Informationsaustausch zusammengeführt werden. Datensätze aus gezielten Abfragen in gesondert geführten staatlichen Registern sowie einzelne gesondert gespeicherte Datensätze aus Internetquellen können ergänzend einbezogen werden. Bei einer Maßnahme nach Satz 1 Nr. 3 dürfen Verkehrs- sowie Telekommunikationsdaten nicht in die Analyse einbezogen werden.

(3) Bei der Anwendung zur automatisierten Datenanalyse gilt § 20 Abs. 1 und 2. Dies wird durch eine Verwaltungsvorschrift sichergestellt, die zu veröffentlichen ist. Sie beinhaltet ein Rollen- und Rechtekonzept und ein Konzept der Kategorisierung und Kennzeichnung personenbezogener Daten. Unter Berücksichtigung der in Abs. 2 Satz 1 nach Schutzgütern und Eingriffsschwellen unterschiedenen Lagebilder orientieren sich diese Konzepte an dem übergeordneten Ziel der Reduzierung des jeweils zu analysierenden Datenvolumens, der Angemessenheit der jeweils angewandten Analysemethode und des größtmöglichen Schutzes Unbeteiligter (funktionale Reduzierung der Eingriffsintensität).

1. Das Rollen- und Rechtekonzept regelt die zweckabhängige Verteilung sachlich eingeschränkter Zugriffsrechte anhand von Phänomenbereichen. Maßstab für dieses Konzept sind das Gewicht der zu schützenden Rechtsgüter und der Grad der Dringlichkeit des polizeilichen Einschreitens. Es ist nach dem Prinzip auszugestalten, wonach mehr Berechtigte Zugriff auf weniger und wenige Berechtigte Zugriff auf mehr der in der Analyseplattform zusammengeführten Daten haben dürfen. Es müssen darin mindestens die einzelnen Phänomenbereiche, ihre Gewichtung und ihr Verhältnis zueinander umschrieben und die dienstrechtliche Stellung der Berechtigten, ihre Funktion und ihre spezifische Qualifizierung bezogen auf den Umfang der jeweiligen Berechtigung festgelegt werden.
2. Das Konzept der Kategorisierung und Kennzeichnung personenbezogener Daten regelt anhand der Maßstäbe des Veranlassungszusammenhangs und der Grundrechtsrelevanz, welche personenbezogenen Daten in welcher Weise in die automatisierte Analyse einbezogen werden dürfen.
 - a) Maßstab für dieses Konzept ist zum einen der sachliche Bezug der von der Analyse betroffenen Personen zum jeweiligen Phänomenbereich (Veranlassungszusammenhang). Es folgt dem Prinzip, wonach eine automatisierte Datenanalyse umso komplexer sein darf, je wichtiger der Veranlassungszusammenhang ist, und dass sie umso einfacher sein muss, je weniger wichtig der Veranlassungszusammenhang ist. Ausgangspunkt ist die Differenzierung nach einerseits verurteilten, beschuldigten, verdächtigen Personen und sonstigen Anlasspersonen sowie deren Kontaktpersonen und andererseits unbeteiligten Personen. Zum Schutz Unbeteiligter werden deren personenbezogene Vorgangsdaten in eine automatisierte Datenanalyse nicht einbezogen. Das Nähere regelt eine Verwaltungsvorschrift, die insbesondere für Verkehrsdaten eine Speicherfrist von regelmäßig zwei Jahren in der Analyseplattform vorsieht.
 - b) Maßstab für dieses Konzept ist zum anderen die Kategorisierung personenbezogener Daten nach der Schwere des Eingriffs in das Recht auf informationelle Selbstbestimmung bei ihrer Erhebung (Grundrechtsrelevanz). Es müssen abstrakte Regelungen getroffen werden, die der eingeschränkten Verwendbarkeit von Daten aus schwerwiegenden Grundrechtseingriffen Rechnung tragen, und es muss durch technisch-organisatorische Vorkehrungen sichergestellt werden, dass diese Regelungen praktisch wirksam werden. In die automatisierte Anwendung zur Datenanalyse werden keine personenbezogenen Daten einbezogen, die aus Wohnraumüberwachung und Online-Durchsuchung gewonnen wurden.

(4) Der Zugang zur automatisierten Anwendung zur Datenanalyse ist reglementiert (Zugriffskontrolle). Die Zugriffe unterliegen hierbei der ständigen Protokollierung. Jeder Fall der automatisierten Anwendung zur Datenanalyse ist von der Anwenderin oder dem Anwender zu begründen. Die Begründung dient der Selbstvergewisserung und der nachträglichen Kontrolle. Die Einzelheiten der Zugriffskontrolle und des notwendigen Inhalts der Begründung

werden in einer Verwaltungsvorschrift geregelt. Die oder der behördliche Datenschutzbeauftragte ist zur Durchführung stichprobenartiger Kontrollen berechtigt.

(5) Die Einrichtung und wesentliche Änderung einer automatisierten Anwendung zur Datenanalyse erfolgen durch Anordnung der Behördenleitung oder einer oder eines von dieser beauftragten Bediensteten. Die oder der Hessische Beauftragte für Datenschutz und Informationsfreiheit ist vor der Einrichtung oder einer wesentlichen Änderung nach Satz 1 anzuhören; bei Gefahr im Verzug ist die Anhörung nachzuholen. Im Übrigen bleiben die Aufgaben und Befugnisse der oder des Hessischen Beauftragten für Datenschutz und Informationsfreiheit unberührt.“

13. § 27 Abs. 4 wird wie folgt gefasst:

„(4) Die Ministerin oder der Minister des Innern, für Sicherheit und Heimatschutz 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 unter Berücksichtigung des Verfahrensausgangs nach Art und Zweck der Speicherung sowie Art und Bedeutung des Anlasses zu unterscheiden ist. In Fällen von geringerer Bedeutung sind kürzere Fristen vorzusehen, die in den Fällen des Satz 2 Nr. 1 fünf Jahre nicht überschreiten dürfen. Die Frist für eine Verlängerung der Datenspeicherung nach Ablauf der Frist nach Satz 2 Nr. 1 darf bei fortbestehendem Verdacht einer terroristischen Straftat oder einer Sexualstraftat nach dem 13. Abschnitt des Strafgesetzbuchs (ausgenommen die §§ 183a, 184, 184f und 184g des Strafgesetzbuchs) oder einer sexuell bestimmten Straftat nach den §§ 211 bis 213 und 223 bis 228 des Strafgesetzbuchs zehn Jahre und bei fortbestehendem Verdacht einer sonstigen Straftat von erheblicher Bedeutung fünf Jahre nicht überschreiten. Weitere Verlängerungen der Frist sind bei fortbestehendem Verdacht einer terroristischen Straftat oder einer Sexualstraftat nach Satz 4 um bis zu fünf Jahre und bei fortbestehendem Verdacht einer sonstigen Straftat von erheblicher Bedeutung um bis zu zwei Jahre nur zulässig, wenn tatsächliche Anhaltspunkte die Annahme rechtfertigen, dass die Person solche Straftaten begehen wird. 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 bis 6 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. Die Gründe für die Verlängerung der Frist nach Satz 4 und 5 sind aktenkundig zu machen. Die Beachtung der Prüfungstermine und Aufbewahrungsfristen ist durch geeignete technische und organisatorische Maßnahmen zu gewährleisten.“

14. § 31a Abs. 1 Satz 2 wird wie folgt gefasst:

„Die Verpflichtung nach Satz 1 umfasst auch die Verpflichtung, ein zur Verfügung gestelltes Mobiltelefon ständig in betriebsbereitem Zustand bei sich zu führen und dessen Funktionsfähigkeit nicht zu beeinträchtigen.“

15. § 98a wird wie folgt gefasst:

„§ 98a

Legitimations- und Kennzeichnungspflicht

(1) Auf Verlangen der von einer Maßnahme betroffenen Person haben sich Polizeivollzugsbeamtinnen und Polizeivollzugsbeamte sowie Angehörige der Wachpolizei und des Freiwilligen Polizeidienstes des Landes Hessen auszuweisen.

(2) Polizeivollzugsbeamtinnen und Polizeivollzugsbeamte sowie Angehörige der Wachpolizei und des Freiwilligen Polizeidienstes des Landes Hessen tragen bei Amtshandlungen an ihrer Dienstkleidung ein Namensschild (namentliche Kennzeichnungspflicht). Das Namensschild wird beim Einsatz geschlossener Einheiten durch eine zur nachträglichen Identifizierung geeignete fünfstellige numerische Kennzeichnung ersetzt. Zweck der Kennzeichnungspflicht nach Satz 1 und 2 ist die Sicherstellung einer auch nachträglichen Identifizierung der Polizeivollzugsbeamtinnen und Polizeivollzugsbeamten sowie der Angehörigen der Wachpolizei und des Freiwilligen Polizeidienstes des Landes Hessen bei der Durchführung von Amtshandlungen.

(3) Die Legitimations- und die Kennzeichnungspflicht nach Abs. 1 und 2 gelten nicht, soweit der Zweck der Maßnahme oder Amtshandlung oder überwiegende schutzwürdige Belange der Polizeivollzugsbeamtinnen und Polizeivollzugsbeamten sowie der Angehörigen der Wachpolizei und des Freiwilligen Polizeidienstes des Landes Hessen dadurch beeinträchtigt werden.

(4) Das Ministerium des Innern, für Sicherheit und Heimatschutz regelt Inhalt, Umfang und Ausnahmen von dieser Verpflichtung sowie zum Schutz der personenbezogenen Daten durch Verwaltungsvorschriften.“

Artikel 2b⁴⁾

Änderung des Hessischen Freiwilligen-Polizeidienst-Gesetzes

In § 9 des Hessischen Freiwilligen-Polizeidienst-Gesetzes vom 13. Juni 2000 (GVBl. I S. 294), zuletzt geändert durch Gesetz vom 16. September 2025 (GVBl. 2025 Nr. 57), wird das Wort „und“ durch ein Komma ersetzt und nach der Angabe „Art. 6 der Verfassung des Landes Hessen“ ein Komma sowie die Angabe „informationelle Selbstbestimmung und Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme (Art. 12a der Verfassung des Landes Hessen) und die Eigentumsgarantie (Art. 45 Abs. 1 der Verfassung des Landes Hessen)“ eingefügt.

Artikel 3⁵⁾

Änderung des Hessischen Versammlungsfreiheitsgesetzes

Das Hessische Versammlungsfreiheitsgesetz vom 22. März 2023 (GVBl. S. 150) wird wie folgt geändert:

1. § 16 Abs. 1 Satz 2 wird wie folgt gefasst:

„Aufgefundene Gegenstände im Sinne des Satz 1 können sichergestellt werden.“

2. § 23 Abs. 1 Satz 2 wird wie folgt gefasst:

„Aufgefundene Gegenstände im Sinne des Satz 1 können sichergestellt werden.“

3. § 27 wird wie folgt gefasst:

⁴⁾ Ändert FFN 310-85

⁵⁾ Ändert FFN 315-10

„§ 27“

Einziehung

Gegenstände, auf die sich eine Straftat nach § 25 oder eine Ordnungswidrigkeit nach § 26 bezieht, können eingezogen werden. § 74a des Strafgesetzbuches und § 23 des Gesetzes über Ordnungswidrigkeiten in der Fassung der Bekanntmachung vom 19. Februar 1987 (BGBl. I S. 602), zuletzt geändert durch Gesetz vom 12. Juli 2024 (BGBl. 2024 I Nr. 234), sind anzuwenden.“

4. In § 29 wird die „nach Art. 1 Abs. 1 in Verbindung mit Art. 2 Abs. 1 des Grundgesetzes und Art. 12a der Verfassung des Landes Hessen“ durch „und Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme nach Art. 12a der Verfassung des Landes Hessen sowie die Eigentumsgarantie nach Art. 45 Abs. 1 der Verfassung des Landes Hessen“ ersetzt.

Artikel 4⁶⁾

Änderung des Hessischen Besoldungsgesetzes

In der Anlage I Besoldungsordnungen A und B des Hessischen Besoldungsgesetzes vom 27. Mai 2013 (GVBl. S. 218, 256, 508), zuletzt geändert durch Gesetz vom 6. März 2025 (GVBl. 2025 Nr. 17), werden in der Besoldungsordnung B in der Besoldungsgruppe B 6 nach den Wörtern „Direktor des Landesbetriebes Bau und Immobilien Hessen“ die Angaben „Direktorin des Landesbetriebes Hessen-Forst“ und „Direktor des Landesbetriebes Hessen-Forst“ eingefügt.

Artikel 5

Einschränkung von Grundrechten

(1) Aufgrund des Art. 1 können die Grundrechte auf die Versammlungsfreiheit (Art. 8 Abs. 1 des Grundgesetzes, Art. 14 Abs. 1 der Verfassung des Landes Hessen), das Brief-, Post- und Fernmeldegeheimnis (Art. 10 Abs. 1 des Grundgesetzes, Art. 12 der Verfassung des Landes Hessen), die informationelle Selbstbestimmung und Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme (Art. 12a der Verfassung des Landes Hessen) und die Unverletzlichkeit der Wohnung (Art. 13 Abs. 1 des Grundgesetzes, Art. 8 der Verfassung des Landes Hessen) eingeschränkt werden.

(2) Aufgrund des Art. 2a können die Grundrechte auf das Brief-, Post- und Fernmeldegeheimnis (Art. 10 Abs. 1 des Grundgesetzes, Art. 12 der Verfassung des Landes Hessen), die informationelle Selbstbestimmung und Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme (Art. 12a der Verfassung des Landes Hessen) und die Unverletzlichkeit der Wohnung (Art. 13 des Grundgesetzes, Art. 8 der Verfassung des Landes Hessen) eingeschränkt werden.

(3) Aufgrund des Art. 3 kann das Grundrecht auf die Eigentumsgarantie nach Art. 45 Abs. 1 der Verfassung des Landes Hessen eingeschränkt werden.

Artikel 6⁷⁾

Aufhebung bisherigen Rechts

Das Hessische Verfassungsschutzgesetz in der Fassung der Bekanntmachung vom 20. Juli 2023 (GVBl. S. 614) wird aufgehoben.

⁶⁾ Ändert FFN 323-153

⁷⁾ Hebt auf FFN 18-7

Artikel 7

Inkrafttreten

Dieses Gesetz tritt am Tag nach der Verkündung in Kraft.

Die verfassungsmäßigen Rechte der Landesregierung sind gewahrt.

Das vorstehende Gesetz wird hiermit ausgefertigt. Es ist im Gesetz- und Verordnungsblatt für das Land Hessen zu verkünden.

Wiesbaden, den 10. Dezember 2025

Der Hessische Ministerpräsident

Rhein

Der Hessische Minister des Innern, für Sicherheit und Heimatschutz

Prof. Dr. Poseck

Hessische Staatskanzlei