Vorblatt

A. Zielsetzung

Wesentliches Ziel des vorliegenden Gesetzentwurfs ist es, die europarechtlichen Vorgaben des Europarechts aus der Richtlinie (EU) 2022/2555 des Europäischen Parlaments und des Rates vom 14. Dezember 2022 über Maßnahmen für ein hohes gemeinsames Cybersicherheitsniveau in der Union, zur Änderung der Verordnung (EU) Nr. 910/2014 und der Richtlinie 2018/1972 sowie zur Aufhebung der Richtlinie (EU) 2016/1148 (Richtlinie (EU) 2022/2555) umzusetzen. Auf diese Weise wird die Informationssicherheit im Land Sachsen-Anhalt erhöht und in angemessener Weise auf die Gefahren für informationstechnische Systeme im Land Sachsen-Anhalt reagiert.

B. Lösung

Durch das Gesetz zur Gewährleistung der Informationssicherheit im Land Sachsen-Anhalt (Informationssicherheitsgesetz Sachsen-Anhalt – InfSG LSA) wird im Land Sachsen-Anhalt erstmalig ein gesetzlicher Rahmen mit definierten Zuständigkeiten und Befugnissen für spezifische Aufsichtsbehörden geschaffen. Das InfSG LSA verfolgt einen risikobasierten und zugleich ganzheitlichen Ansatz, mit dessen Hilfe das Niveau der Informationssicherheit bei der öffentlichen Verwaltung im Land Sachsen-Anhalt auf ein angemessenes Maß angehoben werden soll.

Insofern dient das Gesetz zur Gewährleistung der Informationssicherheit im Land Sachsen-Anhalt der Umsetzung europarechtlicher Vorgaben: Soweit die Richtlinie (EU) 2022/2555 aufgrund von Artikel 3 Absatz 1 Buchstabe d in Verbindung mit Artikel 2 Absatz 2 Buchstabe f Ziffer ii verbindliche Vorgaben für wichtige Einrichtungen der öffentlichen Verwaltung auf regionaler Ebene trifft, dient das vorliegende Gesetz der Identifizierung dieser Einrichtungen und der Umsetzung europarechtlicher Vorgaben.

C. Alternativen

Gesetzgeberische Alternativen, die gleichermaßen geeignet sind, bestehen nicht.

Dieser Einschätzung stehen auch solche landesrechtlichen Regelungsinitiativen nicht entgegen, die wie etwa das Land Niedersachsen die Anforderungen der NIS-2-Richtlinie mittels Verwaltungsvorschrift beziehungsweise Runderlass (Umsetzung der NIS-2-Richtlinie in Niedersachsen (NIS2UmsRdErl)) in nationales Recht umsetzen.

Der vorliegende Gesetzesentwurf regelt im Land Sachsen-Anhalt erstmals umfangreiche informationssicherheitsrechtliche Anforderungen, die an die öffentlichen Stellen des Landes gestellt werden. Mit diesen gehen zugleich weitreichende Befugnisse zur Verarbeitung personenbezogener Daten einher. Dem Regulierungsanliegen wird daher schon allein aus datenschutzrechtlichen Gründen, aber auch auf Grund der erhöhten Bindungswirkung und höheren Symbolwirkung nur ein formelles Gesetz gerecht. Zuletzt bietet das Landesrecht in Sachsen-Anhalt keine Rechtsgrundlage, die eine vergleichbar umfassende Regelung im Wege einer Rechtsverordnung oder eines Runderlasses ermöglichen würde.

D. Kosten

Die Ermittlung des Erfüllungsaufwandes erfolgt in Orientierung an dem Leitfaden zur Ermittlung und Darstellung des Erfüllungsaufwands bei Gesetzgebungsvorhaben des Bundes. Dieser wurde durch das Statistische Bundesamt im Auftrag der Bundesregierung und des Nationalen Normenkontrollrats im April 2025 herausgegeben.[1]

Für alle berücksichtigungswürdigen Bedarfe des Gesetzesentwurfs gilt aus diesem Grund das Ressortdeckungsprinzip und damit die Einordnung in vorhandene Ansätze; erforderliche Stellen- und Sachmittelbedarfe sind im Bestand abzubilden. Sofern Bedarfe nach Einschätzung der Ressorts nicht im Bestand abbildbar sein sollten, werden diese im Verfahren zur Aufstellung des Haushalts eingebracht.

Im Rahmen der Personal- und Sachkostenschätzung wurden die Berechnungen auf die Jahresvollkostendurchschnittssätze der Landesverwaltung Sachsen-Anhalt des Jahres 2024 gestützt. Zusätzlich wurden die Annahme getroffen, dass alle Berechnungen auf Tarifbeschäftigungsbasis beruhen. Die angenommenen Vollzeitäquivalente wurde für Tätigkeiten auf Referentenebene die Eingruppierung in die Entgeltgruppe E14 und für Tätigkeiten auf Ebene der Sachbearbeitung die Eingruppierung in Entgeltgruppe E11 zu Grunde gelegt. Die angenommenen Eingruppierungen entsprechen den durchschnittlich zu erwartenden Arbeitsplatzbewertungen. Die Jahresvollkostendurchschnittssätze der Landesverwaltung Sachsen-Anhalt des Jahres 2024 betragen für die Entgeltgruppe E14 159.637,93 Euro und für die Entgeltgruppe E11 137.256,26 Euro pro Jahr. Beträge wurden auf volle Tausend Euro gerundet.

Eine normbezogene Darstellung der zu erwartenden Kosten findet sich in der Begründung (A.II.2). Die folgende tabellarische Darstellung stellt eine Übersicht dar.

Bezeichnung	**Aufwände einmalig [€]**	**Aufwände jährlich [€]**
Fachpersonal zuständiges Ministerium		1.201.000
Sachaufwand Einrichtung Computer-Sicherheitsnotfallteam	350.000	60.000
Computer Emergency Response Team (CERT) Nord		396.000
Prüfungen der Informationssicherheit, technische Scans, Penetrationstests u.ä.		864.000
Erstellung und Pflege von Dokumenten	250.000	60.000

[1] https://www.destatis.de/DE/Themen/Staat/Buerokratiekosten/Publikationen/Downloads-Buerokratiekosten/erfuellungsaufwand-handbuch.pdf, Abruf am 07.10.2025

Betrieb von Systemen zur Überwachung und Analyse von Cyberbedrohungen, Schwachstellen und Sicherheitsvorfällen im Land Sachsen-Anhalt	400.000	250.000
Identifikation wichtiger öffentlicher Stellen	220.000	
Qualifikation Informationssicherheitsbeauftragte		200.000
Schulungen Beschäftigte und Leitungen		200.000
Vor-Ort-Kontrollen, Auskünfte u.ä.		60.000
Kosten Evaluation (alle 5 Jahre, Kosten jährlich ausgewiesen)		5.000
Aufwände summiert	**1.220.000**	**3.296.000**

* Beträge wurden auf Tausend Euro gerundet.

E. Anhörungsverfahren

Der Gesetzentwurf ist am …. vom Kabinett beschlossen und zur Anhörung freigegeben worden. Die Frist der Anhörung endete am …

I. Angehört wurden:

- Der Landkreistag Sachsen-Anhalt,
- der Städte- und Gemeindebund Sachsen-Anhalt,
- die Landesbeauftragte für den Datenschutz,
- die Landesbeauftragte für die Informationsfreiheit,
- der Verband der IT- und Multimediaindustrie Sachsen-Anhalt e.V.,
- die Kommunale IT-Union eG,
- die Dataport AöR, Niederlassung Magdeburg,
- Bundesamt für Sicherheit in der Informationstechnik,

II. Ergebnis der Anhörung

Wird nach der Anhörung ergänzt.

F. Zuständigkeit

Federführend ist das Ministerium für Infrastruktur und Digitales.

Entwurf

Gesetz zur Gewährleistung der Informationssicherheit im Land Sachsen-Anhalt (Informationssicherheitsgesetz Sachsen-Anhalt – InfSG LSA)

Gesetz
zur Gewährleistung der Informationssicherheit im Land Sachsen-Anhalt
(Informationssicherheitsgesetz Sachsen-Anhalt – InfSG LSA)

Teil 1: Allgemeine Vorschriften

§ 1 Zweck des Gesetzes

Zweck dieses Gesetzes ist, die Informationssicherheit im Land Sachsen-Anhalt zu erhöhen und Gefahren für informationstechnische Systeme abzuwehren.

§ 2 Anwendungsbereich

(1) Dieses Gesetz gilt für wichtige Stellen der unmittelbaren Landesverwaltung.

(2) Wichtige Stellen der unmittelbaren Landesverwaltung sind

a) oberste Landesbehörden nach § 8 Absatz 1 OrgG LSA und
b) obere Landesbehörden, untere Landesbehörden und Einrichtungen des Landes nach §§ 9 Absatz 1, 10 Absatz 1 und 11 OrgG LSA, die nach einer risikobasierten Bewertung Dienste erbringen, deren Störung oder Ausfall über einen Zeitraum von 30 Tagen erhebliche Auswirkungen auf kritische gesellschaftliche oder wirtschaftliche Tätigkeiten haben können.

(3) Wichtige Stellen der unmittelbaren Landesverwaltung sind wichtige Einrichtungen im Sinne von Artikel 3 Absatz 2 Satz 1 i. V. m. Nr. 10 Alternative 2 Anhang I Richtlinie (EU) 2022/2555 in Verbindung mit Artikel 2 Absatz 2 Buchstabe f Doppelbuchstabe ii Richtlinie (EU) 2022/2555.

(4) Dieses Gesetz gilt nicht für

Nr. 1: die Verwaltung des Landtages,
Nr. 2: die Landesbeauftragte oder den Landesbeauftragten für den Datenschutz,
Nr. 3: den Landesrechnungshof;
Nr. 4: Organe der Rechtsprechung und Rechtspflege, die Staatsanwaltschaften sowie die Justizvollzugsanstalten und Jugendstrafanstalten,
Nr. 5: die staatlichen Hochschulen und die Universitätsklinika,
Nr. 6: die Landesbeauftragte oder den Landesbeauftragten für die Informationsfreiheit,
Nr. 7: die Beauftragte oder den Beauftragten des Landes Sachsen-Anhalt zur Aufarbeitung der SED-Diktatur,
Nr. 8: die Kirchen und als öffentlich-rechtliche Körperschaften anerkannte Religionsgemeinschaften und Weltanschauungsgemeinschaften auf dem Gebiet des Landes Sachsen-Anhalt sowie ihre Verbände, ihre Einrichtungen und ihre Anstalten und Stiftungen des öffentlichen Rechts, die ihren Sitz in Sachsen-Anhalt haben.
Nr. 9: die Rundfunkanstalt Mitteldeutscher Rundfunk,
Nr. 10: die öffentlich-rechtlichen Kreditinstitute und öffentlich-rechtlichen Versicherungsanstalten im Land Sachsen-Anhalt und

Nr. 11: Stellen der unmittelbaren Landesverwaltung, soweit diese in den Bereichen nationale Sicherheit, öffentliche Sicherheit, Verteidigung oder Strafverfolgung, einschließlich der Verhütung, Ermittlung, Aufdeckung und Verfolgung von Straftaten sowie des Verfassungsschutzes, tätig werden.

§ 3 Begriffsbestimmungen

(1) Ein „Beinahevorfall“ ist ein Ereignis, das die Verfügbarkeit, Integrität oder Vertraulichkeit gespeicherter, übermittelter oder verarbeiteter Daten oder der Dienste, die über informationstechnische Systeme, Komponenten und Prozesse angeboten werden oder zugänglich sind, beeinträchtigt haben könnte, dessen Eintritt jedoch erfolgreich verhindert worden ist oder aus anderen Gründen nicht erfolgt ist.

(2) Eine „Cyberbedrohung“ ist eine Cyberbedrohung nach Artikel 2 Nummer 8 der Verordnung (EU) 2019/881 des Europäischen Parlaments und des Rates vom 17. April 2019 über die ENISA (Agentur der Europäischen Union für Cybersicherheit) und über die Zertifizierung der Cybersicherheit von Informations- und Kommunikationstechnik und zur Aufhebung der Verordnung (EU) Nr. 526/2013 (Rechtsakt zur Cybersicherheit, Verordnung (EU) 2019/881).

(3) Eine „erhebliche Cyberbedrohung“ ist eine Cyberbedrohung, die das Potenzial besitzt, die informationstechnischen Systeme, Komponenten und Prozesse aufgrund der besonderen technischen Merkmale der Cyberbedrohung erheblich zu beeinträchtigen; eine Beeinträchtigung ist erheblich, wenn sie erheblichen materiellen oder immateriellen Schaden verursachen kann

(4) Ein „erheblicher Sicherheitsvorfall“ ist ein Sicherheitsvorfall, der

Nr. 1: schwerwiegende Betriebsstörungen der Dienste oder materielle Schäden verursacht hat oder verursachen kann oder
Nr. 2: Dritte durch erhebliche materielle oder immaterielle Schäden beeinträchtigt hat oder beeinträchtigen kann.

(5) Ein „Sicherheitsvorfall“ ist ein Ereignis, das die Verfügbarkeit, Integrität oder Vertraulichkeit gespeicherter, übermittelter oder verarbeiteter Daten oder der Dienste, die über informationstechnische Systeme, Komponenten und Prozesse angeboten werden oder zugänglich sind, beeinträchtigt.

(6) Eine „Schwachstelle“ ist eine Schwäche, Anfälligkeit oder Fehlfunktion (Eigenschaft) von IKT-Produkten oder IKT-Diensten, die von Dritten ausgenutzt werden kann, um sich gegen den Willen des Berechtigten Zugang zu den IKT-Produkten oder IKT-Diensten zu verschaffen oder die Funktion der IKT-Produkte oder IKT-Dienste zu beeinflussen;

(7) Ein „IKT-Dienst“, „IKT-Produkt“ und „IKT-Prozess“ sind ein IKT-Dienst, ein IKT-Produkt oder ein IKT-Prozess nach Artikel 2 Nummer 12 bis 14 der Verordnung (EU) 2019/881.

(8) Die „Informationssicherheit“ ist der angemessene Schutz der Vertraulichkeit, Integrität und Verfügbarkeit von Informationen.

(9) Das „Informationssicherheitsmanagement“ ist die Aufstellung von verbindlichen Prozessen und Regeln, die die Informationssicherheit dauerhaft steuern, kontrollieren, aufrechterhalten und fortlaufend verbessern.

(10) „Informationstechnische Systeme“ sind alle technischen Mittel zur Erfassung, Speicherung, Verarbeitung, Nutzung, Übermittlung oder Löschung von Informationen und Daten.

(11) „Inhaltsdaten“ sind Daten, die den Inhalt einer Kommunikation betreffen und die keine Verkehrsdaten gemäß § 3 Nummer 70 des Telekommunikationsgesetzes vom 23. Juni 2021 (BGBl. I S. 1858), das zuletzt durch Artikel 12 des Gesetzes vom 9. Januar 2026 (BGBl. 2026 I Nr. 7) geändert worden ist (Telekommunikationsgesetz), in der jeweils geltenden Fassung, sind.

(12) „Protokolldaten“ sind 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.[1] Protokolldaten können Verkehrsdaten gemäß § 3 Nummer 70 des Telekommunikationsgesetzes und Nutzungsdaten nach § 2 Absatz 2 Nummer 3 des Telekommunikation-Digitale-Dienste-Datenschutz-Gesetzes vom 23. Juni 2021 (BGBl. I S. 1982; 2022 I S. 1045), das zuletzt durch Artikel 10 des Gesetzes vom 9. Januar 2026 (BGBl. 2026 I Nr. 7) geändert worden ist, enthalten.[2]

(13) „Protokollierungsdaten“ sind Aufzeichnungen über technische Ereignisse oder Zustände innerhalb informationstechnischer Systeme.

(14) Ein „Schadprogramm“ sind ein Programm sowie sonstige informationstechnische Routinen und Verfahren, die dem Zweck dienen, unbefugt Daten zu verarbeiten oder unbefugt auf sonstige informationstechnische Abläufe einzuwirken.

(15) Ein „Schwachstellenscan“ ist eine proaktive Überprüfung der informationstechnischen Systeme, Komponenten und Prozesse auf Schwachstellen mit potenziell signifikanten Auswirkungen.

Teil 2: Organisation der Informationssicherheit

§ 4 Informationssicherheit im Land Sachsen-Anhalt

(1) Das für Informationssicherheit zuständige Ministerium nimmt die Aufgaben der Informationssicherheit im Land Sachsen-Anhalt als oberste Landesbehörde wahr.[1] Das für Informationssicherheit zuständige Ministerium ist zuständige Behörde nach Artikel 8 Absatz 1 und 2 der Richtlinie (EU) 2022/2555 des Europäischen Parlaments und des Rates vom 14. Dezember 2022 über Maßnahmen für ein hohes gemeinsames Cybersicherheitsniveau in der Union, zur Änderung der Verordnung

(EU) Nr. 910/2014 und der Richtlinie (EU) 2018/1972 sowie zur Aufhebung der Richtlinie (EU) 2016/1148 (Richtlinie (EU) 2022/2555).[2]

(2) Das für Informationssicherheit zuständige Ministerium fördert die kontinuierliche Verbesserung der Informationssicherheit im Land Sachsen-Anhalt, koordiniert innerhalb der öffentlichen Stellen des Landes übergreifende Informationssicherheitsthemen.[1] Dies umfasst insbesondere

Nr. 1: die Überwachung der Anwendung der Richtlinie (EU) 2022/2555 im Land Sachsen-Anhalt;
Nr. 2: die hierfür erforderliche Erstellung von Handlungs- oder Auswahlempfehlungen, Formulierungsvorschlägen, Erläuterungen, Leitfäden und Mustern sowie die Erarbeitung von empfehlenden Mindeststandards zur Informationssicherheit zur Unterstützung von Maßnahmen im Bereich des Informationssicherheitsmanagements;
Nr. 3: auf Ersuchen oder Anforderungen einer wichtigen Stelle der unmittelbaren Landesverwaltung beratende Maßnahmen insbesondere bei der Erstellung und Pflege eines Informationssicherheitsmanagementsystems, der Erstellung von Sicherheitskonzepten sowie der Umsetzung von Handlungsempfehlungen, Leitfäden und Mindeststandards;
Nr. 4: die Konzeption und Vorbereitung geeigneter Maßnahmen für den Fall von Störungen, Notfällen, Krisen und Katastrophen im Bereich der Informationssicherheit, welche für Katastrophen mit dem für die Umsetzung der Richtlinie (EU) 2022/2557 des Europäischen Parlaments und des Rates vom 14. Dezember 2022 über die Resilienz kritischer Einrichtungen und zur Aufhebung der Richtlinie 2008/114/EG des Rates zuständigen Ministerium abzustimmen ist;
Nr. 5: die Vorbereitung und Koordination von Sensibilisierungs- und Schulungsmaßnahmen zur Informationssicherheit sowie die Erstellung von Schulungs-, Sensibilisierungs- und Informationsunterlagen; sowie
Nr. 6: die regelmäßige und anlassbezogene Unterrichtung der zuständigen Kooperations- und Koordinierungsgremien für Informations- und Cybersicherheit im Land Sachsen-Anhalt und der Öffentlichkeit über wesentliche Entwicklungen der Informationssicherheit im Land Sachsen-Anhalt in Bezug auf die Umsetzung der Richtlinie (EU) 2022/2555.[2]

Das für Informationssicherheit zuständige Ministerium wird ermächtigt, die Inhalte, Zeiträume und Umfänge der Berichtspflichten und die einzubindenden Kooperations- und Koordinierungsgremien nach Satz 2 Nr. 6 im Wege einer Rechtsverordnung näher zu bestimmen.[3]

(3) Im für Informationssicherheit zuständige Ministerium wird eine Stelle zur Wahrnehmung der Aufgaben der zuständigen Behörde nach Absatz 1 Satz 2 eingerichtet.[1] Zu den Aufgaben dieser Stelle gehört die Überwachung der Anwendung dieses Gesetzes, sofern es die Anforderungen der Richtlinie (EU) 2022/2555 auf Ebene des Landes Sachsen-Anhalt umsetzt.[2] Die Stelle nach Satz 1 ist in der Erfüllung ihrer Aufgaben operativ unabhängig und weisungsfrei.[3]

(4) Die zuständige Stelle nach Absatz 3 Satz 1 erstellt eine Liste von wichtigen Stellen der unmittelbaren Landesverwaltung und meldet diese dem zuständigen Bundesministerium und dem Bundesamt für Sicherheit in der Informationstechnik.[1] Das Erstellen der Liste und die Meldung erfolgen erstmals sechs Monate nach Inkrafttreten dieses Gesetzes und danach alle zwei Jahre.[2]

(5) Zur Erfüllung der eigenen Aufgaben können das für Informationssicherheit zuständige Ministerium und die zuständige Stelle nach Absatz 3 Satz 1 des Computer-Sicherheitsnotfallteams nach § 5 oder anderer geeigneter Dritter bedienen.

(6) Die zuständige Stelle nach Absatz 3 Satz 1 notifiziert gegenüber der Europäischen Kommission unverzüglich seine Identität, seine Aufgaben sowie spätere Änderungen dieser Angaben.[1] Die zuständige Stellen nach Absatz 3 Satz 1 notifiziert entsprechendes in Bezug auf das Computer-Sicherheitsnotfallteam gemäß § 5.[2]

§ 5 Computer-Sicherheitsnotfallteam (CSIRT)

(1) Bei dem für Informationssicherheit zuständigen Ministerium wird ein Computer-Sicherheitsnotfallteam (Computer Security Incident Response Team, CSIRT) eingerichtet.[1] Das CSIRT nimmt die Aufgaben als Computer-Sicherheitsnotfallteam im Sinne von Artikel 10 Abs. 1 Richtlinie (EU) 2022/2555 auf der Ebene der unmittelbaren Landesverwaltung wahr.[2]

(2) Das CSIRT unterstützt das für Informationssicherheit zuständige Ministerium in technischen Fragen der Informationssicherheit.[1] Die Aufgaben des CSIRT umfassen insbesondere

Nr. 1: die Überwachung und Analyse von Cyberbedrohungen, Schwachstellen und Sicherheitsvorfällen im Land Sachsen-Anhalt, und auf Anfrage Bereitstellung von Unterstützung für betreffende wichtige Stellen der unmittelbaren Landesverwaltung hinsichtlich der Überwachung ihrer informationstechnischen Systeme, Komponenten und Prozesse in Echtzeit oder nahezu in Echtzeit;

Nr. 2: die Ausgabe von Frühwarnungen und Alarmmeldungen sowie Bekanntmachung und Weitergabe von Informationen über Cyberbedrohungen, Schwachstellen und Sicherheitsvorfälle an die wichtigen Stellen der unmittelbaren Landesverwaltung sowie an die zuständigen Behörden und andere einschlägige Interessenträger möglichst zeitnah;

Nr. 3: die Reaktion auf Sicherheitsvorfälle und die Unterstützung der betroffenen wichtigen Stellen der unmittelbaren Landesverwaltung;

Nr. 4: die Erhebung und Analyse forensischer Daten sowie dynamische Analyse von Risiken und Sicherheitsvorfällen sowie der Lage der Informationssicherheit sowie die Erstellung daraus abgeleiteter Empfehlungen;

Nr. 5: auf Ersuchen einer wichtigen Stelle der unmittelbaren Landesverwaltung ein Schwachstellenscan bei den betroffenen Stellen,

Nr. 6: der Beitrag zum Einsatz sicherer Instrumente für den Informationsaustausch im Sinne der Richtlinie (EU) 2022/2555, insbesondere in Form einer Prüfung auf Risiken im Betrieb von informationstechnischen

Systemen, Komponenten oder Prozesse und die Unterstützung bei deren Beseitigung;
Nr. 7: die Wahrnehmung der zentralen Meldestelle im Sinne des IT-Planungsrates im Verwaltungs-CERT-Verbund;
Nr. 8: die Bereitstellung von Unterstützungsmaßnahmen an öffentliche Stellen des Landes hinsichtlich der Überwachung ihrer informationstechnischen Systeme, Komponenten oder Prozesse;
Nr. 9: die Mitwirkung bei der technischen und technologischen Koordinierung der Informationssicherheit, sowie
Nr. 10: die Wahrnehmung der übrigen Aufgaben des Computer-Notfallteams nach Artikel 10 und 11 der Richtlinie (EU) 2022/2555.[2]

Bei der Durchführung der genannten Aufgaben kann das CSIRT auf der Grundlage eines risikobasierten Ansatzes bestimmten Aufgaben Vorrang einräumen.[3]

(3) Das CSIRT stellt den im Land Sachsen-Anhalt für die Umsetzung der Richtlinie (EU) 2022/2557 zuständigen Behörden Informationen über erhebliche Sicherheitsvorfälle, erhebliche Cyberbedrohungen und Beinahe-Vorfälle zur Verfügung, die nach § 9 von solchen Stellen gemeldet werden, die im Sinne der Richtlinie (EU) 2022/2557 als kritische Einrichtungen gelten.

(4) Das CSIRT gewährleistet einen hohen Grad der Verfügbarkeit seiner Kommunikationskanäle, indem es punktuellen Ausfällen vorbeugt und mehrere Kanäle bereitstellt, damit es jederzeit erreichbar bleibt und selbst mit Anderen Kontakt aufnehmen kann; dafür legt das CSIRT die Kommunikationskanäle genau fest und macht sie den wichtigen Stellen der unmittelbaren Landesverwaltung bekannt.[1] Darüber hinaus gewährleistet das CSIRT, dass seine Räumlichkeiten und unterstützenden informationstechnischen Systeme, Komponenten und Prozesse an einem sicheren Standort eingerichtet werden.[2] Das CSIRT gewährleistet, dass es über ein geeignetes System zur Verwaltung und Weiterleitung von Anfragen verfügt, insbesondere um wirksame und effiziente Übergaben zu erleichtern.[3] Das CSIRT stellt die Vertraulichkeit und Vertrauenswürdigkeit seiner Tätigkeiten sicher.[4] Das CSIRT gewährleistet eine personelle Ausstattung, mit der es eine ständige Bereitschaft seiner Dienste gewährleisten kann.[5] Das CSIRT gewährleistet, dass sein Personal entsprechend seinen Aufgaben und Pflichten geschult ist.[6] Das CSIRT gewährleistet, dass es über Redundanzsysteme und Ausweicharbeitsräume verfügt, um die Kontinuität seiner Dienste sicherzustellen.[7]

(5) Das CSIRT kann sich zur Erfüllung seiner Aufgaben geeigneter Dritter bedienen.

§ 6 Zusammenarbeit in der Informationssicherheit

(1) Das für Informationssicherheit zuständige Ministerium, die zuständige Stelle nach § 4 Absatz 3 Satz 1, das CSIRT und die wichtigen Stellen der unmittelbaren Landesverwaltung arbeiten im Bereich der Informationssicherheit eng und vertrauensvoll zusammen.

(2) Das für Informationssicherheit zuständige Ministerium arbeitet als zuständige Behörde nach Artikel 8 Absatz 1 und 2 der Richtlinie (EU) 2022/2555 zur Erfüllung

ihrer Aufgaben mit den zuständigen Behörden der anderen Länder, dem Bundesamt für Sicherheit in der Informationstechnik als zentrale Anlaufstelle, den Computer-Notfallteams, den Strafverfolgungsbehörden, den Datenschutzbehörden, den nationalen Behörden gemäß den Verordnungen (EG) Nr. 300/2008 des Europäischen Parlaments und des Rates vom 11. März 2008 über gemeinsame Vorschriften für die Sicherheit in der Zivilluftfahrt und zur Aufhebung der Verordnung (EG) Nr. 2320/2002 (ABl. L 97 vom 9.4.2008, S. 72; L 164 vom 23.6.2012, S. 18), geändert durch die Verordnung (EU) Nr. 18/2010 der Kommission vom 8. Januar 2010 (ABl. L 7 vom 12.1.2010, S. 3), und (EU) 2018/1139 des Europäischen Parlaments und des Rates vom 4. Juli 2018 zur Festlegung gemeinsamer Vorschriften für die Zivilluftfahrt und zur Errichtung einer Agentur der Europäischen Union für Flugsicherheit sowie zur Änderung der Verordnungen (EG) Nr. 2111/2005, (EG) Nr. 1008/2008, (EU) Nr. 996/2010, (EU) Nr. 376/2014 und der Richtlinien 2014/30/EU und 2014/53/EU des Europäischen Parlaments und des Rates, und zur Aufhebung der Verordnungen (EG) Nr. 552/2004 und (EG) Nr. 216/2008 des Europäischen Parlaments und des Rates und der Verordnung (EWG) Nr. 3922/91 des Rates (ABl. L 212 vom 22.8.2018, S. 1; L 296 vom 22.11.2018, S. 41), geändert durch die Delegierte Verordnung (EU) 2021/1087 der Kommission vom 7. April 2021 (ABl. L 236 vom 5.7.2021, S. 1), den Aufsichtsstellen gemäß der Verordnung (EU) Nr. 910/2014 des Europäischen Parlaments und des Rates vom 23. Juli 2014 über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt und zur Aufhebung der Richtlinie 1999/93/EG (ABl. L 257 vom 28.8.2014, S. 73; L 23 vom 29.1.2015, S. 19; L 155 vom 14.6.2016, S. 44), geändert durch die Verordnung (EU) 2024/1183 des Europäischen Parlaments und des Rates vom 11. April 2024 (ABl. L, 2024/1183, 30.4.2024), den gemäß der Verordnung (EU) 2022/2554 des Europäischen Parlaments und des Rates vom 14. Dezember 2022 über die digitale operationale Resilienz im Finanzsektor und zur Änderung der Verordnungen (EG) Nr. 1060/2009, (EU) Nr. 648/2012, (EU) Nr. 600/2014, (EU) Nr. 909/2014 und (EU) 2016/1011 (ABl. L 333 vom 27.12.2022, S. 1) zuständigen Behörden, den nationalen Regulierungsbehörden gemäß der Richtlinie (EU) 2018/1972 des Europäischen Parlaments und des Rates vom 11. Dezember 2018 über den europäischen Kodex für die elektronische Kommunikation (ABl. L 321 vom 17.12.2018, S. 36; L 334 vom 27.12.2019, S. 164), den gemäß der Richtlinie (EU) 2022/2557 des Europäischen Parlaments und des Rates vom 14. Dezember 2022 über die Resilienz kritischer Einrichtungen und zur Aufhebung der Richtlinie 2008/114/EG des Rates (ABl. L 333 vom 27.12.2022, S. 164) zuständigen Behörden sowie im Rahmen anderer sektorspezifischer Rechtsakte der Europäischen Union innerhalb des jeweiligen Mitgliedstaats zuständiger Behörden zusammen.

Teil 3: Informationssicherheit bei öffentlichen Stellen des Landes

§ 7 Identifikation der wichtigen Stellen der unmittelbaren Landesverwaltung

(1) Die obersten Landesbehörden identifizieren innerhalb ihrer Zuständigkeit obere Landesbehörden, untere Landesbehörden und Einrichtungen des Landes, die solche Dienste erbringen, deren Störung oder Ausfall über einen Zeitraum von 30 Tagen erhebliche Auswirkungen auf kritische gesellschaftliche oder wirtschaftliche Tätigkeiten haben können, als wichtige Stellen der unmittelbaren Landesverwaltung

nach § 2 Absatz 2 Buchstabe b.[1] Die obersten Landesbehörden nehmen die Identifizierung nach Satz 1 erstmals drei Monate nach Inkrafttreten dieses Gesetzes vor und überprüfen diese alle zwei Jahre.[2]

(2) Das für Informationssicherheit zuständige Ministerium wird ermächtigt, durch Rechtsverordnung Bestimmungen zu erlassen über:

Nr. 1: das Verfahren zur Durchführung der Identifikation nach Absatz 1 Satz 1;
Nr. 2: die Aufgaben und Pflichten im Rahmen der Zusammenarbeit der unterschiedlichen Stellen bei der Identifikation nach Absatz 1 Satz 1,
Nr. 3: die Form der Identifikation nach Absatz 1 Satz 1.[1]

Vorgaben und Hinweise des IT-Planungsrates im Sinne von Artikel 91c Absatz 4 Satz 1 des Grundgesetzes für die Bundesrepublik Deutschland sowie Leitlinien und Vorgaben der Europäischen Kommission für die Verpflichtung nach Artikel 3 Absatz 4 der Richtlinie (EU) 2022/2555 sind bei dieser Rechtsverordnung zu berücksichtigen.[2]

(3) Die obersten Landesbehörden übermitteln dem für Informationssicherheit zuständigen Ministerium für die von ihnen erstmals oder erneut identifizierten wichtigen Stellen der unmittelbaren Landesverwaltung nach § 2 Absatz 2 Buchstabe b) in ihrem Zuständigkeitsbereich:

Nr. 1: den Namen,
Nr. 2: die Anschrift und die aktuellen Kontaktdaten der identifizierten wichtigen öffentlichen Stellen des Landes einschließlich[a] E-Mail-Adresse und Telefonnummer einer Ansprechperson sowie einer Vertreterin oder eines Vertreters;
Nr. 3: die IP-Adressbereiche.[1]

Die identifizierten wichtigen Stellen der unmittelbaren Landesverwaltung nach § 2 Absatz 2 Buchstabe b teilen alle Änderungen der gemäß Satz 1 übermittelten Angaben dem für Informationssicherheit zuständigen Ministerium und der für sie zuständigen obersten Landesbehörde unverzüglich, in jedem Fall jedoch innerhalb von zwei Wochen ab dem Zeitpunkt der Änderung, mit.[2]

§ 8 Pflichten der wichtigen Stellen der unmittelbaren Landesverwaltung zu Risikomanagement im Bereich der Informationssicherheit

(1) Die wichtigen Stellen der unmittelbaren Landesverwaltung sind verpflichtet, geeignete, verhältnismäßige und wirksame technische, operative und organisatorische Maßnahmen zu ergreifen, um die Risiken für die Informationssicherheit dieser Stellen zu beherrschen und die Auswirkungen von Sicherheitsvorfällen auf Dritte zu verhindern oder möglichst gering zu halten.[1] Maßnahmen nach Satz 1 umfassen mindestens

Nr. 1: Konzepte und Verfahren in Bezug auf die Risikoanalyse und Sicherheit für informationstechnische Systeme, Komponenten und Prozesse;
Nr. 2: Konzepte und Verfahren zur Bewältigung von Sicherheitsvorfällen;

Nr. 3: Aufrechterhaltung des Betriebs, wie Backup-Management und Wiederherstellung des Betriebs nach Sicherheitsvorfällen sowie Maßnahmen zum Krisenmanagement der informationstechnischen Systeme, Komponenten und Prozesse;
Nr. 4: Verfahren zur Absicherung von Lieferketten einschließlich sicherheitsbezogener Aspekte der Beziehungen zwischen den einzelnen Einrichtungen und ihren unmittelbaren Anbietern oder Diensteanbietern;
Nr. 5: Sicherheitsmaßnahmen bei Erwerb, Entwicklung und Wartung von informationstechnischen Systemen, Komponenten und Prozessen, einschließlich Management und Offenlegung von Schwachstellen;
Nr. 6: Konzepte und Verfahren zur Bewertung der Wirksamkeit von Risikomanagementmaßnahmen im Bereich der Informationssicherheit;
Nr. 7: grundlegende Verfahren im Bereich der Cyberhygiene und Schulungen im Bereich der Informationssicherheit, welche sich an die Mitarbeiterinnen und Mitarbeiter der jeweiligen wichtigen Stelle der unmittelbaren Landesverwaltung richten;
Nr. 8: Konzepte und Verfahren für den Einsatz von Kryptografie und Verschlüsselung;
Nr. 9: Konzepte und Verfahren für die Sicherheit des Personals, die Zugriffskontrolle und das Management von Anlagen;
Nr. 10: die Verwendung von Lösungen zur Multi-Faktor-Authentifizierung oder kontinuierlichen Authentifizierung;
Nr. 11: die Verwendung kontinuierlich gesicherten Sprach-, Video- und Textkommunikation sowie gegebenenfalls gesicherter Notfallkommunikationssysteme innerhalb der Einrichtung.[2]

(2) Maßnahmen nach Absatz 1 müssen auf einem gefahrenübergreifenden Ansatz beruhen, der darauf abzielt, die informationstechnischen Systeme, Komponenten und Prozesse und die physische Umwelt dieser Systeme vor Sicherheitsvorfällen zu schützen.[1] Maßnahmen nach Absatz 1 müssen den Stand der Technik einhalten und unter Berücksichtigung der einschlägigen europäischen und internationalen Normen sowie der Umsetzungskosten ein Sicherheitsniveau der informationstechnischen Systeme, Komponenten und Prozesse gewährleisten das dem bestehenden Risiko angemessen ist.[2] Soweit die Europäische Kommission einen Durchführungsrechtsakt gemäß Artikel 21 Absatz 5 Unterabs. 2 Richtlinie (EU) 2022/2555 erlässt, in dem die technischen und methodischen Anforderungen sowie erforderlichenfalls die sektoralen Anforderungen der in Absatz 1 genannten Maßnahmen festgelegt werden, so sind diese zu beachten.[3] Bei der Bewertung, ob Maßnahmen dem bestehenden Risiko angemessen sind, sind das Ausmaß der Risikoexposition und die Größe der Einrichtung sowie die Eintrittswahrscheinlichkeit und Schwere von Sicherheitsvorfällen sowie ihre gesellschaftlichen und wirtschaftlichen Auswirkungen zu berücksichtigen.[4]

(3) Wichtige Stellen der unmittelbaren Landesverwaltung berücksichtigen bei der Erwägung geeigneter Maßnahmen nach Absatz 1 Satz 2 Nr. 4 die spezifischen Schwachstellen der einzelnen unmittelbaren Anbieter und Diensteanbieter sowie die Gesamtqualität der Produkte und der Informationssicherheitspraxis ihrer Anbieter und Diensteanbieter, einschließlich der Sicherheit ihrer Entwicklungsprozesse sowie gegebenenfalls die Ergebnisse einer durchgeführten koordinierten Risikobewertung in Bezug auf die Sicherheit kritischer Lieferketten.

(4) Wichtige Stellen der unmittelbaren Landesverwaltung können zur Erfüllung ihrer Pflichten nach den Absätzen 1 bis 3 das CSIRT im Rahmen von dessen Aufgaben und Zuständigkeiten um Unterstützung ersuchen.[1] Das gilt insbesondere in Bezug auf Schwachstellenscans, die Erhebung und Analyse forensischer Daten oder die angemessene Reaktion auf Sicherheitsvorfälle.[2]

(5) Die Einhaltung der Verpflichtungen nach den Absätzen 1 bis 3 ist durch die jeweilige wichtige Stelle der unmittelbaren Landesverwaltung zu dokumentieren.[1] Wichtige Stellen der unmittelbaren Landesverwaltung weisen die Erfüllung der Pflichten spätestens drei Jahre nach Inkrafttreten dieses Gesetzes und anschließend regelmäßig dem für Informationssicherheit zuständigen Ministerium als zuständigen Behörde nach Abschnitt 2 nach deren Vorgaben nach.[2]

§ 9 Melde- und Hinweispflichten

(1) Wichtige Stellen der unmittelbaren Landesverwaltung sind verpflichtet, über jeden erheblichen Sicherheitsvorfall an das CSIRT zu melden:

Nr. 1: unverzüglich, spätestens jedoch innerhalb von 24 Stunden nach Kenntnisnahme des erheblichen Sicherheitsvorfalls, eine frühe Erstmeldung, in der angegeben wird, ob der Verdacht besteht, dass der erhebliche Sicherheitsvorfall auf rechtswidrige oder böswillige Handlungen zurückzuführen ist oder grenzüberschreitende Auswirkungen haben könnte;
Nr. 2: unverzüglich, spätestens jedoch innerhalb von 72 Stunden nach Kenntnisnahme des erheblichen Sicherheitsvorfalls, eine Meldung über diesen erheblichen Sicherheitsvorfall, in der die unter Nr. 1 genannten Informationen bestätigt oder aktualisiert werden und eine erste Bewertung des erheblichen Sicherheitsvorfalls, einschließlich seines Schweregrads und seiner Auswirkungen, sowie gegebenenfalls die Kompromittierungsindikatoren angegeben werden;
Nr. 3: auf Ersuchen des CSIRT oder der zuständigen Stelle nach § 2 Absatz 3 einen Zwischenbericht über relevante Statusaktualisierungen;
Nr. 4: spätestens einen Monat und 72 Stunden nach Kenntnisnahme des erheblichen Sicherheitsvorfalls einen Abschlussbericht, der Folgendes enthält:

a) eine ausführliche Beschreibung des erheblichen Sicherheitsvorfalls, einschließlich seines Schweregrads und seiner Auswirkungen;
b) Angaben zur Art der Bedrohung beziehungsweise zugrunde liegenden Ursache, die wahrscheinlich den erheblichen Sicherheitsvorfall ausgelöst hat;
c) Angaben zu den getroffenen und laufenden Abhilfemaßnahmen;
d) gegebenenfalls die grenzüberschreitenden Auswirkungen des erheblichen Sicherheitsvorfalls; dauert der erhebliche Sicherheitsvorfall zu diesem Zeitpunkt noch an, legt die betreffende Stelle statt eines Abschlussberichts zu diesem Zeitpunkt einen Fortschrittsbericht und einen Abschlussbericht innerhalb eines Monats nach Abschluss der Bearbeitung des erheblichen Sicherheitsvorfalls vor.

(2) Wichtige Stellen der unmittelbaren Landesverwaltung unterrichten Empfänger ihrer Dienste unverzüglich über erhebliche Sicherheitsvorfälle, die die Erbringung des jeweiligen Dienstes beeinträchtigten könnten.[1] Sind Empfänger von Diensten der wichtigen Stellen der unmittelbaren Landesverwaltung potenziell von einer erheblichen Cyberbedrohung betroffenen, informieren wichtige Stellen der unmittelbaren Landesverwaltung diese Empfänger über diese erhebliche Cyberbedrohung und teilen ihnen unverzüglich alle Maßnahmen oder Abhilfemaßnahmen mit, die als Reaktion ergriffen werden können.[2]

(3) Das CSIRT übermittelt der meldenden wichtigen Stelle der unmittelbaren Landesverwaltung unverzüglich und nach Möglichkeit innerhalb von 24 Stunden nach Eingang der frühen Erstmeldung nach Absatz 1 Nr. 1 eine Antwort, einschließlich einer ersten Rückmeldung zu dem erheblichen Sicherheitsvorfall und, auf Ersuchen der meldenden wichtigen Stelle der unmittelbaren Landesverwaltung, Orientierungshilfen oder operative Beratung für die Durchführung möglicher Abhilfemaßnahmen.

(4) Das CSIRT leistet auf Ersuchen der meldenden wichtigen Stelle der unmittelbaren Landesverwaltung zusätzliche technische Unterstützung.

(5) Das CSIRT gibt wichtigen Stellen der unmittelbaren Landesverwaltung Orientierungshilfen für die Meldung eines erheblichen Sicherheitsvorfalls an die Strafverfolgungsbehörden und an den Verfassungsschutz im Land Sachsen-Anhalt.

(6) Das CSIRT meldet der zentralen Anlaufstelle nach Artikel 8 Abs. 3 Richtlinie (EU) 2022/2555 unverzüglich grenzübergreifende erhebliche Sicherheitsvorfälle.

(7) Wichtige Stellen der unmittelbaren Landesverwaltung können unbeschadet etwaiger sonstiger Verpflichtungen im Zusammenhang des Umgangs mit Sicherheitsvorfällen im Bereich der Informationssicherheit freiwillig dem CSIRT sie betreffende aktuelle sonstige Sicherheitsvorfälle, Cyberbedrohungen und Beinahe-Vorfälle melden.[1] Das Verfahren nach den Absätzen 1 bis 6 gilt entsprechend.[2] Das CSIRT kann Meldungen zu erheblichen Sicherheitsvorfällen vorrangig bearbeiten.[3] Erforderlichenfalls übermittelt das CSIRT der zentralen Anlaufstelle nach Artikel 8 Absatz 3 Richtlinie (EU) 2022/2555 die Informationen über die eingegangenen Meldungen, wobei sie die Vertraulichkeit und den angemessenen Schutz der von der meldenden wichtigen Stelle der unmittelbaren Landesverwaltung übermittelten Informationen sicherstellen.[4] Unbeschadet der Verhütung, Ermittlung, Aufdeckung und Verfolgung von Straftaten dürfen die freiwilligen Meldungen nicht dazu führen, dass der meldenden wichtigen Stelle der unmittelbaren Landesverwaltung zusätzliche Verpflichtungen auferlegt werden, die nicht für sie gegolten hätten, wenn sie die Meldung nicht übermittelt hätte.[5]

(8) Das für Informationssicherheit zuständige Ministerium wird ermächtigt, durch Rechtsverordnung Bestimmungen zu erlassen über:

Nr. 1: Einzelheiten des Melde- und Hinweisverfahrens;
Nr. 2: die Möglichkeit zur Nutzung von Melde- und Hinweisstellen;
Nr. 3: die Form und Frist der Meldungen und Hinweise, einschließlich statistischen Auswertungen;

Nr. 4: Vorgaben zu meldepflichtigen Informationen, einschließlich Protokollierungsdaten von Schutzsystemen, etwa Proxies, Virenscannern oder Firewalls in automatisierter Form;
Nr. 5: Vorgaben zu weiteren Ausnahmen und Einschränkungen der Meldepflichten nach Absatz 1.

Soweit die Europäische Kommission für wichtigen Stellen der unmittelbaren Landesverwaltung einen Durchführungsrechtsakt gemäß Artikel 23 Abs. 11 Unterabs. 1 Richtlinie (EU) 2022/2555 erlässt, in dem die Art der Angaben, das Format oder das Verfahren der Meldungen festgelegt oder näher bestimmt werden, sind dessen Vorgaben bei der Erstellung der Rechtsverordnung und der Erfüllung der Melde- und Hinweispflichten nach diesem Gesetz einzuhalten.[2]

§ 10 Governance durch Leitungen und Informationssicherheitsbeauftragte der wichtigen Stellen der unmittelbaren Landesverwaltung

(1) Die Leiterin oder der Leiter einer wichtigen Stellen der unmittelbaren Landesverwaltung stellt die Gewährleistung der Informationssicherheit, die Umsetzung und Überwachung der Risikomanagementpflichten nach § 8 und die Einhaltung der Melde- und Hinweispflichten nach § 9 in ihrem Zuständigkeitsbereich sicher.[1] Kommt eine wichtige Stelle der unmittelbaren Landesverwaltung den Pflichten nach §§ 8 und 9 nicht nach, ergreift deren Leiterin oder deren Leiter unverzüglich alle erforderlichen, angemessenen und verhältnismäßigen Korrekturmaßnahmen.[2]

(2) Leiterinnen und Leiter wichtiger Stellen der unmittelbaren Landesverwaltung nehmen regelmäßig an Schulungen teil, um ausreichende Kenntnisse und Fähigkeiten zur Erkennung und Bewertung von Risiken sowie Managementpraktiken im Bereich der Informationssicherheit und deren Auswirkungen auf die von der Stelle erbrachten Dienste zu erwerben.

(3) Zur Unterstützung der Leiterinnen und Leiter wichtiger Stellen der unmittelbaren Landesverwaltung bei der Umsetzung und Überwachung ihrer Pflichten nach den Absätzen 1 und 2 benennen die Leiterinnen und Leiter der wichtigen Stellen der unmittelbaren Landesverwaltung für ihre jeweilige Stelle eine Beauftragte oder einen Beauftragten für Informationssicherheit sowie eine Vertreterin oder einen Vertreter.[1] Beauftragte für Informationssicherheit und deren Vertretung können für mehrere wichtige Stellen der unmittelbaren Landesverwaltung benannt werden, es sei denn, dies widerspricht auf Grund der Größe der einzelnen Stelle dem Grundsatz der effektiven Wahrnehmung der Aufgaben der oder des Beauftragten oder der Vertretung.[2]

(4) Die wichtigen Stellen der unmittelbaren Landesverwaltung unterrichten die für sie zuständigen obersten Landesbehörden und das für Informationssicherheit zuständige Ministerium als zuständige Behörde innerhalb eines Monats über eine Benennung nach Absatz 3 Satz 1.[1] Hierbei übermitteln sie Namen, Anschrift und aktuelle Kontaktdaten einschließlich E-Mail-Adresse und Telefonnummer der benannten Beauftragten und Vertretungen.[2]

(5) Beauftragte für Informationssicherheit fördern, koordinieren, steuern und überwachen die Belange der Informationssicherheit in ihrem Zuständigkeitsbereich.[1] Sie beraten die Leiterin oder den Leiter der wichtigen Stelle der unmittelbaren Landesverwaltung bezüglich der Informationssicherheit und koordinieren entsprechende Umsetzungs- und Überwachungsmaßnahmen einschließlich der Initiierung und der Fortschreibung von Leit- und Richtlinien.[2]

(6) Die oder der Beauftragte für Informationssicherheit berichtet der Leiterin oder dem Leiter der jeweiligen Stelle unmittelbar und anlassbezogen, mindestens jedoch einmal jährlich zum Stand der Informationssicherheit, über die Mittel und Personalausstattung sowie über Sicherheitsvorfälle und erhebliche Sicherheitsvorfälle.

(7) Beauftragte für Informationssicherheit und ihre Vertretungen sind bei der Ausübung ihrer Aufgaben weisungsfrei und dürfen wegen der Erfüllung der ihr oder ihm übertragenen Aufgaben nicht benachteiligt werden.

(8) Beauftragte für Informationssicherheit und ihre Vertretungen müssen zur Erfüllung ihrer Aufgaben fachlich befähigt und mit angemessenen Ressourcen ausgestattet sein.

Teil 4: Aufsichts- und Durchsetzungsmaßnahmen, Datenerhebung und -auswertung

Abschnitt 1: Aufsichts- und Durchsetzungsmaßnahmen

§ 11 Aufsichtsmaßnahmen

(1) Das für Informationssicherheit zuständige Ministerium beaufsichtigt als zuständige Behörde nach § 4 Absatz 1 Satz 2 die Einhaltung der Verpflichtungen der wichtigen Stellen der unmittelbaren Landesverwaltung nach Teil 3 des vorliegenden Gesetzes.

(2) Das für Informationssicherheit zuständige Ministerium kann als zuständige Behörde nach § 4 Absatz 1 Satz 2, um die Einhaltung der Verpflichtungen nach Teil 3 des vorliegenden Gesetzes zu überprüfen, gegenüber wichtigen Stellen der unmittelbaren Landesverwaltung erforderliche Auskünfte und Unterlagen verlangen.[1] Das umfasst insbesondere

> Nr. 1: Informationen, die für die nachträgliche Bewertung der von der betreffenden wichtigen Stelle der unmittelbaren Landesverwaltung ergriffenen Risikomanagementmaßnahmen im Bereich der Informationssicherheit erforderlich sind, einschließlich dokumentierter Informationssicherheitskonzepte;
> Nr. 2: Nachweise für die Umsetzung der Informationssicherheitskonzepte, z. B. der Ergebnisse von Sicherheitsprüfungen, die von einem qualifizierten Prüfer durchgeführt wurden, und die entsprechenden zugrunde liegenden Nachweise.[2]

Den angefragten wichtigen Stellen der unmittelbaren Landesverwaltung werden der Zweck der Anfrage und die erbetenen Informationen mit der Anfrage angegeben.[3] Wichtige Stellen der unmittelbaren Landesverwaltung können dem Auskunftsverlangen dadurch entsprechen, dass sie dem für Informationssicherheit zuständige Ministerium Zugang zu den Daten, Dokumenten und sonstigen Informationen, die den angefragten Auskünften oder Unterlagen zugrunde liegen, einräumen.[4]

(3) Das für Informationssicherheit zuständige Ministerium kann als zuständige Behörde nach § 4 Absatz 1 Satz 2, um die Einhaltung der Verpflichtungen nach Teil 3 des vorliegenden Gesetzes zu überprüfen, gegenüber wichtigen Stellen der unmittelbaren Landesverwaltung durch geschulte Fachkräfte, insbesondere durch das CSIRT, Vor-Ort-Kontrollen und externe nachträgliche Aufsichtsmaßnahmen durchführen.

(4) Das für Informationssicherheit zuständige Ministerium kann als zuständige Behörde nach § 4 Absatz 1 Satz 2, um die Einhaltung der Verpflichtungen nach Teil 3 des vorliegenden Gesetzes zu überprüfen, gezielte Sicherheitsprüfungen und Sicherheitsscans samt zugehöriger Datenverarbeitungen bei wichtigen Stellen der unmittelbaren Landesverwaltung durchführen.[1] Gezielte Sicherheitsprüfungen stützen sich auf Risikobewertungen oder sonstige verfügbare risikobezogene Informationen; die Ergebnisse werden dem für Informationssicherheit zuständigen Ministerium als zuständige Behörde nach § 4 Absatz 1 Satz 2 zur Verfügung gestellt.[2] Sicherheitsscans müssen auf Grundlage objektiver, nichtdiskriminierender, fairer und transparenter Risikobewertungskriterien, erforderlichenfalls auch hin Zusammenarbeit mit der betreffenden wichtigen Stelle der unmittelbaren Landesverwaltung, durchgeführt werden; erlangt das CSIRT bei Durchführung eines Sicherheitsscans Informationen, die durch Artikel 10 des Grundgesetzes für die Bundesrepublik Deutschland geschützt sind, darf es diese nur nach den entsprechenden Vorschriften aus Abschnitt 9 übermitteln und muss die Informationen andernfalls unverzüglich löschen.[3] Gezielte Sicherheitsprüfungen und Sicherheitsscans werden vom CSIRT oder geeigneten und unabhängigen Dritten im Sinne von Artikel 33 Absatz 2 Buchstabe b der Richtlinie (EU) 2022/2555 durchgeführt.[4]

(5) Rechtfertigen Tatsachen, insbesondere nach einem Auskunftsverlangen nach Absatz 2, einer Vor-Ort-Kontrolle nach Absatz 3 oder einer Sicherheitsprüfung oder einem Sicherheitsscan nach Absatz 4, die Annahme, dass eine wichtige Stelle der unmittelbaren Landesverwaltung ihren Verpflichtungen nach Teil 3 des vorliegenden Gesetzes mutmaßlich nicht nachkommt, teilt das für Informationssicherheit zuständige Ministerium als zuständige Behörde nach § 4 Absatz 1 Satz 2 seine Annahme der betroffenen wichtigen Stelle der unmittelbaren Landesverwaltung und der jeweils zuständigen obersten Landesbehörde mit.[1] Die Mitteilung nach Satz 1 ist zu begründen und kann eine Empfehlung angemessener Abhilfemaßnahmen beinhalten.[2]

(6) Die Aufsichtsmaßnahmen des für Informationssicherheit zuständigen Ministeriums müssen geeignet, erforderlich, verhältnismäßig und wirksam sein.

§ 12 Durchsetzungsmaßnahmen

(1) Das für Informationssicherheit zuständige Ministerium stellt als zuständige Behörde nach § 4 Absatz 1 Satz 2 die Einhaltung der Verpflichtungen der wichtigen Stellen der unmittelbaren Landesverwaltung nach Teil 3 des vorliegenden Gesetzes sicher.

(2) Das für Informationssicherheit zuständige Ministerium kann als zuständige Behörde nach § 4 Absatz 1 Satz 2 gegenüber wichtigen Stellen der unmittelbaren Landesverwaltung

Nr. 1: Warnungen über Verstöße gegen diese Festlegungen durch die betroffene wichtige Stelle der unmittelbaren Landesverwaltung aussprechen;
Nr. 2: Anordnungen erlassen, um die betroffene wichtige Stelle der unmittelbaren Landesverwaltung aufzufordern, die festgestellten Mängel oder den Verstoß gegen diese Festlegungen zu beheben;
Nr. 3: Anordnungen erlassen, um die betroffene wichtige Stelle der unmittelbaren Landesverwaltung anzuweisen, das gegen diese Festlegungen verstoßende Verhalten einzustellen und von Wiederholungen abzusehen;
Nr. 4: Anordnungen erlassen, um die betroffene wichtige Stelle der unmittelbaren Landesverwaltung anzuweisen, entsprechend bestimmten Vorgaben und innerhalb einer bestimmten Frist ihre Risikomanagementmaßnahmen im Bereich der Informationssicherheit mit den Vorgaben dieser Festlegungen in Einklang zu bringen;
Nr. 5: Anordnungen erlassen, um die betroffene wichtige Stelle der unmittelbaren Landesverwaltung anzuweisen, potenziell von einer erheblichen Cyberbedrohung betroffene Dritte über die Art der Bedrohung und mögliche Abwehr- oder Abhilfemaßnahmen zu unterrichten, die von diesen als Reaktion auf diese Bedrohung ergriffen werden können;
Nr. 6: Anordnungen erlassen, um die betroffene wichtige Stelle der unmittelbaren Landesverwaltung anzuweisen, die im Rahmen einer Sicherheitsprüfung formulierten Empfehlungen innerhalb einer angemessenen Frist umzusetzen;
Nr. 7: Anordnungen erlassen, um die betroffene wichtige Stelle der unmittelbaren Landesverwaltung anzuweisen, bestimmte Informationen zu festgestellten Verstößen öffentlich bekannt zu machen.

(3) Maßnahmen nach Absatz 2 müssen im Einklang mit den rechtlichen und institutionellen Rahmenbedingungen den Umständen des Einzelfalls Rechnung tragen und dabei zumindest die Schwere des Verstoßes und die Wichtigkeit der Bestimmungen, gegen die verstoßen wurde, die Dauer des Verstoßes; einschlägige frühere Verstöße der betreffenden wichtigen Stelle der unmittelbaren Landesverwaltung, der verursachte materielle oder immaterielle Schaden, darunter finanzieller oder wirtschaftlicher Verlust, Auswirkungen auf andere Dienste und die Zahl der Betroffenen, die von der betroffenen wichtigen Stelle der unmittelbaren Landesverwaltung ergriffenen Maßnahmen zur Verhinderung oder Minderung des materiellen oder immateriellen Schadens sowie die Einhaltung genehmigter Verhaltensregeln oder genehmigter Zertifizierungsverfahren gebührend berücksichtigt werden.[1] Das für Informationssicherheit zuständige Ministerium muss seine Durchsetzungsmaßnahmen ausführlich begründen.[2] Bevor es seine

Durchsetzungsmaßnahmen ergreift, muss es der betroffenen wichtigen Stelle der unmittelbaren Landesverwaltung ihre vorläufigen Erkenntnisse mitteilen und eine angemessene Frist zur Stellungnahme einräumen, es sei denn, dass sofortige Maßnahmen zur Verhütung von Sicherheitsvorfällen oder zur Reaktion auf Sicherheitsvorfälle erforderlich sind.[3]

(4) Das für Informationssicherheit zuständige Ministerium darf Anordnungen und Maßnahmen nach Absatz 2 gegenüber wichtigen Stellen der unmittelbaren Landesverwaltung nur mit dessen Einvernehmen treffen und ergreifen.[1] Im Falle von wichtigen Stellen der unmittelbaren Landesverwaltung nach § 2 Absatz 2 Buchstabe b erteilt das Einvernehmen die für die betroffene Stelle zuständige oberste Landesbehörde.[2] Von der Einhaltung der Vorgaben in den Sätzen 1 und 2 kann das für Informationssicherheit zuständige Ministerium absehen, wenn und soweit zur Gefahrenabwehr ein unverzügliches Handeln erforderlich ist.[3]

(5) Stellt das für Informationssicherheit zuständige Ministerium fest, dass ein Verstoß einer öffentlichen Stelle des Landes gegen Verpflichtungen aus Teil 3 des vorliegenden Gesetzes

> Nr. 1: eine Verletzung des Schutzes personenbezogener Daten im Sinne von Artikel 4 Nummer 12 der Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung) (Abl. L 119 vom 4.5.2016, S. 1, L 314 vom 22.11.2016, S. 72, L 127 vom 23.5.2018, L 74 vom 4.3.2021, S. 35),
> Nr. 2: eine Verletzung von Vorgaben des Gesetzes zur Ausfüllung der Verordnung (EU) 2016/679 und zur Anpassung des allgemeinen Datenschutzrechts in Sachsen-Anhalt vom 18. Februar 2020 (GVBl. LSA S. 25), zuletzt durch das Gesetz vom 10. Mai 2023 (GVBl. LSA S. 228) oder
> Nr. 3: eine Verletzung von Vorgaben des Gesetzes zur Umsetzung der Richtlinie (EU) 2016/680 vom 2. August 2019 (GVBl. LSA S. 218), zuletzt berichtigt am 17.09.2021 (GVBl. LSA S. 490), oder
> Nr. 4: eine Verletzung von Vorgaben des Datenschutzgesetzes Sachsen-Anhalt in der Fassung der Bekanntmachung vom 13. Januar 2016 (GVBl. LSA S. 24) in der jeweils anzuwendenden Fassung, soweit ein Gesetz auf dieses Gesetz verweist,

zur Folge haben kann, unterrichtet es unverzügliche die Landesbeauftragte oder den Landesbeauftragten für den Datenschutz.

Abschnitt 2: Schutz personenbezogener Daten

§ 13 Zweckändernde Datenverarbeitung

(1) Im Zuge der Maßnahmen nach den Teilen 3 und 4 des vorliegenden Gesetzes ist die Verarbeitung personenbezogener Daten zu anderen Zwecken als demjenigen, zu dem die Daten ursprünglich erhoben wurden, zur Sammlung, Auswertung oder Untersuchung von Informationen zu Schwachstellen, Schadprogrammen, erfolgten

oder versuchten Angriffen auf die Sicherheit in den informationstechnischen Systemen und der dabei beobachteten Vorgehensweise oder zur Unterstützung oder Beratung zu Fragen der Informationssicherheit zulässig, wenn sie zur Gewährleistung der Informationssicherheit erforderlich ist und kein Grund zu der Annahme besteht, dass das schutzwürdige Interesse der betroffenen Person an dem Ausschluss der Verarbeitung überwiegt.[1] Die Verarbeitung personenbezogener Daten im Sinne von Artikel 9 Absatz 1 der Verordnung (EU) 2016/679 ist zulässig, wenn die Verarbeitung erforderlich ist zur Abwehr einer erheblichen Gefahr für die Netz-, Daten- oder Informationssicherheit, ein Ausschluss dieser Daten von der Verarbeitung die Erfüllung der Aufgaben des für Informationssicherheit zuständige Ministeriums oder des CSIRT unmöglich machen oder diese erheblich gefährden würde und kein Grund zu der Annahme besteht, dass das schutzwürdige Interesse der betroffenen Person an dem Ausschluss dieser Daten von der Verarbeitung überwiegt.[2]

(2) Im Zuge der Maßnahmen nach den Teilen 3 und 4 des vorliegenden Gesetzes erhobene personenbezogene Daten sind unverzüglich zu löschen, sobald sie für die Abwehr von Gefahren für die Informationssicherheit und informationstechnische Systeme, Komponenten und Prozesse nicht mehr benötigt werden.

§ 14 Datenverarbeitung und -übertragung

(1) Sofern nicht die Absätze 2 bis 9 eine weitere Verarbeitung gestatten, muss eine automatisierte Auswertung der Daten im Zuge der Maßnahmen nach den Teilen 3 und 4 des vorliegenden Gesetzes unverzüglich erfolgen und diese müssen nach erfolgtem Abgleich sofort und nach dem Stand der Technik sicher gelöscht werden.[1] Daten, die weder personenbezogen sind noch dem Fernmeldegeheimnis unterliegen, sind von den Verarbeitungseinschränkungen dieser Vorschrift ausgenommen.[2] Die Daten sind im Gebiet der Europäischen Union zu speichern.[3] Durch organisatorische und technische Maßnahmen nach dem Stand der Technik ist sicherzustellen, dass eine Auswertung der nach Satz 1 gespeicherten Daten nur automatisiert erfolgt.[4] Die Daten sind zu pseudonymisieren, soweit dies automatisiert möglich ist.[5]

(2) Protokolldaten und Protokollierungsdaten dürfen über den für die automatisierte Auswertung erforderlichen Zeitraum hinaus, längstens jedoch für 180 Tage, gespeichert werden, soweit tatsächliche Anhaltspunkte bestehen, dass die Daten erforderlich sein können und eine Speicherung nicht durch andere Rechtsvorschriften gestattet wird:

> Nr. 1: für den Fall der Bestätigung eines Verdachts nach Absatz 4 Satz 1 zur Abwehr von Gefahren für die informationstechnischen Systeme oder
> Nr. 2: zur Verhütung, Unterbindung oder Verfolgung damit zusammenhängender Straftaten und Ordnungswidrigkeiten.[1]

Eine nicht automatisierte Auswertung oder eine personenbezogene Verarbeitung ist nur nach Maßgabe der Absätze 4 bis 8 zulässig.[2] Soweit die Wiederherstellung des Personenbezugs pseudonymisierter Daten erforderlich ist, muss diese durch die zuständige Leiterin oder den zuständigen Leiter der jeweiligen öffentlichen Stelle des Landes angeordnet werden.[3] Diese Entscheidung ist zu dokumentieren.[4]

(3) Inhaltsdaten dürfen über den für die automatisierte Auswertung erforderlichen Zeitraum hinaus, längstens für 180 Tage gespeichert werden, soweit tatsächliche Anhaltspunkte bestehen, dass die Daten erforderlich sein können:

> Nr. 1: für den Fall der Bestätigung eines Verdachts nach Absatz 4 Satz 1 zur Abwehr von Gefahren für die informationstechnischen Systeme,
> Nr. 2: zur Verhütung, Unterbindung oder Verfolgung damit zusammenhängender Straftaten und die Speicherung zum Schutz der technischen Systeme unerlässlich ist.[1]

Die Speicherung und Auswertung der Inhaltsdaten ist von der zuständigen Leiterin oder dem zuständigen Leiter der jeweiligen öffentlichen Stelle des Landes und einer oder einem weiteren Bediensteten dieser Stelle mit fachlicher Befähigung gemäß Absatz 9 anzuordnen.[2] Eine nicht automatisierte Auswertung oder eine personenbezogene Verarbeitung ist nur nach Maßgabe der Absätze 4 bis 8 zulässig.[3] Soweit die Wiederherstellung des Personenbezugs pseudonymisierter Daten erforderlich ist, muss diese durch die zuständige Leiterin oder den zuständigen Leiter der öffentlichen Stelle des Landes und einer oder einen weiteren Bediensteten dieser Stelle mit fachlicher Befähigung gemäß Satz 3 angeordnet werden.[4] Sofern diese Stelle keine weitere Bedienstete oder keinen weiteren Bediensteten mit der Befähigung gemäß Satz 3 beschäftigt, ist die Anordnung der Speicherung und Auswertung der Inhaltsdaten oder der Wiederherstellung des Personenbezugs pseudonymisierter Daten von der Leiterin oder dem Leiter der öffentlichen Stelle des Landes und einer oder einem Bediensteten der Aufsichtsbehörde mit der Befähigung gemäß Absatz 9 zu treffen.[5] Die Anordnung gilt längstens für zwei Monate; sie kann verlängert werden.[6] Diese Entscheidung ist zu dokumentieren.[7]

(4) Die Verarbeitung der in den Absätzen 1 bis 3 genannten Daten ist auch zulässig, wenn

> Nr. 1: bestimmte Tatsachen den Verdacht begründen, dass die Daten Gefahren für die informationstechnischen Systeme etwa durch Schadprogramme, Schwachstellen oder unbefugte Datenverarbeitung enthalten oder Hinweise auf solche Gefahren geben können, und
> Nr. 2 soweit die Datenverarbeitung erforderlich ist, um den Verdacht zu bestätigen oder zu widerlegen.[1]

Im Falle der Bestätigung des Verdachts ist die weitere Verarbeitung der Daten zulässig, soweit die Datenverarbeitung zur Abwehr von Gefahren für die informationstechnischen Systeme erforderlich ist.[2] Ein Schadprogramm darf beseitigt oder in seiner Funktionsweise gehindert werden.[3] Die nicht automatisierte Verarbeitung der Daten nach den Sätzen 1 und 2 darf nur von der Leiterin oder dem Leiter der öffentlichen Stelle des Landes und einer oder einem Bediensteten dieser Stelle mit der Befähigung gemäß Absatz 9 angeordnet werden.[4] Sofern diese Stelle keine weitere Bedienstete oder keinen weiteren Bediensteten mit der Befähigung gemäß Absatz 9 beschäftigt, ist die Anordnung nach Satz 4 von der Leiterin oder dem Leiter der unmittelbaren öffentlichen Stelle des Landes und einer oder einem Bediensteten der Aufsichtsbehörde mit der Befähigung gemäß Absatz 9 zu treffen.[5]

(5) Die von den Maßnahmen nach Absatz 4 betroffenen Personen und betroffenen Stellen sind spätestens nach dem Erkennen und der Abwehr eines Schadprogramms oder von Gefahren, die von einem Schadprogramm ausgehen, zu benachrichtigen, wenn sie bekannt sind oder ihre Identifikation ohne unverhältnismäßigen Aufwand möglich ist sowie nicht überwiegende schutzwürdige Belange Dritter entgegenstehen.[1] Die Benachrichtigung kann unterbleiben, wenn die Person nur unerheblich betroffen wurde und anzunehmen ist, dass sie an einer Benachrichtigung kein Interesse hat.[2] Die unmittelbaren öffentlichen Stellen des Landes legen Fälle, in denen sie von einer Benachrichtigung absehen, der oder dem zuständigen Datenschutzbeauftragten dieser Stellen und einer oder einem weiteren Bediensteten dieser Stellen mit Befähigung gemäß Absatz 9 zur Kontrolle vor.[3] Wenn die oder der zuständige Datenschutzbeauftragte der Entscheidung der öffentlichen Stelle des Landes widerspricht, ist die Benachrichtigung nachzuholen.[4] Die Entscheidung über die Nichtbenachrichtigung ist zu dokumentieren.[5] Die Dokumentation nach Satz 5 darf ausschließlich für Zwecke der Datenschutzkontrolle verwendet werden. Sie ist nach zwölf Monaten zu löschen.[6] In den Fällen der Absätze 7 und 8 erfolgt die Benachrichtigung durch die dort genannten Behörden nach den für diese Behörden geltenden Vorschriften.[7] Enthalten diese keine Bestimmungen zu Benachrichtigungspflichten, sind die Vorschriften der Strafprozessordnung in der Fassung der Bekanntmachung vom 7. April 1987 (BGBl. I S. 1074, 1319), die zuletzt durch Artikel 3 des Gesetzes vom 18. April 2019 (BGBl. I S. 466) geändert worden ist, in der jeweils geltenden Fassung, entsprechend anzuwenden.[8]

(6) Die nach Absatz 4 verarbeiteten personenbezogenen Daten dürfen an die Strafverfolgungsbehörden zur Verfolgung einer Straftat nach den §§ 202a, 202b, 303a oder 303b des Strafgesetzbuches übermittelt werden.[1] Ferner dürfen diese Daten zur Abwehr einer Gefahr für die öffentliche Sicherheit, die unmittelbar von einem Schadprogramm ausgeht, an die zuständigen Polizeibehörden des Landes Sachsen-Anhalt übermittelt werden.[2]

(7) Für sonstige Zwecke dürfen die Daten übermittelt werden an:

> Nr. 1: die Strafverfolgungsbehörden zur Verfolgung einer Straftat von auch im Einzelfall erheblicher Bedeutung, insbesondere einer in § 100a Absatz 2 der Strafprozessordnung bezeichneten Straftat,
> Nr. 2: die Polizeibehörden zur Abwehr einer gegenwärtigen Gefahr für Leib, Leben oder Freiheit einer Person sowie zur Verhütung und Unterbindung von in Nummer 1 genannten Straftaten,
> Nr. 3: die Verfassungsschutzbehörde, wenn tatsächliche Anhaltspunkte für Tätigkeiten nach § 4 Absatz 1 Nummer 3 des Gesetzes über den Verfassungsschutz im Land Sachsen-Anhalt vom 06. April 2006, das zuletzt durch das Gesetz vom 11. Dezember 2024 (GVBl. LSA S. 352) geändert worden ist, oder für Bestrebungen vorliegen, die durch Anwendung von Gewalt oder darauf gerichtete Vorbereitungshandlungen gegen die in § 4 Absatz 1 Nummer 1, 2, 4 und 5 des Gesetzes über den Verfassungsschutz im Land Sachsen-Anhalt genannten Schutzgüter gerichtet sind; die Vorschriften des Gesetzes über den Verfassungsschutz im Land Sachsen-Anhalt bleiben unberührt.[1]

Die Übermittlung nach Satz 1 Nummer 1 und Nummer 2 bedarf der vorherigen

gerichtlichen Zustimmung.[2] Für das Verfahren nach Satz 1 Nummer 1 und Nummer 2 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), das zuletzt durch Artikel 13 des Gesetzes vom 18. Dezember 2018 (BGBl. I S. 2639) geändert worden ist, entsprechend.[3] Zuständig ist das Amtsgericht, in dessen Bezirk die übermittelnde Stelle ihren Sitz hat.[4] Die §§ 9 bis 16 des Artikel 10-Gesetzes vom 26. Juni 2001 (BGBl. I S. 1254, 2298; 2007 I S. 154), das zuletzt durch Artikel 12 des Gesetzes vom 14. August 2017 (BGBl. I S. 3202) geändert worden ist, gelten entsprechend.[5]

(8) Eine über die Absätze 1 bis 7 hinausgehende inhaltliche Auswertung zu anderen Zwecken und die Weitergabe von personenbezogenen Daten an Dritte sind unzulässig.[1] Soweit möglich, ist bei der Datenverarbeitung technisch sicherzustellen, dass Daten, die den Kernbereich privater Lebensgestaltung betreffen, nicht erhoben werden.[2] Werden Erkenntnisse aus dem Kernbereich privater Lebensgestaltung erlangt, dürfen diese Daten nicht verwendet werden und sind unverzüglich zu löschen.[3] Dies gilt auch in Zweifelsfällen. Die Tatsache ihrer Erlangung und Löschung ist zu dokumentieren.[4]

(9) Das für Informationssicherheit zuständige Ministerium wird ermächtigt, Einzelheiten der Anforderungen an die erforderliche fachliche Befähigung bestimmter Stellen im Rahmen der vorstehenden Absätze durch Rechtsverordnung näher zu bestimmen.

Teil 5: Schlussvorschriften

§ 15 Einschränkung von Grundrechten

Das Fernmeldegeheimnis (Artikel 10 des Grundgesetzes für die Bundesrepublik Deutschland, Artikel 14 der Verfassung des Landes Sachsen-Anhalt) und das Recht auf Datenschutz (Artikel 6 Absatz 1 der Verfassung des Landes Sachsen-Anhalt) werden durch §§ 11, 12, 13 und 14 eingeschränkt.

§ 16 Experimentierklausel

Jede oberste Landesbehörde wird im Rahmen ihrer fachlichen Zuständigkeit ermächtigt, durch Rechtsverordnung zur Erprobung neuer Systeme zur Datenanalyse, die der Abwehr von Gefahren für die informationstechnischen Systeme des Landes Sachsen-Anhalt dienen, im Einvernehmen mit der nach § 4 Absatz 3 Satz 1 zuständigen Stelle und mit Zustimmung der oder des Landesbeauftragten für Datenschutz sachlich und örtlich begrenzte Ausnahmen zur Auswertung von anderen nicht in § 14 Absatz 2 genannten Daten für einen Zeitraum von höchstens drei Jahren zuzulassen.

§ 17 Evaluierung

(1) Das für Informationssicherheit zuständige Ministerium legt dem Landtag erstmals zum 31. Dezember 2027 einen Bericht vor, in dem es darlegt, welche Auswirkungen dieses Gesetz auf die Informationssicherheit im Land Sachsen-Anhalt hat, welche Projekte auf Basis der Experimentierklausel des § 16 durchgeführt wurden, welche

Kosten und welcher Nutzen bei der Umsetzung des Gesetzes entstanden sind und ob eine Weiterentwicklung der Vorschriften dieses Gesetzes erforderlich ist.

(2) Nach der Evaluierung gemäß Absatz 1 werden dem Landtag entsprechende Erfahrungsberichte jeweils nach Ablauf weiterer fünf Jahre vorgelegt.

§ 18 Inkrafttreten

Dieses Gesetz tritt am Tag nach der Verkündung in Kraft.

Begründung

A. Allgemeiner Teil

I. Anlass, Ziele und wesentlicher Inhalt des Gesetzes

Die Digitalisierung schafft nicht nur zahlreiche Möglichkeiten, sondern birgt auch Gefahren wie Cyberangriffe, also die gezielte Attacke auf Computer oder Computernetzwerke. Solche Angriffe können neben der Störung von Betriebsabläufen und der Manipulation, Beschädigung oder Zerstörung von Daten, Netzwerken oder technischen Systemen auch den Abfluss von Daten und Informationen oder die Verweigerung von Zugängen nach sich ziehen.

Gerade elementare Einrichtungen, wie sie insbesondere die öffentliche Verwaltung darstellt, müssen sich vor solchen Angriffen schützen und die genannten Risiken für ihre Daten und Informationen und informationstechnischen Systeme minimieren. Vor dem Hintergrund der durch aktuelle geopolitische Entwicklungen („Zeitenwende“) abermals verschärften Bedrohungslage hat sich das Risiko für staatliche Einrichtungen zudem weiter erhöht, durch Gefährdungen aus dem Cyberraum in ihrer Handlungsfähigkeit eingeschränkt zu werden. Ein prägnantes Beispiel für die Folgen unzureichender Cyber- und Informationssicherheit ist der Cyberangriff auf den sich in Sachsen-Anhalt befindenden Landkreis Anhalt-Bitterfeld im Juli 2021, durch den die gesamte IT-Landschaft blockiert und nicht mehr nutzbar wurde. Als Folge konnten etwa Sozial- und Unterhaltsleistungen vorübergehend nicht ausgezahlt werden. Der Landkreis rief den Katstrophenfall aus, die Wiederherstellung der angegriffenen Systeme brachte neben finanziellen auch zeitliche und personelle Herausforderungen mit sich.

Die Resilienz der Verwaltung und ihrer digitalen Systeme ist daher eine fundamentale Anforderung. Um die aus der fortwährend ansteigenden Komplexität der eingesetzten informationstechnischen Systeme erwachsenden Risiken zu vermindern, zunehmend professioneller ausgeführten Angriffe effektiv abzuwehren und die Handlungsfähigkeit der öffentlichen Verwaltung zu wahren, bedarf es neuer gesetzlicher Regelungen und innovativer Technologien. Die Schaffung solcher resilienten Infrastrukturen ist nicht nur eine technische, sondern auch eine strategische Aufgabe. Der zwischen den Landesverbänden der Christlich Demokratischen Union Deutschlands (CDU), der Sozialdemokratischen Partei Deutschlands (SPD) und der Freien Demokratischen Partei (FDP) geschlossene Koalitionsvertrag „Wir gestalten Sachsen-Anhalt. Stark. Modern. Krisenfest. Gerecht.“ hält vor diesem Hintergrund den gemeinsamen Willen fest, für das Land Sachsen-Anhalt ein Landes-IT-Sicherheitsgesetz zu erarbeiten, und sich der Gewährleistung der Informationssicherheit im Land Sachsen-Anhalt ganzheitlich anzunehmen.

Das Gesetz zur Gewährleistung der Informationssicherheit im Land Sachsen-Anhalt verfolgt einen risikobasierten und zugleich ganzheitlichen Ansatz. Das Niveau der Informationssicherheit soll auf ein angemessenes Maß angehoben werden.

Das vorliegende Gesetz zur Gewährleistung der Informationssicherheit im Land Sachsen-Anhalt dient der Umsetzung europarechtlicher Vorgaben: Die Richtlinie (EU) 2022/2555 des Europäischen Parlaments und des Rates vom 14. Dezember 2022

über Maßnahmen für ein hohes gemeinsames Cybersicherheitsniveau in der Union, zur Änderung der Verordnung (EU) Nr. 910/2014 und der Richtlinie (EU) 2018/1972 sowie zur Aufhebung der Richtlinie (EU) 2016/1148 (NIS-2-Richtlinie) (ABl. L. 2333 vom 27.12.2022, S. 80, im Folgenden Richtlinie (EU) 2022/2555), welche die bislang geltende NIS-Richtlinie ablöst, ist nach ihrer Veröffentlichung am 27. Dezember 2022 im Amtsblatt der EU am 16. Januar 2023 in Kraft getreten und war bis zum 17. Oktober 2024 von den Mitgliedstaaten umzusetzen. Die Vorgaben der Richtlinie (EU) 2022/2555 stützen sich auf Artikel 114 AEUV und dienen der Harmonisierung des Binnenmarktes der Europäischen Union. Mit ihnen soll vermieden werden, dass sich die Cybersicherheitsanforderungen im Rahmen ihres Anwendungsbereichs von Mitgliedstaat zu Mitgliedstaat unterscheiden.

II. Voraussichtliche Kosten und haushaltsmäßige Auswirkungen

II. 1 Auswirkungen auf Wirtschaft und Arbeitsmarkt

Aus dem Gesetzesentwurf ergeben sich für Unternehmen allenfalls aus der vorgeschriebenen Verpflichtung von Beliehenen Aufwände. Die Verpflichtung zur Umsetzung von Informationssicherheit besteht aber bereits durch Art. 32 Absatz 1 der Datenschutz-Grundverordnung, so dass durch die Regelung allenfalls unbedeutende Kostenfolgen oder sonstige Belastungen entstehen.
Etwaige Arbeitsmarkteffekte werden daher mit diesem Gesetzesentwurf nicht erzielt.

II. 2 Auswirkungen auf die öffentliche Hand

Übersicht

Bezeichnung	Rechtsquelle	Aufwände einmalig [€]	Aufwände jährlich [€]
Fachpersonal zuständiges Ministerium	§ 4		1.201.000
Sachaufwand Einrichtung Computer-Sicherheitsnotfallteam	§ 5	350.000	60.000
Computer Emergency Response Team (CERT) Nord	§ 5 Absatz 5		396.000
Prüfungen der Informationssicherheit, technische Scans, Penetrationstests u.ä.	§ 5 Absatz 2, § 11		864.000
Erstellung und Pflege von Dokumenten	§ 4 Absatz 2 Satz 2 Nummer 2	250.000	60.000
Betrieb von Systemen zur Überwachung und Analyse von Cyberbedrohungen, Schwachstellen und Sicherheitsvorfällen im Land Sachsen-Anhalt	§ 5 Absatz 2	400.000	250.000
Identifikation wichtiger öffentlicher Stellen	§ 7	220.000	

Qualifikation Informationssicherheitsbeauftragte	§ 10 Absatz 8		200.000
Schulungen Beschäftigte und Leitungen	§ 8 Absatz 1 Nummer 7, § 10 Absatz 2		200.000
Vor-Ort-Kontrollen, Auskünfte u.ä.	§ 11		60.000
Kosten Evaluation (alle 5 Jahre, Kosten jährlich ausgewiesen)	§ 17		5.000
Aufwände summiert		**1.220.000**	**3.296.000**

* Beträge wurden auf Tausend Euro gerundet.

* Nicht quantifizierte/quantifizierbare Kosten wurden in der Übersicht nicht berücksichtigt.

Erläuterung

Die Ermittlung des Erfüllungsaufwandes erfolgt in Orientierung an dem Leitfaden zur Ermittlung und Darstellung des Erfüllungsaufwands bei Gesetzgebungsvorhaben des Bundes. Dieser wurde durch das Statistische Bundesamt im Auftrag der Bundesregierung und des Nationalen Normenkontrollrats im April 2025 herausgegeben.[2]

Für alle berücksichtigungswürdigen Bedarfe des Gesetzesentwurfs gilt aus diesem Grund das Ressortdeckungsprinzip und damit die Einordnung in vorhandene Ansätze; erforderliche Stellen- und Sachmittelbedarfe sind im Bestand abzubilden. Sofern Bedarfe nach Einschätzung der Ressorts nicht im Bestand abbildbar sein sollten, werden diese im Verfahren zur Aufstellung des Haushalts eingebracht. Für die Personalmehrbedarfe der Stelle nach § 4 wird von der Ermöglichung der Neueinstellung bzw. Wiederbesetzung ausgegangen und die hierdurch entstehenden Personalkosten nachfolgend beziffert.

Im Rahmen der Personal- und Sachkostenschätzung wurden die Berechnungen auf die Jahresvollkostendurchschnittssätze der Landesverwaltung Sachsen-Anhalt des Jahres 2024 gestützt. Zusätzlich wurden die Annahme getroffen, dass alle Berechnungen auf Tarifbeschäftigungsbasis beruhen. Die angenommenen Vollzeitäquivalente wurde für Tätigkeiten auf Referentenebene die Eingruppierung in die Entgeltgruppe E14 und für Tätigkeiten auf Sachbearbeiterebene die Eingruppierung in Entgeltgruppe E11 zu Grunde gelegt. Die angenommenen Eingruppierungen entsprechen den durchschnittlich zu erwartenden Arbeitsplatzbewertungen. Die Jahresvollkostendurchschnittssätze der Landesverwaltung Sachsen-Anhalt des Jahres 2024 betragen für die Entgeltgruppe E14 159.637,93 Euro und für die Entgeltgruppe E11 137.256,26 Euro pro Jahr. Beträge wurden auf volle Tausend Euro gerundet.

§ 4 institutionalisiert in Umsetzung von Artikel 8 Absatz 1 und Absatz 2 der Richtlinie (EU) 2022/2555 eine Stelle beim für Informationssicherheit in der Landesverwaltung

[2] https://www.destatis.de/DE/Themen/Staat/Buerokratiekosten/Publikationen/Downloads-Buerokratiekosten/erfuellungsaufwand-handbuch.pdf, Abruf am 07.10.2025

zuständigen Ministerium. Die Stelle nimmt die Aufgabe der kontinuierlichen Verbesserung, Förderung und Koordination der Informations- und Cybersicherheit im Land Sachsen-Anhalt einschließlich der Abwehr von Gefahren für informationstechnische Systeme wahr.

Die Stelle aus § 4 ist bereits beim zuständigen Ministerium als Stabsstelle eingerichtet. Durch den erheblichen Aufgabenzuwachs und die Einrichtung der durchgängigen Rufbereitschaft entsteht zusätzlicher Personalaufwand in Höhe von 1.200.250,72 Euro (1,5 Vollzeitäquivalente Referent/in (E14) zuzüglich 7 Vollzeitäquivalente Sachbearbeiter/in (E11)). Durch diese Kosten werden die zusätzlichen Aufgaben im Bereich Notfall- und Krisenmanagement, kontinuierliche Verbesserung der Informationssicherheit im Land Sachsen-Anhalt, die Koordination der Informationssicherheitsbeauftragten sowie die Durchsetzung und Aufsicht über die verpflichteten öffentlichen Stellen und Abwehr von Gefahren für die Informationssicherheit im Land Sachsen-Anhalt abgedeckt.

In Umsetzung von Artikel 10 Absatz 1 der Richtlinie (EU) 2022/2555 wird bei der Stelle durch § 5 ein qualifiziertes Computer-Sicherheitsnotfallteam (Computer Security Incident Response Team, CSIRT) eingerichtet. Für die Einrichtung eines solchen Computer-Sicherheitsnotfallteams werden Sachaufwände in Höhe von einmalig 350.000 Euro und zusätzlichen 60.000 Euro pro Jahr geschätzt auf der Grundlage von Erfahrungswissen des zuständigen Ministeriums.

Durch die Wahrnehmung von Teilen der Aufgaben des Computer-Sicherheitsnotfallteams durch das Computer Emergency Response Team (CERT) Nord, der Warn- und Informationsdienste, der systematischen Reaktion auf Sicherheitsvorfälle (sogenanntes Incident Response), der Verarbeitung von gemeldeten Sicherheits- und Beinahevorfällen sowie den damit verbundenen Rückgriff auf externe Dienstleistungen entstehen Kosten in Höhe von 396.000 Euro pro Jahr. Diese sind bereits in den Haushaltsmitteln des Einzelplans 19 10 Titelgruppe 682 65 ab dem Jahr 2025 enthalten.

Bei Umsetzung und Erfüllung der insbesondere in § 4 und § 5 aufgelisteten Aufgaben des zuständigen Ministeriums entstehen Personal- und Sachaufwände. Letztere sind zum aktuellen Zeitpunkt nicht sicher und abschließbar quantifizierbar. Die nachfolgend geschätzten Kosten werden nach Tätigkeiten aufgeschlüsselt und setzen sich unter anderem aus Folgenden zusammen:

Für die Durchführung von Prüfungen der Informationssicherheit nach § 11 sowie Maßnahmen nach § 5 Absatz 2 werden Personal- und Sachaufwände von insgesamt 864.000 Euro pro Jahr veranschlagt. Die Schätzung basiert auf der Annahme von sechs Prüfungen der Informationssicherheit und 36 Maßnahmen, wie vorgeschriebene Penetrationstests und berechnet sich anhand von Erfahrungswissen des zuständigen Ministeriums.

Für die Erstellung von Dokumenten gemäß § 4 Absatz 2 fallen einmalig 250.000 Euro Kosten an. Die Überarbeitung und Aktualisierung belaufen sich auf 60.000 Euro pro Jahr. Beide Schätzungen ergeben sich aus Erfahrungswerten des zuständigen Ministeriums. Soweit die Erfüllungsaufwände sich auf wichtige öffentliche Stellen des Landes nach § 2 beziehen, sind sie gemäß Artikel 8 Absatz 5 und Artikel 10 Absätze 2

und 3 der Richtlinie (EU) 2022/2555 als vorgeschriebene, angemessene Ressourcen zur wirksamen und effizienten Aufgabenwahrnehmung anzusehen.

Für den Betrieb von Systemen zur Überwachung und Analyse von Cyberbedrohungen, Schwachstellen und Sicherheitsvorfällen im Land Sachsen-Anhalt gemäß § 20 5 Absatz 2 Nr. 1 fallen schätzungsweise einmalig 400.000 Euro und jährlich 250.000 Euro an. Die Schätzungen basieren auf internen Erfahrungswerten des zuständigen Ministeriums.

§ 7 verpflichtet die obersten Landesbehörden in Umsetzung von Artikel 3 Absatz 3 der Richtlinie (EU) 2022/2555 dazu, solche öffentliche Stellen nach § 2 Absatz 2 Buchstabe b innerhalb ihrer Zuständigkeit, welche Dienste erbringen, deren Störung oder Ausfall über einen Zeitraum von 30 Tagen erhebliche Auswirkungen auf kritische gesellschaftliche oder wirtschaftliche Tätigkeiten haben können, als wichtige öffentliche Stellen des Landes zu identifizieren und gegenüber dem zuständigen Ministerium zu melden. Zur Erfüllung dieser Aufgabe wird in der Regel eine Kooperation mit Behörden im eigenen Zuständigkeitsbereich erforderlich werden.

Hierdurch entstehen bei den obersten Landesbehörden, den ihnen zugewiesenen oberen Landesbehörden, unteren Landesbehörden und Einrichtungen des Landes und dem zuständigen Ministerium einmalig Personalaufwände in Höhe von schätzungsweise 220.000 Euro. Die Schätzung fußt auf der Annahme von 250 öffentlichen Stellen des potentiellen Adressatenkreises. Je öffentlicher Stelle wird von der Bewertung von je fünf Kernprozessen zu je zwei Stunden Aufwand pro Bewertungsvorgang ausgegangen.

Wichtigen öffentlichen Stellen des Landes werden durch § 8 in Umsetzung von Artikel 21 der Richtlinie (EU) 2022/2555 zu Risikomanagementmaßnahmen verpflichtet, die das Ergreifen geeigneter und verhältnismäßiger technischer, operativer und organisatorischer Maßnahmen zur Beherrschung und Verringerung von Risiken für die Informationssicherheit ermöglichen. Hierzu gehören insbesondere auch Schulungen des Leitungspersonals gemäß § 10 Absatz 2. Die hierdurch entstehenden Kosten (Sachkosten, Personalaufwände) bei den wichtigen öffentlichen Stellen des Landes können zum jetzigen Zeitpunkt nicht quantifiziert werden.

Soweit § 8 wichtige öffentliche Stellen des Landes zu angemessenen organisatorischen, operativen und technischen Vorkehrungen zur Gewährleistung der Informationssicherheit verpflichtet, so ist festzustellen, dass der weitaus überwiegende Teil der Verpflichtungen bereits durch bestehende europäische, nationale und landesrechtliche Regelungen normiert ist. Insofern handelt es sich bei den für die Erfüllung dieser Vorgaben erwartbaren Aufwänden größtenteils um Sowieso-Kosten. Neu entstehende Aufwände sind für die Sicherheit der Lieferkette, die Einführung von sicherer Authentifikation und Sicherheit des Personals zu erwarten. Diese Aufwände sind zum aktuellen Zeitpunkt aufgrund der Heterogenität der Landesverwaltung nicht mit verhältnismäßigem Aufwand quantifizierbar.

Bei öffentlichen Stellen des Landes sind Informationssicherheitsbeauftragte und Vertretungen zu benennen gemäß § 10 Absatz 3. Die Aufgaben der Informationssicherheitsbeauftragen sind im Rahmen der bestehenden

Vollzeitäquivalent-Ziele abzubilden. Personelle Kosten sind daher nicht zu veranschlagen.

Die Qualifikationspflichten der Informationssicherheitsbeauftragten nach § 10 Absatz 8 bestehen bereits und sind in Höhe von 200.000 Euro im Einzelplan 19 10 Titel 525 65 ab dem Jahr 2025 berücksichtigt. § 10 Absatz 2 sowie § 8 Absatz 1 Nummer 7 lösen schätzungsweise einen Sachaufwand in Höhe von 200.000 Euro pro Jahr aus. Dieser Schätzwert ergibt sich aus Erfahrungswerten des zuständigen Ministeriums. Der durch das Gesetz verursachte Bedarf in Höhe von 200.000 Euro wird durch das zuständige Ministerium gemäß § 4 zum Haushalt 2027/2028 angemeldet.

Soweit das zuständige Ministerium aus § 4 auf Grund von § 11 zur Auskunft oder Übermittlung von Unterlagen zur Überprüfung der Einhaltung der Vorgaben aus den §§ 7 bis 10 anfordert oder Vor-Ort-Kontrollen durchführt, werden die verpflichteten öffentlichen Stellen des Landes zur Kooperation aufgefordert. Der hierfür erforderliche Personalaufwand beläuft sich schätzungsweise auf 60.000 Euro pro Jahr. Die Schätzungen beruhen auf Erfahrungswerten des zuständigen Ministeriums.

§ 9 verpflichtet wichtige öffentliche Stellen des Landes zu Hinweis- und Meldepflichten gegenüber dem zuständigen Ministerium. Der Erfüllungsaufwand für diese Mitteilungspflichten wurde nicht quantifiziert, da diese aufgrund bisheriger Erfahrungswerte aus dem Land Sachsen-Anhalt und weiterer Bundesländer mit einer zu erwartenden Fallzahl von 50 bis zu 200 pro Jahr für das gesamte Landesgebiet als unwesentlich zu qualifizieren sind.

Mitteilungspflichten der Informationssicherheitsbeauftragten, die sich aus ihrer Bestellung gemäß § 10 Absatz 4 oder aus der Durchführung eigener Prüfungen der Informationssicherheit nach § 10 Absatz 5 ergeben, wurden wegen Unerheblichkeit nicht quantifiziert. Dasselbe gilt für Mitteilungspflichten gegenüber der oder dem Landesbeauftragten für Datenschutz.

Weitergehende Aufwände, die durch eine vertrauensvolle und sachgerechte Kooperation und Zusammenarbeit unterschiedlicher Stellen im Land Sachsen-Anhalt insbesondere aufgrund von Benehmens- oder Einvernehmensvorbehalten, einzuräumenden Vortragsrechten oder Einbeziehungspflichten entstehen, wurden als Sowieso-Kosten nicht quantifiziert.

§ 17 verpflichtet zur regelmäßigen Evaluation dieses Gesetzes. Zur Erfüllung dieser Pflicht entstehen alle fünf Jahre Personalkosten in Höhe von schätzungsweise 25.000 Euro.

II.3 Gesellschaftliche Folgen

Aus dem Gesetzesentwurf ergeben sich für Bürgerinnen und Bürger keine unmittelbaren Verpflichtungen, aus denen sich Kostenfolgen ergeben. Dies umfasst auch spezifische gesellschaftliche Gruppen.

II.4 Sonstige Auswirkungen

Auswirkungen auf Verwaltungsverfahren und Arbeitsaufwand bei öffentlicher Verwaltung und Justiz sind nicht absehbar.

Der vorliegende Gesetzesentwurf ermächtigt zu unterschiedlichen Rechtsverordnungen, die in Folge des Gesetzes zu erwarten sind:

- Ermächtigung des für Informationssicherheit zuständigen Ministeriums zur Bestimmung der Inhalte, Zeiträume und Umfänge der Berichtspflichten nach § 4 Absatz 2 Satz 2 Nr. 6, § 4 Absatz 2 Satz 3;
- Ermächtigung des für Informationssicherheit zuständigen Ministeriums zum Erlass von Bestimmungen zur Identifikation wichtiger Stellen der unmittelbaren Landesverwaltung, § 7 Absatz 2;
- Ermächtigung des für Informationssicherheit zuständigen Ministeriums zur Bestimmung von Einzelheiten zum Meldeverfahren und den zu meldenden Sachverhalten und Informationen, § 9 Absatz 8;
- Ermächtigung des für Informationssicherheit zuständigen Ministeriums zur Bestimmung von Einzelheiten der Anforderungen an die fachliche Befähigung bestimmter Stellen, § 14 Absatz 9;
- Ermächtigung jeder obersten Landesbehörde zur Bestimmung von Regelungen zur Erprobung neuer Systeme zur Datenanalyse, § 16.

Darüber hinaus setzt der Gesetzesentwurf als Teil des Informationssicherheitsmanagements die Erarbeitung und Umsetzung von Informationssicherheitskonzepten bei den verpflichteten Stellen vor.

III. Konnexität

Das Konnexitätsprinzip gemäß Art. 87 Abs. 3 der Verfassung des Landes Sachsen-Anhalt soll sicherstellen, dass Kommunen nicht ohne finanziellen Ausgleich mit zusätzlichen Aufgaben belastet werden. Maßgeblich ist, ob das Gesetz zur Gewährleistung der Informationssicherheit eine neue Aufgabe für die Kommunen schafft oder lediglich bestehende Verpflichtungen konkretisiert. Nach der Rechtsprechung des Landesverfassungsgerichts Sachsen-Anhalt liegt eine neue Aufgabe nur dann vor, wenn eine bisher nicht bestehende Zuständigkeit eingeführt oder eine bestehende Aufgabe wesentlich erweitert wird.

Das Informationssicherheitsgesetz Sachsen-Anhalt schafft für Kommunen keine Verpflichtungen. Es löst somit keinen finanziellen Ausgleichsanspruch der Kommunen gegenüber dem Land aus.

Besonderer Teil

Zu den Bestimmungen im Einzelnen:

Teil 1: Allgemeine Vorschriften

Zu § 1 (Zweck des Gesetzes)
Zentraler Zweck dieses Gesetzes die Erhöhung der Informationssicherheit im Land Sachsen-Anhalt und die Abwehr von Gefahren für informationstechnische Systeme. Beide Begriffe werden in den Begriffsbestimmungen in § 3 definiert.

Informationen und informationstechnische Systeme werden ein immer wichtigerer Bestandteil der digitalen Infrastruktur und damit auch der Digitalisierung der Verwaltung im Land Sachsen-Anhalt. Auch weil die Verwaltung mit Informationen und Daten von Bürgerinnen und Bürgern befasst ist, muss Sachsen-Anhalt einen verantwortungsvollen Umgang mit Informationen und Daten gewährleisten und sicherstellen, dass gerade in Bezug auf diese die informationssicherheitsrechtlichen Schutzziele der Vertraulichkeit, Integrität und Verfügbarkeit nicht beeinträchtigt werden.

Um den immer komplexeren Angriffen auf digitale Infrastrukturen, informationstechnische Systeme, Informationen und Daten erfolgreich begegnen zu können, muss die Verwaltung in der Lage sein, angemessene Abwehrmaßnahmen treffen zu können. Hierfür bedarf es Rechtsgrundlagen, die den strengen Vorgaben des europäischen, nationalen und landesrechtlichen Datenschutzrechtes und der höchstrichterlichen Rechtsprechung genügen. Nur wenn diese Ziele beachtet und Informationen und Daten innerhalb der von der öffentlichen Verwaltung genutzten informationstechnischen Systeme geschützt verarbeitet werden, ist eine vertrauenswürdige, bürgernahe digitale Verwaltung möglich.

Das Informationssicherheitsgesetz Sachsen-Anhalt verpflichtet die wichtigen Stellen der unmittelbaren Landesverwaltung (ein Begriff, der in § 2 Absatz 2 definiert wird) dazu, ein gefahrenübergreifendes und angemessenes Informationssicherheitsniveau herzustellen, zu dokumentieren und einzuhalten, das für die Umsetzung und Erhaltung der genannten Schutzziele erforderlich sind. Das Gesetz verfolgt dabei einen risikobasierten Ansatz, mit dessen Hilfe das Niveau der Informationssicherheit bei öffentlichen Stellen des Landes Sachsen-Anhalt auf ein angemessenes Maß angehoben werden soll. Zugleich schafft das Gesetz erstmalig im Land Sachsen-Anhalt gesetzlich verankerte Organisationsstrukturen zur Sicherung der Informationssicherheit in der Verwaltung.

Das vorliegende Gesetz dient insofern der Umsetzung europarechtlicher Vorgaben und trifft verbindliche Vorgaben für wichtige Einrichtungen der öffentlichen Verwaltung auf regionaler Ebene im Sinne von Richtlinie (EU) 2022/2555 aufgrund von Artikel 3 Absatz 1 Buchstabe d) in Verbindung mit Artikel 2 Absatz 2 Buchstabe f) ii).

Die Gewährleistung der Informationssicherheit und die Abwehr von Gefahren für informationstechnische Systeme ist zugleich eine wichtige im öffentlichen Interesse liegende Aufgabe im Sinne der Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei

der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung) (ABl. L 119 vom 4.5.2016, S. 1; L 314 vom 22.11.2016, S. 72; L 127 vom 23.5.2018, S. 2, im Folgenden Verordnung (EU) 2016/679). Nach dieser stellt die Verarbeitung personenbezogener Daten unter anderem von Computer-Notdiensten (CERT) ein berechtigtes Interesse des jeweiligen Verantwortlichen dar, wie dies für die Gewährleistung der Netz- und Informationssicherheit unbedingt notwendig und verhältnismäßig ist, d.h. soweit dadurch die Fähigkeit eines informationstechnischen Systems gewährleitet wird, mit einem vorgegebenen Grad der Zuverlässigkeit Störungen oder widerrechtliche oder mutwillige Eingriffe abzuwehren, die zur Verfügbarkeit, Authentizität, Vollständigkeit und Vertraulichkeit von gespeicherten oder übermittelten personenbezogenen Daten sowie die Sicherheit damit zusammenhängender Dienste und informationstechnischen Systeme beeinträchtigen. Ein solches berechtigtes Interesse besteht etwa darin, den Zugang Unbefugter zu elektronischen Kommunikationsnetzen und die Verbreitung schädlicher Programmcodes zu verhindern sowie Angriffe in Form der gezielten Überlastung von Servern und Schädigungen von Computer- und elektronischen Kommunikationssystemen abzuwehren. Um Gefahren vorzubeugen gehören auch das Sammeln, Auswerten und Untersuchen von Informationen über Sicherheitsrisiken und -vorkehrungen zu dem Schutz der Informationssicherheit.

Zu § 2 (Anwendungsbereich)

Zu Absatz 1

Das vorliegende Gesetz trifft verpflichtende Regelungen für die und gegenüber den wichtigen Stellen der unmittelbaren Landesverwaltung. Der Begriff greift die Terminologie der „Stellen der unmittelbaren Landesverwaltung“ aus § 1 Absatz 2 Nr. 1 des Gesetzes zur Förderung der elektronischen Verwaltung im Land Sachsen-Anhalt (E-Government-Gesetz Sachsen-Anhalt- EGovG LSA) vom 24. Juli 2019, zuletzt neu gefasst durch das Gesetz vom 16. Februar 2023 (GVBl. LSA S. 34; im Folgenden EGovG LSA) und der „unmittelbaren Landesverwaltung“ im Sinne von § 1 Absatz 1 des Gesetzes über die Organisation der Landesverwaltung Sachsen-Anhalt (Organisationsgesetz Sachsen-Anhalt - OrgG LSA) vom 27. Oktober 2015 zuletzt geändert durch das Gesetz vom 10. Dezember 2015 (GVBl. LSA S. 627, im Folgenden: OrgG LSA) auf und nimmt eine informationssicherheitsrechtliche Qualifizierung auf Grundlage europarechtlicher Vorgaben vor.

Zu Absatz 2

Die wichtigen Stellen der unmittelbaren Landesverwaltung werden definiert. Wichtige Stellen der unmittelbaren Landesverwaltung sind die unter Buchstabe a) genannten obersten Landesbehörden nach § 8 Absatz 1 OrgG LSA und § 1 Absatz 2 Nr. 1 EGovG LSA, sowie die unter Buchstabe b) genannten oberen und unteren Landesbehörden sowie Einrichtungen des Landes nach §§ 9 Absatz 1, 10 Absatz 1 und 11 OrgG LSA, die nach einer risikobasierten Bewertung Dienste erbringt, deren Störung oder Ausfall über einen Zeitraum von 30 Tagen erhebliche Auswirkungen auf kritische gesellschaftliche oder wirtschaftliche Tätigkeiten haben können. Die Definition steht im Einklang mit den verbindlichen Vorgaben des Beschlusses 2023/39 des IT-Planungsrates vom 03.11.2023 und dem dort dargelegten Identifizierungskonzept.

Zu Absatz 3

Absatz 3 stellt klar, dass trotz unterschiedlicher Begrifflichkeiten ein Gleichlauf zu europarechtlichen Vorgaben besteht.

Zu Absatz 4
Absatz 4 zählt in Anlehnung an § 1 Absatz 3 OrgG LSA auf, welche Stellen vom Geltungs- und Anwendungsbereich dieses Gesetzes ausdrücklich ausgenommen sind.

Zu Nummer 1
Der Landtag und seine Verwaltung werden zur Wahrung seiner in Artikel 2 Absatz 2 Satz 3 der Verfassung des Landes Sachsen-Anhalt vom 16. Juli 2022, zuletzt neu verfasst durch das Gesetz vom 20. März 2020 (GVBl. LSA S. 64, im Folgenden Verfassung LSA) verankerten Unabhängigkeit vom Anwendungsbereich des Gesetzes ausgenommen.

Zu Nummer 2, 6 und 7
Die in den Nummern 2, 3 und 5 aufgeführten Landesbeauftragten sind auf Grund ihrer Rechtsstellung in der Ausübung ihrer Ämter unabhängig und nur dem Gesetz unterworfen und werden daher vom Anwendungsbereich des Gesetzes ausgenommen.

Zu Nummer 3
Der Landesrechnungshof wird im Einklang mit § 1 Absatz 3 OrgG LSA vom vorliegenden Gesetz ausgenommen.

Zu Nummer 4
Die Organe der Rechtsprechung und Rechtspflege, die Staatsanwaltschaften sowie die Justizvollzugsanstalten und Jugendstrafanstalten werden im Einklang mit § 1 Absatz 3 OrgG LSA vom vorliegenden Gesetz ausgenommen. Auf diese Weise wird deren Unabhängigkeit gewährleistet.

Zu Nummer 5
Die staatlichen Hochschulen und Universitätsklinika werden vom Anwendungsbereich des Gesetzes ausgenommen.

Zu Nummer 8
Kirchen und als öffentlich-rechtliche Körperschaften anerkannte Religionsgemeinschaften und Weltanschauungsgemeinschaften auf dem Gebiet des Landes Sachsen-Anhalt sowie ihre Verbände, ihre Einrichtungen und ihre Anstalten und Stiftungen des öffentlichen Rechts, die ihren Sitz in Sachsen-Anhalt haben, gehören auf Grund der Trennung von Staat und Kirche nicht zur Landesverwaltung. Sie bleiben Organisationsformen eigener Art und verwalten ihre Angelegenheiten weitgehend selbstständig.

Zu Nummer 9
Der Mitteldeutsche Rundfunk wird im Hinblick auf die in Artikel 5 Absatz 1 des Grundgesetzes für die Bundesrepublik Deutschland vom 23. Mai 1949, zuletzt geändert durch Gesetz vom 20. Dezember 2024 (BGBl. I Nr. 439, im Folgenden GG) bzw. die in Artikel 10 Absatz 1 der Verfassung LSA verankerte Medienfreiheit vom Anwendungsbereich des Gesetzes ausgenommen.

Zu Nummer 10
Um Wettbewerbsverzerrungen zu vermeiden, werden auch die öffentlich-rechtlichen Kreditinstitute und öffentlich-rechtliche Versicherungsanstalten im Land Sachsen-Anhalt vom Anwendungsbereich des Gesetzes ausgenommen. Kreditinstitute unterliegen in der Ausgestaltung ihrer IT-Landschaft spezifischen bankaufsichtsrechtlichen Anforderungen. Es gilt, konkurrierende Anforderungen zu vermeiden. Hierzu gehören etwa die Verordnung (EU) 2022/2554 über die digitale operationale Resilienz im Finanzsektor (Digital Operational Resilience Act) und die bankaufsichtsrechtlichen Anforderungen an die IT (BAIT) der Bundesanstalt für Finanzdienstleistungsaufsicht.

Zu Nummer 11
Die Richtlinie (EU) 2022/2555 gilt ausweislich Artikel 2 Absatz 7 nicht für Einrichtungen der öffentlichen Verwaltung, die ihre Tätigkeiten in den Bereichen nationale Sicherheit, öffentliche Sicherheit, Verteidigung oder Strafverfolgung ausüben, einschließlich der Verhütung, Ermittlung, Aufdeckung und Verfolgung von Straftaten. § 2 Absatz 4 Nr. 11 setzt diese Beschränkung des Geltungsbereichs in Landesrecht um.

Zu § 3 (Begriffsbestimmungen)

In § 3 werden zentral die in diesem Gesetz verwendeten Begriffe im Einklang mit übergeordnetem europäischen, nationalen und Landesrecht definiert.

Zu Absatz 1
Ein „Beinahevorfall“ ist gegeben, sobald eines der drei Schutzziele der Informationssicherheit, mithin Vertraulichkeit, Integrität oder Verfügbarkeit im beschriebenen Maße verletzt wird. Hierunter fallen auch aber nicht nur Zugriffsversuche auf vermutete Sicherheitslücken in den informationstechnischen Systemen der unmittelbaren und mittelbaren Landesverwaltung in Sachsen-Anhalt. Die Definition stellt eine Umsetzung von Artikel 6 Nummer 5 der Richtlinie (EU) 2022/2555 dar.

Zu Absatz 2
Der Begriff der „Cyberbedrohung“ wird im Einklang mit der Definition einer Cyberbedrohung im Sinne des Artikel 6 Nummer 10 der Richtlinie (EU) 2022/2555 definiert.

Zu Absatz 3
Der Begriff der „erheblichen Cyberbedrohung“ wird im Einklang mit der Definition einer erheblichen Cyberbedrohung im Sinne des Artikel 6 Nummer 11 der Richtlinie (EU) 2022/2555 definiert.

Zu Absatz 4
Die Begriffsbestimmung des „erheblichen Sicherheitsvorfalls“ dient der Umsetzung von Artikel 23 Absatz 3 und Absatz 11 Unterabs. 2 der Richtlinie (EU) 2022/2555 und damit der europaweiten Vereinheitlichung der Terminologie.

Zu Absatz 5

Ein „Sicherheitsvorfall“ tritt ein, sofern eines der drei Schutzziele (Verfügbarkeit, Vertraulichkeit oder Integrität) beeinträchtigt wurde. Die Begriffsbestimmung dient damit der Umsetzung von Artikel 6 Absatz 6 Nummer 6 der Richtlinie (EU) 2022/2555 und muss europarechtskonform ausgelegt und angewandt werden.

Zu Absatz 6

Die Begriffsbestimmung der „Schwachstelle“ dient der Umsetzung von Artikel 6 Nummer 15 der Richtlinie (EU) 2022/2555. Eine Schwachstelle ist eine unerwünschte Eigenschaft von informationstechnischen Systemen, insbesondere Computerprogrammen, die es Dritten erlauben, gegen den Willen der Berechtigten deren Informationstechnik zu beeinflussen. Hierfür genügt es, wenn die Funktionsweise in sonstiger Weise beeinträchtigt wird, z.B. durch ungewolltes Abschalten, Umleiten von Eingaben oder sonstige mittelbare Beeinflussung. Notwendig ist es nicht, dass sich Dritte Zugang zu dem System verschaffen und dieses manipulieren. Der Begriff ist bewusst und notwendigerweise weit gefasst, da Schwachstellen in unterschiedlichsten Zusammenhängen, oftmals abhängig von der Konfiguration oder Einsatzumgebung, entstehen können.

Zu Absatz 7

Die Begriffsbestimmungen dienen der Umsetzung von Artikel 6 Nummer 12 und 13 der Richtlinie (EU) 2022/2555.

Mit „IKT-Dienst“ ist nach der Verordnung (EU) 2019/881 ein Dienst gemeint, der vollständig oder überwiegend aus der Übertragung, Speicherung, Abfrage oder Verarbeitung von Informationen mittels informationstechnischer Systeme, Komponenten und Prozessen besteht.

Mit „IKT-Produkt“ ist in der Verordnung (EU) 2019/881 ein Element oder eine Gruppe von Elementen eines Netz- oder Informationssystems gemeint. Hierunter fallen sowohl Hardwareprodukte als auch Softwareprodukte. Der Begriff wird zur europaweiten Vereinheitlichung der Terminologie im Rahmen der Umsetzung der Richtlinie (EU) 2022/2555 eingeführt.

Ein „IKT-Prozess“ bezeichnet nach der Verordnung (EU) 2019/881 jegliche Tätigkeiten, mit denen ein ITK-Produkt oder -Dienst konzipiert, entwickelt, bereitgestellt oder gepflegt werden soll.

Zu Absatz 8

Absatz 8 definiert den Begriff der „Informationssicherheit“ und setzt Artikel 6 Nummer 5 der Richtlinie (EU) 2022/2555 um. Dem Gesetz liegt ein weites Verständnis von Informationssicherheit zu Grunde. Dieses orientiert sich an der etablierten Definition des IT-Grundschutz-Kompendiums des BSI und umfasst insbesondere die von Artikel 1 Absatz 1 der Richtlinie (EU) 2022/2555 genannte Cybersicherheit, die sich an der Begriffsbestimmung nach Artikel 2 Nummer 1 der Verordnung (EU) 2019/881 des Europäischen Parlaments und des Rates vom 17. April 2019 über die ENISA (Agentur der Europäischen Union für Cybersicherheit) und über die Zertifizierung der Cybersicherheit von Informations- und Kommunikationstechnik und zur Aufhebung der Verordnung (EU) Nr. 526/2013 (Rechtsakt zur Cybersicherheit, im Folgenden Verordnung (EU) 2019/881) orientiert.

Ziel der Informationssicherheit im Sinne des vorliegenden Gesetzes ist der Schutz von Informationen und Daten, unabhängig von ihrer digitalen oder analogen Beschaffenheit. Schutz von Informationen und Daten ist gewährleistet, sofern die drei grundlegenden Schutzziele (Vertraulichkeit, Integrität und Verfügbarkeit) gewährleistet werden, und zwar sowohl innerhalb als auch außerhalb einer konkreten Gefahrensituation. Die Informationssicherheit umfasst neben den eigentlichen Informationen und Daten insbesondere auch die informationstechnischen Systeme, in denen diese verarbeitet werden, sowie auch organisatorische und personelle Rahmenbedingungen. Der Begriff der Informationssicherheit umfasst insbesondere auch die Gewährleistung und Wiederherstellung der genannten Schutzziele im Falle einer Störung, eines Notfalls oder einer Großschadenslage.

Zu Absatz 9
Ein „Informationssicherheitsmanagementsystem“ (ISMS) dient der Steuerung der Informationssicherheit einer Organisation. Ein solches ISMS existiert auch ohne schriftliche Dokumentation oder anderweitige Beschreibung. Aufgabe eines ISMS ist es, ein angemessenes Informationssicherheitsniveau festzulegen und dieses umzusetzen bzw. aufrechtzuhalten. Die Standards des BSI bilden hierfür (in der jeweils geltenden Fassung) den Rahmen. Grundvoraussetzung ist das Vorliegen einer Informationssicherheitsorganisation.

Das ISMS ist in der Organisation verankert und umfasst neben der Erstellung und Umsetzung von Sicherheitskonzepten die Festlegung und Dokumentation von Verantwortlichen. Hinzu kommt die Erstellung jeweils verbindlicher Leitlinien und Richtlinien für die Informationssicherheit, die Festlegung und Dokumentation von Abläufen bei Sicherheitsvorfällen sowie die Etablierung von Prozessen, durch die die Informationssicherheitsmaßnahmen regelmäßig kontrolliert und gegebenenfalls durch die Einleitung erforderlicher Maßnahmen sichergestellt werden. Auch die Sensibilisierung aller Beschäftigten der öffentlichen Verwaltung zu Themen der Informationssicherheit gehört zu dem ISMS.

Zu Absatz 10
Als „informationstechnisches System“ im Sinne dieses Gesetzes gilt jedes daten- oder informationsverarbeitende System, unabhängig von seiner Größe oder seinem Zweck.

Hierunter fallen insbesondere, aber nicht abschließend: Server, Netzwerkgeräte, PCs, Notebooks, Telefone, Tablets, Drucker, Heizungssteuerungen, intelligente mit dem Internet verbundene (Haushalts-) Geräte, Industriesteuerungen sowie die jeweils dazugehörige Software und Netze sowie auch verteile Systeme aus mehreren verschiedenen der hier aufgelisteten Komponenten oder Teile bzw. das gesamte Internet.

Der Begriff ist bewusst offen gestaltet, um zukünftigen technischen Entwicklungen Rechnung zu tragen. Insgesamt fällt unter den Begriff eines informationstechnischen Systems jedes System, welches in elektronischer Weise Informationen oder Daten erfasst, speichert, verarbeitet, nutzt, übermittelt oder löscht.

Zu Absatz 11

Unter dem Begriff der „Inhaltsdaten“ werden solche Daten verstanden, die den Inhalt der Kommunikation betreffen. Damit wird eine Negativabgrenzung zu den Begriffen der Verkehrsdaten und den Protokolldaten aufgenommen. Da diese in § 3 Nummer 70 des Telekommunikationsgesetz vom 23. Juni 2021, zuletzt geändert durch Gesetz vom 06.05.2024 (BGBl. 2024 I Nr. 149, im Folgenden TKG) legal definiert sind, werden sie nicht zusätzlich im Rahmen dieses Gesetzes definiert.

Zu Absatz 12
Absatz 12 grenzt „Protokolldaten“ von den „Protokollierungsdaten“ nach Absatz 13, aber auch von „Inhaltsdaten“ nach Absatz 11 ab und definiert sie als technische Steuerdaten, die beim Aufbau und der Aufrechterhaltung von Kommunikationsverbindungen zwischen IT-Systemen ausgetauscht werden.

Protokolldaten enthalten keine inhaltlichen Informationen der Kommunikation selbst, sind aber notwendig für deren Funktion – z. B. IP-Adressen, Zeitstempel oder Portnummern. Diese Daten können sowohl Verkehrsdaten im Sinne des TKG als auch Nutzungsdaten nach dem Gesetz über den Datenschutz und den Schutz der Privatsphäre in der Telekommunikation und bei digitalen Diensten vom 23.06.2021 (Telekommunikation-Digitale-Dienste-Datenschutz-Gesetz-TDDDG), zuletzt geändert durch Gesetz vom 12.07.2024 (BGBl. 2024 I Nr. 234, im Folgenden TDDDG), umfassen.

Ihre rechtliche Erfassung und Verarbeitung ist unter datenschutzrechtlichen Vorgaben möglich, insbesondere wenn sie der Absicherung der IT-Kommunikation dienen. Die Definition schafft Klarheit über die datenschutzrechtliche Einordnung und ermöglicht eine differenzierte Behandlung im Rahmen von Sicherheitsmaßnahmen.

Zu Absatz 13
Absatz 13 definiert „Protokollierungsdaten“ als Aufzeichnungen über technische Ereignisse oder Zustände innerhalb informationstechnischer Systeme. Diese Daten dienen der Nachvollziehbarkeit und Kontrolle von Vorgängen im System – etwa bei der Anmeldung von Nutzerinnen und Nutzern, dem Zugriff auf Dateien oder der Konfiguration von Systemkomponenten. Sie sind ein zentrales Element zur Sicherstellung von IT-Sicherheit und ermöglichen sowohl Fehleranalysen als auch die Aufklärung von Sicherheitsvorfällen.

Zu Absatz 14
„Schadprogramme“ beziehen sich auf Daten und ermöglichen die unbefugte Verarbeitung oder Einflussnahme auf informationstechnische Abläufe.

Die Begriffsbestimmung umfasst den weiten Verarbeitungsbegriff des Datenschutzrechts, der das Erfassen, Speichern, Verändern, Verwenden, Übermitteln, Einschränken, Löschen oder Vernichten von Daten beinhalten kann. Eine unbefugte Datenverarbeitung ist gegeben, sofern irregulär auf den Datenverarbeitungsprozess eingewirkt wird. Ausgenommen hiervon sind unbeabsichtigte Sicherheitslücken in normalen Programmen.

Ein Schadprogramm ist hiernach jede Software, die genutzt wird, um einen Schaden zu verursachen. Es kommt hierbei entscheidend auf den tatsächlichen Einsatz der Software an, also auf das unbefugte und unerwünschte Ausführen von Funktionen.

Ausschlaggebend ist hingegen nicht die Intention des Programmierers bei der Entwicklung der Software.

Die Verursachung eines materiellen oder immateriellen Schadens ist ebenfalls keine zwingende Voraussetzung, um den Begriff des Schadprogrammes zu erfüllen. Auch der Versand von Spam, also die massenhafte Versendung unerwünschter E-Mails oder sogenannte „DDoS-Angriffe“ (Distributed Denial of Service; Massenanfragen, um Server durch Überlastung lahmzulegen) ist eine informationstechnische Routine, die geeignet ist, unbefugt informationstechnische Prozesse zu beeinflussen.

Zu Absatz 15
Die Begriffsbestimmung dient der Überführung des Begriffs in Artikel 11 Absatz 3 Buchstabe e) der Richtlinie (EU) 2022/2555 in Landesrecht. Der Begriff ist offen formuliert, um zukünftigem technischem Fortschritt Rechnung zu tragen.

Teil 2: Organisation der Informationssicherheit

Zu § 4 (Informationssicherheit im Land Sachsen-Anhalt)

Zu Absatz 1
Absatz 1 bestimmt das für Informationssicherheit zuständige Ministerium zur obersten Landesbehörde im Bereich der Informationssicherheit. Damit wird eine klare Zuständigkeitsverteilung im Land Sachsen-Anhalt geschaffen, die den unionsrechtlichen Vorgaben der Richtlinie (EU) 2022/2555 entspricht. Nach Artikel 8 Absätze 1 und 2 der Richtlinie (EU) 2022/2555 sind die Mitgliedstaaten verpflichtet, eine oder mehrere zuständige Behörden im Bereich der Informationssicherheit zu benennen. Diese Behörden müssen für die Umsetzung, die Koordinierung und die Überwachung der Einhaltung der Richtlinie sorgen. Absatz 1 trägt dieser Verpflichtung Rechnung, indem die Aufgaben zentral dem für Informationssicherheit zuständigen Ministerium zugewiesen werden.

Zu Absatz 2
Absatz 2 konkretisiert nicht abschließend die strategischen und koordinierenden Aufgaben des für Informationssicherheit zuständigen Ministeriums. Er dient damit insbesondere der Umsetzung von Artikel 8 Absätze 1 und 2, Artikel 9 sowie Artikel 23 Absatz 7 der Richtlinie (EU) 2022/2555 und legt die Rolle des Ministeriums als zentrale Koordinierungs- und Aufsichtsbehörde im Bereich der Informationssicherheit im Land Sachsen-Anhalt fest. Satz 3 ermächtigt das Ministerium, die Inhalte, Zeiträume und Umfänge der Berichtspflichten im Sinne des Artikel 23 Absatz 7 der Richtlinie (EU) 2022/2555 im Wege einer Rechtsverordnung näher zu bestimmen. Dies gewährleistet Flexibilität, um auf veränderte Bedrohungslagen und organisatorische Erfordernisse reagieren zu können, ohne dass es einer Gesetzesänderung bedarf.

Zu Absatz 3
Nach Absatz 3 wird beim für Informationssicherheit zuständigen Ministerium eine spezifische Stelle eingerichtet; deren Aufgabe besteht insbesondere darin, die Einhaltung des Gesetzes in Sachsen-Anhalt zu überwachen und die Umsetzung der Richtlinie (EU) 2022/2555 auf Landesebene zu koordinieren.

Absatz 3 dienst der Umsetzung der europarechtlichen Vorgaben aus Artikel 8 Absätze 1 und 2 der Richtlinie (EU) 2022/2555 um. Danach sind die Mitgliedstaaten verpflichtet, eine oder mehrere zuständige Behörden für die Umsetzung der Richtlinie zu benennen, welche in ihrer Aufgabenwahrnehmung weisungsfrei und operativ unabhängig handeln können muss.

Zu Absatz 4
Absatz 4 regelt die europarechtlich vorgegebene Meldepflicht der zuständigen Behörden gegenüber dem zuständigen Bundesministerium sowie dem Bundesamt für Sicherheit und Informationstechnik, dass sie zuständige Behörde im Sinne des Artikel 8 der Richtlinie (EU) 2022/2555 ist, vgl. Artikel 3 Absatz 3 der Richtlinie (EU) 2022/2555.

Zu Absatz 5
Die zuständige Behörde nach Absatz 1 und die nach Absatz 3 eingerichtete Stelle können sich zur Wahrnehmung ihrer Aufgaben des Computer-Sicherheitsnotfallteams nach § 5 sowie anderer geeigneter Dritter bedienen. Damit kann die bereits etablierte Praxis der Zusammenarbeit mit bestehenden Strukturen – etwa dem Computer Emergency Response Team (CERT Nord) der Dataport AöR – weitergeführt und vertieft werden. Alternativ können auch andere sogenannte Security Operation Center (kurz: SOC)-Dienstleister eingebunden werden, die ein angemessenes Schutzniveau gewährleisten können.

Zu Absatz 6
Absatz 6 setzt die Vorgaben des Artikel 3 Absatz 4 der Richtlinie (EU) 2022/2555 um.

Zu § 5 (Computer-Sicherheitsnotfallteam (CSIRT))

Zu Absatz 1
Absatz 1 dient der Umsetzung von Artikel 10 Absatz 1 der Richtlinie (EU) 2022/2555. Danach sind für die Mitgliedstaaten Computer-Sicherheitsnotfallteams (CSIRTs) einzurichten oder zu benennen, die auch die öffentliche Verwaltung auf Landesebene abdecken. Das CSIRT wird daher bei dem für Informationssicherheit zuständigen Ministerium eingerichtet.

Die organisatorische Verortung gewährleistet die Nähe zu den ressortübergreifenden Steuerungs- und Koordinierungsaufgaben im Bereich der Informationssicherheit. Damit wird zugleich die Anbindung an bundesweite und europäische Strukturen des CSIRT-Netzwerks (Artikel 12 der Richtlinie (EU) 2022/2555) sichergestellt.

Zu Absatz 2
Absatz 2 konkretisiert die in Artikel 11 Absatz 3 und Absatz 5 der Richtlinie (EU) 2022/2555 formulierten Aufgabenbereiche und passt sie an die Gegebenheiten des Landes Sachsen-Anhalt an. Je nach Aufgabenzuweisung stehen die genannten Aufgaben im Zusammenhang mit Befugnisnormen und den dort genannten Anforderungen. Durch diese Aufgabenzuweisung wird sichergestellt, dass das CSIRT über ein vollständiges Mandat verfügt, um sowohl präventive als auch reaktive Maßnahmen ergreifen zu können. Gleichzeitig wird ein enger Bezug zu den nationalen und europäischen CSIRT-Strukturen hergestellt.

Satz 3 setzt Artikel 11 Absatz 3 Unterabs. 3 der Richtlinie (EU) 2022/2555 um.

Zu Absatz 3
Absatz 3 setzt die Vorgaben aus Artikel 23 Absatz 10 der Richtlinie (EU) 2022/2555 um.

Zu Absatz 4
Absatz 4 konkretisiert die einzuhaltenden Anforderungen aus Artikel 11 der Richtlinie (EU) 2022/2555 an die Ausstattung eines CSIRT. Danach müssen CSIRTs jederzeit erreichbar sein, ihre Kommunikationskanäle redundant auslegen, über sichere Standorte verfügen und mit einem System zur effizienten Weiterleitung von Anfragen arbeiten. Damit wird sichergestellt, dass das CSIRT jederzeit funktionsfähig bleibt, auch bei physischen oder technischen Störungen.

Zu Absatz 5
Das CSIRT kann sich zur Erfüllung seiner Aufgaben solcher Dritter bedienen, die aufgrund ihrer Befähigung, technischen Ausstattung und vergleichbaren Rahmenbedingungen geeigneter Dritter bedienen. Damit wird die bereits etablierte Praxis der Zusammenarbeit mit bestehenden Strukturen – etwa dem Computer Emergency Response Team (CERT Nord) der Dataport AöR – weitergeführt und vertieft. Die politische Verantwortung für das CSIRT verbleibt beim zuständigen Ministerium.

Zu § 6 (Zusammenarbeit in der Informationssicherheit)

Zu Absatz 1
Absatz 1 wiederholt den Grundsatz der kooperativen Kommunikation und Zusammenarbeit, der die unmittelbare Landesverwaltung im Bereich der Informationssicherheit insbesondere auch hinsichtlich der Abwehr von Gefahren für informationstechnische Systeme zu enger und vertrauensvoller Zusammenarbeit verpflichtet.

Zu Absatz 2
Absatz 2 setzt verschiedene Kooperationspflichten etwa aus Artikel 31 Absatz 3 und Artikel 33 Absatz 6 der Richtlinie (EU) 2022/2555 in Landesrecht hat um.

Teil 3: Informationssicherheit bei öffentlichen Stellen des Landes

Zu § 7 (Identifikation der wichtigen Stellen der unmittelbaren Landesverwaltung)

Zu Absatz 1
Absatz 1 dient der Umsetzung von Artikel 2 Absatz 2 Buchstabe f Unterbuchstabe ii und Artikel 3 Absatz 3 der Richtlinie (EU) 2022/2555.

Die obersten Landesbehörden identifizieren innerhalb ihrer Zuständigkeit jene oberen Landesbehörden, unteren Landesbehörden, Einrichtungen des Landes und Landesbetriebe im Sinne der §§ 9 bis 12 OrgG LSA, die nach der Definition des § 2 Absatz 2 Buchstabe b) als wichtige Stellen der unmittelbaren Landesverwaltung zu

gelten haben. § 7 ist insofern im engen Zusammenhang mit § 2 Absatz 1 und Absatz 2 zu verstehen.

Die Identifikation hat nach den Vorgaben der Rechtsverordnung nach Absatz 2 zu erfolgen.

Satz 2 bestimmt eine erste Identifikationsfrist sowie eine regelmäßige Überprüfungs- und Meldepflicht der obersten Landesbehörden.

Zu Absatz 2
Absatz 2 stellt die Ermächtigungsgrundlage dar, nach der das nach § 4 Absatz 1 Satz 1 für Informationssicherheit zuständige Ministerium eine Rechtsverordnung erlassen kann, die Bestimmungen über das Verfahren zur Durchführung der Identifikation wichtiger öffentlicher Stellen des Landes nach Absatz 1, die Aufgaben und die Pflichten im Rahmen der Zusammenarbeit bei der Identifikation und die Form dieser Identifikation enthält.

Ziel ist, die Empfehlungen des IT-Planungsrates, insbesondere jene aus dem Beschluss 2023/39 vom 03.11.2023 und dem dort vorgeschlagenen Identifizierungskonzept, vollumfänglich in Landesrecht umzusetzen. Die Ermächtigung zur Rechtsverordnung erscheint zur Gewährleistung einer flexiblen Anpassung der Identifizierungsgrundsätze angemessen.

Zu Absatz 3
Absatz 3 bestimmt, welche Informationen nach erfolgter Identifizierung nach Absatz 1 weiterzureichen sind.

Zu § 8 (Pflichten der wichtigen Stellen der unmittelbaren Landesverwaltung zu Risikomanagement im Bereich der Informationssicherheit)

Zu Absatz 1
Absatz 1 verpflichtet die wichtigen Stellen der unmittelbaren Landesverwaltung zu geeigneten, verhältnismäßigen und wirksamen Risikomanagementmaßnahmen im Bereich der Informationssicherheit, und setzt damit die Vorgaben aus Artikel 21 Absatz 1 Unterabs. 1 der Richtlinie (EU) 2022/2555 in Landesrecht um. Die in Satz 2 genannten Teilmaßnahmen setzen die Vorgaben aus Artikel 21 Absatz 2 der Richtlinie (EU) 2022/2555 in Landesrecht um.

Zu Absatz 2
Absatz 2 normiert Maßgaben und Rahmenbedingungen für die nach Absatz 1 vorzunehmenden Risikomanagementmaßnahmen. Dabei setzt Absatz 2 die Vorgaben aus Artikel 21 Absatz 1 Unterabs. 2 sowie aus Artikel 21 Absatz 2 Satz 1 Halbsatz 1 der Richtlinie (EU) 2022/2555 in Landesrecht um.

Zu Absatz 3
Absatz 3 setzt die Vorgaben aus Artikel 21 Absatz 3 der Richtlinie (EU) 2022/2555 in Landesrecht um.

Zu Absatz 4

Absatz 4 stellt klar, dass wichtige Stellen der unmittelbaren Landesverwaltung das CSIRT zur Erfüllung ihrer Pflichten nach den Absätzen 1 bis 3 um Unterstützung ersuchen dürfen. Damit setzt Absatz 4 insbesondere Maßgaben aus Artikel 11 Absatz 3 Buchstabe c) und Artikel 23 Absatz 5 Satz 2 und Satz 3 der Richtlinie (EU) 2022/2555 in Landesrecht um.

Zu Absatz 5
Absatz 5 ermöglicht eine ordnungsgemäße Umsetzung der Vorgaben aus Artikel 33 Absatz 2 Buchstabe f) der Richtlinie (EU) 2022/2555.

Zu § 9 (Melde- und Hinweispflichten)

Zu Absatz 1
§ 9 Absatz 1 setzt die Berichts- und Informationspflichten nach Artikel 23 Absatz 4 der Richtlinie (EU) 2022/2555 in Landesrecht um.

Zu Absatz 2
Absatz 2 setzt die Vorgaben aus Artikel 23 Absatz 1 Satz 2 und Absatz 2 der Richtlinie (EU) 2022/2555 in Landesrecht um.

Zu Absatz 3
Absatz 3 setzt die Vorgaben aus Artikel 23 Absatz 5 Satz 1 der Richtlinie (EU) 2022/2555 in Landesrecht um.

Zu Absatz 4
Absatz 4 setzt die Vorgaben aus Artikel 23 Absatz 5 Satz 3 der Richtlinie (EU) 2022/2555 in Landesrecht um.

Zu Absatz 5
Absatz 5 setzt die Vorgaben aus Artikel 23 Absatz 5 Satz 4 der Richtlinie (EU) 2022/2555 in Landesrecht um.

Zu Absatz 6
Absatz 6 setzt die Vorgaben aus Artikel 23 Absatz 6 der Richtlinie (EU) 2022/2555 in Landesrecht um.

Zu Absatz 7
Absatz 7 setzt die Vorgaben zu freiwilligen Meldungen aus Artikel 30 Absatz 1 und Absatz 2 der Richtlinie (EU) 2022/2555 in Landesrecht um.

Satz 1 setzt die Vorgaben aus Artikel 3 Absatz 1 der Richtlinie (EU) 2022/2555 in Landesrecht um. Satz 2 setzt Artikel 30 Absatz 2 Unterabs. 1 Satz 1 der Richtlinie (EU) 2022/2555 in Landesrecht um. Satz 3 setzt Artikel 30 Absatz 2 Unterabs. 1 Satz 2 der Richtlinie (EU) 2022/2555 in Landesrecht um. Satz 4 stellt sicher, dass Artikel 23 Absatz 6 der Richtlinie (EU) 2022/2555 in Landesrecht umfassend umgesetzt wird. Satz 5 setzt Artikel 30 Absatz 2 Unterabs. 2 der Richtlinie (EU) 2022/2555 in Landesrecht um.

Zu Absatz 8

Absatz 8 enthält die Verordnungsermächtigung des für Informationssicherheit zuständigen Ministeriums zum Erlass einer Rechtsverordnung, die Einzelheiten des Meldeverfahrens, die Möglichkeit zur Nutzung von Meldestellen sowie die Form und Frist der Meldung näher bestimmt. Ferner werden unter Nummer 4 die Inhalte, die durch diese Rechtsverordnung vorgegeben werden können, festgelegt. Hierunter fallen meldepflichtige Informationen, die mit der Rechtsverordnung kategorisiert werden können, wie Art des Angriffs und notwendige Beschreibung der verursachten Gefährdung. Informationen, die als Grundlage zu der Ermittlung von Angriffsmustern dienen, fallen ebenfalls hierunter. Schließlich können in der Rechtsverordnung Vorgaben zu weiteren Ausnahmen und Einschränkungen der Meldepflicht nach Absatz 1 gemacht werden.

Satz 2 stellt klar, dass im Wege der Rechtsverordnung meldebezogene Vorgaben der Europäischen Union in Landesrecht umzusetzen sind.

Zu § 10 (Governance durch Leitungen und Informationssicherheitsbeauftragte der wichtigen Stellen der unmittelbaren Landesverwaltung

Zu Absatz 1
Absatz 1 stellt sicher, dass die Leitungsorgane wichtiger Stellen der unmittelbaren Landesverwaltung die Risikomanagementmaßnahmen nach § 8 und die Einhaltung der Melde- und Hinweispflichten nach § 9 in ihrer Stelle billigen, ihre Umsetzung überwachen und für ihre Realisierung verantwortlich sind. Absatz 1 setzt damit die Vorgaben aus Artikel 20 Absatz 1 und Artikel 21 Absatz 4 der Richtlinie (EU) 2022/2555 in Landesrecht um, wobei die Berichtspflichten aus Artikel 23 der Richtlinie (EU) Nr. 2022/2555 als Bestandteil eines angemessenen Risikomanagementsystems nach Artikel 21 Absatz 2 der Richtlinie (EU) 2022/2555 verstanden werden.

Zu Absatz 2
Absatz 2 verpflichtet Leiterinnen und Leiter wichtiger Stellen der unmittelbaren Landesverwaltung zu regelmäßigen Schulungen, um ausreichende Kenntnisse und Fähigkeiten zur effektiven Wahrnehmung der Verantwortungen aus Absatz 1 zu erwerben. Absatz 2 setzt die Vorgaben aus Artikel 20 Absatz 2 der Richtlinie (EU) 2022/2555 in Landesrecht um.

Zu Absatz 3
Satz 1 verpflichtet wichtige öffentliche Stellen des Landes, zur Unterstützung ihrer Leiterinnen und Leiter bei der Umsetzung der Pflichten nach den Absätzen 1 und 2 eine Informationssicherheitsbeauftragte oder einen Informationssicherheits-beauftragten sowie eine Vertretung zu benennen. Die Benennung von Informationssicherheitsbeauftragten stellt gemäß der IT-Grundschutz-Methodik BSI-Standard 200-2 des Bundesamts für Sicherheit in der Informationstechnik eine erforderliche Teilmaßnahmen zur Ergreifung geeigneter und verhältnismäßiger organisatorischer Maßnahmen, wie sie von Artikel 21 Absatz 1 Unterabs. 1 und Unterabs. 2 der Richtlinie (EU) 2022/2555 in Landesrecht vorgeschrieben sind.

Nach Satz 2 ist es möglich, dass eine Beauftragte oder ein Beauftragter für Informationssicherheit für mehrere wichtige Stellen der unmittelbaren Landesverwaltung nach Satz 1 zuständig ist. Die enthaltene Rückausnahme stellt sicher, dass eine solche Mehrfachzuständigkeit dann nicht möglich sein kann, wenn

die betroffene Stelle aufgrund ihrer Größe (> 250 an Beschäftigten) eine ungeteilte Zuständigkeit der Informationssicherheitsbeauftragten oder ihrer Vertretungen benötigt.

Zu Absatz 4
Absatz 4 trägt zu einer im Land Sachsen-Anhalt flächendeckend effektiven Informationssicherheit bei, indem beim für Informationssicherheit zuständigen Ministerium alle Informationssicherheitsbeauftragten und deren Vertretungen in den wichtigen Stellen der unmittelbaren Landesverwaltung an zentraler Stelle mit den erforderlichen Kontaktinformationen hinterlegt sind.

Zu Absatz 5
Der oder die Beauftrage für Informationssicherheit fördert in seiner Rolle die Belange der Informationssicherheit, steuert, überwacht und koordiniert Maßnahmen nach § 8 Das umfasst auch die Fortschreibung und Aktualisierung der Leit- und Richtlinien zur Informationssicherheit.

Die oder der Beauftragte für Informationssicherheit wirkt auf die operative Umsetzung des Informationssicherheitskonzepts hin und kontrolliert die Umsetzung innerhalb ihres oder seines Zuständigkeitsbereichs. Welche Häufigkeit für diese Kontrolle konkret angemessen ist, hängt von den Umständen des jeweiligen Einzelfalls unter Abwägung des Schadenspotenzials ab. Hieraus ergibt sich auch die Befugnis, die Umsetzung des Informationssicherheitskonzepts einzufordern.

Weiterhin ist die oder der Beauftragte für Informationssicherheit für die Einhaltung der Hinweis- und Meldepflichten nach den § 9 in ihrem oder seinem Zuständigkeitsbereich unterstützend verantwortlich.

Zu Absatz 6
Gemäß Absatz 6 haben die Beauftragten für Informationssicherheit eine einmal im Jahr auszuführende Berichtspflicht gegenüber der Leiterin oder dem Leiter der jeweiligen Stelle zum Stand der Informationssicherheit in ihrem oder seinen Zuständigkeitsbereich, über die Mittel und Personalausstattung sowie über Sicherheitsvorfälle. Die Pflicht umfasst die regelmäßige und anlassbezogene Berichterstattung über den Stand der Informationssicherheit, die Ressourcenlage und Sicherheitsvorfälle.

Absatz 7
Absatz 7 normiert die Weisungsfreiheit der oder des Beauftragten für Informationssicherheit, um Interessens- und Rollenkonflikte zu vermeiden. Die Weisungsfreiheit ist Ausfluss der operativen Unabhängigkeit des oder der Beauftragten für Informationssicherheit und im Einklang mit dem IT-Grundschutz-Methodik BSI-Standard 200-2 des Bundesamts für Sicherheit in der Informationstechnik.

Absatz 7 stellt zudem sicher, dass sie oder er wegen der Erfüllung ihrer oder seiner Aufgaben nicht benachteiligt werden darf. Ihm oder ihr dürfen keine unmittelbaren sowie mittelbaren Nachteile aus der Aufgabenwahrnehmung erwachsen.

Zu Absatz 8

Um ihre Aufgaben sachgerecht erfüllen zu können, müssen die Beauftragten für Informationssicherheit sowie deren Vertretungen über die notwendige fachliche Qualifikation verfügen. Die Anforderungen an eine effektive, also wirksame und zielorientierte Befähigung – beispielsweise durch hinreichend tiefgehende und zeitlich umfangreiche Schulungen - gewährleisten, dass sie im Ergebnis über die erforderliche Fachkunde verfügen, um ihre Aufgaben wirksam auszuführen. Hierzu gehört auch eine ausreichende Ausstattung mit Ressourcen.

Teil 4: Aufsichts- und Durchsetzungsmaßnahmen, Abwehr von Gefahren, Datenerhebung und -auswertung

Abschnitt 1: Aufsichts- und Durchsetzungsmaßnahmen

Zu § 11 (Aufsichtsmaßnahmen)

Zu Absatz 1
Absatz 1 setzt die Vorgaben aus Artikel 31 Absatz 1 und Artikel 33 Absatz 1 und Absatz 2 der Richtlinie (EU) 2022/2555 in Landesrecht um.

Zu Absatz 2
Absatz 2 setzt die Vorgaben aus Artikel 33 Absatz 2 Unterabs. 1 Buchstabe d), Buchstabe e) und Buchstabe f) und Absatz 3 der Richtlinie (EU) 2022/2555 in Landesrecht um.

Zu Absatz 3
Absatz 3 setzt die Vorgaben aus Artikel 33 Absatz 2 Unterabs. 1 Buchstabe a) der Richtlinie (EU) 2022/2555 in Landesrecht um.

Zu Absatz 4
Absatz 4 Satz 1 und Satz 4 setzen die Vorgaben aus Artikel 33 Absatz 2 Unterabs. 1 Buchstabe b) und Buchstabe c) der Richtlinie (EU) 2022/2555 in Landesrecht um. Satz 2 setzt die Vorgaben aus Artikel 33 Absatz 2 Unterabs. 2, Satz 3 und Unterabs. 3 der Richtlinie (EU) 2022/2555 um. Satz 3 setzt die Vorgaben aus Artikel 33 Absatz 2 Unterabs. 1 Buchstabe c) der Richtlinie (EU) 2022/2555 um und passt die Vorgaben an bundes- und landesrechtliche Vorgaben an.

Zu Absatz 5
Absatz 5 stellt eine wirksame Beaufsichtigung und Einhaltung der Verpflichtungen nach Teil 3 sicher, und achtet dabei auf eine eine verhältnismäßige Anwendung der Aufsichtsbefugnisse nach § 11. Auf diese Weise setzt Absatz 5 die Vorgaben aus Artikel 31 Absatz 1 und Absatz 4 sowie aus 33 Absatz 4 Buchstabe a), Absatz 5 und Artikel 32 Absatz 8 der Richtlinie (EU) 2022/2555 landesrechtlich um.

Zu Absatz 6
Absatz 6 fordert eine geeignete. Erforderliche, verhältnismäßige und wirksame Aufsicht, und setzt die Vorgaben aus Artikel 33 Absatz 1 Satz 2 der Richtlinie (EU) 2022/2555 in Landesrecht um.

Zu § 12 (Durchsetzungsmaßnahmen)

Zu Absatz 1
Absatz 1 setzt die Vorgaben aus Artikel 31 Absatz 1 und Artikel 33 Absatz 1 und Absatz 2 der Richtlinie (EU) 2022/2555 in Landesrecht um.

Zu Absatz 2
Absatz 2 setzt die Vorgaben aus Artikel 33 Absatz 4 der Richtlinie (EU) 2022/2555 unter Berücksichtigung nationaler Rahmenbedingungen (Artikel 31 Absatz 4 Satz 1 der Richtlinie (EU) 2022/2555) in Landesrecht um.

Zu Absatz 3
Satz 1 setzt die Vorgaben aus Artikel 33 Absatz 1 Satz 2, Absatz 5 in Verbindung mit Artikel 32 Absatz 7 der Richtlinie (EU) 2022/2555 in Landesrecht um. Die Begründungs- und Stellungnahmevorschriften nach Satz 2 und 3 setzen die Vorgaben aus Artikel 33 Absatz 5 in Verbindung mit Artikel 32 Absatz 8 der Richtlinie (EU) 2022/2555 in Landesrecht um.

Zu Absatz 4
Absatz 4 nimmt einen angemessenen Ausgleich von Durchsetzungsbefugnissen im Sinne einer effektiven Informationssicherheit und der Umsetzung europäischer Vorschriften einerseits und dem bundes- und landesrechtlich verfassungsrechtlich verankerten Ressortprinzip andererseits vor, vgl. Artikel 31 Absatz 4 Satz 1 der Richtlinie (EU) 2022/2555.

Zu Absatz 5
Absatz 5 errichtet eine Meldepflicht des für Informationssicherheit zuständigen Ministeriums gegenüber der Landesbeauftragte oder dem Landesbeauftragten für den Datenschutz, sollte eine der vier Varianten (Nummer 1 bis 4) einschlägig sein. Damit dient Absatz 5 auch der Umsetzung des Artikel 35 Absatz 1 der Richtlinie (EU) 2022/2555.

Abschnitt 2: Schutz personenbezogener Daten

Zu § 13 (Zweckändernde Datenverarbeitung)

Absatz 1
Absatz 1 schafft die eng begrenzte Rechtsgrundlage für eine Zweckänderung der Verarbeitung personenbezogener Daten, die im Zusammenhang mit Maßnahmen nach den Teilen 3 und 4 des vorliegenden Gesetzes anfallen können. Er erlaubt eine Verarbeitung zu anderen Zwecken als dem ursprünglichen Erhebungszweck, soweit dies zur Sammlung, Auswertung oder Untersuchung von Informationen zu Schwachstellen, Schadprogrammen, erfolgten oder versuchten Angriffen auf die Sicherheit informationstechnischer Systeme sowie den dabei beobachteten Vorgehensweisen, oder zur Unterstützung oder Beratung in Fragen der Informationssicherheit erforderlich ist.

Die Vorschrift konkretisiert den unionsrechtlichen Rahmen für eine Zweckänderung im öffentlichen Interesse (Art. 6 Abs. 1 Buchst. e i. V. m. Art. 6 Abs. 4 DSGVO). Maßgeblich sind die Grundsätze der Erforderlichkeit, Verhältnismäßigkeit,

Datenminimierung und Zweckbindung; sie lässt fachgesetzliche Zweckänderungsanforderungen unberührt.

Die Zulässigkeit einer Zweckänderung hängt zudem von einer Interessenabwägung ab: Eine Verarbeitung ist nur statthaft, wenn kein Grund zu der Annahme besteht, dass das schutzwürdige Interesse der betroffenen Person am Ausschluss der Verarbeitung überwiegt. Dadurch wird sichergestellt, dass eine weitergehende Verwendung personenbezogener Daten nur anlassbezogen und auf das notwendige Maß beschränkt erfolgt.

Satz 2 regelt ausdrücklich die Verarbeitung besonderer Kategorien personenbezogener Daten (Art. 9 Abs. 1 DSGVO). Eine solche Verarbeitung ist nur zulässig, wenn sie zur Abwehr einer erheblichen Gefahr für die Netz-, Daten- oder Informationssicherheit erforderlich ist, die Aufgabenwahrnehmung des für Informationssicherheit zuständigen Ministeriums oder des CSIRT ohne Einbeziehung dieser Daten unmöglich wäre oder erheblich gefährdet würde und die Interessenabwägung nicht zulasten der betroffenen Person ausfällt. Damit wird Art. 9 Abs. 2 Buchst. g DSGVO (erhebliches öffentliches Interesse) nachvollzogen und zugleich ein strenger Prüfungsmaßstab eingeführt (erhöhte Eingriffsschwelle „erhebliche Gefahr“, zusätzliche Abwägung). Ergänzend sind spezifische Schutzmaßnahmen umzusetzen (u. a. Pseudonymisierung, Zugriffsbeschränkung, Protokollierung, Vier-Augen-Prinzip bei eingriffsintensiven Schritten).

Absatz 2
Absatz 2 normiert eine unverzügliche Löschpflicht: Personenbezogene Daten, die im Zuge der Maßnahmen den Teilen 3 und 4 des vorliegenden Gesetzes erhoben wurden, sind sofort zu löschen, sobald sie für die Abwehr von Gefahren für die Informationssicherheit sowie für informationstechnische Systeme, Komponenten und Prozesse nicht mehr benötigt werden.

Zu § 14 (Datenverarbeitung und -übertragung)

Absatz 1
Absatz 1 regelt die sofortige und unverzügliche Löschung nach einer automatisierten Auswertung der Daten im Zuge der Maßnahmen nach den Teilen 3 und 4 des vorliegenden Gesetzes. Dies steht im Einklang mit Artikel 17 Verordnung (EU) 2016/679, dem Recht auf Löschung. Dabei stellt Satz 2 klar, dass die Verarbeitungseinschränkungen dieser Vorschrift für Daten, die weder personenbezogen sind noch dem Fernmeldegeheimnis unterliegen, nicht gültig sind. Hierdurch wird auch das Prinzip der Datensparsamkeit, also der Grundsatz der Vermeidung der Verarbeitung personenbezogener Daten, berücksichtigt. Das Recht auf informationelle Selbstbestimmung der von der Datenspeicherung betroffenen Personen wird umfassend berücksichtigt. Satz 4 stellt die automatisierte Auswertung der gespeicherten Daten sicher und Satz 5 die automatisierte Pseudonymisierung der Daten. Letztere Regelung steht im Einklang mit Artikel 25 Absatz 1 und Artikel 32 Absatz 1 Buchstabe a) Verordnung (EU) 2016/679.

Satz 2 dient der Erfüllung der Vorgaben des Europäischen Gerichtshofs (EuGH). Laut diesem sollen auf Vorrat gespeicherte Daten wirksam vor Missbrauchsrisiken, unbefugten Zugriffen und unberechtigten Nutzungen geschützt werden (EuGH, Urteil

vom 08.04.2014 – C-293/12, Rn. 66; EuGH, Urteil vom 21.12.2016 – verbundene Rechtssache C-203/15 und C-698,15 – Rn. 122). Dies kann nur vollumfänglich gewährleistet werden, sofern die Daten im Gebiet der Europäischen Union gespeichert werden (Satz 3). Nach Satz 4 muss die automatisierte Auswertung zudem durch organisatorische, operative und technische Maßnahmen nach dem Stand der Technik sichergestellt werden, einschließlich Pseudonymisierung (Satz 5). Die einfachgesetzliche Rechtsfigur des „Stand der Technik“ entspricht den Vorgaben des Bundesverfassungsgerichts (BVerfG, Urteil vom 02.10.2010 – 1 BvR 256/08, Rn. 10).

Absatz 2
Absatz 2 ordnet den Umgang mit Protokolldaten und Protokollierungsdaten an. Diese dürften höchstens für 180 Tage gespeichert werden, solange eine Speicherung nicht durch andere Rechtsvorschriften gestattet wird. Voraussetzung ist, dass tatsächliche Anhaltspunkte für die Erforderlichkeit der Daten bestehen. Es handelt sich zudem um eine Prüffrist mit Löschpflicht.

Nach Nr. 1 liegt ein solcher Anhaltspunkt bei der Bestätigung eines Verdachts nach Absatz 4 Satz 1 zur Abwehr von Gefahren für die informationstechnischen Systeme vor. Es handelt sich also nicht um eine anlasslose Speicherung, sondern vielmehr um eine solche, die nur im Einzelfall und zu dem Zeitpunkt stattfindet, zu dem ein Anhaltspunkt auch tatsächlich gegeben ist (sog. Quick-Freeze-Verfahren). Solche tatsächlichen Anhaltspunkte sind gegeben, sofern die Protokolldaten und Protokollierungsdaten zur Gefahrenabwehr erforderlich sein könnten und orientiert sich an dem Begriff des Anfangsverdachts nach § 152 Absatz 2 Strafprozessordnung in der Fassung der Bekanntmachung vom 7. April 1987, zuletzt geändert durch Gesetz vom 7. November 2024 (BGBl. 2024 I. Nr. 351, im Folgenden StPO).

Nach Nr. 2 besteht ein solcher Anhaltspunkt auch zur Verhütung, Unterbindung oder Verfolgung damit zusammenhängender Straftaten und Ordnungswidrigkeiten. So besteht für Geschädigte die Möglichkeit, strafrechtliche Ermittlungen einleiten zu lassen. Auch können mit diesen Daten laufende Straftaten unterbunden oder zukünftige Straftaten verhindert werden. Sofern ein solcher Anhaltspunkt nach Nr. 2 besteht, sollten die Daten nicht gelöscht werden, damit diese im Falle eines Verfahrens als Beweis eingebracht werden können.

Die in Absatz 1 festgelegte Speicherhöchstdauer von 180 Tagen ist verhältnismäßig. Sie verfolgt den legitimen Zweck der Sicherung des Gemeinwohls und ist geeignet, erforderlich und angemessen, um diesen Zweck zu erreichen. Artikel 10 Absatz 1 GG verbietet die Speicherung von personenbezogenen Daten „auf Vorrat“ zu unbestimmten oder noch nicht bestimmbaren Zwecken, nicht jedoch auch jede andere Art der Speicherung von Daten im Allgemeinen. Durch die Sicherung der informationstechnischen Systeme und die sich hier befindenden, möglicherweise sensiblen, Informationen, wird die Sicherheit und Integrität der Landesverwaltung und eine reibungslos ablaufende Landesverwaltung gesichert. Dies dient der Sicherung des Gemeinwohls. Um diesen Zweck zu erreichen, ist das Prüfen der gespeicherten Protokolldaten und Protokollierungsdaten geeignet. Hierdurch können Angriffe erkannt und unterbunden werden. Es handelt sich hierbei um das einzige Mittel, um ein Eindringen in betroffene informationstechnische Systeme zu entdecken und anschließend zu verhindern. Damit ist dieses Mittel das mildeste. Die Maßnahme der Speicherung ist zudem auch angemessen, also verhältnismäßig im engeren Sinne.

Schadprogramme, die in informationstechnische Systeme eingeschleust wurden, können oft erst mit zeitlichem Verzug erkannt werden. Die Behörden müssen genügend Zeit haben, betroffene Daten zu analysieren und Erkenntnisse zu erlangen.

Satz 2 legt fest, dass eine Ausnahme der automatisierten Auswertung oder personenbezogenen Verarbeitung nur nach den Absätzen 4 bis 8 zulässig ist. Satz 3 regelt die Wiederherstellung des Personenbezugs pseudonymisierter Daten; eine hierzu getroffene Anordnung kann nur durch die Leiterin oder den Leiter der unmittelbaren öffentlichen Stelle des Landes getroffen werden. Die Entscheidung ist gemäß Satz 4 aus Gründen des Dokumentations- und Kontrollzwecks zu dokumentieren.

Absatz 3
Während Absatz 2 den Umgang mit Protokolldaten und Protokollierungsdaten regelt, geht es in Absatz 3 um Inhaltsdaten. Diese bedürfen einer restriktiveren Regelung und dürfen nach Satz 1 längstens 180 Tage gespeichert werden. Für die Speicherung der Inhaltsdaten müssen tatsächliche Anhaltspunkte dafür bestehen, dass die Daten erforderlich sein können. Dies ist der Fall, wenn ein Verdacht nach Absatz 3 Satz 1 zur Abwehr von Gefahren für informationstechnische Systeme bestätigt wird (Nr. 1) oder zur Verhütung, Unterbindung oder Verfolgung damit zusammenhängender Straftaten und die Speicherung zum Schutz der technischen Systeme unerlässlich ist (Nr. 2). Da es sich hier entweder um ein gesteigertes Risiko oder um das Vorliegen einer konkreten Gefahrenlage handelt, ist die Speicherung dieser Inhaltsdaten für längstens 180 Tage zulässig und angemessen.

Die Speicherung und Auswertung der Inhaltsdaten ist von der zuständigen Leiterin oder dem zuständigen Leiter der unmittelbaren öffentlichen Stelle des Landes und zusätzlich von einer oder einem weiteren Bediensteten dieser Stelle mit fachlicher Eignung anzuordnen (Satz 2); die Befähigung bestimmt sich nach Absatz 9. Grund hierfür ist die gesteigerte Sensibilität der Daten. Sowohl die Einschätzung einer fachlich geeigneten Person als auch das Vier-Augen-Prinzip sollen sicherstellen, dass die Speicherung und Auswertung der Inhaltsdaten verhältnismäßig sind. Die Anordnung ist zeitlich beschränkt und gilt längstens zwei Monate, kann jedoch verlängert werden (Satz 6). Auch diese Anordnung ist aus Gründen des Dokumentations- und Kontrollzwecks zu dokumentieren (Satz 7).

Absatz 4
Absatz 4 bezieht sich auch auf die inhaltliche Prüfung von Dokumenten. Voraussetzung hierfür ist ein hinreichender Verdacht. Dieser ist gegeben, wenn Anhaltspunkte vorliegen, dass die Daten Gefahren für die informationstechnischen Systeme enthalten oder Hinweise auf solche Gefahren geben können wahrscheinlicher ist, als dass eine solche Gefahr nicht besteht. Der Begriff des hinreichenden Verdachts orientiert sich an dem des hinreichenden Tatverdachts nach § 170 Absatz 1 StPO. Liegt ein solcher hinreichender Verdacht vor, können auch nicht automatisierte Maßnahmen erfolgen. Diese sind zulässig, um den Verdacht einer Gefahr für die informationstechnischen Systeme etwa durch Schadprogramme, Schwachstellen, unbefugte Datenverarbeitung oder Hinweise auf solche Gefahren zu bestätigen (Nr. 1). Hat sich dieser Verdacht bestätigt, so ist eine Verarbeitung dieser Daten auch zulässig, sofern sie erforderlich ist, um den Verdacht zu bestätigen oder

zu widerlegen (Nr. 2). Beispielsweise kann hier die Funktionsweise einer Schadsoftware untersucht werden.

Sofern bei der Analyse der Daten Hinweise auf eine Gefahr für die öffentliche Sicherheit oder Ordnung entdeckt werden, die zu der Verhütung oder Unterbindung einer Straftat oder Verfolgung einer solchen benötigt werden, dürfen diese Daten gespeichert werden. Damit werden auch die sogenannten Zufallsfunde umfasst.

Bestätigt sich der Verdacht letztlich nicht, ändert dies nichts an der Rechtmäßigkeit der Speicherung der Daten. So wird die Möglichkeit sichergestellt, die Daten an die Polizei- bzw. Strafverfolgungsbehörden nach Absatz 8 zu übermitteln.

Nach Satz 3 dürfen Schadprogramme beseitigt werden oder in ihrer Funktionsweise gehindert werden. Diese Norm dient der Klarstellung und dem Ausschluss der Strafbarkeit der Datenveränderung nach § 303a Absatz 1 Strafgesetzbuch in der Fassung der Bekanntmachung vom 13. November 1998, zuletzt geändert durch Gesetz vom 7. November 2024 (BGBl. 2024 I Nr. 351, im Folgenden StGB).

Hinsichtlich der Anordnung der nicht automatisierten Verarbeitung der Daten nach Satz 4 soll das hier normierte Vier-Augen-Prinzip durch die Leiterin oder den Leiter der unmittelbaren öffentlichen Stelle des Landes und einer oder einem Bediensteten dieser Stelle mit der entsprechenden Befähigung der Abwägung und damit der Wahrung der Verhältnismäßigkeit dienen. Sofern die Stelle keine weiteren befähigten Personen beschäftigt, ist diese Person durch eine oder einen Bediensteten der Aufsichtsbehörde mit der entsprechenden Befähigung nach Absatz 9 zu ersetzen. Hierdurch besteht auch für kleinere öffentliche Stellen des Landes die Möglichkeit, eine solche Anordnung nach Absatz 4 zu treffen.

Absatz 5

Nach Satz 1 sind die betroffenen Personen und die betroffenen Stellen zu benachrichtigen. Dies ist allerdings nur möglich und vorgeschrieben, sofern sie bekannt sind oder ihre Identifikation ohne unverhältnismäßigen Aufwand möglich ist und keine überwiegenden schutzwürdigen Belange Dritter entgegenstehen. In der Regel dürfte dies an der Kenntnis über die Person oder Stelle scheitern, da der Absender bereits technisch, etwa durch gefälschte IP-Adressen, nicht zu ermitteln ist. Sofern die Daten nach Absatz 7 oder 8 für ein Strafverfahren weiterverwendet werden, erfolgt die Benachrichtigung für die hierfür zuständige Behörde nach den für diese geltenden Vorschriften der StPO, der einschlägigen Polizeigesetze oder Verfassungsschutzgesetze.

Absatz 6

Angriffe auf die informationstechnischen Systeme des Landes Sachsen-Anhalt mittels Schadprogrammen stellen Straftaten nach §§ 202a, 202b, 303a und 303b StGB (Ausspähen oder Abfangen von Daten oder das Verändern von Daten oder Datensabotage) dar. Satz 1 gewährt daher die Übermittlung der verarbeiteten personenbezogenen Daten an die Strafverfolgungsbehörde zum Zweck der Verfolgung einer solchen Straftat. Diese Daten dürfen zudem zur Abwehr einer Gefahr für die öffentliche Sicherheit, die unmittelbar von einem gefundenen Schadprogramm ausgeht, an die Polizei des Landes Sachsen-Anhalt übermittelt werden.

Absatz 7
Die Übermittlung möglicher Zufallsfunde an die Strafverfolgungs-, Polizeibehörden oder die Verfassungsschutzbehörde ist nur unter den engen Voraussetzungen des Absatz 8 zulässig. Dies betrifft auch den Fall der Gefahrenabwehr. Diese Regelung stellt eine Zweckänderungs- und Weiterverarbeitungserlaubnis dar und hat damit den Grundsatz der Verhältnismäßigkeit zu wahren. Dies wird vorliegend durch die in Nr. 1 aufgezählten limitierten Fälle des § 100a Absatz 2 der StPO gewahrt. Die dortige Aufzählung der Katalogstraftaten würden eine Telekommunikationsüberwachung rechtfertigen. Auf diese Straftaten bezieht sich auch der Zweck der Gefahrenabwehr nach Nr. 2. Für die Übermittlung der Daten an die Verfassungsschutzbehörde nach Nr. 3 müssen tatsächliche Anhaltspunkte für Tätigkeiten nach § 4 Absatz 1 Nummer 3 des Gesetzeses über den Verfassungsschutz im Land Sachsen-Anhalt (VerfSchG-LSA) in der Fassung der Bekanntmachung vom 6. April 2006, zuletzt neu gefasst durch das Gesetz vom 11. Dezember 2024 (GVBl. LSA S. 352, im Folgenden VerfSchG-LSA) oder für Bestrebungen vorliegen, die durch Anwendung von Gewalt oder darauf gerichtete Vorbereitungshandlungen gegen die in § 4 Absatz 1 Nummer 1, 2, 4, und 5 VerfSchG-LSA genannten Schutzgüter gerichtet sind.

Absatz 8
Inhaltsdaten können immer auch einen Aufschluss über den Kernbereich privater Lebensgestaltung geben. Diesem Umstand trägt Absatz 8 Rechnung und stellt sicher, dass Daten, die diesen Bereich betreffen, nicht erhoben werden. Werden Kenntnisse aus diesem Kernbereich erlangt dürfen sie nicht verwendet und müssen sofort gelöscht werden. Aus Artikel 1 Absatz 1 GG ergibt sich, dass der Kernbereich privater Lebensgestaltung absolut unantastbar ist und daher besonderen Schutz genießt. Hierunter fällt etwa die Kommunikation mit engen persönlichen Vertrauten bzw. Freunden, die Kommunikation mit Berufsgeheimnisträgern, die Möglichkeit, innere Vorgänge wie Empfindungen und Gefühle, Ansichten, Erlebnisse und Überlegungen höchstpersönlicher Art auszudrücken. Umfasst sind auch Ausdrucksformen der Sexualität und Gefühlsäußerungen.

Absatz 9
Absatz 9 enthält eine Rechtsverordnungsermächtigung zur Bestimmung relevanter Einzelheiten und Anforderungen an die die fachliche Befähigung bestimmter Stellen. Die Geeignetheit der Person sollte über einen volljuristischen oder informationstechnischen Hintergrund mit mehrjähriger Berufserfahrung sichergestellt werden. Zugleich ermöglicht die Rechtsverordnungsermächtigung einen angemessenen Spielraum, um eine adäquate Befähigung und Erfahrung sicherzustellen, ohne den Kreis der möglichen Personen zu weit einzuschränken.

Teil 5: Schlussvorschriften

Zu § 15 (Einschränkung von Grundrechten)
Das vorliegende Gesetz sieht verschiedene Eingriffs- und Maßnahmenbefugnisse zur Datenverarbeitung und Auswertung der Daten eines Telekommunikationsvorgangs vor. Hierdurch könnte das Fernmeldegeheimnis verletzt werden. Nach Artikel 10 GG als auch nach Artikel 14 der Verfassung LSA dürfen Beschränkungen des Fernmeldegeheimnisses nur auf Grund eines Gesetzes angeordnet werden, das wiederum das Grundrecht unter Angabe des Artikels nennen muss. Auch eine Verletzung des Rechts auf Datenschutz kommt in Betracht, welches nach Artikel 6 der

Verfassung LSA unter einem Gesetzesvorbehalt steht. Anders allerdings nach Bundesrecht, wo das Recht auf Datenschutz aus Artikel 2 Absatz 1 i.V.m. Artikel 1 Absatz 1 GG hergeleitet wird, die hier keinen maßgeblichen Gesetzesvorbehalt enthalten und daher nicht zitiert werden müssen.

Zu § 16 (Experimentierklausel)
Durch das dynamische Voranschreiten informationstechnischer Systeme ist zum Zeitpunkt der Erstellung des Gesetzes nicht vorhersehbar, welche Daten und Informationen durch welche informationstechnischen Systeme zukünftig ausgewertet werden müssen, um Gefahren für die Informationssicherheit effektiv abzuwehren.

Um die Informationssicherheit insgesamt und die informationstechnischen Systeme im Besonderem im Einklang mit diesem Gesetz angemessen zu schützen, soll es im Land Sachsen-Anhalt möglich sein, auch solche Daten zu verarbeiten, die weder zu den üblichen Protokolldaten und Protokollierungsdaten gehören, noch an Schnittstellen der informationstechnischen Systeme erfasst werden oder zum Zeitpunkt der Gesetzgebung elektronisch vorliegen. Dies betrifft auch Daten, die bisher gar nicht oder für andere Zwecke verarbeitet werden.

Zu § 17 (Evaluierung)

Zu Absatz 1
Absatz 1 regelt, dass das für Informationssicherheit zuständige Ministerium dem Landtag erstmals zum 31. Dezember 2027 einen Bericht vorlegt, der darlegt, welche Auswirkungen dieses Gesetz auf die Informationssicherheit des Landes Sachsen-Anhalt hat, welche Projekte auf Basis der Experimentierklausel des § 16 durchgeführt wurden, welche Kosten und welcher Nutzen bei der Umsetzung des Gesetzes entstanden sind und ob eine Weiterentwicklung der Vorschriften dieses Gesetzes erforderlich ist. Bei der Evaluation sollen auch qualitative Indikatoren wie durchgeführte Schulungen, erarbeitete Schulungs- und Sensibilisierungskonzepte und etablierte Prozesse des Informationssicherheitsmanagement einbezogen und angemessene Darstellungsweisen genutzt werden, um auf diese Weise auch präventive Wirkungen des Gesetzes greifbar zu machen.

Zu Absatz 2
Berichte im Sinne des Absatzes 1 sind gemäß Absatz 2 nach der ersten Evaluierung kontinuierlich innerhalb von jeweils fünf Jahren zu erstellen. Hierdurch wird gewährleistet, dass die Fortschritte der Informationssicherheit in der Verwaltung in Sachsen-Anhalt in regelmäßigen Abständen geprüft wird und die Auswirkungen für die rechtlichen Vorgaben der Informationssicherheit in den Behörden untersucht werden.

Zu § 18 (Inkrafttreten)
Das Gesetz tritt am Tag nach seiner Verkündung in Kraft.

(Stand: 01.04.2026, 09:38 Uhr)