

§ 8 BSIG 2025 — Abwehr von Schadprogrammen und Gefahren für die Kommunikationstechnik des Bundes

BSI-Gesetz

Stand: 07.12.2025 (konsolidierte Textfassung, kein amtliches Inkrafttretensdatum)

(1) Das Bundesamt darf zur Abwehr von Gefahren für die Kommunikationstechnik des Bundes

1. Protokolldaten, die beim Betrieb von Kommunikationstechnik des Bundes anfallen, erheben und automatisiert auswerten, soweit dies zum Erkennen, Eingrenzen oder Beseitigen von Störungen oder Fehlern bei der Kommunikationstechnik des Bundes oder von Angriffen auf die Informationstechnik des Bundes erforderlich ist,
2. die an den Schnittstellen der Kommunikationstechnik des Bundes anfallenden Daten automatisiert auswerten, soweit dies für die Erkennung und Abwehr von Schadprogrammen und sonstigen erheblichen Gefahren für die Kommunikationstechnik des Bundes erforderlich ist.

Sofern nicht die nachfolgenden Absätze eine weitere Verwendung gestatten, müssen die automatisierte Auswertung dieser Daten und deren anschließende vollständige und nicht wiederherstellbare Löschung unverzüglich erfolgen. Die Verwendungsbeschränkungen gelten nicht für Protokolldaten, sofern diese weder personenbezogene noch dem Fernmeldegeheimnis unterliegende Daten beinhalten. Die Einrichtungen der Bundesverwaltung sind verpflichtet, das Bundesamt bei Maßnahmen nach Satz 1 zu unterstützen und hierbei den Zugang des Bundesamtes zu einrichtungsinternen Protokolldaten nach Satz 1 Nummer 1 sowie zu Schnittstellendaten nach Satz 1 Nummer 2 sicherzustellen. Protokolldaten der Bundesgerichte dürfen nur in deren Einvernehmen erhoben werden.

(2) Protokolldaten nach Absatz 1 Satz 1 Nummer 1 dürfen über den für die automatisierte Auswertung nach Absatz 1 Satz 1 Nummer 1 erforderlichen Zeitraum hinaus, längstens jedoch für 18 Monate, gespeichert werden, soweit tatsächliche Anhaltspunkte dafür bestehen, dass diese im Falle der Bestätigung eines Verdachts nach Absatz 4 Satz 2 zur Abwehr von Gefahren, die von dem gefundenen Schadprogramm ausgehen, oder zur Erkennung und Abwehr anderer Schadprogramme oder sonstiger erheblicher Gefahren für die Kommunikationstechnik des Bundes erforderlich sein können. Durch organisatorische und technische Maßnahmen ist sicherzustellen, dass eine Auswertung der nach diesem Absatz gespeicherten Daten nur automatisiert erfolgt und dass ein Zugriff auf Daten, die länger als drei Monate gespeichert sind, nur bei Vorliegen tatsächlicher Erkenntnisse über die Betroffenheit des Bundes mit einem Schadprogramm oder einer sonstigen erheblichen Gefahr für die Kommunikationstechnik des Bundes erfolgt. Die Daten sind zu pseudonymisieren, soweit dies automatisiert möglich ist. Eine nicht automatisierte Verarbeitung ist nur nach Maßgabe der nachfolgenden Absätze zulässig. Soweit hierzu die Wiederherstellung pseudonymisierter Protokolldaten erforderlich ist, muss diese durch die Präsidentin oder den Präsidenten des Bundesamtes oder die Vertretung im Amt angeordnet werden. Die Entscheidung ist zu dokumentieren.

(3) Protokolldaten dürfen vor ihrer Pseudonymisierung und Speicherung nach Absatz 2 zur Sicherstellung einer fehlerfreien automatisierten Auswertung manuell verarbeitet werden. Liegen Hinweise vor, dass die fehlerfreie automatisierte Auswertung wegen eines erheblichen Fehlers erschwert wird, darf der Personenbezug von Protokolldaten zur Sicherstellung der fehlerfreien automatisierten Auswertung wiederhergestellt werden, sofern dies im Einzelfall erforderlich ist. Absatz 2 Satz 3 bis 6 gilt entsprechend.

(4) Eine über die Absätze 1 und 2 hinausgehende Verwendung personenbezogener Daten ist nur zulässig, wenn bestimmte Tatsachen den Verdacht begründen, dass

1. diese Daten ein Schadprogramm enthalten,
2. diese Daten durch ein Schadprogramm übermittelt wurden,

3. diese Daten im Zusammenhang mit einer sonstigen erheblichen Gefahr für die Kommunikationstechnik des Bundes stehen oder
4. sich aus diesen Daten Hinweise auf ein Schadprogramm oder eine sonstige erhebliche Gefahr für die Kommunikationstechnik des Bundes ergeben können,

und soweit die Datenverarbeitung erforderlich ist, um den Verdacht zu bestätigen oder zu widerlegen. Im Falle der Bestätigung des Verdachts ist die weitere Verarbeitung personenbezogener Daten zulässig, soweit dies erforderlich ist

1. zur Abwehr des Schadprogramms der sonstigen erheblichen Gefahren für die Kommunikationstechnik des Bundes,
2. zur Abwehr von Gefahren, die von dem aufgefundenen Schadprogramm ausgehen, oder
3. zur Erkennung und Abwehr anderer Schadprogramme oder Gefahren für die Kommunikationstechnik des Bundes.

Ein Schadprogramm kann beseitigt oder in seiner Funktionsweise gehindert werden. Es dürfen die erforderlichen technischen Maßnahmen getroffen werden, um eine sonstige erhebliche Gefahr für die Kommunikationstechnik des Bundes zu beseitigen. Das Bundesamt kann die Daten an die betroffene Einrichtung der Bundesverwaltung übermitteln, soweit dies für eine Verwendung nach den Sätzen 1 bis 4 erforderlich ist. Die nicht automatisierte Verwendung der Daten nach den Sätzen 1 und 2 darf nur durch einen Bediensteten des Bundesamtes mit der Befähigung zum Richteramt angeordnet werden. Die Anordnung nach Satz 4 muss die daraus erwachsenden Übermittlungsbefugnisse nach Absatz 6 berücksichtigen.

(5) Die Beteiligten des Kommunikationsvorgangs sind spätestens nach dem Erkennen und der Abwehr eines Schadprogramms oder seiner Wirkungen oder von sonstigen erheblichen Gefahren für die Kommunikationstechnik des Bundes, die von einem Schadprogramm ausgehen, zu benachrichtigen, wenn sie bekannt sind oder ihre Identifikation ohne unverhältnismäßige weitere Ermittlungen möglich ist und nicht überwiegende schutzwürdige Belange Dritter entgegenstehen. Die Unterrichtung kann unterbleiben, wenn die Person nur unerheblich betroffen wurde und wenn anzunehmen ist, dass sie an einer Benachrichtigung kein Interesse hat. Das Bundesamt legt Fälle, in denen es von einer Benachrichtigung absieht, dem behördlichen Datenschutzbeauftragten des Bundesamtes sowie einem weiteren Bediensteten des Bundesamtes, der die Befähigung zum Richteramt hat, zur Kontrolle vor. Wenn der behördliche Datenschutzbeauftragte der Entscheidung des Bundesamtes 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 in entsprechender Anwendung der für diese Behörden geltenden Vorschriften. Enthalten diese Vorschriften keine Bestimmungen zu Benachrichtigungspflichten, sind die Vorschriften der Strafprozessordnung entsprechend anzuwenden.

(6) Das Bundesamt kann die nach Absatz 4 verwendeten personenbezogenen Daten an die Strafverfolgungsbehörden zur Verfolgung einer mittels eines Schadprogramms oder im Rahmen einer sonstigen erheblichen Gefahr für die Kommunikationstechnik des Bundes begangenen Straftat nach den §§ 202a, 202b, 303a oder 303b des Strafgesetzbuches übermitteln. Es kann diese Daten ferner übermitteln

1. an die Polizeien des Bundes und der Länder zur Abwehr einer Gefahr für die öffentliche Sicherheit, die unmittelbar von einem Schadprogramm ausgeht,
2. an das Bundesamt für Verfassungsschutz zur Unterrichtung über Tatsachen, die sicherheitsgefährdende oder geheimdienstliche Tätigkeiten für eine fremde Macht erkennen lassen, sowie an den Militärischen Abschirmdienst, wenn sich diese Tätigkeiten gegen Personen, Dienststellen oder Einrichtungen im Geschäftsbereich des Bundesministeriums der Verteidigung

richten,

3. an den Bundesnachrichtendienst zur Unterrichtung über Tatsachen, die einen internationalen kriminellen, terroristischen oder staatlichen Angriff mittels Schadprogrammen oder vergleichbarer schädlich wirkender informationstechnischer Mittel auf die Vertraulichkeit, Integrität oder Verfügbarkeit von IT-Systemen in Fällen von erheblicher Bedeutung mit Bezug zur Bundesrepublik Deutschland erkennen lassen.

(7) Für sonstige Zwecke kann das Bundesamt die Daten nach Absatz 4 Satz 1 übermitteln

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

2. an die Polizeien 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 Verfassungsschutzbehörden des Bundes und der Länder sowie an den Militärischen Abschirmdienst, wenn tatsächliche Anhaltspunkte für Bestrebungen in der Bundesrepublik Deutschland vorliegen, die durch Anwendung von Gewalt oder darauf gerichtete Vorbereitungshandlungen gegen die in § 3 Absatz 1 des Bundesverfassungsschutzgesetzes oder § 1 Absatz 1 des MAD-Gesetzes genannten Schutzgüter gerichtet sind,

4. an den Bundesnachrichtendienst, wenn tatsächliche Anhaltspunkte für den Verdacht bestehen, dass jemand Straftaten nach § 3 Absatz 1 Nummer 8 des Artikel 10-Gesetzes plant, begeht oder begangen hat und dies von außen- und sicherheitspolitischer Bedeutung für die Bundesrepublik Deutschland ist.

Die Übermittlung nach Satz 2 Nummer 1 und 2 bedarf der vorherigen gerichtlichen Zustimmung. Für das Verfahren nach Satz 2 Nummer 1 und 2 gelten die Vorschriften des Gesetzes über das Verfahren in Familiensachen und in den Angelegenheiten der freiwilligen Gerichtsbarkeit entsprechend. Zuständig ist das Amtsgericht, in dessen Bezirk das Bundesamt seinen Sitz hat. Die Übermittlung nach Satz 2 Nummer 3 und 4 erfolgt nach Anordnung des Bundesministeriums des Innern. Die §§ 9 bis 16 des Artikel 10-Gesetzes gelten entsprechend.

(8) Eine über die vorstehenden Absätze hinausgehende inhaltliche Auswertung zu anderen Zwecken und die Weitergabe von personenbezogenen Daten an Dritte sind unzulässig. Soweit möglich, ist technisch sicherzustellen, dass Daten, die den Kernbereich privater Lebensgestaltung betreffen, nicht erhoben werden. Werden aufgrund der Maßnahmen der Absätze 1 bis 4 Erkenntnisse aus dem Kernbereich privater Lebensgestaltung oder Daten nach Artikel 9 Absatz 1 der Verordnung (EU) 2016/679 erlangt, dürfen diese Erkenntnisse und Daten nicht verwendet werden. Erkenntnisse aus dem Kernbereich privater Lebensgestaltung sind unverzüglich zu löschen. Dies gilt auch in Zweifelsfällen. Die Tatsache der Erlangung und Löschung dieser Erkenntnisse ist zu dokumentieren. Die Dokumentation darf ausschließlich für Zwecke der Datenschutzkontrolle verwendet werden. Sie ist zu löschen, wenn sie für diese Zwecke nicht mehr erforderlich ist, spätestens jedoch am Ende des Kalenderjahres, das dem Jahr folgt, in dem die Dokumentation erstellt worden ist. Werden im Rahmen der Absätze 5 oder 6 Inhalte oder Umstände der Kommunikation von in § 53 Absatz 1 Satz 1 der Strafprozessordnung genannten Personen übermittelt, auf die sich das Zeugnisverweigerungsrecht dieser Personen erstreckt, ist die Verwertung dieser Daten zu Beweis Zwecken in einem Strafverfahren nur insoweit zulässig, als Gegenstand dieses Strafverfahrens eine Straftat ist, die im Höchstmaß mit mindestens fünf Jahren Freiheitsstrafe bedroht ist.

(9) Vor Aufnahme der Datenerhebung und -verwendung hat das Bundesamt ein Datenerhebungs- und -verwendungskonzept zu erstellen und für Kontrollen durch die Bundesbeauftragte oder den Bundesbeauftragten für den Datenschutz und die Informationsfreiheit bereitzuhalten. Das Konzept hat dem besonderen Schutzbedürfnis der Regierungskommunikation Rechnung zu tragen. Die für die

automatisierte Auswertung verwendeten Kriterien sind zu dokumentieren. Die oder der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit teilt das Ergebnis seiner Kontrollen nach § 16 des Bundesdatenschutzgesetzes auch den Ressorts mit.

(10) Das Bundesamt unterrichtet die Bundesbeauftragte oder den Bundesbeauftragten für den Datenschutz und die Informationsfreiheit kalenderjährlich jeweils bis zum 30. Juni des dem Berichtsjahr folgenden Jahres über

1. die Anzahl der Vorgänge, in denen Daten nach Absatz 6 Satz 1, 2 Nummer 1 oder Absatz 7 Nummer 1 übermittelt wurden, aufgegliedert nach den einzelnen Übermittlungsbefugnissen,
2. die Anzahl der personenbezogenen Auswertungen nach Absatz 4 Satz 1, in denen der Verdacht widerlegt wurde,
3. die Anzahl der Fälle, in denen das Bundesamt nach Absatz 5 Satz 2 oder 3 von einer Benachrichtigung der Betroffenen abgesehen hat.

(11) Das Bundesamt unterrichtet kalenderjährlich jeweils bis zum 30. Juni des dem Berichtsjahr folgenden Jahres den Innenausschuss des Deutschen Bundestages über die Anwendung dieser Vorschrift.

Zitiervorschlag: § 8 BSIG 2025

Quelle: Bundesamt für Justiz, abgerufen 02.07.2026

Nicht-amtliche Lesefassung — verbindlich ist das Bundesgesetzblatt

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/BSIG%202025/8>