§ 6 SächsISichG (Sachsen) — Sicherheitsnotfallteam

Sächsisches Informationssicherheitsgesetz
Landesrecht Sachsen
Stand: 26.08.2026 (konsolidierte Textfassung, kein amtliches Inkrafttretensdatum)

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

Das 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) Das 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. Erlangt 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. Liegen dessen Voraussetzungen nicht vor, sind diese Informationen unverzüglich zu löschen. Das Sicherheitsnotfallteam unterrichtet die für das informationstechnische System Verantwortlichen unverzüglich über die durch Maßnahmen gemäß Satz 1 erkannten Sicherheitslücken. Es soll dabei auf bestehende Abhilfemöglichkeiten hinweisen.

(2) 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. 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. Daten 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. 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. Für Hochschulen im Sinne von § 1 Absatz 1 Satz 1 des Sächsischen Hochschulgesetzes vom 31. Mai 2023 (SächsGVBl. S. 329) gilt Satz 2 nicht.

(3) 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 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. Das umfasst insbesondere die dazu erforderliche Datenverarbeitung.

(4) 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. Die 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.

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

(5) Das Sicherheitsnotfallteam sieht angemessene und spezifische Maßnahmen zur Wahrung der Interessen der betroffenen Person vor. § 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.