Der Landtag hat das folgende Gesetz beschlossen:

Hessisches Gesetz zum Schutz der elektronischen Verwaltung (Hessisches IT-Sicherheitsgesetz - HITSiG)*)

Vom 29. Juni 2023

ERSTER TEIL
Allgemeine Vorschriften

§ 1
Geltungsbereich

Soweit andere Rechtsvorschriften nicht entgegenstehen, gilt dieses Gesetz für die Verwaltungstätigkeit mittels Informationstechnik

1. der Behörden und sonstigen öffentlichen Stellen des Landes sowie nicht öffentlicher Stellen, soweit sie hoheitliche Aufgaben unter Aufsicht der vorgenannten Stellen wahrnehmen,
2. der nicht unter Nr. 3 fallenden der Aufsicht des Landes unterstehenden juristischen Personen des öffentlichen Rechts und deren Vereinigungen ungeachtet ihrer Rechtsform sowie nicht öffentlicher Stellen, soweit sie hoheitliche Aufgaben unter Aufsicht der vorgenannten Stellen wahrnehmen,
3. der Behörden und sonstigen öffentlichen Stellen der Gemeinden und Gemeindeverbände sowie nicht öffentlicher Stellen, soweit sie hoheitliche Aufgaben unter Aufsicht der vorgenannten Stellen wahrnehmen.

§ 2
Begriffsbestimmungen

Im Sinne dieses Gesetzes

1. ist Informationstechnik jedes technische Mittel zur Verarbeitung von Informationen,
2. ist Informationssicherheit die Einhaltung bestimmter Sicherheitsstandards, die die Verfügbarkeit, Integrität oder Vertraulichkeit (Schutzziele) von Informationen betreffen, durch Sicherheitsvorkehrungen
   a) in informationstechnischen Systemen, Komponenten oder Prozessen oder
   b) bei der Anwendung von informationstechnischen Systemen, Komponenten oder Prozessen,
3. sind Schadprogramme Programme und sonstige informationstechnische Routinen und Verfahren, die dem Zweck dienen, unbefugt
   a) Daten zu nutzen oder zu löschen oder
   b) auf sonstige informationstechnische Abläufe einzuwirken,
4. sind Sicherheitslücken Eigenschaften von Programmen oder sonstigen informationstechnischen Systemen, durch deren Ausnutzung es möglich ist, dass sich Dritte gegen den Willen der Berechtigten Zugang zu fremden informationstechnischen Systemen verschaffen oder die Funktion der informationstechnischen Systeme beeinflussen können,
5. sind Übergabe- und Knotenpunkte IT-Systeme, über die der Datenverkehr in ein anderes Netz fließt (Übergabepunkt) oder innerhalb eines Netzes verteilt wird (Knotenpunkt),
6. sind Protokolldaten Steuerdaten eines informationstechnischen Protokolls zur Datenübertragung, die unabhängig vom Inhalt eines Kommunikationsvorgangs übertragen oder auf den am Kommunikationsvorgang beteiligten Servern gespeichert werden und zur Gewährleistung der Kommunikation zwischen Empfänger und Sender notwendig sind; Protokolldaten können Verkehrsdaten nach § 3 Nr. 70 des Telekommunikationsgesetzes vom 23. Juni 2021 (BGBl. I S. 1858), zuletzt geändert durch Gesetz vom 20. Juli 2022 (BGBl. I S. 1166), und Nutzungsdaten nach § 2 Abs. 2 Nr. 3 des Telekommunikation-Telemedien-Datenschutz-Gesetzes vom 23. Juni 2021 (BGBl. I S. 1982; 2022 I S. 1045), zuletzt geändert durch Gesetz vom 12. August 2021 (BGBl. I S. 3544; 2022 I S. 1045), enthalten.

§ 3
Grundsätze der Informationssicherheit

(1) Die Stellen nach § 1 Nr. 1 und 2, mit Ausnahme der Schulen in öffentlicher Trägerschaft sowie genehmigter und anerkannter Ersatzschulen im Sinne des Hessischen Schulgesetzes, treffen angemessene technische und organisatorische Maßnahmen zur Gewährleistung der Informationssicherheit. Hierbei soll der Stand der Technik maßgeblich sein. Maßnahmen sind angemessen, wenn der dafür erforderliche Aufwand nicht außer Verhältnis zu den möglichen Folgen der Verletzung der Schutzziele steht. Um die Erreichung und Aufrechterhaltung eines angemessenen Informationssicherheitsniveaus zu gewährleisten, haben die Stellen nach § 1 Nr. 1 und 2 sich an der IT-Grundschutzmethodik des Bundesamtes für Sicherheit in der Informationstechnik zu orientieren und setzen ein Informationssicherheitsmanagementsystem um.

(2) Die jeweils geltenden Standards und das jeweils geltende IT-Grundschutz-Kompendium des Bundesamtes für Sicherheit in der Informationstechnik werden zur Anwendung empfohlen. Werden dem Land Hessen Informationssicherheitsstandards verbindlich durch Beschlüsse des IT-Planungsrates nach Art. 91c Abs. 2 Satz 1 des Grundgesetzes für die Bundesrepublik Deutschland i. V. m. § 1 Abs. 1 Satz 1 Nr. 2 des IT-Staatsvertrages vom 30. Oktober 2009 bis 30. November 2009 (GVBl. I 2010 S. 65, 66), geändert durch Staatsvertrag vom 15. März 2019 bis

*) FFN 210-105

21. März 2019 (GVBl. S. 150, 151), vorgeschrieben oder nach § 5 des Onlinezugangsgesetzes vom 14. August 2017 (BGBl. I S. 3122, 3138), zuletzt geändert durch Gesetz vom 28. Juni 2021 (BGBl. I S. 2250), in der jeweils geltenden Fassung, festgelegt, sind diese Standards durch die Stellen nach § 1 Nr. 1 und 2 bei den von ihnen eingesetzten informationstechnischen Systemen einzuhalten.

(3) Die Verantwortung für die Gewährleistung der Informationssicherheit im Sinne des Abs. 1 trägt die jeweilige Leiterin oder der Leiter der Stelle für ihren oder seinen jeweiligen Verantwortungsbereich. Sie oder er stellt im Rahmen der ihr oder ihm zugewiesenen Aufgaben und Befugnisse die erforderlichen personellen und finanziellen Ressourcen zur Verfügung. Für jede Stelle nach § 1 Nr. 1 und 2 ist eine Informationssicherheitsbeauftragte oder ein Informationssicherheitsbeauftragter und deren oder dessen Vertretung zu benennen. Für die Geschäftsbereiche der Staatskanzlei und der Ministerien der hessischen Landesverwaltung sind jeweils zentrale Informationssicherheitsbeauftragte des Geschäftsbereichs (Ressort-ISB) zu benennen; diese unterstützen die Leitung des Geschäftsbereichs in Belangen der Informationssicherheit.

(4) Wesentliche Änderungen an den informationstechnischen Systemen einer Stelle nach § 1 Nr. 1 und 2 dürfen nur im Benehmen mit der oder dem nach Abs. 3 Satz 3 benannten Informationssicherheitsbeauftragten durchgeführt werden.

(5) Den Stellen nach § 1 Nr. 3 und den Schulen in öffentlicher Trägerschaft sowie den genehmigten und anerkannten Ersatzschulen im Sinne des Hessischen Schulgesetzes wird die Einhaltung der Grundsätze nach Abs. 1 bis 4 empfohlen.

ZWEITER TEIL

Organisation

§ 4

Die oder der Zentrale Informationssicherheitsbeauftragte der Landesverwaltung

(1) Auf Vorschlag der für IT- und Cybersicherheit in der Landesverwaltung zuständigen Ministerin oder des hierfür zuständigen Ministers setzt die Landesregierung zur Gewährleistung der Informationssicherheit in der Landesverwaltung eine Zentrale Informationssicherheitsbeauftragte oder einen Zentralen Informationssicherheitsbeauftragten (Chief Information Security Officer, CISO) ein. Die oder der CISO ist ressortübergreifend tätig, hat ein umfassendes Informationsrecht und ist von den Dienststellen der Landesverwaltung bei ihrer oder seiner Aufgabenerfüllung zu unterstützen, soweit Rechtsvorschriften nicht entgegenstehen. Er oder sie koordiniert ressortübergreifende Informationssicherheitsthemen und nimmt die Außenvertretung der hessischen Landesverwaltung in Belangen der Informationssicherheit wahr.

(2) Die Aufgaben der oder des CISO umfassen insbesondere

1. die Fortschreibung der Informationssicherheitsleitlinie der hessischen Landesverwaltung in Abstimmung mit der Staatskanzlei und den Ministerien und die kontinuierliche Verbesserung der Informationssicherheit in der Landesverwaltung,
2. die Beratung der Beauftragten oder des Beauftragten der Landesregierung für E-Government und Informationstechnik (CIO), der Staatskanzlei und der Ministerien sowie die Entwicklung von Empfehlungen in Fragen der Informationssicherheit,
3. die Koordinierung der Abwehrmaßnahmen nach § 5 Abs. 2 Satz 1 Nr. 2,
4. regelmäßige Berichte an die Landesregierung über den Sachstand der Informationssicherheit in der Landesverwaltung sowie über Maßnahmen und Anordnungen nach Abs. 3,
5. die Koordinierung des IT-Krisenmanagements der Landesverwaltung.

(3) Die oder der CISO ist berechtigt, zur Erfüllung der Aufgaben nach Abs. 2, insbesondere bei dienststellenübergreifenden informationstechnischen Sicherheitsvorfällen, unter Einbeziehung des jeweils betroffenen Geschäftsbereichs Maßnahmen zu empfehlen. Bei unmittelbaren und erheblichen Gefahren für die Informationssicherheit in der Landesverwaltung kann er oder sie erforderliche Sicherheitsmaßnahmen anordnen; die betroffenen Stellen sind unverzüglich zu informieren.

(4) Die oder der CISO hat ein Vortragsrecht bei der für IT- und Cybersicherheit in der Landesverwaltung zuständigen Ministerin oder dem hierfür zuständigen Minister und bei der oder dem CIO. Bei schwerwiegenden Anlässen hat die oder der CISO ein Vortragsrecht bei den Staatssekretärinnen oder Staatssekretären der Ministerien und bei der Chefin oder dem Chef der Staatskanzlei.

§ 5

Zentrum für Informationssicherheit

(1) Die für IT- und Cybersicherheit in der Landesverwaltung zuständige Ministerin oder der hierfür zuständige Minister richtet zur Förderung der Informationssicherheit ein Zentrum für Informationssicherheit ein.

(2) Das Zentrum für Informationssicherheit nimmt folgende Aufgaben wahr:

1. die Zusammenarbeit mit den für die Informationssicherheit zuständigen zentralen Stellen des Bundes, der anderen Länder, der Kommunen und privater Dritter, unbeschadet besonderer Zuständigkeiten anderer Stellen,
2. die Erkennung, Untersuchung und Abwehr von Gefahren für die Informationssicherheit der Stellen nach § 1 Nr. 1 und 2,
3. die Unterstützung bei der Erkennung, Untersuchung und Abwehr von Gefahren für die Informationssicherheit der Stellen nach § 1 Nr. 3 auf deren Ersuchen,
4. die Unterstützung bei der Wiederherstellung der Sicherheit oder Funktionsfähigkeit informationstechnischer Systeme in

herausgehobenen Fällen der Beeinträchtigung nach § 16,

5. die technische Unterstützung und Beratung auf Ersuchen
   a) der Polizei- und Strafverfolgungsbehörden,
   b) des Landesamts für Verfassungsschutz,
   c) der oder des Hessischen Beauftragten für Datenschutz und Informationsfreiheit

   im Zusammenhang mit Tätigkeiten oder Ereignissen, die gegen die Informationssicherheit gerichtet sind oder die unter Nutzung der Informationstechnik erfolgen,
6. die Unterstützung des Krisenstabs der Landesregierung,
7. die Sammlung und Auswertung von Informationen über Risiken, Beeinträchtigungen, Störungen und Vorkehrungen zur Abwehr von Gefahren für die Informationssicherheit,
8. die Information der Stellen nach § 1 sowie Dritter über die nach Nr. 7 gewonnenen Erkenntnisse, soweit dies zur Erfüllung ihrer staatlichen Aufgaben oder zur Wahrung ihrer Sicherheitsinteressen erforderlich ist,
9. die Beratung, Warnung und Empfehlung in Fragen der Informationssicherheit, einschließlich der Erstellung einer werktäglichen Übersicht, sowie im Zusammenhang mit Tätigkeiten oder Ereignissen, die die öffentliche Sicherheit oder Ordnung beeinträchtigen und unter Nutzung der Informationstechnik erfolgen,
10. die Entgegennahme von Sofortmeldungen aus der Landesverwaltung und die Koordinierung der Bearbeitung von Sicherheitsvorfällen,
11. die Untersuchung von Sicherheitsrisiken bei der Anwendung der Informationstechnik sowie der Test von vorhandenen Verfahren und Werkzeugen sowie deren Entwicklung zur Erkennung und Abwehr von Gefahren für die Informationssicherheit in Zusammenarbeit mit Wissenschaft und Forschung.

Ersuchen nach Satz 1 Nr. 5 sind durch das Zentrum für Informationssicherheit aktenkundig zu machen.

(3) Bestandteil des Zentrums für Informationssicherheit ist das Computer Emergency Response Team (CERT), durch das Teile der in Abs. 2 genannten Aufgaben wahrgenommen werden. Das CERT ist zentrale Kontaktstelle nach § 8b Abs. 2 Nr. 4 Buchst. c des BSI-Gesetzes in der Fassung der Bekanntmachung vom 14. August 2009 (BGBl. I S. 2821), zuletzt geändert durch Gesetz vom 23. Juni 2021 (BGBl. I S. 1982). Das CERT unterhält Mobile Incident Response Teams (MIRTs), die die Stellen nach § 1 bei der Wiederherstellung ihrer IT-Systeme nach § 16 unterstützen. Das CERT kann seine Dienstleistungen neben den in § 1 genannten Stellen auch privaten Unternehmen im Land Hessen anbieten, sofern die Kapazitäten des CERT dies erlauben; ein Anspruch privater Unternehmen auf eine Dienstleistung seitens des CERT besteht nicht.

§ 6

Zentraler IT-Dienstleister des Landes

Der zentrale IT-Dienstleister des Landes gewährleistet die Informationssicherheit im Landesdatennetz und der von ihm betriebenen informationstechnischen Systeme und berät das Zentrum für Informationssicherheit bei der Erledigung seiner Aufgaben, soweit diese die Informationssicherheit in der Landesverwaltung betreffen. Er berichtet der oder dem CISO zum Stand der Informationssicherheit in der Landesverwaltung.

DRITTER TEIL

Maßnahmen

§ 7

Datenverarbeitung

(1) Das Zentrum für Informationssicherheit darf personenbezogene Daten verarbeiten, wenn die Verarbeitung zur Erfüllung seiner im öffentlichen Interesse liegenden Aufgaben erforderlich ist.

(2) Die Verarbeitung personenbezogener Daten durch das Zentrum für Informationssicherheit zu anderen Zwecken als demjenigen, zu dem die Daten ursprünglich erhoben wurden, ist unbeschadet des Art. 6 Abs. 4 der Datenschutz-Grundverordnung und des § 21 des Hessischen Datenschutz- und Informationsfreiheitsgesetzes zulässig, wenn

1. die Verarbeitung erforderlich ist
   a) zur Sammlung, Auswertung oder Untersuchung von Informationen über Risiken oder Vorkehrungen für die Informationssicherheit oder
   b) zur Unterstützung, Beratung oder Warnung in Fragen der Informationssicherheit und
2. kein Grund zu der Annahme besteht, dass das schutzwürdige Interesse der betroffenen Person an dem Ausschluss der Verarbeitung überwiegt.

Eine Verarbeitung von besonderen Kategorien personenbezogener Daten durch das Zentrum für Informationssicherheit ist abweichend von Art. 9 Abs. 1 der Datenschutz-Grundverordnung und unbeschadet des § 20 Abs. 1 des Hessischen Datenschutz- und Informationsfreiheitsgesetzes zulässig, wenn

1. die Verarbeitung erforderlich ist zur Abwehr einer erheblichen Gefahr für die Informationssicherheit,
2. ein Ausschluss dieser Daten von der Verarbeitung die Erfüllung der Aufgaben des Zentrums für Informationssicherheit unmöglich machen oder diese erheblich gefährden würde und
3. kein Grund zu der Annahme besteht, dass das schutzwürdige Interesse der betroffenen Person an dem Ausschluss dieser Daten von der Verarbeitung überwiegt.

Im Fall des Satz 2 sind angemessene und spezifische Maßnahmen zur Wahrung der Interessen der betroffenen Person nach § 20 Abs. 2 Satz 2 des Hessischen Datenschutz- und Informationsfreiheitsgesetzes vorzusehen.

(3) Ist die Verarbeitung der Daten über den Abschluss des Auswertungsvorgangs hinaus erforderlich, sind darin enthaltene personenbezogene Daten unverzüglich automatisiert zu anonymisieren. Ist eine Verarbeitung der Daten im Sinne des Satz 1 mit anonymisierten personenbezogenen Daten nicht möglich, sind für die weitere Verarbeitung der personenbezogenen Daten die §§ 10, 11, 13 und 17 entsprechend anzuwenden.

(4) Soweit die Auswertungen nach §§ 7 bis 11 ein Schadprogramm identifizieren, kann dieses jederzeit beseitigt oder in seiner Funktionsweise gehindert werden.

(5) Die Verwendungsbeschränkungen nach § 7 Abs. 3 und §§ 8 bis 11 betreffen nur Daten, die dem Fernmeldegeheimnis aus Art. 10 des Grundgesetzes für die Bundesrepublik Deutschland unterliegen oder einen Personenbezug aufweisen.

§ 8

Verwendung von auf informationstechnischen Systemen gespeicherten Daten

(1) Die auf den informationstechnischen Systemen der Stellen nach § 1 sowie auf sonstigen informationstechnischen Systemen, die mit dem Landesdatennetz verbunden sind, gespeicherten Protokolldaten von:

1. Firewall-Systemen,
2. Systemen zur Erkennung und Beseitigung von Schadsoftware,
3. Systemen zur Erkennung von unerwünschten E-Mails,
4. Datenbankservern,
5. Web-, Proxy- und Anwendungsservern und
6. der Betriebssoftware von Computersystemen

dürfen automatisiert ausgewertet werden, soweit dies zum Erkennen, Eingrenzen, Nachverfolgen oder Beseitigen von Störungen oder Fehlern oder zum Erkennen und Abwehren von Gefahren für die Informationssicherheit durch Sicherheitslücken, Schadprogramme oder erfolgte oder versuchte Angriffe auf die Informationstechnik der Stellen nach § 1 erforderlich ist.

(2) Eine Auswertung von während der automatisierten Verarbeitung nach Abs. 1 anfallenden Inhaltsdaten ist nur unter den Voraussetzungen des § 11 zulässig. Die Daten der Auswertung nach Abs. 1 sind nach ihrer automatisierten Auswertung unverzüglich zu löschen, es sei denn, §§ 10 oder 11 sehen eine weitere Verwendung vor.

§ 9

Erhebung und Auswertung des Datenverkehrs im Landesdatennetz

(1) Soweit dies zum Erkennen und Abwehren von Gefahren für die Informationssicherheit durch Sicherheitslücken, Schadprogramme oder erfolgte oder versuchte Angriffe auf die Informationstechnik der Stellen nach § 1 erforderlich ist, darf der an den Übergabe- und Knotenpunkten des Landesdatennetzes anfallende Datenverkehr automatisiert erhoben und dürfen

1. der Erhebungszeitpunkt, die IP-Adresse einschließlich der Subnetzmaske, die Präfixlänge, der Port und die Medienzugriffskontrolladresse (Media-Access-Control-Address, MAC-Adresse), der vollständige Domänenname sowie die Kopf- und Statusdaten von Netzwerkpaketen für ein- und ausgehende Verbindungen,
2. für ein- und ausgehende Verbindung auf Basis der Hypertext-Übertragungsprotokolle (Hypertext Transfer Protocol, HTTP, und Hypertext Transfer Protocol Secure, HTTPS) zusätzlich zu Nr. 1 der vollständige einheitliche Ressourcenzeiger (Uniform Resource Locator, URL) und die Kopfdaten exklusive Cookie,

unverzüglich automatisiert ausgewertet werden.

(2) Eine Auswertung des während der automatisierten Erhebung des Datenverkehrs nach Abs. 1 anfallenden Inhalts der Kommunikation ist nur unter den Voraussetzungen des § 11 zulässig. Die nach Abs. 1 erhobenen Daten sowie die Daten der Auswertung sind nach der automatisierten Auswertung unverzüglich zu löschen, es sei denn, die §§ 10 oder 11 sehen eine weitere Verwendung vor.

§ 10

Auswertung ohne Inhaltsdaten

(1) Soweit die automatisierte Auswertung nach § 8 Abs. 1 oder § 9 Abs. 1 zureichende tatsächliche Anhaltspunkte dafür bietet, dass bestimmte Daten zur Abwehr von Gefahren im Sinne von § 8 Abs. 1 oder § 9 Abs. 1 erforderlich sind, dürfen diese für höchstens 90 Tage gespeichert werden. Die Daten sind unverzüglich automatisiert zu pseudonymisieren, soweit dies technisch möglich ist und die Daten nicht bereits pseudonym vorliegen. Die weitere Auswertung der nach Satz 1 gespeicherten Daten erfolgt nur automatisiert.

(2) Eine über Abs. 1 hinausgehende, insbesondere nicht automatisierte oder direkt personenbezogene Verarbeitung der Daten nach § 8 Abs. 1 und § 9 Abs. 1 ist nur zulässig, soweit und solange

1. hinreichende tatsächliche Anhaltspunkte den Verdacht begründen, dass
   a) die Daten ein Schadprogramm enthalten,
   b) die Daten durch einen Angriff oder ein Schadprogramm verursacht wurden oder
   c) sich aus den Daten Hinweise auf einen Angriff oder ein Schadprogramm ergeben können und
2. die Datenverarbeitung zur Abwehr des Schadprogramms oder Angriffs, zur Abwehr von Gefahren, die von dem Schadprogramm oder Angriff ausgehen, oder zur Erkennung und Abwehr anderer Schadprogramme oder Angriffe erforderlich ist.

Die Datenverarbeitung nach Satz 1 bedarf der Anordnung durch die Leiterin oder den Leiter der nach § 12 zur Ergreifung der Maßnahme zuständigen Stelle. Sofern das Zentrum für Informationssicherheit zuständige Stelle ist, darf die Anordnung nur durch eine Beschäftigte oder einen Beschäftigten des für IT- und Cybersicherheit in der Landesverwaltung zuständigen Geschäftsbereichs mit der Befähigung zum Richteramt getroffen werden.

§ 11

Auswertung von Inhaltsdaten

(1) Nach § 8 Abs. 1 und § 9 Abs. 1 verarbeitete Daten dürfen unverzüglich automatisiert nach technischen Indikatoren für Schadprogramme ausgewertet werden. Die nach Satz 1 ausgewerteten Daten sind nach ihrer automatisierten Auswertung unverzüglich zu löschen, es sei denn, die nachfolgenden Absätze sehen eine weitere Verwendung vor.

(2) Soweit die automatisierte Auswertung nach Abs. 1 zureichende tatsächliche Anhaltspunkte dafür bietet, dass bestimmte Daten zum Schutz vor Schadprogrammen erforderlich sind, dürfen diese für höchstens 90 Tage gespeichert werden. Die Daten sind unverzüglich automatisiert zu pseudonymisieren, soweit sie nicht bereits pseudonym sind. Die weitere Auswertung der nach Satz 1 und 2 gespeicherten Daten erfolgt nur automatisiert. Die Datenverarbeitung nach Satz 1 bedarf der Anordnung durch die Leiterin oder den Leiter der nach § 12 zur Ergreifung der Maßnahme zuständigen Stelle. Sofern das Zentrum für Informationssicherheit zuständige Stelle ist, darf die Anordnung nur durch eine Beschäftigte oder einen Beschäftigten des für IT- und Cybersicherheit in der Landesverwaltung zuständigen Geschäftsbereichs mit der Befähigung zum Richteramt getroffen werden.

(3) Eine über die Abs. 1 und 2 hinausgehende, insbesondere nicht automatisierte oder direkt personenbezogene Auswertung der Daten nach Abs. 1 Satz 1 ist nur zulässig, soweit und solange

1. hinreichende tatsächliche Anhaltspunkte den Verdacht begründen, dass
   a) die Daten durch ein Schadprogramm verursacht wurden oder
   b) sich aus den Daten Hinweise auf ein Schadprogramm ergeben und
2. die Datenverarbeitung zur Abwehr des Schadprogramms, zur Abwehr von Gefahren, die von dem Schadprogramm ausgehen oder zur Erkennung und Abwehr anderer Schadprogramme erforderlich ist.

Die Datenverarbeitung nach Satz 1 ebenso wie eine erforderliche Wiederherstellung des Personenbezugs bereits pseudonymisierter Daten bedarf der Anordnung durch die Leiterin oder den Leiter der nach § 12 zur Ergreifung der Maßnahme zuständigen Stelle. Sofern das Zentrum für Informationssicherheit zuständige Stelle ist, darf die Anordnung nur durch eine Beschäftigte oder einen Beschäftigten des für IT- und Cybersicherheit in der Landesverwaltung zuständigen Ministeriums mit der Befähigung zum Richteramt getroffen werden.

(4) Soweit möglich, ist bei der Datenverarbeitung nach Abs. 1 bis 3 technisch sicherzustellen, dass Daten, die den Kernbereich privater Lebensgestaltung betreffen, nicht erhoben werden. Werden aufgrund der Maßnahmen nach Abs. 1 bis 3 Erkenntnisse aus dem Kernbereich privater Lebensgestaltung erlangt, dürfen diese nicht verwendet werden. Auswertungsergebnisse, die den Kernbereich privater Lebensgestaltung betreffen, sind unverzüglich zu löschen. Dies gilt auch in Zweifelsfällen. Die Erlangung und Löschung ist zu dokumentieren. Die Dokumentation darf ausschließlich für Zwecke der nachträglichen Überprüfung der Rechtmäßigkeit der Verarbeitung verwendet werden. Sie ist zu löschen, wenn sie für diese Zwecke nicht mehr erforderlich ist, spätestens jedoch zum Ablauf des Kalenderjahres, das dem Jahr der Dokumentation folgt. Satz 1 bis 6 gelten nicht, sofern für die Verarbeitung der in Satz 1 bis 3 genannten Daten eine Ausnahmeregelung nach Art. 9 Abs. 2 oder 3 der Datenschutz-Grundverordnung oder nach dem Hessischen Datenschutz- und Informationsfreiheitsgesetz greift.

§ 12

Zuständigkeit

(1) Soweit das Landesdatennetz einschließlich der Übergabe- und Knotenpunkte oder die informationstechnischen Systeme der Stellen nach § 1 Nr. 1 und 2 betroffen sind, ist das Zentrum für Informationssicherheit für die Ergreifung der Maßnahmen nach §§ 8 bis 11 zuständig. Dies betrifft alle Systeme, Verfahren und Plattformen, die beim zentralen IT-Dienstleister des Landes betrieben und für mehrere Geschäftsbereiche bestimmt sind. Die Bereitstellung von Daten oder von Analyseergebnissen zu Daten, die nicht vom zentralen IT-Dienstleister verarbeitet werden oder für einen einzelnen Geschäftsbereich verarbeitet werden, sind in einer Landesrichtlinie zu regeln. Daten des Hessischen Landtags, des Hessischen Rechnungshofs, des Hessischen Beauftragten für Datenschutz und Informationsfreiheit, der Gerichte und Staatsanwaltschaften sowie der Hochschulen nach § 2 des Hessischen Hochschulgesetzes dürfen nur einvernehmlich mit diesen verarbeitet werden. Daten, die dem richterlichen, staatsanwaltschaftlichen oder rechtspflegerischen Arbeitsprozess oder der Abgeordnetentätigkeit zuzurechnen sind, dürfen von dem Zentrum für Informationssicherheit nicht verarbeitet werden.

(2) Die Stellen nach § 1 sind für die Ergreifung der Maßnahmen nach §§ 8 bis 11 für ihren Verantwortungsbereich zuständig. Sie können das Zentrum für Informationssicherheit mit den erforderlichen Maßnahmen nach §§ 8 bis 11 im Wege der Auftragsverarbeitung im Sinne von Art. 28 der Datenschutz-Grundverordnung betrauen, sofern die Kapazitäten des Zentrums für Informationssicherheit dies erlauben. Ein Anspruch auf Übernahme der Maßnahmen durch das Zentrum für Informationssicherheit besteht nicht.

§ 13

Übermittlung personenbezogener oder dem Fernmeldegeheimnis unterliegender Daten

(1) Die nach § 12 zuständigen Stellen können die jeweils von ihnen nach § 10 Abs. 2 und § 11 Abs. 3 verarbeiteten personenbezogenen oder dem Fernmeldegeheimnis unterliegenden Daten an die für den Betrieb der Informationstechnik der Verwaltung zuständigen Stellen oder damit beauftragte Dritte übermitteln, wenn und soweit dies zur Abwehr oder Beseitigung von Gefahren für die Informationssicherheit erforderlich ist.

(2) Die nach § 12 zuständigen Stellen können die jeweils von ihnen nach § 10 Abs. 2 und § 11 Abs. 3 verarbeiteten personenbezogenen oder dem Fernmeldegeheimnis unterliegenden Daten an die Strafverfolgungsbehörden zur Verfolgung einer mittels eines Schadprogramms begangenen Straftat nach den §§ 202a, 202b, 202c, 269, 271, 274 Abs. 1 Nr. 2, §§ 303a, 303b und 348 des Strafgesetzbuches übermitteln. Sie können diese Daten ferner übermitteln

1. zur Abwehr einer Gefahr für die öffentliche Sicherheit, die unmittelbar von einem Schadprogramm ausgeht, an die Polizeibehörden,
2. zur Unterrichtung über Tatsachen, die sicherheitsgefährdende oder geheimdienstliche Tätigkeiten für eine fremde Macht oder einen internationalen kriminellen, terroristischen oder staatlichen Angriff mittels Schadprogrammen oder vergleichbaren schädlich wirkenden informationstechnischen Mitteln auf die Vertraulichkeit, Integrität oder Verfügbarkeit von IT-Systemen in Fällen von erheblicher Bedeutung mit Bezug zur Bundesrepublik Deutschland oder zum Land Hessen erkennen lassen, an das Landesamt für Verfassungsschutz Hessen.

(3) Für sonstige Zwecke können die nach § 12 zuständigen Stellen übermitteln

1. an die Strafverfolgungsbehörden zur Verfolgung einer Straftat von auch im Einzelfall erheblicher Bedeutung, insbesondere einer in § 100a Abs. 2 der Strafprozessordnung bezeichneten Straftat,
2. an die Polizeibehörden zur Abwehr einer Gefahr für den Bestand oder die Sicherheit des Staates oder für Leib, Leben oder Freiheit einer Person oder für Sachen von bedeutendem Wert, deren Erhalt im öffentlichen Interesse geboten ist.

Die Übermittlung nach Satz 1 bedarf der vorherigen gerichtlichen Zustimmung. Für das Verfahren gelten die Vorschriften des Gesetzes über das Verfahren in Familiensachen und in den Angelegenheiten der freiwilligen Gerichtsbarkeit entsprechend. Zuständig ist das Amtsgericht, in dessen Bezirk die nach § 12 zuständige Stelle ihren Sitz hat.

(4) Ist das Zentrum für Informationssicherheit in den Fällen des Abs. 2 zuständige Stelle nach § 12, darf es die nach § 10 Abs. 2 und § 11 Abs. 3 verarbeiteten personenbezogenen oder dem Fernmeldegeheimnis unterliegenden Daten auch abweichend von § 10 Abs. 2 und § 11 Abs. 3 bis zur Beendigung der Unterstützung der Behörden, an die die Daten übermittelt wurden, weiterverarbeiten. § 11 Abs. 4 bleibt unberührt.

§ 14

Gewährleistung der Informationssicherheit und des Datenschutzes

(1) Die nach §§ 8 bis 11 erhobenen oder gespeicherten Daten sind durch technische und organisatorische Maßnahmen nach dem Stand der Technik gegen unbefugte Kenntnisnahme, Veränderung und Verwendung zu schützen. Bei der Umsetzung dieser Maßnahmen ist ein besonders hohes Maß an Informationssicherheit zu gewährleisten.

(2) Die zu treffenden Maßnahmen umfassen insbesondere

1. die organisatorische Trennung von den für die üblichen Aufgaben des IT-Betriebs verantwortlichen Organisationseinheiten,
2. die technische Trennung von den für die üblichen Aufgaben des IT-Betriebs vorgehaltenen informationstechnischen Systemen, insbesondere die Speicherung in gesonderten, von den für die üblichen betrieblichen Aufgaben getrennten Speichereinrichtungen,
3. besondere Sicherungsmaßnahmen gegen unberechtigte Zugriffe aus anderen Netzen, insbesondere aus dem Internet,
4. die Umsetzung von Maßnahmen nach dem Stand der Technik zur Gewährleistung der Vertraulichkeit, Integrität und Verfügbarkeit der gespeicherten Daten,
5. die Beschränkung des Zutritts zu den und des Zugriffs auf die Datenverarbeitungsanlagen auf Personen, die durch die jeweilige Leitung der Stelle hierzu besonders ermächtigt sind, und
6. das Zusammenwirken von mindestens zwei Personen beim Zugriff auf die Daten.

(3) Zum Zwecke der Datenschutzkontrolle ist jeder Zugriff auf die Datenverarbeitungsanlagen, insbesondere das Lesen, Kopieren, Ändern, Löschen und Sperren von den nach §§ 8 bis 11 erhobenen oder gespeicherten Daten, in einem Protokoll aufzunehmen. Das Protokoll hat Zeitpunkt und Art des Zugriffs sowie eine eindeutige Kennung der auf die Daten zugreifenden Personen zu enthalten. Das Protokoll darf ausschließlich zum Zwecke der Rechtmäßigkeitskontrolle verwendet werden. Die Einträge in das Protokoll sind nach zwölf Monaten zu löschen.

(4) Der oder dem Hessischen Datenschutzbeauftragten ist durch das Zentrum für Informationssicherheit einmal im Jahr eine Aufstellung über die nach den §§ 8 bis 11, 13 und 16 erfolgten Verarbeitungen vorzulegen. Inhalt und Frist der Aufstellung erfolgen im Einvernehmen mit der oder dem Hessischen Datenschutzbeauftragten. Soweit Daten der hessischen Justiz betroffen sind, ist eine Aufstellung über die betreffenden Verarbeitungen zusätzlich dem Kontrollgremium bei der IT-Stelle der hessischen Justiz vorzulegen. Das Kontrollgremium ist berechtigt, Auskünfte zu verlangen und Einsicht in die Datenverarbeitungen durch das Zentrum für Informationssicherheit zu nehmen.

§ 15

Sicherheitskonzept

Maßnahmen nach den §§ 7 bis 11 dürfen nur ergriffen werden, wenn ein Sicherheitskonzept erstellt wurde und die Umsetzung aller darin vorgesehenen technischen und organisatorischen Maßnahmen von der zuständigen Stelle aktenkundig gemacht wurde. Das Sicherheitskonzept ist vor jeder wesentlichen Veränderung der eingesetzten technischen Systeme zu aktualisieren und alle zwei Jahre einer Revision zu unterziehen. Für jede wesentliche Veränderung des Sicherheitskonzeptes gilt Satz 1 entsprechend.

§ 16

Wiederherstellung der Sicherheit oder Funktionsfähigkeit informationstechnischer Systeme in herausgehobenen Fällen der Beeinträchtigung

(1) Handelt es sich bei einer Beeinträchtigung der Sicherheit oder Funktionsfähigkeit eines informationstechnischen Systems einer Stelle nach § 1 um einen herausgehobenen Fall, so kann das Zentrum für Informationssicherheit auf Ersuchen der betroffenen Stelle die Maßnahmen treffen, die zur Wiederherstellung der Sicherheit oder Funktionsfähigkeit des betroffenen informationstechnischen Systems erforderlich sind. Sofern Notfallkonzepte bei der betroffenen Stelle vorhanden sind, ist auf diese zurückzugreifen.

(2) Ein herausgehobener Fall nach Abs. 1 liegt insbesondere dann vor, wenn es sich um einen Angriff von besonderer technischer Qualität handelt oder die zügige Wiederherstellung der Sicherheit oder Funktionsfähigkeit des betroffenen informationstechnischen Systems von besonderem öffentlichen Interesse ist.

(3) Das Zentrum für Informationssicherheit darf bei Maßnahmen nach Abs. 1 personenbezogene oder dem Fernmeldegeheimnis unterliegende Daten verarbeiten, soweit dies zur Wiederherstellung der Sicherheit oder Funktionsfähigkeit des betroffenen informationstechnischen Systems erforderlich und angemessen ist. Die Daten sind unverzüglich zu löschen, sobald sie für die Wiederherstellung der Sicherheit oder Funktionsfähigkeit des informationstechnischen Systems nicht mehr benötigt werden. Wenn die Daten nach Abs. 4 an eine andere Behörde zur Erfüllung von deren gesetzlichen Aufgaben übermittelt worden sind, darf das Zentrum für Informationssicherheit die Daten abweichend von Satz 2 bis zur Beendigung der Unterstützung dieser Behörde weiterverarbeiten. Eine Nutzung zu anderen Zwecken ist unzulässig. § 11 Abs. 4 ist entsprechend anzuwenden. Im Übrigen sind die Regelungen der Datenschutz-Grundverordnung und des Hessischen Datenschutz- und Informationsfreiheitsgesetzes anzuwenden.

(4) Das Zentrum für Informationssicherheit darf Informationen, von denen es im Rahmen dieser Vorschrift Kenntnis erlangt, nur mit Einwilligung der ersuchenden Stelle nach Abs. 1 übermittelt, es sei denn, die Informationen lassen keine Rückschlüsse auf die Identität des Ersuchenden zu oder die Informationen können nach § 13 übermittelt werden. Zugang zu den in Verfahren nach Abs. 1 geführten Akten wird Dritten nicht gewährt.

(5) Das Zentrum für Informationssicherheit kann sich bei Maßnahmen nach Abs. 1 mit der Einwilligung der ersuchenden Stelle nach Abs. 1 der Hilfe Dritter bedienen, wenn dies zur rechtzeitigen oder vollständigen Wiederherstellung der Sicherheit oder Funktionsfähigkeit des betroffenen informationstechnischen Systems erforderlich ist. Die hierdurch entstehenden Kosten hat die ersuchende Stelle zu tragen. Das Zentrum für Informationssicherheit kann die ersuchende Stelle auch auf Dritte verweisen. Das Zentrum für Informationssicherheit und von der ersuchenden Stelle oder vom Zentrum für Informationssicherheit nach Satz 1 beauftragte Dritte können einander bei Maßnahmen nach Abs. 1 mit der Einwilligung der ersuchenden Stelle Daten übermitteln. Hierfür gilt Abs. 3 entsprechend.

(6) Soweit es zur Wiederherstellung der Sicherheit oder Funktionsfähigkeit des informationstechnischen Systems erforderlich ist, kann das Zentrum für Informationssicherheit vom Hersteller des informationstechnischen Systems verlangen, an der Wiederherstellung der Sicherheit oder Funktionsfähigkeit mitzuwirken.

(7) In begründeten Einzelfällen kann das Zentrum für Informationssicherheit auch bei nicht in § 1 genannten Einrichtungen tätig werden, wenn es darum ersucht wurde und es sich um einen herausgehobenen Fall im Sinne des Abs. 2 handelt und soweit Rechtsvorschriften dem nicht entgegenstehen.

VIERTER TEIL

Informations- und Dokumentationspflichten

§ 17

Information der Betroffenen

Die von Maßnahmen nach § 10 Abs. 2 oder § 11 Abs. 3 Betroffenen sind spätestens nach dem Erkennen und der Abwehr eines Schadprogramms oder von Gefahren, die von einem Schadprogramm ausgehen, zu informieren, wenn sie bekannt sind oder ihre Identifikation ohne unverhältnismäßigen Aufwand möglich ist. Die Pflicht zur Information gemäß den Artikeln 13 und 14 der Verordnung (EU) 2016/679 besteht ergänzend zu den in Artikel 13 Absatz 4 und Artikel 14 Absatz 5 der Verordnung (EU) 2016/679 genannten Ausnahmen nicht, wenn

1. die Informationserteilung die ordnungsgemäße Erfüllung der in der Zuständigkeit der jeweiligen Stelle gemäß § 12 liegenden Aufgaben gefährden würde oder
2. die Informationserteilung die öffentliche Sicherheit oder Ordnung oder die Gewährleistung der Netz- und Informationssicherheit auf sonstige Weise gefährden oder sonst dem Wohl des Landes Nachteile bereiten würde

und deswegen das Interesse der betroffenen Person an der Informationserteilung zurücktreten muss. Der Verantwortliche hält schriftlich fest, aus welchen Gründen er von einer Information abgesehen hat. Die Information kann unterbleiben, wenn hierdurch der Ermittlungszweck eines Straf- oder Disziplinarverfahrens oder die Tätigkeit der Verfassungsschutzbehörden gefährdet würde. Im Falle einer Übermittlung der Daten nach § 13 Abs. 2 erfolgt die Information durch die dort genannten Behörden in entsprechender Anwendung der für diese Behörden geltenden Vorschriften. Enthalten diese keine Bestimmungen zu Informationspflichten, sind die Vorschriften der Strafprozessordnung entsprechend anzuwenden.

§ 18

Meldepflichten

(1) Werden den Stellen nach § 1 Nr. 1 und 2 Informationen bekannt, die zur Abwehr von Gefahren für die Informationssicherheit von Bedeutung sind, unterrichten diese das Zentrum für Informationssicherheit unverzüglich hierüber, soweit andere Vorschriften oder Vereinbarungen mit Dritten nicht entgegenstehen.

(2) Die Pflicht gilt nicht für den Hessischen Landtag, den Hessischen Rechnungshof, den Hessischen Beauftragten für Datenschutz und Informationsfreiheit, die Gerichte und Staatsanwaltschaften sowie die Hochschulen nach § 2 des Hessischen Hochschulgesetzes.

§ 19

Dokumentationspflichten

Anordnungen nach § 10 Abs. 2 Satz 2, § 11 Abs. 2 Satz 4 und § 11 Abs. 3 Satz 2 sind zu dokumentieren. Die Dokumentation darf ausschließlich für Zwecke der nachträglichen Überprüfung der Rechtmäßigkeit der Verarbeitung der Daten verwendet werden. Sie ist zu löschen, wenn sie für diese Zwecke nicht mehr erforderlich ist, spätestens jedoch zum Ablauf des Kalenderjahres, das dem Jahr der Dokumentation folgt.

FÜNFTER TEIL

Schlussvorschriften

§ 20

Einschränkung von Grundrechten

Das Fernmeldegeheimnis nach Art. 10 des Grundgesetzes für die Bundesrepublik Deutschland, Art. 12 der Verfassung des Landes Hessen und das Recht auf informationelle Selbstbestimmung nach Art. 1 Abs. 1 in Verbindung mit Art. 2 Abs. 1 des Grundgesetzes für die Bundesrepublik Deutschland, Art. 12a der Verfassung des Landes Hessen werden durch die §§ 7 bis 11, 13 und 16 eingeschränkt.

§ 21

Inkrafttreten, Außerkrafttreten

Dieses Gesetz tritt am Tag nach der Verkündung in Kraft. Es tritt mit Ablauf des 31. Dezember 2030 außer 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 29. Juni 2023

Der Hessische Ministerpräsident

Rhein

Die Hessische Minister des Innern und für Sport

Beuth