

§ 13 SächsISichG (Sachsen) — Datenspeicherung und -auswertung

Sächsisches Informationssicherheitsgesetz

Landesrecht Sachsen

Stand: 26.08.2026 (konsolidierte Textfassung, kein amtliches Inkrafttretensdatum)

(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 erfolgreichem Abgleich sofort und nach dem Stand der Technik sicher gelöscht werden. Daten, die weder personenbezogen sind noch dem Fernmeldegeheimnis unterliegen, sind von den Verarbeitungseinschränkungen dieser Vorschrift ausgenommen.

(2) 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.

Die Daten sind im Gebiet der Europäischen Union zu speichern. Durch organisatorische und technische Maßnahmen nach dem Stand der Technik ist sicherzustellen, dass eine Auswertung der nach Satz 1 gespeicherten Daten nur automatisiert erfolgt. Die Daten sind zu pseudonymisieren, soweit dies automatisiert möglich ist. Eine nicht automatisierte Auswertung oder eine personenbezogene Verarbeitung ist nur nach Maßgabe der Absätze 4 bis 8 zulässig. Soweit 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. Diese Entscheidung ist zu dokumentieren.

(3) 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. Die 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. Die Daten sind im Gebiet der Europäischen Union zu speichern. Durch organisatorische und technische Maßnahmen nach dem Stand der Technik ist sicherzustellen, dass eine Auswertung der nach Satz 1 gespeicherten Daten nur automatisiert erfolgt. Die Daten sind zu pseudonymisieren, soweit dies automatisiert möglich ist. Eine nicht automatisierte Auswertung oder eine personenbezogene Verarbeitung ist nur nach Maßgabe der Absätze 4 bis 8 zulässig. Soweit 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. Sofern 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. Die Anordnung gilt längstens für zwei Monate; sie kann verlängert werden. Diese Entscheidung ist zu dokumentieren.

(4) 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.

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. Ein Schadprogramm darf beseitigt oder in seiner Funktionsweise gehindert werden. Die 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 inner oder einem Bediensteten dieser Stelle mit der Befähigung zum Richteramt angeordnet werden. Sofern 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) 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. Die Benachrichtigung kann unterbleiben, wenn die Person nur unerheblich betroffen wurde und anzunehmen ist, dass sie an einer Benachrichtigung kein Interesse hat. Die 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. Die 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). Wenn die oder der zuständige Datenschutzbeauftragte der Entscheidung der staatlichen oder nicht-staatlichen Stelle widerspricht, ist die Benachrichtigung nachzuholen. Die Entscheidung über die Nichtbenachrichtigung ist zu dokumentieren. Die Dokumentation darf ausschließlich für Zwecke der Datenschutzkontrolle verwendet werden. Sie ist nach zwölf Monaten zu löschen. In den Fällen der Absätze 6 und 7 erfolgt die Benachrichtigung durch die dort genannten Behörden nach den für diese Behörden geltenden Vorschriften. 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) 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. 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) 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 Tätigkeiten nach § 2 Absatz 1 Nummer 2 des Sächsischen Verfassungsschutzgesetzes vom 22. Juli 2024 (SächsGVBl. S. 706) oder für Bestrebungen vorliegen, die durch Anwendung von Gewalt oder darauf gerichtete

Vorbereitungshandlungen gegen die in § 2 Absatz 1 Nummer 1, 3 und 4 des Sächsischen Verfassungsschutzgesetzes genannten Schutzgüter gerichtet sind; § 21 des Sächsischen Verfassungsschutzgesetzes bleibt unberührt.

Die Übermittlung nach Satz 1 Nummer 1 und 2 bedarf der vorherigen gerichtlichen Zustimmung. 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. Zuständig ist das Amtsgericht, in dessen Bezirk die übermittelnde Stelle ihren Sitz hat. 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) Eine über die Absätze 1 bis 7 hinausgehende inhaltliche Auswertung zu anderen Zwecken und die Weitergabe von personenbezogenen Daten an Dritte sind unzulässig. Soweit möglich, ist bei der Datenverarbeitung technisch sicherzustellen, dass Daten, die den Kernbereich privater Lebensgestaltung betreffen, nicht erhoben werden. Werden Erkenntnisse aus dem Kernbereich privater Lebensgestaltung erlangt, dürfen diese Daten nicht verwendet werden und sind unverzüglich zu löschen. Dies gilt auch in Zweifelsfällen. 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.

Zitiervorschlag: § 13 SächsISichG (Sachsen)

Quelle: revosax, abgerufen 26.08.2026

Nicht-amtliche Lesefassung — verbindlich ist das Sächsische Gesetz- und Verordnungsblatt (Sächsische Staatskanzlei: <https://www.sk.sachsen.de>)

Provided by nu:legal (<https://recht.nulegal.eu>), the leading open legal database: AI-first, expanding daily, German and European law and case law in full text, free, with an open API for AI agents. Text and data mining expressly permitted.

Herausgeber: Nulegal GmbH, Potsdam.

Dieses Dokument: <https://recht.nulegal.eu/gesetze/S%C3%A4chsISichG/13>