

§ 49 BKAG 2018 — Verdeckter Eingriff in informationstechnische Systeme

Bundeskriminalamtgesetz

Stand: 10.07.2026 (konsolidierte Textfassung, kein amtliches Inkrafttretensdatum)

(1) Das Bundeskriminalamt darf ohne Wissen der betroffenen Person mit technischen Mitteln in von der betroffenen Person genutzte informationstechnische Systeme eingreifen und aus ihnen Daten erheben, wenn bestimmte Tatsachen die Annahme rechtfertigen, dass eine Gefahr vorliegt für

1. Leib, Leben oder Freiheit einer Person oder
2. solche Güter der Allgemeinheit, deren Bedrohung die Grundlagen oder den Bestand des Bundes oder eines Landes oder die Grundlagen der Existenz der Menschen berührt.

Eine Maßnahme nach Satz 1 ist auch zulässig, wenn

1. bestimmte Tatsachen die Annahme rechtfertigen, dass innerhalb eines übersehbaren Zeitraums auf eine zumindest ihrer Art nach konkretisierte Weise eine Schädigung der in Satz 1 genannten Rechtsgüter eintritt oder
2. das individuelle Verhalten einer Person die konkrete Wahrscheinlichkeit begründet, dass sie innerhalb eines übersehbaren Zeitraums die in Satz 1 genannten Rechtsgüter schädigen wird.

Die Maßnahme darf nur durchgeführt werden, wenn sie für die Aufgabenerfüllung nach § 5 erforderlich ist und diese ansonsten aussichtslos oder wesentlich erschwert wäre.

(2) Es ist technisch sicherzustellen, dass

1. an dem informationstechnischen System nur Veränderungen vorgenommen werden, die für die Datenerhebung unerlässlich sind, und
2. die vorgenommenen Veränderungen bei Beendigung der Maßnahme soweit technisch möglich automatisiert rückgängig gemacht werden.

Das eingesetzte Mittel ist nach dem Stand der Technik gegen unbefugte Nutzung zu schützen. Kopierte Daten sind nach dem Stand der Technik gegen Veränderung, unbefugte Löschung und unbefugte Kenntnisnahme zu schützen.

(3) Die Maßnahme darf sich nur gegen eine Person richten, die entsprechend § 17 oder § 18 des Bundespolizeigesetzes verantwortlich ist. Die Maßnahme darf auch durchgeführt werden, wenn andere Personen unvermeidbar betroffen werden.

(4) Die Maßnahme darf nur auf Antrag der zuständigen Abteilungsleitung des Bundeskriminalamtes oder deren Vertretung durch das Gericht angeordnet werden.

(5) Im Antrag sind anzugeben:

1. die Person, gegen die sich die Maßnahme richtet, soweit möglich, mit Name und Anschrift,
2. eine möglichst genaue Bezeichnung des informationstechnischen Systems, in das zur Datenerhebung eingegriffen werden soll,
3. Art, Umfang und Dauer der Maßnahme,
4. der Sachverhalt sowie
5. eine Begründung.

(6) Die Anordnung ergeht schriftlich. In ihr sind anzugeben:

1. die Person, gegen die sich die Maßnahme richtet, soweit möglich, mit Name und Anschrift,
2. eine möglichst genaue Bezeichnung des informationstechnischen Systems, in das zur Datenerhebung eingegriffen werden soll,
3. Art, Umfang und Dauer der Maßnahme unter Benennung des Endzeitpunktes sowie
4. die wesentlichen Gründe.

Die Anordnung ist auf höchstens drei Monate zu befristen. Eine Verlängerung um jeweils nicht mehr als drei weitere Monate ist zulässig, soweit die Anordnungsvoraussetzungen unter Berücksichtigung der gewonnenen Erkenntnisse fortbestehen. Liegen die Voraussetzungen der Anordnung nicht mehr vor, sind die aufgrund der Anordnung ergriffenen Maßnahmen unverzüglich zu beenden.

(7) Liegen tatsächliche Anhaltspunkte für die Annahme vor, dass durch die Maßnahme allein Erkenntnisse aus dem Kernbereich privater Lebensgestaltung erlangt würden, ist die Maßnahme unzulässig. Soweit möglich, ist technisch sicherzustellen, dass Daten, die den Kernbereich privater Lebensgestaltung betreffen, nicht erhoben werden. Erkenntnisse, die durch Maßnahmen nach Absatz 1 erlangt worden sind, sind dem anordnenden Gericht unverzüglich vorzulegen. Das Gericht entscheidet unverzüglich über die Verwertbarkeit oder Löschung. Daten, die den Kernbereich privater Lebensgestaltung betreffen, dürfen nicht verwertet werden und sind unverzüglich zu löschen. Die Tatsachen der Erfassung der Daten und der Löschung sind zu dokumentieren. Die Dokumentation darf ausschließlich für Zwecke der Datenschutzkontrolle verwendet werden. Sie ist sechs Monate nach der Benachrichtigung nach § 74 oder sechs Monate nach Erteilung der gerichtlichen Zustimmung über das endgültige Absehen von der Benachrichtigung zu löschen. Ist die Datenschutzkontrolle nach § 69 Absatz 1 noch nicht beendet, ist die Dokumentation bis zu ihrem Abschluss aufzubewahren.

(8) Bei Gefahr im Verzug kann die zuständige Abteilungsleitung des Bundeskriminalamtes oder deren Vertretung im Benehmen mit der oder dem Datenschutzbeauftragten des Bundeskriminalamtes über die Verwertung der Erkenntnisse entscheiden. Bei der Sichtung der erhobenen Daten kann sie sich der technischen Unterstützung von zwei weiteren Bediensteten des Bundeskriminalamtes bedienen, von denen einer die Befähigung zum Richteramt haben muss. Die Bediensteten des Bundeskriminalamtes sind zur Verschwiegenheit über die ihnen bekannt werdenden Erkenntnisse, die nicht verwertet werden dürfen, verpflichtet. Die gerichtliche Entscheidung nach Absatz 7 ist unverzüglich nachzuholen.

Zitiervorschlag: § 49 BKAG 2018

Quelle: Bundesamt für Justiz, abgerufen 10.07.2026

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/BKAG%202018/49>