A. Amtliche Texte

Gesetze

171 **Gesetz Nr. 1965 zur Abwehr von Gefahren für die Daten in der Informations- und Kommunikationsinfrastruktur des Landes (Informationssicherheitsgesetz Saarland — IT-SiG SL) sowie zur Änderung weiterer Vorschriften**

Vom 15. Mai 2019

Der Landtag des Saarlandes hat folgendes Gesetz beschlossen, das hiermit verkündet wird:

Artikel 1
Gesetz zur Abwehr von Gefahren für die Daten in der Informations- und Kommunikationsinfrastruktur des Landes (Informationssicherheitsgesetz Saarland – IT-SiG SL)

Inhaltsübersicht

§ 1
Zweck und Geltungsbereich

Dieses Gesetz dient der Informationssicherheit des Landesdatennetzes, der informationstechnischen Systeme, der genutzten Anwendungen und der darüber verarbeiteten Informationen der Behörden des Saarlandes. Dieses Gesetz gilt für die Verwaltungstätigkeit der Behörden des Landes, der Gemeinden und Gemeindeverbände und der sonstigen der Aufsicht des Landes unterstehenden juristischen Personen des öffentlichen Rechts. Verwaltungstätigkeit im Sinne dieses Gesetzes umfasst die öffentlich-rechtliche Verwaltungstätigkeit und rechtsgeschäftliche oder tatsächliche Tätigkeiten im allgemeinen privatrechtlichen Rechtsverkehr einschließlich der fiskalischen Hilfsgeschäfte. Behörde im Sinne dieses Gesetzes ist jede Stelle, die Aufgaben der öffentlichen Verwaltung wahrnimmt. Die Vorschriften dieses Gesetzes gelten entsprechend für die Gerichte und Staatsanwaltschaften.

§ 2
Begriffsbestimmungen

Im Sinne dieses Gesetzes sind:

1. Informationssicherheit:

   die Gewährleistung der Vertraulichkeit, Verfügbarkeit, Integrität und Authentizität von Informationen durch Sicherheitsvorkehrungen in oder bei der Anwendung von informationstechnischen Systemen, Komponenten oder Prozessen,

2. Schadprogramme:

   Programme und sonstige informationstechnische Routinen und Verfahren, die dem Zweck dienen, unbefugt Daten auszuspähen, zu manipulieren, zu nutzen oder zu löschen oder die dem Zweck dienen, unbefugt auf sonstige informationstechnische Abläufe einzuwirken,

3. das Landesdatennetz:

   eine Kommunikationsinfrastruktur, die eine gesicherte Verbindung zwischen den lokalen Netzen der damit verbundenen Behörden sowie zu Netzen anderer Verwaltungen ermöglicht und durch das Land oder im Auftrag des Landes betrieben wird,

4. informationstechnische Systeme mit dem Landesdatennetz verbunden:

   wenn sie direkt, über ein behördeneigenes Subnetz oder über einen IT-Dienstleister technisch angeschlossen sind,

5. Angriffe:

   Versuche, die Informationssicherheit eines Computersystems unbefugt zu beeinflussen,

6. Sicherheitslücken:

   Eigenschaften von Programmen oder sonstigen informationstechnischen Systemen, durch deren Ausnutzung es möglich ist, dass sich Unbefugte Zugang zu informationstechnischen Systemen verschaffen oder die Funktion der informationstechnischen Systeme beeinflussen können,

7. Protokolldaten:

   Steuerungsdaten und Ereignisprotokolle einer informationstechnischen Datenverarbeitung oder eines informationstechnischen Protokolls zur Datenübertragung, die unabhängig vom Inhalt einer Datenverarbeitung gespeichert oder unabhängig

vom Inhalt eines Kommunikationsvorgangs übertragen oder auf den am Kommunikationsvorgang beteiligten Servern gespeichert werden und zur Gewährleistung der Kommunikation zwischen Empfänger und Sender notwendig sind. Protokolldaten können Verkehrsdaten gemäß § 3 Nummer 30 des Telekommunikationsgesetzes und Nutzungsdaten nach § 15 Absatz 1 des Telemediengesetzes enthalten,

8. Inhaltsdaten:

   Informationen, die den Inhalt einer Datenverarbeitung oder eines Telekommunikationsvorgangs betreffen und die keine Protokolldaten sind,

9. Informationstechnik:

   alle technischen Mittel zur Verarbeitung oder Übertragung von Informationen,

10. Informationstechnik des Landes:

    Informationstechnik, die von einer oder mehreren Landesbehörden oder im Auftrag einer oder mehrerer Landesbehörden betrieben wird.

§ 3
Behördenübergreifende Pflichten

(1) Die Sicherheit der informationstechnischen Systeme der Behörden ist nach dem Stand der Technik im Rahmen der Verhältnismäßigkeit und unter Beachtung der Vorschriften 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. Mai 2016, S. 1; L 314 vom 22. November 2016, S. 72) sowie des Saarländischen Datenschutzgesetzes vom 16. Mai 2018 (Amtsbl. I S. 254) sicherzustellen. Die Behörden treffen zu diesem Zweck angemessene technische und organisatorische Maßnahmen und erstellen die hierzu erforderlichen Informationssicherheitskonzepte.

(2) Werden Behörden Informationen bekannt, die zur Abwehr von Gefahren für die Informationssicherheit von Bedeutung sind, unterrichten diese den zentralen IT-Dienstleister des Landes unverzüglich hierüber, soweit andere Vorschriften oder Vereinbarungen mit Dritten nicht entgegenstehen, Meldepflichten aufgrund gesetzlicher Vorschriften bestehen oder sie einem Meldesystem innerhalb eines anderen deutschen CERT-Verbundes angeschlossen sind.

§ 4
Abwehr von Gefahren für die Informationssicherheit

(1) Der zentrale IT-Dienstleister kann nach Maßgabe dieser und der nachfolgenden Regelungen die zur Erfüllung seiner Aufgaben als Betreiber des Landesdatennetzes und Auftragsverarbeiter nach dem Gesetz zur Errichtung eines Landesamtes für IT-Dienstleistungen vom 2. Dezember 2015 (Amtsbl. I S. 967), geändert durch Gesetz vom 24. Oktober 2017 (Amtsbl. I S. 1005), in der jeweils geltenden Fassung, notwendigen und angemessenen Maßnahmen ergreifen, um Gefahren für die Informationssicherheit des Landesdatennetzes, aller daran angeschlossenen und mit ihm und miteinander verbundenen informationstechnischen Systeme (IT-Systeme), der genutzten Anwendungen und der darüber verarbeiteten Informationen zu erkennen, einzugrenzen und abzuwehren. Dies umfasst die Ermächtigung zur Verarbeitung personenbezogener Daten, soweit die Verarbeitung zur Erfüllung der nach diesem Gesetz übertragenen Befugnisse erforderlich ist.

(2) Der zentrale IT-Dienstleister kann zum in Absatz 1 genannten Zweck, soweit dies erforderlich ist, die beim Betrieb von Informationstechnik des Landes sowie die an den Schnittstellen des Landesdatennetzes und anderen Netzen und innerhalb des Landesdatennetzes anfallenden Protokolldaten und Inhaltsdaten erheben und automatisiert auswerten.

(3) Zur Ermöglichung einer automatisierten Auswertung nach Absatz 2 können die an das Landesdatennetz angeschlossenen Stellen dem zentralen IT-Dienstleister die bei ihnen gespeicherten Protokolldaten auf Anfrage zur Verfügung stellen.

(4) Sofern nicht die nachfolgenden Vorschriften eine weitere Verwendung gestatten, muss eine automatisierte Auswertung der Daten unverzüglich erfolgen und müssen die Daten nach erfolgtem Abgleich sofort und spurlos gelöscht werden. Die Speicherung und sonstige Verarbeitung nach dem ursprünglichen Verwendungszweck bleiben hiervon unberührt. Daten, die weder dem Fernmeldegeheimnis unterliegen noch Personenbezug aufweisen, sind von den Verwendungsbeschränkungen dieser Vorschrift ausgenommen.

(5) Personenbezogene Daten, die zum Zweck der Gewährleistung der Informationssicherheit nach diesem Gesetz ausgewertet werden dürfen, dürfen nicht für andere Zwecke, insbesondere nicht zur Verhaltens- und Leistungskontrolle, verarbeitet werden.

§ 5
Auswertung von Protokolldaten

(1) Bestehen tatsächliche Anhaltspunkte für das Vorliegen einer Gefahr für die Informationssicherheit, dürfen Protokolldaten über den für die automatisierte Auswertung erforderlichen Zeitraum hinaus gespeichert und automatisiert ausgewertet werden, soweit und solange dies zur weiteren Eingrenzung und Abwehr dieser Gefahr erforderlich ist. Entsprechendes gilt, wenn diese Daten zur Verfolgung damit zusammenhängender Straftaten erforderlich sein können.

(2) Durch organisatorische und technische Maßnahmen nach dem Stand der Technik ist sicherzustellen, dass eine Auswertung der nach Absatz 1 gespeicherten Daten nur automatisiert erfolgt. Die Daten sind zu pseudonymisieren, soweit dies automatisiert möglich ist.

(3) Sofern im Rahmen der automatisierten Auswertung ein Verdachtsfall auf eine Gefährdung der Informationssicherheit entdeckt wird und für die weitere Analyse die Wiederherstellung des Personenbezugs pseudonymisierter Daten erforderlich ist, muss diese durch die Leitung des zentralen IT-Dienstleisters angeordnet werden. Die Entscheidung ist zu dokumentieren. Eine nicht automatisierte Auswertung oder eine personenbezogene Verwendung ist nur nach Maßgabe der nachfolgenden Vorschriften zulässig.

§ 6
Auswertung von Inhaltsdaten

(1) Für die Datenverarbeitung von Inhaltsdaten gilt § 5 mit der Maßgabe, dass eine Speicherung für höchstens zwei Monate zulässig ist, die Speicherung und Auswertung von der Leitung des zentralen IT-Dienstleisters und von einer oder einem Bediensteten des für die Fachaufsicht über den zentralen IT-Dienstleister zuständigen Ministeriums mit der Befähigung zum Richteramt angeordnet sind und dies zum Schutz der technischen Systeme unerlässlich ist. Die Entscheidung ist zu dokumentieren.

(2) Die Anordnung gilt längstens für zwei Monate und kann höchstens um einen weiteren Monat verlängert werden.

§ 7
Weitergehende Auswertungen

(1) Eine über die in den §§ 5 und 6 hinausgehende Verarbeitung der Protokoll- und Inhaltsdaten ist nur zulässig,

1. wenn bestimmte Tatsachen den hinreichenden Verdacht begründen, dass die Daten Hinweise auf Gefahren für die Informationssicherheit, etwa durch Schadprogramme oder Sicherheitslücken, Angriffe oder unbefugten Datenzugriff enthalten und soweit die Datenverarbeitung erforderlich ist, um den Verdacht zu bestätigen oder zu widerlegen

   oder

2. wenn sich der Verdacht nach Nummer 1 bestätigt und dies zur Abwehr von Gefahren für die Informationssicherheit erforderlich ist.

   Werden Daten, welche die richterliche Unabhängigkeit berühren, nach dieser Vorschrift verarbeitet, ist der jeweils zuständigen obersten Dienstbehörde unverzüglich zu berichten. Berührt die Datenverarbeitung die Aufgabenwahrnehmung anderer unabhängiger Stellen oder ein Berufs- oder besonderes Amtsgeheimnis, ist die betroffene Stelle unverzüglich zu unterrichten. Die jeweiligen Stellen nach Satz 2 und 3 können vom zentralen IT-Dienstleister Auskunft über die Verarbeitung von Daten nach dieser Vorschrift verlangen.

(2) Soweit möglich, ist bei der Datenverarbeitung technisch und organisatorisch sicherzustellen, dass Daten, die den Kernbereich privater Lebensgestaltung betreffen, nicht erhoben werden. Werden Erkenntnisse aus dem Kernbereich privater Lebensgestaltung erlangt, dürfen diese nicht verwendet werden und sind unverzüglich zu löschen. Die Tatsache ihrer Erlangung und Löschung ist zu dokumentieren. Dies gilt auch in Zweifelsfällen.

§ 8
Sicherheitskonzept

(1) Von den Ermächtigungen nach den §§ 4 bis 7 darf nur Gebrauch gemacht werden, wenn hierfür durch den zentralen IT-Dienstleister ein Sicherheitskonzept erstellt wurde und die Umsetzung aller darin vorgesehenen technischen und organisatorischen Maßnahmen in einem Steuerungssystem dokumentiert, überwacht und fortgeschrieben wird. Das Sicherheitskonzept ist vor jeder Veränderung der eingesetzten technischen Systeme zu aktualisieren. Für jede Veränderung des Sicherheitskonzeptes gilt Satz 1 entsprechend.

(2) Das Sicherheitskonzept nach Absatz 1 bedarf in Bezug auf den Umgang mit der Verarbeitung personenbezogener Daten im Sinne des § 4 sowie von Protokoll- und Inhaltsdaten im Sinne der §§ 5 bis 7, soweit es sich um Daten der Landesmedienanstalt Saarland (LMS) oder privater Rundfunkveranstalter und Telemedienanbieter bei der LMS handelt, der Zustimmung der Landesmedienanstalt Saarland.

§ 9
Benachrichtigung der Betroffenen

(1) Die von Maßnahmen nach § 7 Betroffenen und betroffenen Behörden sind spätestens nach dem Erkennen und der Abwehr eines Schadprogramms oder von sonstigen Gefahren zu benachrichtigen, wenn sie bekannt sind oder ihre Identifikation ohne unverhältnismäßigen Aufwand möglich ist. Die Benachrichtigung kann unterbleiben, solange hierdurch der Ermittlungszweck eines Straf- oder Disziplinarverfahrens oder die Informationssicherheit gefährdet würde.

(2) Sofern die Benachrichtigung nach Absatz 1 Sätzen 2 und 3 unterbleiben soll, ist dies durch eine Bedienstete oder einen Bediensteten des für die Fachaufsicht über den zentralen IT-Dienstleister zuständigen Ministeriums mit der Befähigung zum Richteramt anzuordnen und zu dokumentieren.

§ 10
Übermittlung personenbezogener Daten

(1) Der zentrale IT-Dienstleister soll personenbezogene Daten nach den §§ 6 und 7 unverzüglich übermitteln

1. an die Polizeibehörden des Bundes und der Länder zur Abwehr einer Gefahr für die öffentliche Sicherheit, die unmittelbar von einem Schadprogramm ausgeht,

2. an die Polizeibehörden des Bundes und der Länder zur Abwehr einer Gefahr für den Bestand oder die Sicherheit des Staates oder Leib, Leben oder Freiheit einer Person oder Sachen von bedeutendem Wert, deren Erhalt im öffentlichen Interesse geboten ist,

3. an die Strafverfolgungsbehörden zur Verfolgung einer Straftat von auch im Einzelfall erheblicher Bedeutung, insbesondere einer in § 100a Absatz 2 der Strafprozessordnung bezeichneten Straftat,

4. an die Verfassungsschutzbehörde zur Unterrichtung über Tatsachen, die sicherheitsgefährdende oder geheimdienstliche Tätigkeiten für eine fremde Macht erkennen lassen.

(2) Die Übermittlung nach Absatz 1 Nummern 2 und 3 bedarf der vorherigen gerichtlichen Zustimmung. Für das Verfahren nach Absatz 1 Nummern 2 und 3 gelten die Vorschriften des Gesetzes über das Verfahren in Familiensachen und in den Angelegenheiten der freiwilligen Gerichtsbarkeit entsprechend. Die Übermittlung nach Absatz 1 Nummer 4 bedarf der vorherigen Zustimmung eines Bediensteten oder einer Bediensteten des für die Fachaufsicht über den zentralen IT-Dienstleister zuständigen Ministeriums mit der Befähigung zum Richteramt. Die Entscheidung ist zu dokumentieren.

§ 11
Befugnisse bei lokalen Netzen

Die §§ 4 bis 10 gelten für jede Behörde entsprechend bezüglich ihrer lokalen Netze. Der nach § 5 Absatz 3 erforderliche Leitungsvorbehalt sowie die in § 6 Absatz 1, § 9 Absatz 2 und § 10 Absatz 2 Satz 3 erforderlichen Zustimmungserfordernisse werden insoweit durch die jeweilige Behördenleitung bzw. ihre Vertretung wahrgenommen.

§ 12
Datenschutzrechtliche Kontrolle

(1) Der oder dem Landesbeauftragten für Datenschutz ist vom zentralen IT-Dienstleister einmal im Jahr eine Aufstellung über die nach § 5 Absatz 3, § 6, § 7 und § 10 erfolgten Verarbeitungen vorzulegen.

(2) Die nach diesem Gesetz anzufertigenden Dokumentationen dürfen ausschließlich für Zwecke der Datenschutzkontrolle verwendet werden. Sie sind zu löschen, wenn sie für diese Zwecke nicht mehr erforderlich sind, spätestens jedoch am Ende des Kalenderjahres, das dem Jahr der Dokumentation folgt.

§ 13
Einschränkung von Grundrechten

Das Fernmeldegeheimnis nach Artikel 10 des Grundgesetzes und Artikel 17 der Verfassung des Saarlandes wird durch die §§ 4 bis 7, § 10 und § 11 eingeschränkt.

Artikel 2
Änderung des E-Government-Gesetzes Saarland

Das Gesetz zur Förderung der elektronischen Verwaltung im Saarland vom 15. November 2017 (Amtsbl. I S. 1007), zuletzt geändert durch Gesetz vom 16. Mai 2018 (Amtsbl. I S. 254), wird wie folgt geändert:

1. Die Inhaltsübersicht wird wie folgt geändert:

   a) Nach der Angabe zu § 10 wird folgende Angabe eingefügt:

   „§ 10a Elektronischer Rechnungsempfang; Verordnungsermächtigung".

   b) Nach der Angabe zu § 20 wird folgende Angabe angefügt:

   „§ 21 Experimentierklausel".

2. Nach § 10 wird folgender § 10a eingefügt:

„§ 10a
Elektronischer Rechnungsempfang, Verordnungsermächtigung

(1) Elektronische Rechnungen, die nach Erfüllung von öffentlichen Aufträgen und Aufträgen sowie zu Konzessionen von Stellen im Sinne von § 98 des Gesetzes gegen Wettbewerbsbeschränkungen in der Fassung vom 26. Juni 2013 (BGBl. I S. 1750, 3245), zuletzt geändert durch Artikel 10 des Gesetzes vom 12. Juli 2018 (BGBl. I S. 1151), in der jeweils geltenden Fassung, mit Sitz im Saarland ausgestellt wurden, sind nach Maßgabe einer Rechtsverordnung nach Absatz 3 zu empfangen und zu verarbeiten. Diese Verpflichtung gilt unabhängig von dem Geltungsbereich gemäß § 1 und unabhängig davon, ob der Wert des vergebenen öffentlichen Auftrags, des vergebenen Auftrags oder der Vertragswert der vergebenen Konzession den gemäß § 106 des Gesetzes gegen Wettbewerbsbeschränkungen jeweils maßgeblichen Schwellenwert erreicht oder überschreitet. Vertragliche Regelungen, die die elektronische Rechnungsstellung vorschreiben, bleiben unberührt.

(2) Eine Rechnung ist elektronisch, wenn

1. sie in einem strukturierten elektronischen Format ausgestellt, übermittelt und empfangen wird

   und

2. das Format die automatische und elektronische Verarbeitung der Rechnung ermöglicht.

(3) Die Landesregierung wird ermächtigt, durch Rechtsverordnung besondere Vorschriften zur Ausgestaltung des elektronischen Rechnungsverkehrs zu erlassen. Diese Vorschriften können sich beziehen auf

1. die Art und Weise der Verarbeitung der elektronischen Rechnung, insbesondere auf die elektronische Verarbeitung,
2. die Anforderungen an die elektronische Rechnungsstellung und zwar insbesondere auf die von den elektronischen Rechnungen zu erfüllenden Voraussetzungen, den Schutz personenbezogener Daten, das zu verwendende Rechnungsdatenmodell sowie auf die Verbindlichkeit der elektronischen Form,
3. die Befugnis von öffentlichen Auftraggebern, Sektorenauftraggebern und Konzessionsgebern, in Ausschreibungsbedingungen die Erteilung elektronischer Rechnungen vorzusehen sowie
4. Ausnahmen für sicherheitsspezifische Aufträge."

3. Nach § 20 wird folgender § 21 angefügt:

„§ 21
Experimentierklausel

Die Landesregierung wird ermächtigt, zur Einführung und Fortentwicklung elektronischer Verwaltungsstrukturen durch Rechtsverordnung sachlich und räumlich begrenzte Abweichungen von folgenden Vorschriften vorzusehen:

1. Zuständigkeits- und Formvorschriften nach den §§ 3, 3a, 27a, 33, 34, 37 Absatz 2 bis 5, 41, 57, 64, 69 Absatz 2 des Saarländischen Verwaltungsverfahrensgesetzes vom 15. Dezember 1976 (Amtsbl. S. 1151), zuletzt geändert durch Gesetz vom 25. Juni 2014 (Amtsbl. I S. 306),
2. § 1 Absatz 2 des Saarländischen Verwaltungszustellungsgesetzes vom 13. Dezember 2005 (Amtsbl. 2006, S. 214) in Verbindung mit § 5 Absatz 4 bis 7, § 5a und § 10 Absatz 2 des Verwaltungszustellungsgesetzes vom 12. August 2005 (BGBl. I S. 2354), zuletzt geändert durch Artikel 11 Absatz 3 des Gesetzes vom 18. Juli 2017 (BGBl. I S. 2745), und
3. sonstigen landesgesetzlichen Zuständigkeits- und Formvorschriften, soweit dies zur Erprobung neuer elektronischer Formen des Schriftformersatzes, der Übermittlung und Bekanntgabe von Dokumenten und Erklärungen, der Vorlage von Nachweisen, der Erhebung, Verarbeitung, Nutzung oder Weitergabe von Daten oder für die Erprobung der Dienste von zentralen Portalen erforderlich ist.

Die Rechtsverordnung ist auf höchstens drei Jahre zu befristen."

Artikel 3
Änderung des Saarländischen Besoldungsgesetzes

In der Besoldungsordnung B in der Anlage des Saarländischen Besoldungsgesetzes in der Fassung der Bekanntmachung vom 10. Januar 1989 (Amtsbl. S. 301), zuletzt geändert durch Gesetz vom 13. Juni 2018 (Amtsbl. I S. 358), wird in der Besoldungsgruppe B 5 vor der Amtsbezeichnung „Direktor der Landesmedienanstalt Saarland" die Amtsbezeichnung „Direktor des Landesamtes für Zentrale Dienste" mit dem Funktionszusatz „– als Leiter des Landesamtes für Zentrale Dienste und Landesbeauftragter für Informationssicherheit" eingefügt.

Artikel 4
Inkrafttreten

(1) Dieses Gesetz tritt vorbehaltlich des Absatzes 2 am Tag nach seiner Verkündung in Kraft.

(2) Artikel 2 Nummer 2 § 10a Absätze 1 und 2 treten am 18. April 2020 in Kraft.

Saarbrücken, den 28. August 2019

Die Regierung des Saarlandes:

Der Ministerpräsident

Hans

Die Ministerin für Wirtschaft, Arbeit, Energie und Verkehr

Rehlinger

Der Minister für Finanzen und Europa

Der Minister der Justiz

Strobel

Der Minister für Inneres, Bauen und Sport

Bouillon

Die Ministerin für Soziales, Gesundheit, Frauen und Familie

Bachmann

Der Minister für Bildung und Kultur

Commerçon

Der Minister für Umwelt und Verbraucherschutz

Jost