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

Inhaltsübersicht

Abschnitt 1
Allgemeine Vorschriften

§ 1
Zweck des Gesetzes

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

§ 2
Anwendungsbereich

(1) [1]Dieses 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). [2]Auf Beliehene finden ausschließlich die Absätze 4 und 5 Anwendung.

(2) [1]Der 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. [2]Für 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, den Mitteldeutschen Rundfunk, die öffentlich-rechtlichen Kreditinstitute im Freistaat Sachsen und die Sachsen-Finanzgruppe.

(4) Dieses Gesetz gilt nicht, soweit auf Behörden des Freistaates Sachsen und die seiner Aufsicht unterstehenden Körperschaften, Anstalten und Stiftungen des öffentlichen Rechts die Regelungen des BSI-Gesetzes vom 14. August 2009 (BGBl. I S. 2821), das zuletzt durch Artikel 1 des Gesetzes vom 23. Juni 2017 (BGBl. I S. 1885) geändert worden ist, in der jeweils geltenden Fassung, Anwendung finden.

(5) 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.

§ 3
Begriffsbestimmungen

(1) Informationssicherheit im Sinne dieses Gesetzes bedeutet Gewährleistung von 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 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 22. Juni 2004 (BGBl. I S. 1190), das zuletzt durch Artikel 1 des Gesetzes vom 29. November 2018 (BGBl. I S. 2230) geändert worden ist, in der jeweils geltenden Fassung, sind.

(9) [1]Protokolldaten im Sinne dieses Gesetzes beschreiben oder historisieren Zustände und Aktionen von informationstechnischen Systemen. [2]Protokolldaten können Verkehrsdaten gemäß § 3 Nummer 30 des Telekommunikationsgesetzes und Nutzungsdaten nach § 15 Absatz 1 des Telemediengesetzes vom 26. Februar 2007 (BGBl. I S. 179), das zuletzt durch Artikel 1 des Gesetzes vom 28. September 2017 (BGBl. I S. 3530) geändert worden ist, enthalten.

§ 4
Grundsätze der Informationssicherheit

(1) [1]Die staatlichen Stellen treffen angemessene organisatorische und technische Vorkehrungen sowie sonstige Maßnahmen zur Gewährleistung der Informationssicherheit. [2]Für technische Maßnahmen soll der

Stand der Technik maßgeblich sein. [3]Maßnahmen sind angemessen, wenn der dafür erforderliche Aufwand nicht außer Verhältnis zu den Folgen der Verletzung der Schutzziele steht. [4]Um die Erreichung und Aufrechterhaltung eines angemessenen Informationssicherheitsniveaus zu gewährleisten, haben alle staatlichen Stellen die jeweils geltenden Standards und das jeweils geltende IT-Grundschutz-Kompendium des Bundesamtes für Sicherheit in der Informationstechnik zu berücksichtigen. [5]Die staatlichen Stellen erstellen und pflegen ein Informationssicherheitsmanagementsystem.

(2) [1]Für die nicht-staatlichen Stellen gilt Absatz 1 Satz 1 bis 3 entsprechend. [2]Die jeweils geltenden Standards und das jeweils geltende IT-Grundschutz-Kompendium des Bundesamtes für Sicherheit in der Informationstechnik werden zur Anwendung empfohlen. [3]Werden 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) [1]Die Verantwortung für die Informationssicherheit im Sinne des Absatzes 1 trägt der jeweilige Leiter der staatlichen oder nicht-staatlichen Stelle, bei Schulen der jeweilige Schulträger. [2]Er stellt im Rahmen der ihm zugewiesenen Aufgaben und Befugnisse die erforderlichen personellen und finanziellen Ressourcen zur Verfügung.

(4) Wesentliche Änderungen an den informationstechnischen Systemen einer staatlichen oder nicht-staatlichen Stelle dürfen nur im Benehmen mit 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.

Abschnitt 2
Organisation der Informationssicherheit

§ 5
Beauftragter für Informationssicherheit des Landes

(1) [1]Der Beauftragte für Informationssicherheit des Landes wird vom Beauftragten für Informationstechnologie des Freistaates Sachsen ernannt und nimmt seine Aufgaben hauptamtlich wahr. [2]Er fördert und unterstützt durch die Erstellung von konkreten Handlungsempfehlungen, Maßnahme- und Formulierungsvorschlägen, Erläuterungen, Leitfäden und auf Anforderung durch individuelle Beratung die Beauftragten für Informationssicherheit nach § 7 Absatz 1 bei der Erfüllung ihrer Aufgaben, insbesondere bei der Erstellung und Pflege eines Informationssicherheitsmanagementsystems. [3]Er initiiert und koordiniert landesweite Sensibilisierungs- und Schulungsmaßnahmen und Projekte zur Informationssicherheit. [4]Der Beauftragte für Informationssicherheit des Landes hat ein direktes Vorspracherecht beim Beauftragten für Informationstechnologie des Freistaates Sachsen. [5]Er berät ihn bei seiner Aufgabenwahrnehmung bezüglich der Informationssicherheit und unterstützt ihn bei der Umsetzung.

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

(3) [1]Gegenüber an das Sächsische Verwaltungsnetz angeschlossenen staatlichen Stellen kann 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. [2]Zur Abwehr von stellenübergreifenden Sicherheitsvorfällen ihrer informationstechnischen Systeme oder Prozesse darf er bei Gefahr im Verzug vorübergehende Netztrennungen anordnen. [3]Der Leiter der staatlichen Stelle und der für die staatliche Stelle ernannte Beauftragte für Informationssicherheit sind unverzüglich zu unterrichten. [4]Für die Umsetzung der Maßnahmen bedient sich der Beauftragte für Informationssicherheit des Landes des Sicherheitsnotfallteams.

(4) [1]Gegenüber nicht-staatlichen Stellen kann der Beauftragte für Informationssicherheit des Landes Anordnungen im Benehmen mit dem Beauftragten für Informationssicherheit des Betreibers des Kommunalen Datennetzes treffen, um Gefahren für die informationstechnischen Systeme, die mit dem Kommunalen Datennetz verbunden sind, abzuwehren. [2]Zur Abwehr von stellenübergreifenden

Sicherheitsvorfällen auf informationstechnische Systeme oder Prozesse innerhalb des Sächsischen Verwaltungsnetzes darf er bei Gefahr im Verzug vorübergehende Trennungen des Kommunalen Datennetzes vom Sächsischen Verwaltungsnetz anordnen. [3]Der Leiter der nicht-staatlichen Stelle, der für diese ernannte Beauftragte für Informationssicherheit und der Beauftragte für Informationssicherheit des Betreibers des Kommunalen Datennetzes sind unverzüglich zu unterrichten. [4]Die vom Beauftragten für Informationssicherheit des Landes angeordneten Maßnahmen nach Satz 2 werden durch das Sicherheitsnotfallteam umgesetzt.

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

(6) [1]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 vom 9. Juli 2014 (SächsGVBl. S. 398), das zuletzt durch Artikel 2 des Gesetzes vom 2. August 2019 (SächsGVBl. S. 630) geändert worden ist, in der jeweils geltenden Fassung, zur Entscheidung vor. [2]Die Arbeitsgruppe Informationssicherheit unterstützt den Beauftragten für Informationssicherheit des Landes dabei. [3]Den nicht-staatlichen Stellen wird die Anwendung der Mindeststandards empfohlen. [4]Auf Ersuchen berät der Beauftragte für Informationssicherheit des Landes die staatlichen oder nicht-staatlichen Stellen bei der Umsetzung und Einhaltung der Mindeststandards.

(7) [1]Um die Wirksamkeit des Informationssicherheitsmanagementsystems und den Stand der Erfüllung der Mindeststandards zu überprüfen, kann der Beauftragte für Informationssicherheit des Landes die erforderlichen Auskünfte und die Überlassung von entsprechenden Unterlagen der staatlichen Stellen verlangen. [2]Zu diesem Zweck darf er eigene Revisionen durchführen, wobei für den Sächsischen Rechnungshof, den Sächsischen Datenschutzbeauftragten, die Gerichte und Staatsanwaltschaften sowie die Behörden und Organisationen mit Sicherheitsaufgaben hierfür deren Einvernehmen einzuholen ist. [3]Er ist über geplante Audits oder Revisionen zu unterrichten. [4]Vorliegende Zertifikate auf der Basis von IT-Grundschutz nach dem BSI-Gesetz und der Zertifizierungsverordnung zum BSI-Gesetz sind dabei zu beachten.

(8) [1]Der Beauftragte für Informationssicherheit des Landes unterrichtet den Landtag jährlich allgemein über 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.

[2]Die staatlichen und nicht-staatlichen Stellen, die die Maßnahmen nach §§ 12 und 13 in eigener Zuständigkeit ausüben, unterrichten den Beauftragten für Informationssicherheit des Landes jährlich über ihre Tätigkeit gemäß Satz 1 Nummern 3 bis 10.

(9) 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 seine Tätigkeit.

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

§ 6
Sicherheitsnotfallteam

(1) [1]Das Sicherheitsnotfallteam ist im Staatsbetrieb Sächsische Informatik Dienste angesiedelt. [2]Aufgaben des Sicherheitsnotfallteams sind:

1. das Aufzeigen von Lösungen bei konkreten Sicherheitsereignissen oder -vorfällen,
2. die Prüfung auf Risiken im Betrieb von informationstechnischen Systemen und die Unterstützung bei ihrer Beseitigung,
3. die Information zu Sicherheitslücken,
4. die Erfassung und Analyse der Lage der Informationssicherheit sowie die Erstellung daraus abgeleiteter Empfehlungen,
5. die Wahrnehmung der zentralen Meldestelle im Sinne des BSI-Gesetzes,
6. die Wahrnehmung der zentralen Meldestelle im Sinne des IT-Planungsrates im Verwaltungs-CERT-Verbund,
7. die Mitwirkung bei der technischen und technologischen Koordinierung der Informationssicherheit in den staatlichen und nicht-staatlichen Stellen sowie
8. die regelmäßige Information über die Lage der Informationssicherheit im Freistaat Sachsen.

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

(2) [1]Das 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. [2]Die 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. [3]Daten des Sächsischen Rechnungshofs, 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. [4]Sind 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. [5]Für Hochschulen im Sinne von § 1 Absatz 1 des Sächsischen Hochschulfreiheitsgesetzes in der Fassung der Bekanntmachung vom 15. Januar 2013 (SächsGVBl. S. 3), das zuletzt durch Artikel 2 Absatz 27 des Gesetzes vom 5. April 2019 (SächsGVBl. S. 245) geändert worden ist, und hochschulnahe Einrichtungen gilt Satz 2 nicht.

(3) [1]Das 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 dem Beauftragten für Informationssicherheit des Landes und im Benehmen mit 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. [2]Das umfasst insbesondere die dazu erforderliche Datenverarbeitung.

(4) [1]Die 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. [2]Die Verarbeitung personenbezogener Daten im Sinne von Artikel 9 Absatz 1 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) 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.

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

(5) [1]Das Sicherheitsnotfallteam sieht angemessene und spezifische Maßnahmen zur Wahrung der Interessen der betroffenen Person vor. [2]§ 22 Absatz 2 Satz 2 des Bundesdatenschutzgesetzes vom 30. Juni 2017 (BGBl. I S. 2097) gilt entsprechend.

§ 7
Beauftragte für Informationssicherheit der staatlichen Stellen

(1) [1]In 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 dem Sächsischen Datenschutzbeauftragten werden je ein hauptamtlicher Beauftragter für Informationssicherheit und ein Vertreter ernannt. [2]Der Beauftragte für Informationssicherheit berichtet dem Leiter der staatlichen Stelle und dem Beauftragten für Informationssicherheit des Landes mindestens einmal jährlich zum Stand der Informationssicherheit in seinem Zuständigkeitsbereich.

(2) [1]Für jede nachgeordnete staatliche Stelle werden je ein Beauftragter für Informationssicherheit und ein Vertreter ernannt. [2]Die jeweils zuständigen Beauftragten für Informationssicherheit der Aufsichtsbehörden sind innerhalb eines Monats über die Ernennung zu unterrichten. [3]Bei der organisatorischen Zuweisung der Aufgaben sollen Interessenkonflikte vermieden werden. [4]Der Beauftragte für Informationssicherheit einer nachgeordneten staatlichen Stelle muss nicht Beschäftigter der staatlichen Stelle sein. [5]Beauftragte und Vertreter können jeweils für mehrere staatliche Stellen zuständig sein. [6]Der Beauftragte für Informationssicherheit berichtet dem Leiter der staatlichen Stelle und dem Beauftragten für Informationssicherheit der zuständigen Aufsichtsbehörde in angemessenen Abständen zum Stand der Informationssicherheit in seinem Zuständigkeitsbereich.

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

§ 8
Beauftragte für Informationssicherheit der nicht-staatlichen Stellen

(1) [1]Für nicht-staatliche Stellen sollen ein Beauftragter für Informationssicherheit und ein Vertreter ernannt werden. [2]Der Beauftragte für Informationssicherheit muss nicht Beschäftigter der nicht-staatlichen Stelle sein. [3]Beauftragte und Vertreter können jeweils für mehrere nicht-staatliche Stellen zuständig sein. [4]Für Schulen in kommunaler Trägerschaft ist der Beauftragte für Informationssicherheit des jeweiligen Schulträgers zuständig. [5]Der Beauftragte für Informationssicherheit des Landes ist innerhalb eines Monats

über die Ernennung zu unterrichten.

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

§ 9
Informationssicherheitsmanagement-Teams

[1]In 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 dem Sächsischen Datenschutzbeauftragten sollen Informationssicherheitsmanagement-Teams im Rahmen des Informationssicherheitsmanagementsystems eingerichtet werden. [2]In den anderen staatlichen Stellen können Informationssicherheitsmanagement-Teams im Rahmen des Informationssicherheitsmanagementsystems eingerichtet werden. [3]Sie unterstützen den jeweiligen Beauftragten für Informationssicherheit bei seiner Arbeit.

§ 10
Arbeitsgruppe Informationssicherheit

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

(2) Der IT- und Informationssicherheitsbeauftragte des Landtages kann an den Sitzungen teilnehmen.

(3) [1]Die Arbeitsgruppe Informationssicherheit wird vom Beauftragten für Informationssicherheit des Landes geleitet. [2]Die Arbeitsgruppe Informationssicherheit gibt sich eine Geschäftsordnung.

Abschnitt 3
Maßnahmen zur Sicherstellung der Informationssicherheit

§ 11
Datenübermittlung der nicht-staatlichen Stellen

(1) [1]Den 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. [2]Stattdessen 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. [3]Soweit 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) [1]Die Staatsregierung wird ermächtigt, die Eigenschaften der Schnittstelle gemäß Absatz 1 Satz 2 durch Rechtsverordnung näher zu bestimmen. [2]In 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.

[3]Vom IT-Kooperationsrat und den Trägern der Selbstverwaltung sind frühzeitig Stellungnahmen einzuholen. [4]Beschließt 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. [5]Gleiches 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 Behörden bei den von ihnen eingesetzten und mit dem Verbindungsnetz zumindest mittelbar verbundenen informationstechnischen Systemen einzuhalten.

§ 12
Abwehr von Gefahren für die informationstechnischen Systeme im Freistaat Sachsen

(1) Zur 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.

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

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

§ 13
Datenspeicherung und -auswertung

(1) [1]Sofern 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 erfolgtem Abgleich sofort und nach dem Stand der Technik sicher gelöscht werden. [2]Daten, die weder personenbezogen sind noch dem Fernmeldegeheimnis unterliegen, sind von den Verarbeitungseinschränkungen dieser Vorschrift ausgenommen.

(2) [1]Protokolldaten 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.

[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]Eine nicht automatisierte Auswertung oder eine personenbezogene

Verarbeitung ist nur nach Maßgabe der Absätze 4 bis 8 zulässig. [6]Soweit hierzu die Wiederherstellung des Personenbezugs pseudonymisierter Daten erforderlich ist, muss diese durch den zuständigen Leiter der staatlichen oder nicht-staatlichen Stelle angeordnet werden. [7]Diese Entscheidung ist zu dokumentieren.

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

(4) [1]Die 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.

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

(5) [1]Die 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. [2]Die Benachrichtigung kann unterbleiben, wenn die Person nur unerheblich betroffen wurde und anzunehmen ist, dass sie an einer Benachrichtigung kein Interesse hat. [3]Die staatlichen und nicht-staatlichen Stellen legen Fälle, in denen sie von einer Benachrichtigung absehen, dem zuständigen Datenschutzbeauftragten der staatlichen oder nicht-staatlichen Stelle sowie einem weiteren Bediensteten dieser Stelle, der die Befähigung zum Richteramt hat, zur Kontrolle vor. [4]Der zuständige Datenschutzbeauftragte ist bei Ausübung dieser Aufgabe weisungsfrei und darf deswegen nicht benachteiligt werden (Artikel 38 Absatz 3 der Verordnung [EU] 2016/679 beziehungsweise § 11 Absatz 2 des Sächsischen Datenschutzgesetzes). [5]Wenn der zuständige Datenschutzbeauftragte der Entscheidung der staatlichen oder nicht-staatlichen Stelle widerspricht, ist die Benachrichtigung nachzuholen. [6]Die Entscheidung über die Nichtbenachrichtigung ist zu dokumentieren. [7]Die Dokumentation darf ausschließlich für Zwecke der Datenschutzkontrolle verwendet werden. [8]Sie ist nach zwölf Monaten zu löschen. [9]In 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 des Schulleiters ist für Anordnungen nach den Absätzen 3 und 4 ein vom Schulträger zu bestimmender Bediensteter des Schulträgers zuständig.

§ 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. [2]Von der Meldung darf abgesehen werden, wenn die Information bereits in öffentlich zugänglichen Medien verbreitet

wurde.

§ 16
Meldepflichten der staatlichen Stellen

(1) [1]Staatliche Stellen des Freistaates Sachsen haben Sicherheitsereignisse und Sicherheitsvorfälle ihrer informationstechnischen Systeme oder Prozesse an das Sicherheitsnotfallteam zu melden. [2]Die Meldungen haben unverzüglich zu erfolgen, wenn es sich um Sicherheitsvorfälle handelt, die

1. zu einer erheblichen Beeinträchtigung der Schutzziele geführt haben oder
2. behördenübergreifend zu einer erheblichen Beeinträchtigung der Schutzziele führen können.

[3]Zu Sicherheitsereignissen und sonstigen Sicherheitsvorfällen sind mit Inkrafttreten der Rechtsverordnung nach Absatz 2 regelmäßig zu melden:

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

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

§ 17
Meldepflichten der nicht-staatlichen Stellen

[1]Für nicht-staatliche Stellen gelten die Meldepflichten nach § 16 nur, soweit deren informationstechnischen Systeme mit dem Sächsischen Verwaltungsnetz oder dem Kommunalen Datennetz verbunden sind. [2]Soweit 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. [3]Im Übrigen steht es den nicht-staatlichen Stellen frei, Sicherheitsvorfälle und Sicherheitsereignisse entsprechend § 16 an das Sicherheitsnotfallteam zu melden.

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

[1]Die 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 dem Beauftragten für Informationstechnologie des Freistaates Sachsen und mit Zustimmung 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. [2]Satz 1 findet keine Anwendung für die Daten der Gerichte und Staatsanwaltschaften.

§ 20
Übergangsregelung

[1]Sicherheitskonzepte nach § 14 sind erstmals im Jahre 2024 einer Revision nach § 14 Satz 2 zu unterziehen. [2]Die §§ 7 bis 9 finden mit der Maßgabe Anwendung, dass die Umsetzung der Maßnahmen bis zum 31. Dezember 2020 nur im Rahmen der zur Verfügung stehenden Haushaltsmittel erfolgen muss.

§ 21
Evaluierung

(1) Die Staatsregierung legt dem Landtag fünf Jahre nach Verkündung dieses Gesetzes 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.