

**Gesetz
zur Gewährleistung der Informationssicherheit
im Freistaat Sachsen
(Sächsisches Informationssicherheitsgesetz - SächsISichG)**

erlassen als Artikel 1 des Gesetzes zur Neuordnung der Informationssicherheit im Freistaat Sachsen

Vom 2. August 2019

Inhaltsübersicht¹

Abschnitt 1
Allgemeine Vorschriften

- § 1 Zweck des Gesetzes
- § 2 Anwendungsbereich
- § 3 Begriffsbestimmungen
- § 4 Grundsätze der Informationssicherheit

Abschnitt 2
Organisation der Informationssicherheit

- § 5 Beauftragte oder Beauftragter für Informationssicherheit des Landes
- § 6 Sicherheitsnotfallteam
- § 7 Beauftragte für Informationssicherheit der staatlichen Stellen
- § 8 Beauftragte für Informationssicherheit der nicht-staatlichen Stellen
- § 9 Informationssicherheitsmanagement-Teams
- § 10 Arbeitsgruppe Informationssicherheit

Abschnitt 3
Maßnahmen zur Sicherstellung der Informationssicherheit

- § 11 Datenübermittlung der nicht-staatlichen Stellen
- § 12 Abwehr von Gefahren für die informationstechnischen Systeme im Freistaat Sachsen
- § 13 Datenspeicherung und -auswertung
- § 14 Sicherheitskonzept

Abschnitt 4
Meldepflichten

- § 15 Stellenübergreifende Meldepflichten
- § 16 Meldepflichten der staatlichen Stellen
- § 17 Meldepflichten der nicht-staatlichen Stellen

Abschnitt 5
Schlussvorschriften

- § 18 Einschränkung von Grundrechten
- § 19 Experimentierklausel
- § 20 Übergangsregelung
- § 21 Evaluierung

**Abschnitt 1
Allgemeine Vorschriften**

**§ 1
Zweck des Gesetzes**

¹Zweck dieses Gesetzes ist, die Informationssicherheit im Freistaat Sachsen zu erhöhen und Gefahren für informationstechnische Systeme abzuwehren. ²Die Gewährleistung der Informationssicherheit ist eine wichtige im öffentlichen Interesse liegende Aufgabe.

§ 2 Anwendungsbereich

(1) ¹Dieses Gesetz gilt für die Behörden und die Gerichte des Freistaates Sachsen (staatliche Stellen) sowie die seiner Aufsicht unterstehenden Körperschaften, Anstalten und Stiftungen des öffentlichen Rechts (nicht-staatliche Stellen). ²Auf Beliehene findet ausschließlich Absatz 4 Anwendung.

(2) ¹Der Landtag gewährleistet die ihn betreffende Informationssicherheit durch den Beschluss einer für ihn, seine Gremien, seine Mitglieder und deren Beschäftigte, seine Fraktionen und deren Beschäftigte sowie für die Landtagsverwaltung geltenden Informationssicherheitsleitlinie. ²Für den Landtag gelten im Übrigen ausschließlich die §§ 10 und 12 bis 15 entsprechend den in der Informationssicherheitsleitlinie getroffenen Maßgaben.

(3) Dieses Gesetz gilt nicht für den Verfassungsgerichtshof des Freistaates Sachsen, die Rundfunkanstalt Mitteldeutscher Rundfunk, die Deutsche Rentenversicherung Mitteldeutschland, die AOK PLUS, die öffentlich-rechtlichen Kreditinstitute im Freistaat Sachsen und die Sachsen-Finanzgruppe.

(4) Soweit Beliehene an das Sächsische Verwaltungsnetz oder an das Kommunale Datennetz angeschlossen sind oder Dienste aus diesen Netzen heraus anbieten, sind sie zur Gewährleistung einer gleichwertigen Informationssicherheit gemäß § 4 Absatz 1 Satz 1 bis 3 zu verpflichten.²

§ 3 Begriffsbestimmungen

(1) Informationssicherheit im Sinne dieses Gesetzes bedeutet die Gewährleistung der Schutzziele Vertraulichkeit, Integrität und Verfügbarkeit der in informationstechnischen Systemen verarbeiteten Informationen und Daten.

(2) Informationstechnische Systeme im Sinne dieses Gesetzes sind alle technischen Mittel zur Erfassung, Speicherung, Verarbeitung, Nutzung, Übermittlung oder Löschung von Informationen und Daten.

(3) Schadprogramme im Sinne dieses Gesetzes sind Programme sowie sonstige informationstechnische Routinen und Verfahren, die dem Zweck dienen, unbefugt Daten zu verarbeiten oder auf sonstige informationstechnische Abläufe einzuwirken.

(4) Sicherheitslücken im Sinne dieses Gesetzes sind Eigenschaften von Systemen oder Prozessen, durch deren Ausnutzung es Unbefugten möglich ist, Zugang zu informationstechnischen Systemen und den verarbeiteten Daten zu erhalten oder die Funktion der informationstechnischen Systeme zu beeinflussen.

(5) Ein Sicherheitsvorfall ist ein Ereignis, das tatsächlich nachteilige Auswirkungen auf die Informationssicherheit hat.

(6) Ein Sicherheitsereignis ist ein Versuch, eines der Schutzziele Vertraulichkeit, Integrität oder Verfügbarkeit zu verletzen.

(7) Ein Informationssicherheitsmanagementsystem ist die Aufstellung von verbindlichen Prozessen und Regeln, die die Informationssicherheit in einer staatlichen oder nicht-staatlichen Stelle dauerhaft steuern, kontrollieren, aufrechterhalten und fortlaufend verbessern.

(8) Inhaltsdaten sind Daten, die den Inhalt einer Kommunikation betreffen und die keine Verkehrsdaten im Sinne des [Telekommunikationsgesetzes](#) vom 23. Juni 2021 (BGBl. I S. 1858), das zuletzt durch Artikel 35 des Gesetzes vom 6. Mai 2024 (BGBl. 2024 I Nr. 149) geändert worden ist, in der jeweils geltenden Fassung, sind.

(9) ¹Protokolldaten im Sinne dieses Gesetzes beschreiben oder historisieren Zustände und Aktionen von informationstechnischen Systemen. ²Protokolldaten können Verkehrsdaten gemäß § 3 Nummer 70 des [Telekommunikationsgesetzes](#) und Nutzungsdaten nach § 2 Absatz 2 Nummer 3 des [Telekommunikation-Telemedien-Datenschutz-Gesetzes](#) vom 23. Juni 2021 (BGBl. I S. 1982; 2022 I S. 1045), das zuletzt durch Artikel 8 des Gesetzes vom 6. Mai 2024 (BGBl. 2024 I Nr. 149) geändert worden ist, enthalten.³

§ 4 Grundsätze der Informationssicherheit

(1) ¹Die staatlichen Stellen treffen angemessene organisatorische und technische Vorkehrungen sowie sonstige Maßnahmen zur Gewährleistung der Informationssicherheit. ²Für technische Maßnahmen soll der Stand der Technik maßgeblich sein. ³Maßnahmen sind angemessen, wenn der dafür erforderliche Aufwand nicht außer Verhältnis zu den Folgen der Verletzung der Schutzziele steht. ⁴Um die Erreichung und Aufrechterhaltung eines angemessenen Informationssicherheitsniveaus zu gewährleisten, haben alle staatlichen Stellen die jeweils geltenden Standards und das jeweils geltende IT-Grundschrift-Kompendium des Bundesamtes für Sicherheit in der Informationstechnik zu berücksichtigen. ⁵Die staatlichen Stellen erstellen und pflegen ein Informationssicherheitsmanagementsystem.

(1a) Die Verpflichtung nach Absatz 1 Satz 1 umfasst für staatliche Stellen mindestens Maßnahmen

1. zur Risikoanalyse und zur Sicherheit von informationstechnischen Systemen,
2. zur Bewältigung von Sicherheitsvorfällen,
3. zur Aufrechterhaltung des Betriebs und zum Krisenmanagement der informationstechnischen Systeme,
4. zur Absicherung von Lieferketten zu unmittelbaren Lieferanten oder Diensteanbietern,
5. zur Sicherheit bei Erwerb, Entwicklung und Wartung von informationstechnischen Systemen einschließlich Management und Offenlegung von Sicherheitslücken,
6. zur Bewertung der Wirksamkeit von Risikomanagementmaßnahmen,
7. zu Sensibilisierungen zu grundlegenden Verfahren und Schulungen,
8. für den Einsatz von Kryptografie und Verschlüsselung,
9. für die Zugriffskontrolle und das Management von Anlagen,
10. zur Multi-Faktor- oder kontinuierlichen Authentifizierung,
11. zur gesicherten Sprach-, Video- und Textkommunikation sowie zur gesicherten Notfallkommunikation innerhalb der staatlichen Stelle.

(2) ¹Für die nicht-staatlichen Stellen gilt Absatz 1 Satz 1 bis 3 entsprechend. ²Die jeweils geltenden Standards und das jeweils geltende IT-Grundschrift-Kompendium des Bundesamtes für Sicherheit in der Informationstechnik werden zur Anwendung empfohlen. ³Werden dem Freistaat Sachsen Informationssicherheitsstandards verbindlich durch Beschlüsse des IT-Planungsrates gemäß Artikel 91c Absatz 2 Satz 1 des [Grundgesetzes](#) für die Bundesrepublik Deutschland vorgeschrieben oder nach § 5 des [Onlinezugangsgesetzes](#) vom 14. August 2017 (BGBl. I S. 3122, 3138), in der jeweils geltenden Fassung, festgelegt, sind diese Standards durch die nicht-staatlichen Stellen bei den von ihnen eingesetzten informationstechnischen Systemen einzuhalten.

(3) ¹Die Verantwortung für die Informationssicherheit im Sinne des Absatzes 1 trägt die jeweilige Leiterin oder der jeweilige Leiter der staatlichen oder nicht-staatlichen Stelle, bei Schulen der jeweilige Schulträger. ²Sie oder er stellt im Rahmen der ihr oder ihm zugewiesenen Aufgaben und Befugnisse die erforderlichen personellen und finanziellen Ressourcen zur Verfügung. ³Leiterinnen oder Leiter der staatlichen Stellen müssen regelmäßig an Schulungen zur Informationssicherheit teilnehmen, um ausreichende Kenntnisse und Fähigkeiten zur Erkennung und Bewertung von Risiken sowie Managementpraktiken im Bereich Informationssicherheit und deren Auswirkungen auf die von ihrer staatlichen Stelle erbrachten Dienste zu erwerben.

(4) Wesentliche Änderungen an den informationstechnischen Systemen einer staatlichen oder nicht-staatlichen Stelle dürfen nur im Benehmen mit der oder dem für diese staatliche oder nicht-staatliche Stelle ernannten Beauftragten für Informationssicherheit durchgeführt werden.

(5) Im Einzelfall ist auf den Einsatz informationstechnischer Systeme zu verzichten, wenn die erforderlichen Vorkehrungen zur Gewährleistung der Informationssicherheit außer Verhältnis zur erreichbaren Herabsetzung des Risikos für die in § 3 Absatz 1 genannten Schutzziele stehen.⁴

Abschnitt 2 **Organisation der Informationssicherheit**

§ 5 **Beauftragte oder Beauftragter für Informationssicherheit des Landes**

(1) ¹(1) Die oder der Beauftragte für Informationssicherheit des Landes wird von der oder dem Beauftragten für Informationstechnologie des Freistaates Sachsen ernannt und nimmt ihre oder seine

Aufgaben hauptamtlich wahr. ²Sie oder er

1. fördert und unterstützt durch die Erstellung von konkreten Handlungsempfehlungen, Maßnahme- und Formulierungsvorschlägen, Erläuterungen, Leitfäden und auf Anforderungen durch individuelle Beratung die Beauftragten für Informationssicherheit nach § 7 Absatz 1 bei der Erfüllung ihrer Aufgaben, insbesondere bei der Erstellung und Pflege eines Informationssicherheitsmanagementsystems,
2. initiiert und koordiniert landesweite Sensibilisierungs- und Schulungsmaßnahmen sowie Projekte zur Informationssicherheit,
3. hat ein direktes Vorspracherecht bei der oder dem Beauftragten für Informationstechnologie des Freistaates Sachsen,
4. berät und unterstützt die Beauftragte oder den Beauftragten für Informationstechnologie des Freistaates Sachsen bei ihrer oder seiner Aufgabenwahrnehmung bezüglich der Informationssicherheit,
5. 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 (NIS-2-Richtlinie) (ABl. L. ²333 vom 27.12.2022, S. 80) für die Aufsicht über die staatlichen Stellen.

³Die oder der Beauftragte für Informationssicherheit des Landes meldet dem Bundesamt für Sicherheit in der Informationstechnik die nach § 7 Absatz 4 identifizierten staatlichen Stellen erstmals sechs Monate nach Inkrafttreten dieses Gesetzes und danach alle zwei Jahre.

(2) Zur Erfüllung ihrer oder seiner Aufgaben kann die oder der Beauftragte für Informationssicherheit des Landes dem Sicherheitsnotfallteam fachliche Weisungen erteilen.

(3) ¹Gegenüber an das Sächsische Verwaltungsnetz angeschlossenen staatlichen Stellen kann die oder der Beauftragte für Informationssicherheit des Landes Anordnungen treffen oder Maßnahmen ergreifen, um Gefahren für die informationstechnischen Systeme, die mit dem Sächsischen Verwaltungsnetz verbunden sind, abzuwehren. ²Zur Abwehr von stellenübergreifenden Sicherheitsvorfällen ihrer informationstechnischen Systeme oder Prozesse darf sie oder er bei Gefahr im Verzug vorübergehende Netztrennungen anordnen. ³Die Leiterin oder der Leiter der staatlichen Stelle und die oder der für die staatliche Stelle ernannte Beauftragte für Informationssicherheit sind unverzüglich zu unterrichten. ⁴Für die Umsetzung der Maßnahmen bedient sich die oder der Beauftragte für Informationssicherheit des Landes des Sicherheitsnotfallteams. ⁵Gegenüber staatlichen Stellen kann im Benehmen mit der jeweils zuständigen obersten Staatsbehörde die oder der Beauftragte für Informationssicherheit des Landes Anordnungen treffen oder Maßnahmen zur Umsetzung der Verpflichtungen aus § 4 Absatz 1 und 1a ergreifen, soweit Tatsachen die Annahme rechtfertigen, dass Anforderungen aus § 4 Absatz 1 und 1a nicht oder nicht richtig umgesetzt wurden. ⁶Gegenüber dem Sächsischen Rechnungshof sowie der oder dem Sächsischen Datenschutzbeauftragten können statt Anordnungen oder Maßnahmen nach Satz 1 nur Hinweise gegeben werden.

(4) ¹Gegenüber nicht-staatlichen Stellen kann die oder der Beauftragte für Informationssicherheit des Landes Anordnungen im Benehmen mit der oder dem Beauftragten für Informationssicherheit des Betreibers des Kommunalen Datennetzes treffen, um Gefahren für die informationstechnischen Systeme, die mit dem Kommunalen Datennetz verbunden sind, abzuwehren. ²Zur Abwehr von stellenübergreifenden Sicherheitsvorfällen auf informationstechnische Systeme oder Prozesse innerhalb des Sächsischen Verwaltungsnetzes darf sie oder er bei Gefahr im Verzug vorübergehende Trennungen des Kommunalen Datennetzes vom Sächsischen Verwaltungsnetz anordnen. ³Die Leiterin oder der Leiter der nicht-staatlichen Stelle, die oder der für diese ernannte Beauftragte für Informationssicherheit und die oder der Beauftragte für Informationssicherheit des Betreibers des Kommunalen Datennetzes sind unverzüglich zu unterrichten. ⁴Die von der oder dem Beauftragten für Informationssicherheit des Landes angeordneten Maßnahmen nach Satz 2 werden durch das Sicherheitsnotfallteam umgesetzt.

(5) Die oder der Beauftragte für Informationssicherheit des Landes ist für die Erstellung des Informationssicherheitsmanagementsystems für die sächsische Staatsverwaltung zuständig.

(6) ¹Die oder der Beauftragte für Informationssicherheit des Landes erstellt verbindliche Mindeststandards zur Informationssicherheit für die staatlichen Stellen und legt sie nach Anhörung der Arbeitsgruppe Informationssicherheit dem Gremium nach § 17 Absatz 1 des [Sächsischen E-](#)

Government-Gesetzes in der Fassung der Bekanntmachung vom 8. November 2019, (SächsGVBl. S. 718), das durch Artikel 3 der Verordnung vom 12. April 2021 (SächsGVBl. S. 517) geändert worden ist, in der jeweils geltenden Fassung, zur Entscheidung vor. ²Die Arbeitsgruppe Informationssicherheit unterstützt die Beauftragte oder den Beauftragten für Informationssicherheit des Landes dabei. ³Den nicht-staatlichen Stellen wird die Anwendung der Mindeststandards empfohlen. ⁴Auf Ersuchen berät die oder der Beauftragte für Informationssicherheit des Landes die staatlichen oder nicht-staatlichen Stellen bei der Umsetzung und Einhaltung der Mindeststandards.

(7) ¹Um die Umsetzung der Anforderungen aus § 4 Absatz 1 und 1a, die Wirksamkeit des Informationssicherheitsmanagementsystems und den Stand der Erfüllung der Mindeststandards zu überprüfen, kann die oder der Beauftragte für Informationssicherheit des Landes die erforderlichen Auskünfte und die Überlassung von entsprechenden Unterlagen der staatlichen Stellen verlangen. ²Zu diesem Zweck darf sie oder er eigene Revisionen durchführen, wobei für den Sächsischen Rechnungshof, die Sächsische Datenschutzbeauftragte oder den Sächsischen Datenschutzbeauftragten, die Gerichte und Staatsanwaltschaften sowie die Behörden und Organisationen mit Sicherheitsaufgaben hierfür deren Einvernehmen einzuholen ist. ³Staatliche Stellen haben im Benehmen mit der jeweils zuständigen obersten Staatsbehörde der oder dem Beauftragten für Informationssicherheit des Landes und den in deren oder dessen Auftrag handelnden Personen zum Zweck der Überprüfung das Betreten der Behörden- und Betriebsräume während der üblichen Dienst- und Betriebszeiten zu gestatten und auf Verlangen die in Betracht kommenden Aufzeichnungen, Schriftstücke und sonstige Unterlagen vorzulegen, Auskunft zu erteilen und die erforderliche Unterstützung zu gewähren. ⁴Sie oder er ist über geplante Audits und Revisionen zu unterrichten. ⁵Vorliegende Zertifikate nach dem **BSI-Gesetz** vom 14. August 2009 (BGBl. I S. 2821), das zuletzt durch Artikel 12 des Gesetzes vom 23. Juni 2021 (BGBl. I S. 1982) geändert worden ist, und der BSI-Zertifizierungs- und -Anerkennungsverordnung vom 17. Dezember 2014 (BGBl. I S. 2231), die zuletzt durch Artikel 74 der Verordnung vom 19. Juni 2020 (BGBl. I S. 1328) geändert worden ist, in den jeweils geltenden Fassungen, sind dabei zu beachten. ⁶Bei der Überprüfung festgestellte Verstöße einer staatlichen Stelle gegen Verpflichtungen aus § 4 Absatz 1 und 1a oder § 16, die 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) zur Folge haben können, teilt die oder der Beauftragte für Informationssicherheit des Landes unverzüglich der oder dem Sächsischen Datenschutzbeauftragten mit.

(8) ¹Die oder der Beauftragte für Informationssicherheit des Landes unterrichtet den Landtag jährlich allgemein über ihre oder seine Tätigkeit und über

1. die durch das Sicherheitsnotfallteam getroffenen Anordnungen und ergriffenen Maßnahmen gemäß § 6 Absatz 3,
2. die Anzahl von Fällen der Verarbeitung personenbezogener Daten durch das Sicherheitsnotfallteam zu anderen Zwecken als demjenigen, zu dem die Daten ursprünglich erhoben wurden, gemäß § 6 Absatz 4,
3. die zur Abwehr von Gefahren für die informationstechnischen Systeme ergriffenen Maßnahmen gemäß § 12,
4. die Anzahl von Fällen der nicht automatisierten Auswertung, der personenbezogenen Verarbeitung und der Wiederherstellung des Personenbezugs pseudonymisierter Daten bei Protokolldaten gemäß § 13 Absatz 2,
5. die Anzahl von Fällen der Speicherung und der Auswertung von Inhaltsdaten und Wiederherstellung des Personenbezugs pseudonymisierter Daten gemäß § 13 Absatz 3,
6. die Anzahl von Fällen der nicht automatisierten Verarbeitung von Daten gemäß § 13 Absatz 4,
7. die Anzahl der durchgeführten, unterbliebenen sowie nachgeholten Benachrichtigungen gemäß § 13 Absatz 5,
8. die Anzahl von Fällen der Übermittlung von Daten gemäß § 13 Absatz 6 und 7,
9. den Umgang mit unzulässig erlangten Daten, die den Kernbereich privater Lebensgestaltung betreffen, gemäß § 13 Absatz 8, sowie
10. die Anzahl von gemäß §§ 15 bis 17 gemeldeten Sicherheitsereignissen und Sicherheitsvorfällen.

²Die staatlichen und nicht-staatlichen Stellen, die die Maßnahmen nach §§ 12 und 13 in eigener Zuständigkeit ausüben, unterrichten die Beauftragte oder den Beauftragten für Informationssicherheit

des Landes jährlich über ihre Tätigkeit gemäß Satz 1 Nummer 3 bis 10.

(9) Die oder der Beauftragte für Informationssicherheit des Landes unterrichtet die Gremien nach § 17 Absatz 1 und § 18 Absatz 2 des [Sächsischen E-Government-Gesetzes](#) und die Arbeitsgruppe Informationssicherheit regelmäßig über ihre oder seine Tätigkeit.

(10) Die oder der Beauftragte für Informationssicherheit des Landes unterrichtet die Öffentlichkeit über wesentliche Entwicklungen der Informationssicherheit im Freistaat Sachsen.⁵

§ 6

Sicherheitsnotfallteam

(1) ¹Das Sicherheitsnotfallteam ist im Staatsbetrieb Sächsische Informatik Dienste angesiedelt.

²Aufgaben des Sicherheitsnotfallteams sind

1. die Wahrnehmung der Aufgaben des Computer-Notfallteams nach Artikel 10 und 11 der Richtlinie (EU) 2022/2555 für die staatlichen Stellen,
2. das Aufzeigen von Lösungen bei konkreten Sicherheitsereignissen oder -vorfällen,
3. die Prüfung auf Risiken im Betrieb von informationstechnischen Systemen und die Unterstützung bei ihrer Beseitigung,
4. die Information zu Sicherheitslücken,
5. die Erfassung und Analyse der Lage der Informationssicherheit sowie die Erstellung daraus abgeleiteter Empfehlungen,
6. die Wahrnehmung der zentralen Meldestelle im Sinne des [BSI-Gesetzes](#),
7. die Wahrnehmung der zentralen Meldestelle im Sinne des IT-Planungsrates im Verwaltungs-CERT-Verbund,
8. die Mitwirkung bei der technischen und technologischen Koordinierung der Informationssicherheit in den staatlichen und nicht-staatlichen Stellen sowie
9. die regelmäßige Information über die Lage der Informationssicherheit im Freistaat Sachsen.

³Das Sicherheitsnotfallteam unterstützt die Beauftragte oder den Beauftragten für Informationssicherheit des Landes und die Beauftragten für Informationssicherheit der staatlichen oder nicht-staatlichen Stellen des Freistaates Sachsen in technischen Sicherheitsfragen.

(1a) ¹Das Sicherheitsnotfallteam kann im Rahmen seiner Aufgaben nach Absatz 1 zur Erkennung von Sicherheitslücken bei staatlichen Stellen oder auf Ersuchen einer staatlichen Stelle Maßnahmen an den Schnittstellen öffentlich erreichbarer informationstechnischer Systeme zu öffentlichen Telekommunikationsnetzen durchführen, um festzustellen, ob diese ungeschützt und dadurch in ihrer Sicherheit oder Funktionsfähigkeit gefährdet sind. ²Erlangt das Sicherheitsnotfallteam dabei Informationen, die durch Artikel 10 des [Grundgesetzes](#) für die Bundesrepublik Deutschland geschützt sind, darf es diese nur nach § 13 Absatz 6 und 7 übermitteln. ³Liegen dessen Voraussetzungen nicht vor, sind diese Informationen unverzüglich zu löschen. ⁴Das Sicherheitsnotfallteam unterrichtet die für das informationstechnische System Verantwortlichen unverzüglich über die durch Maßnahmen gemäß Satz 1 erkannten Sicherheitslücken. ⁵Es soll dabei auf bestehende Abhilfemöglichkeiten hinweisen.

(2) ¹Das Sicherheitsnotfallteam hat zur Wahrnehmung seiner Aufgaben alle für die Abwehr von Gefahren für die Informationssicherheit erforderlichen Informationen, insbesondere zu Sicherheitslücken, Schadprogrammen, erfolgten oder versuchten Angriffen auf die Sicherheit in den informationstechnischen Systemen und der dabei beobachteten Vorgehensweise, zu sammeln und auszuwerten. ²Die staatlichen oder nicht-staatlichen Stellen im Freistaat Sachsen stellen dem Sicherheitsnotfallteam die Daten unverzüglich und unentgeltlich für die Zwecke nach Satz 1 je nach Anforderung kontinuierlich oder auf Anforderung zur Verfügung. ³Daten des Sächsischen Rechnungshofs, der oder des Sächsischen Datenschutzbeauftragten, der Gerichte und Staatsanwaltschaften sowie der Behörden und Organisationen mit Sicherheitsaufgaben dürfen nur einvernehmlich mit diesen erhoben, gespeichert, ausgewertet, genutzt oder sonst verarbeitet werden. ⁴Sind Daten betroffen, die dem richterlichen, staatsanwaltschaftlichen oder rechtspflegerischen Arbeitsprozess zuzurechnen sind, ist § 41c des [Sächsischen Justizgesetzes](#) vom 24. November 2000 (SächsGVBl. S. 482; 2001 S. 704), das zuletzt durch Artikel 15 des Gesetzes vom 11. Mai 2019 (SächsGVBl. S. 358) geändert worden ist, in der jeweils geltenden Fassung, entsprechend anzuwenden. ⁵Für Hochschulen im Sinne von § 1 Absatz 1 Satz 1 des [Sächsischen Hochschulgesetzes](#) vom 31. Mai 2023 (SächsGVBl. S. 329) gilt Satz 2 nicht.

(3) ¹Das Sicherheitsnotfallteam kann zur Erfüllung seiner Aufgaben gegenüber staatlichen Stellen und

nicht-staatlichen Stellen, soweit sie an das Sächsische Verwaltungsnetz oder das Kommunale Datennetz angeschlossen sind, im Einvernehmen mit der oder dem Beauftragten für Informationssicherheit des Landes und im Benehmen mit der oder dem jeweils zuständigen Beauftragten für Informationssicherheit die erforderlichen Anordnungen treffen oder Maßnahmen ergreifen, um die Gefahren für die informationstechnischen Systeme etwa durch Schadprogramme, Sicherheitslücken, unbefugte Datennutzung oder unbefugte Datenverarbeitung durch Dritte zu erkennen und abzuwehren. ²Das umfasst insbesondere die dazu erforderliche Datenverarbeitung.

(4) ¹Die Verarbeitung personenbezogener Daten durch das Sicherheitsnotfallteam zu anderen Zwecken als demjenigen, zu dem die Daten ursprünglich erhoben wurden, ist zur Sammlung, Auswertung oder Untersuchung von Informationen zu Sicherheitslücken, 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. ²Die Verarbeitung personenbezogener Daten im Sinne von Artikel 9 Absatz 1 der Verordnung (EU) 2016/679 durch das Sicherheitsnotfallteam ist zulässig, wenn

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

³Personenbezogene Daten sind unverzüglich zu löschen, sobald sie für die Erfüllung der Aufgaben des Sicherheitsnotfallteams nicht mehr benötigt werden. ⁴Sie sind spätestens 90 Tage nach ihrer Erhebung zu pseudonymisieren; § 13 Absatz 2 Satz 6 und 7 gilt entsprechend. ⁵Satz 1 gilt nicht für Daten, die dem richterlichen, staatsanwaltschaftlichen oder rechtspflegerischen Arbeitsprozess zuzurechnen sind.

(5) ¹Das Sicherheitsnotfallteam sieht angemessene und spezifische Maßnahmen zur Wahrung der Interessen der betroffenen Person vor. ²§ 22 Absatz 2 Satz 2 des [Bundesdatenschutzgesetzes](#) gilt entsprechend.

(6) Das Sicherheitsnotfallteam muss an einem sicheren Standort eingerichtet werden und ausgestattet sein mit

1. einer geeigneten, sicheren und belastbaren Kommunikations- und Informationsinfrastruktur,
2. einer Anzahl an Kommunikationskanälen, die einen hohen Grad von deren Verfügbarkeit gewährleistet,
3. einem geeigneten System zur Verwaltung und Weiterleitung von Anfragen, insbesondere um wirksame und effiziente Übergaben zu erleichtern,
4. Personal, das die ständige Bereitschaft seiner Dienste gewährleistet, sowie
5. Redundanzsystemen und Ausweicharbeitsräumen.⁶

§ 7

Beauftragte für Informationssicherheit der staatlichen Stellen

(1) ¹In jedem Staatsministerium, in der Staatskanzlei, dem Landespolizeipräsidium, der Leitstelle für Informationstechnologie der sächsischen Justiz, dem Staatsbetrieb Sächsische Informatik Dienste sowie bei dem Sächsischen Rechnungshof und der oder dem Sächsischen Datenschutzbeauftragten werden je eine hauptamtliche Beauftragte oder ein hauptamtlicher Beauftragter für Informationssicherheit und eine Vertreterin oder ein Vertreter ernannt. ²Die oder der Beauftragte für Informationssicherheit berichtet der Leiterin oder dem Leiter der staatlichen Stelle und der oder dem Beauftragten für Informationssicherheit des Landes mindestens einmal jährlich zum Stand der Informationssicherheit in seinem Zuständigkeitsbereich. ³Die Leiterin oder der Leiter unterstützt die oder den Beauftragten für Informationssicherheit bei der Erfüllung ihrer oder seiner Aufgaben nach Absatz 3, indem er die für die Erfüllung dieser Aufgaben erforderlichen Ressourcen zur Verfügung stellt.

(2) ¹Für jede nachgeordnete staatliche Stelle werden je eine Beauftragte oder ein Beauftragter für Informationssicherheit und eine Vertreterin oder ein Vertreter ernannt. ²Die jeweils zuständigen Beauftragten für Informationssicherheit der Aufsichtsbehörden sind innerhalb eines Monats über die

Ernennung zu unterrichten.³Bei der organisatorischen Zuweisung der Aufgaben sollen Interessenkonflikte vermieden werden.⁴Die oder der Beauftragte für Informationssicherheit einer nachgeordneten staatlichen Stelle muss nicht Beschäftigte oder Beschäftigter der staatlichen Stelle sein.⁵Beauftragte und Vertreter können jeweils für mehrere staatliche Stellen zuständig sein.⁶Die oder der Beauftragte für Informationssicherheit berichtet der Leiterin oder dem Leiter der staatlichen Stelle und der oder dem Beauftragten für Informationssicherheit der zuständigen Aufsichtsbehörde in angemessenen Abständen zum Stand der Informationssicherheit in ihrem oder seinem Zuständigkeitsbereich.

(3)¹Die oder der Beauftragte für Informationssicherheit fördert die Belange der Informationssicherheit innerhalb ihres oder seines Zuständigkeitsbereichs und koordiniert entsprechende Maßnahmen.²Die oder der Beauftragte für Informationssicherheit hat ein unmittelbares Vortragsrecht bei der Leiterin oder dem Leiter der staatlichen Stelle.³Die oder der Beauftragte für Informationssicherheit ist für die Einhaltung der Meldepflichten nach den §§ 15 und 16 in ihrem oder seinem Zuständigkeitsbereich verantwortlich.⁴Im Fall eines Sicherheitsvorfalls oder eines Sicherheitsereignisses ist die oder der Beauftragte für Informationssicherheit oder deren oder dessen Vertreterin oder Vertreter berechtigt, Einsicht in die Protokoll Daten ihres oder seines Zuständigkeitsbereichs zu nehmen oder diese anzufordern.⁵Daten des Sächsischen Rechnungshofs, der oder des Sächsischen Datenschutzbeauftragten, der Gerichte und Staatsanwaltschaften, der Behörden und Organisationen mit Sicherheitsaufgaben sowie der Hochschulen im Sinne von § 1 Absatz 1 des **Sächsischen Hochschulgesetzes** dürfen nur einvernehmlich mit diesen erhoben, gespeichert, ausgewertet, genutzt oder sonst verarbeitet werden.⁶Sind Daten betroffen, die dem richterlichen, staatsanwaltschaftlichen oder rechtspflegerischen Arbeitsprozess zuzurechnen sind, ist § 41c des **Sächsischen Justizgesetzes** entsprechend anzuwenden.⁷Die oder der Beauftragte für Informationssicherheit ist bei der Ausübung ihrer oder seiner Aufgaben weisungsfrei.⁸Sie oder er darf wegen der Erfüllung der ihr oder ihm übertragenen Aufgaben nicht benachteiligt werden.

(4)¹Das Gremium nach § 17 Absatz 1 des Sächsischen E-Government-Gesetzes beschließt ein Konzept zur Identifizierung der staatlichen Stellen nach Artikel 2 Absatz 2 Buchstabe f Ziffer ii der Richtlinie (EU) 2022/2555.²Die obersten Staatsbehörden identifizieren für ihre jeweiligen Geschäftsbereiche auf der Grundlage dieses Identifizierungskonzeptes die betroffenen staatlichen Stellen und übermitteln der oder dem Beauftragten für Informationssicherheit des Landes für die von ihnen erstmals oder erneut identifizierten staatlichen Stellen

1. den Namen der staatlichen Stelle,
2. die Anschrift und die aktuellen Kontaktdaten der oder des Beauftragten für Informationssicherheit der staatlichen Stelle, einschließlich E-Mail-Adresse und Telefonnummer,
3. die IP-Adressbereiche der staatlichen Stelle.

³Die erste Identifizierung nehmen die obersten Staatsbehörden zum 17. Januar 2025 vor und überprüfen diese alle zwei Jahre.⁷

§ 8

Beauftragte für Informationssicherheit der nicht-staatlichen Stellen

(1)¹Für nicht-staatliche Stellen sollen eine Beauftragte oder ein Beauftragter für Informationssicherheit und eine Vertreterin oder ein Vertreter ernannt werden.²Die oder der Beauftragte für Informationssicherheit muss nicht Beschäftigte oder Beschäftigter der nicht-staatlichen Stelle sein.³Beauftragte und Vertreter können jeweils für mehrere nicht-staatliche Stellen zuständig sein.⁴Für Schulen in kommunaler Trägerschaft ist die oder der Beauftragte für Informationssicherheit des jeweiligen Schulträgers zuständig.⁵Die oder der Beauftragte für Informationssicherheit des Landes ist innerhalb eines Monats über die Ernennung zu unterrichten.

(2) Für die oder den Beauftragten für Informationssicherheit der nicht-staatlichen Stelle gilt § 7 Absatz 3 entsprechend.⁸

§ 9

Informationssicherheitsmanagement-Teams

¹In jedem Staatsministerium, in der Staatskanzlei, dem Landespolizeipräsidium, der Leitstelle für Informationstechnologie der sächsischen Justiz, dem Staatsbetrieb Sächsische Informatik Dienste sowie bei dem Sächsischen Rechnungshof und der oder dem Sächsischen Datenschutzbeauftragten

sollen Informationssicherheitsmanagement-Teams im Rahmen des Informationssicherheitsmanagementsystems eingerichtet werden. ²In den anderen staatlichen Stellen können Informationssicherheitsmanagement-Teams im Rahmen des Informationssicherheitsmanagementsystems eingerichtet werden. ³Sie unterstützen die jeweilige Beauftragte oder den jeweiligen Beauftragten für Informationssicherheit bei ihrer oder seiner Arbeit.⁹

§ 10

Arbeitsgruppe Informationssicherheit

(1) ¹Die Arbeitsgruppe Informationssicherheit berät die Beauftragte oder den Beauftragten für Informationssicherheit des Landes in Fragen der Informationssicherheit. ²Sie besteht aus den Beauftragten für Informationssicherheit der Staatskanzlei, der Staatsministerien, des Sächsischen Rechnungshofs, der oder des Sächsischen Datenschutzbeauftragten, des Landespolizeipräsidiums, der Leitstelle für Informationstechnologie der sächsischen Justiz und des Staatsbetriebes Sächsische Informatik Dienste sowie zwei Personen, die die Kommunen vertreten. ³Weitere Mitglieder können aufgenommen werden.

(2) Die oder der IT- und Informationssicherheitsbeauftragte des Landtages kann an den Sitzungen teilnehmen.

(3) ¹Die Arbeitsgruppe Informationssicherheit wird von der oder dem Beauftragten für Informationssicherheit des Landes geleitet. ²Die Arbeitsgruppe Informationssicherheit gibt sich eine Geschäftsordnung.¹⁰

Abschnitt 3

Maßnahmen zur Sicherstellung der Informationssicherheit

§ 11

Datenübermittlung der nicht-staatlichen Stellen

(1) ¹Den Zugang zu dem Sächsischen Verwaltungsnetz können die kommunalen Träger der Selbstverwaltung über das Kommunale Datennetz und die sonstigen nicht-staatlichen Stellen über einen unmittelbaren Anschluss herstellen. ²Stattdessen kann der Zugang der nicht-staatlichen Stellen zu dem Sächsischen Verwaltungsnetz über eine Schnittstelle hergestellt werden, die eine vergleichbare Funktionalität und eine gleichwertige Informationssicherheit nach § 4 Absatz 1 Satz 1 bis 3 gewährleistet. ³Soweit auf speziellen Rechtsvorschriften beruhende technische und organisatorische Maßnahmen eine zuverlässige und sichere Datenübertragung für einzelne Fachverfahren gewährleisten, muss die verwaltungsübergreifende elektronische Datenübermittlung im Sinne von § 15 des [Sächsischen E-Government-Gesetzes](#) zwischen den staatlichen und den nicht-staatlichen Stellen nicht über das Sächsische Verwaltungsnetz geführt werden.

(2) ¹Die Staatsregierung wird ermächtigt, die Eigenschaften der Schnittstelle gemäß Absatz 1 Satz 2 durch Rechtsverordnung näher zu bestimmen. ²In dieser Rechtsverordnung können Vorgaben vorgesehen werden zu:

1. der Informationssicherheit für die in § 3 Absatz 1 genannten Schutzziele Vertraulichkeit, Integrität und Verfügbarkeit,
2. der Informationssicherheit bei der Verarbeitung personenbezogener Daten,
3. der Art der Datenverarbeitung,
4. der Mindest-Verfügbarkeit der Schnittstelle,
5. der Mindest-Bandbreite der Schnittstelle,
6. den für die Datenverbindung eingesetzten Protokollen,
7. der verwendeten Systeminfrastruktur und
8. der internen Organisation, die durch die jeweiligen Anbieter der Datenverbindung zu berücksichtigen sind.

³Vom IT-Kooperationsrat und den Trägern der Selbstverwaltung sind frühzeitig Stellungnahmen einzuholen. ⁴Beschließt der IT-Kooperationsrat daraufhin eine Empfehlung im Sinne von § 18 Absatz 3 Satz 1 Nummer 6 des [Sächsischen E-Government-Gesetzes](#), ist diese bei Erlass der Rechtsverordnung zu berücksichtigen. ⁵Gleiches gilt für die Stellungnahmen der Träger der Selbstverwaltung.

(3) Werden dem Freistaat Sachsen Anforderungen für die Zugangsschnittstellen zu dem Verbindungsnetz im Sinne von Artikel 91c Absatz 4 Satz 1 des [Grundgesetzes für die Bundesrepublik Deutschland](#) durch Beschlüsse des IT-Planungsrates als Koordinierungsgremium gemäß § 1 in Verbindung mit § 4 des Gesetzes über die Verbindung der informationstechnischen Netze des Bundes und der Länder – Gesetz zur Ausführung von Artikel 91c Absatz 4 des [Grundgesetzes](#) – vom 10. August 2009 (BGBl. I S. 2702, 2706), in der jeweils geltenden Fassung, vorgegeben oder nach § 5 des [Onlinezugangsgesetzes](#) festgelegt, sind diese Standards durch die nicht-staatlichen Stellen bei den von ihnen eingesetzt und mit dem Verbindungsnetz zumindest mittelbar verbundenen informationstechnischen Systemen einzuhalten.¹¹

§ 12

Abwehr von Gefahren für die informationstechnischen Systeme im Freistaat Sachsen

(1) ¹Zur Erkennung und Abwehr von Gefahren für die informationstechnischen Systeme im Freistaat Sachsen etwa durch Schadprogramme, Sicherheitslücken oder unbefugte Datenverarbeitung dürfen das Sicherheitsnotfallteam sowie die staatlichen und nicht-staatlichen Stellen im Freistaat Sachsen innerhalb ihres jeweiligen Zuständigkeitsbereichs

1. Protokolldaten erheben und automatisiert auswerten sowie
2. die an den Schnittstellen der informationstechnischen Systeme anfallenden Protokoll- und Inhaltsdaten erheben und automatisiert auswerten,

soweit dies zur Verhinderung oder Abwehr von Angriffen auf informationstechnische Systeme der staatlichen und nicht-staatlichen Stellen im Freistaat Sachsen oder zum Erkennen, Eingrenzen oder Beseitigen dieser Störungen der Informationssicherheit erforderlich ist. ²Jede staatliche Stelle kann ihre Befugnisse nach den §§ 12 und 13 im Einvernehmen mit dem Sicherheitsnotfallteam auf dieses übertragen.

(2) Die staatlichen und nicht-staatlichen Stellen im Freistaat Sachsen sind verpflichtet, das Sicherheitsnotfallteam bei Maßnahmen nach Absatz 1 Satz 1 und § 13 zu unterstützen sowie hierbei dem Sicherheitsnotfallteam behördeninterne Protokoll- und Daten nach Absatz 1 Satz 1 Nummer 1 und Daten nach Absatz 1 Satz 1 Nummer 2 zur Verfügung zu stellen.

(3) ¹Daten des Landtags, des Sächsischen Rechnungshofs, der oder des Sächsischen Datenschutzbeauftragten, der Gerichte und Staatsanwaltschaften, der Behörden und Organisationen mit Sicherheitsaufgaben sowie der Hochschulen im Sinne von § 1 Absatz 1 des [Sächsischen Hochschulgesetzes](#) dürfen nur einvernehmlich mit diesen erhoben, gespeichert, ausgewertet, genutzt oder sonst verarbeitet werden. ²Sind Daten betroffen, die dem richterlichen, staatsanwaltschaftlichen oder rechtspflegerischen Arbeitsprozess zuzurechnen sind, ist § 41c des [Sächsischen Justizgesetzes](#) entsprechend anzuwenden.¹²

§ 13

Datenspeicherung und -auswertung

(1) ¹Sofern nicht die Absätze 2 bis 8 eine weitere Verarbeitung gestatten, muss eine automatisierte Auswertung der Daten nach § 12 Absatz 1 unverzüglich erfolgen und diese müssen nach erfolgreichem Abgleich sofort und nach dem Stand der Technik sicher gelöscht werden. ²Daten, die weder personenbezogen sind noch dem Fernmeldegeheimnis unterliegen, sind von den Verarbeitungseinschränkungen dieser Vorschrift ausgenommen.

(2) ¹Protokolldaten dürfen über den für die automatisierte Auswertung erforderlichen Zeitraum hinaus, längstens jedoch für 90 Tage, gespeichert werden, soweit tatsächliche Anhaltspunkte bestehen, dass die Daten erforderlich sein können:

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

²Die Daten sind im Gebiet der Europäischen Union zu speichern. ³Durch organisatorische und technische Maßnahmen nach dem Stand der Technik ist sicherzustellen, dass eine Auswertung der nach Satz 1 gespeicherten Daten nur automatisiert erfolgt. ⁴Die Daten sind zu pseudonymisieren, soweit dies automatisiert möglich ist. ⁵Eine nicht automatisierte Auswertung oder eine personenbezogene Verarbeitung ist nur nach Maßgabe der Absätze 4 bis 8 zulässig. ⁶Soweit hierzu die Wiederherstellung des Personenbezugs pseudonymisierter Daten erforderlich ist, muss diese durch die

zuständige Leiterin oder den zuständigen Leiter der staatlichen oder nicht-staatlichen Stelle angeordnet werden. ⁷Diese Entscheidung ist zu dokumentieren.

(3) ¹Inhaltsdaten dürfen über den für die automatisierte Auswertung erforderlichen Zeitraum hinaus, längstens für 60 Tage gespeichert werden, soweit tatsächliche Anhaltspunkte bestehen, dass die Daten erforderlich sein können:

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

und die Speicherung zum Schutz der technischen Systeme unerlässlich ist. ²Die Speicherung und Auswertung der Inhaltsdaten ist von der zuständigen Leiterin oder dem zuständigen Leiter der staatlichen oder nicht-staatlichen Stelle und einer oder einem weiteren Bediensteten dieser Stelle mit Befähigung zum Richteramt anzuordnen. ³Die Daten sind im Gebiet der Europäischen Union zu speichern. ⁴Durch organisatorische und technische Maßnahmen nach dem Stand der Technik ist sicherzustellen, dass eine Auswertung der nach Satz 1 gespeicherten Daten nur automatisiert erfolgt. ⁵Die Daten sind zu pseudonymisieren, soweit dies automatisiert möglich ist. ⁶Eine nicht automatisierte Auswertung oder eine personenbezogene Verarbeitung ist nur nach Maßgabe der Absätze 4 bis 8 zulässig. ⁷Soweit hierzu die Wiederherstellung des Personenbezugs pseudonymisierter Daten erforderlich ist, muss diese durch die zuständige Leiterin oder den zuständigen Leiter der staatlichen oder nicht-staatlichen Stelle und einer oder einen weiteren Bediensteten dieser Stelle mit der Befähigung zum Richteramt angeordnet werden. ⁸Sofern diese Stelle keine weitere Bedienstete oder keinen weiteren Bediensteten mit der Befähigung zum Richteramt beschäftigt, ist die Anordnung der Speicherung und Auswertung der Inhaltsdaten oder der Wiederherstellung des Personenbezugs pseudonymisierter Daten von der Leiterin oder dem Leiter der staatlichen oder nicht-staatlichen Stelle und einer oder einem Bediensteten der Aufsichtsbehörde mit der Befähigung zum Richteramt zu treffen. ⁹Die Anordnung gilt längstens für zwei Monate; sie kann verlängert werden. ¹⁰Diese Entscheidung ist zu dokumentieren.

(4) ¹Die Verarbeitung der in § 12 Absatz 1 genannten Daten ist auch zulässig,

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

²Im 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.

³Ein Schadprogramm darf beseitigt oder in seiner Funktionsweise gehindert werden. ⁴Die nicht automatisierte Verarbeitung der Daten nach den Sätzen 1 und 2 darf nur von der Leiterin oder dem Leiter der staatlichen oder nicht-staatlichen Stelle und einer oder einem Bediensteten dieser Stelle mit der Befähigung zum Richteramt angeordnet werden. ⁵Sofern diese Stelle keine weitere Bedienstete oder keinen weiteren Bediensteten mit der Befähigung zum Richteramt beschäftigt, ist die Anordnung nach Satz 4 von der Leiterin oder dem Leiter der staatlichen oder nicht-staatlichen Stelle und einer oder einem Bediensteten der Aufsichtsbehörde mit der Befähigung zum Richteramt zu treffen.

(5) ¹Die von den Maßnahmen nach Absatz 4 betroffenen Personen und betroffenen staatlichen oder nicht-staatlichen 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. ²Die Benachrichtigung kann unterbleiben, wenn die Person nur unerheblich betroffen wurde und anzunehmen ist, dass sie an einer Benachrichtigung kein Interesse hat. ³Die staatlichen und nicht-staatlichen Stellen legen Fälle, in denen sie von einer Benachrichtigung absehen, der oder dem zuständigen Datenschutzbeauftragten dieser Stelle und einer oder einem weiteren Bediensteten dieser Stelle mit Befähigung zum Richteramt zur Kontrolle vor. ⁴Die oder der zuständige Datenschutzbeauftragte ist bei Ausübung dieser Aufgabe weisungsfrei und darf deswegen nicht benachteiligt werden (Artikel 38 Absatz 3 der Verordnung [EU] 2016/679). ⁵Wenn die oder der zuständige Datenschutzbeauftragte der Entscheidung der staatlichen oder nicht-staatlichen Stelle widerspricht, ist die Benachrichtigung nachzuholen. ⁶Die Entscheidung über die Nichtbenachrichtigung ist zu dokumentieren. ⁷Die Dokumentation darf ausschließlich für Zwecke der Datenschutzkontrolle verwendet werden. ⁸Sie ist nach zwölf Monaten zu löschen. ⁹In den Fällen der Absätze 6 und 7 erfolgt die Benachrichtigung durch die dort genannten Behörden nach den für diese

Behörden geltenden Vorschriften.¹⁰ 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.

(6)¹ 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.² Ferner dürfen diese Daten zur Abwehr einer Gefahr für die öffentliche Sicherheit, die unmittelbar von einem Schadprogramm ausgeht, an die Polizei des Freistaates Sachsen übermittelt werden.

(7)¹ Für sonstige Zwecke dürfen die Daten übermittelt werden an:

1. die Strafverfolgungsbehörden zur Verfolgung einer Straftat von auch im Einzelfall erheblicher Bedeutung, insbesondere einer in § 100a Absatz 2 der **Strafprozessordnung** bezeichneten Straftat,
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,
3. das Landesamt für Verfassungsschutz, wenn tatsächliche Anhaltspunkte für Bestrebungen nach § 2 Absatz 1 Nummer 2 des **Sächsischen Verfassungsschutzgesetzes** vom 16. Oktober 1992 (SächsGVBl. S. 459), das zuletzt durch Artikel 1 des Gesetzes vom 3. Mai 2019 (SächsGVBl. S. 312) geändert worden ist, oder für Bestrebungen vorliegen, die durch Anwendung von Gewalt oder darauf gerichtete Vorbereitungshandlungen gegen die in § 2 Absatz 1 Nummer 1, 3 und 3a des **Sächsischen Verfassungsschutzgesetzes** genannten Schutzgüter gerichtet sind.² § 10 des **Sächsischen Verfassungsschutzgesetzes** bleibt unberührt.

² Die Übermittlung nach Satz 1 Nummer 1 und 2 bedarf der vorherigen gerichtlichen Zustimmung.³ Für das Verfahren nach Satz 1 Nummer 1 und 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.⁴ Zuständig ist das Amtsgericht, in dessen Bezirk die übermittelnde Stelle ihren Sitz hat.⁵ Die Übermittlung nach Satz 1 Nummer 3 erfolgt nach Zustimmung des Staatsministeriums des Innern; 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.

(8)¹ Eine über die Absätze 1 bis 7 hinausgehende inhaltliche Auswertung zu anderen Zwecken und die Weitergabe von personenbezogenen Daten an Dritte sind unzulässig.² Soweit möglich, ist bei der Datenverarbeitung technisch sicherzustellen, dass Daten, die den Kernbereich privater Lebensgestaltung betreffen, nicht erhoben werden.³ Werden Erkenntnisse aus dem Kernbereich privater Lebensgestaltung erlangt, dürfen diese Daten nicht verwendet werden und sind unverzüglich zu löschen.⁴ Dies gilt auch in Zweifelsfällen.⁵ Die Tatsache ihrer Erlangung und Löschung ist zu dokumentieren.

(9) Anstelle der Schulleiterin oder des Schulleiters ist für Anordnungen nach den Absätzen 3 und 4 eine Bedienstete oder ein Bediensteter zuständig, die oder der vom Schulträger zu bestimmen ist.¹³

§ 14 Sicherheitskonzept

¹ Vor Aufnahme der Datenverarbeitung nach den §§ 12 und 13 ist ein für diesen Gebrauch erarbeitetes Sicherheitskonzept innerhalb des Informationssicherheitsmanagementsystems zu erstellen sowie die Umsetzung aller darin vorgesehenen technischen und organisatorischen Maßnahmen aktenkundig zu machen.² Das Sicherheitskonzept ist vor jeder wesentlichen Veränderung der eingesetzten technischen Systeme zu aktualisieren und alle drei Jahre einer Revision zu unterziehen.

Abschnitt 4 Meldepflichten

§ 15 Stellenübergreifende Meldepflichten

¹ Werden staatlichen oder nicht-staatlichen Stellen im Freistaat Sachsen oder Beliehenen, die an das

Sächsische Verwaltungsnetz oder das Kommunale Datennetz angeschlossen sind, Informationen bekannt, die zur Abwehr von Gefahren für die informationstechnischen Systeme von Bedeutung sind, teilen sie dies unverzüglich dem Sicherheitsnotfallteam mit, soweit andere Vorschriften nicht entgegenstehen. ²Von der Meldung darf abgesehen werden, wenn die Information bereits in öffentlich zugänglichen Medien verbreitet wurde.

§ 16

Meldepflichten der staatlichen Stellen

(1) ¹(1) Staatliche Stellen des Freistaates Sachsen haben Sicherheitsereignisse und Sicherheitsvorfälle ihrer informationstechnischen Systeme oder Prozesse an das Sicherheitsnotfallteam zu melden. ²Die Meldungen haben unverzüglich zu erfolgen, wenn es sich um erhebliche Sicherheitsvorfälle handelt. ³Ein erheblicher Sicherheitsvorfall ist ein Sicherheitsvorfall, der

1. schwerwiegende Betriebsstörungen der Dienste oder materielle Schäden für die betreffende Einrichtung verursacht hat oder verursachen kann oder
2. Dritte durch erhebliche materielle oder immaterielle Schäden beeinträchtigt hat oder beeinträchtigen kann,

soweit durch die Rechtsverordnung nach Absatz 2 keine abweichende Begriffsbestimmung erfolgt. ⁴Zu Sicherheitsereignissen und sonstigen Sicherheitsvorfällen sind mit Inkrafttreten der Rechtsverordnung nach Absatz 2 zusätzlich zu melden:

1. statistische Auswertungen und
2. Protokolldaten von Schutzsystemen, etwa Proxies, Virenscannern oder Firewalls in automatisierter Form.

(2) ¹Die Staatsregierung wird ermächtigt, Einzelheiten des Meldeverfahrens durch Rechtsverordnung näher zu bestimmen. ²In dieser Rechtsverordnung können Vorgaben zu meldepflichtigen Informationen und Meldeprozessen vorgesehen werden.¹⁴

§ 17

Meldepflichten der nicht-staatlichen Stellen

¹Für nicht-staatliche Stellen gelten die Meldepflichten nach § 16 nur, soweit deren informationstechnische Systeme mit dem Sächsischen Verwaltungsnetz oder dem Kommunalen Datennetz verbunden sind. ²Hochschulen im Sinne von § 1 Absatz 1 des [Sächsischen Hochschulgesetzes](#) sind nach § 16 Absatz 1 hinsichtlich erheblicher Sicherheitsvorfälle meldepflichtig. ³Soweit das Kommunale Datennetz betroffen ist, ist der Beauftragte für Informationssicherheit des Betreibers des Kommunalen Datennetzes unverzüglich durch die nicht-staatliche Stelle über die Meldung zu informieren. ⁴Im Übrigen steht es den nicht-staatlichen Stellen frei, Sicherheitsvorfälle und Sicherheitsereignisse entsprechend § 16 an das Sicherheitsnotfallteam zu melden.¹⁵

Abschnitt 5

Schlussvorschriften

§ 18

Einschränkung von Grundrechten

Das Fernmeldegeheimnis (Artikel 10 des [Grundgesetzes](#) für die Bundesrepublik Deutschland, Artikel 27 der [Verfassung des Freistaates Sachsen](#)) und das Recht auf informationelle Selbstbestimmung (Artikel 33 der [Verfassung des Freistaates Sachsen](#)) werden durch die § 6 Absatz 3 und 4, §§ 12 und 13 eingeschränkt.

§ 19

Experimentierklausel

¹Die jeweils fachlich zuständige oberste Staatsbehörde wird ermächtigt, durch Rechtsverordnung zur Erprobung neuer Systeme zur Datenanalyse, die der Abwehr von Gefahren für die informationstechnischen Systeme des Freistaates Sachsen dienen, im Einvernehmen mit der oder dem Beauftragten für Informationstechnologie des Freistaates Sachsen und mit Zustimmung der oder des Sächsischen Datenschutzbeauftragten sachlich und örtlich begrenzte Ausnahmen zur Auswertung von

anderen nicht in § 12 Absatz 1 genannten Daten für einen Zeitraum von höchstens drei Jahren zuzulassen. ²Satz 1 findet keine Anwendung für die Daten der Gerichte und Staatsanwaltschaften.¹⁶

§ 20 Übergangsregelung

Sicherheitskonzepte nach § 14 sind erstmals im Jahre 2024 einer Revision nach § 14 Satz 2 zu unterziehen.¹⁷

§ 21 Evaluierung

(1) Die Staatsregierung legt dem Landtag erstmals zum 31. Dezember 2024 einen Bericht vor, in dem sie darlegt,

1. welche Auswirkungen dieses Gesetz auf die Informationssicherheit in den Behörden im Freistaat Sachsen hat,
2. welche Projekte auf Basis der Experimentierklausel des § 19 durchgeführt wurden,
3. welche Kosten und welcher Nutzen bei der Umsetzung des Gesetzes entstanden sind und
4. 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

-
- 1 Inhaltsübersicht geändert durch [Gesetz vom 5. Juli 2024](#) (SächsGVBl. S. 590)
 - 2 § 2 geändert durch [Gesetz vom 5. Juli 2024](#) (SächsGVBl. S. 590)
 - 3 § 3 geändert durch [Gesetz vom 5. Juli 2024](#) (SächsGVBl. S. 590)
 - 4 § 4 geändert durch [Gesetz vom 5. Juli 2024](#) (SächsGVBl. S. 590)
 - 5 § 5 geändert durch [Gesetz vom 5. Juli 2024](#) (SächsGVBl. S. 590)
 - 6 § 6 geändert durch [Artikel 14 des Gesetzes vom 31. Mai 2023](#) (SächsGVBl. S. 329) und durch [Gesetz vom 5. Juli 2024](#) (SächsGVBl. S. 590)
 - 7 § 7 geändert durch [Artikel 14 des Gesetzes vom 31. Mai 2023](#) (SächsGVBl. S. 329) und durch [Gesetz vom 5. Juli 2024](#) (SächsGVBl. S. 590)
 - 8 § 8 geändert durch [Gesetz vom 5. Juli 2024](#) (SächsGVBl. S. 590)
 - 9 § 9 geändert durch [Gesetz vom 5. Juli 2024](#) (SächsGVBl. S. 590)
 - 10 § 10 geändert durch [Gesetz vom 5. Juli 2024](#) (SächsGVBl. S. 590)
 - 11 § 11 geändert durch [Gesetz vom 5. Juli 2024](#) (SächsGVBl. S. 590)
 - 12 § 12 geändert durch [Artikel 14 des Gesetzes vom 31. Mai 2023](#) (SächsGVBl. S. 329) und durch [Gesetz vom 5. Juli 2024](#) (SächsGVBl. S. 590)
 - 13 § 13 geändert durch [Gesetz vom 5. Juli 2024](#) (SächsGVBl. S. 590)
 - 14 § 16 geändert durch [Gesetz vom 5. Juli 2024](#) (SächsGVBl. S. 590)
 - 15 § 17 geändert durch [Gesetz vom 5. Juli 2024](#) (SächsGVBl. S. 590)
 - 16 § 19 geändert durch [Gesetz vom 5. Juli 2024](#) (SächsGVBl. S. 590)
 - 17 § 20 geändert durch [Gesetz vom 5. Juli 2024](#) (SächsGVBl. S. 590)
 - 18 § 21 geändert durch [Gesetz vom 5. Juli 2024](#) (SächsGVBl. S. 590)

Änderungsvorschriften

Änderung des Sächsischen Informationssicherheitsgesetzes

Art. 14 des Gesetzes vom 31. Mai 2023 (SächsGVBl. S. 329)

Gesetz zur Änderung des Sächsischen Informationssicherheitsgesetzes

vom 5. Juli 2024 (SächsGVBl. S. 590)