Landesbeauftragte
für Datenschutz
und Akteneinsicht

Meldung von Datenschutzverletzungen in Brandenburg

Hinweise zu den Anforderungen der Datenschutz-Grundverordnung
Stand: August 2025

Die Landesbeauftragte für den Datenschutz
und für das Recht auf Akteneinsicht
Stahnsdorfer Damm 77
14532 Kleinmachnow

Telefon: 033203 356-0
Telefax: 033203 356-49
E-Mail: Poststelle@LDA.Brandenburg.de

www.LDA.Brandenburg.de

Inhaltsverzeichnis

Alle Verantwortlichen und Auftragsverarbeiter, die personenbezogene Daten verarbeiten, müssen die gesetzlichen Regeln zur Sicherstellung des Datenschutzes einhalten. Falls es zu einer Verletzung des vorgeschriebenen Schutzes personenbezogener Daten gekommen ist, müssen die verarbeitenden Stellen den Vorfall intern dokumentieren und in vielen Fällen unverzüglich an die Aufsichtsbehörde melden.[1] Gegebenenfalls müssen sie auch diejenigen Personen, die von der Datenschutzverletzung betroffen sind, informieren.[2]

1 Zum Begriff „Datenschutzverletzung“

Eine Verletzung des Schutzes personenbezogener Daten ist gemäß Artikel 4 Nummer 12 Datenschutz-Grundverordnung „eine Verletzung der Sicherheit, die, ob unbeabsichtigt oder unrechtmäßig, zur Vernichtung, zum Verlust, zur Veränderung oder zur unbefugten Offenlegung von beziehungsweise zum unbefugten Zugang zu personenbezogenen Daten führt, die übermittelt, gespeichert oder auf sonstige Weise verarbeitet wurden.“

Als Datenschutzverletzung ist daher die Nichteinhaltung von mindestens einem der drei Grundsätze der Informationssicherheit einzustufen. Mögliche Folgen sind:

- „Vertraulichkeitsverletzung“ wenn es zu einer unbefugten oder versehentlichen Offenlegung von oder einem Zugriff auf personenbezogene Daten kommt.
- „Integritätsverletzung“ wenn es zu einer unbefugten oder versehentlichen Änderung von personenbezogenen Daten kommt.
- „Verfügbarkeitsverletzung“ wenn ein versehentlicher oder unbefugter Verlust des Zugriffs auf oder die Zerstörung von personenbezogenen Daten vorliegt.[3]

Beispiel:

> Ein Firmenlaptop mit Kundendaten wird gestohlen. Die Kundendaten befanden sich unverschlüsselt auf dem Laptop, ein Backup ist nicht vorhanden.

In diesem Fall ist es zu einer Vertraulichkeits- und Verfügbarkeitsverletzung gekommen, da unberechtigte Dritte Zugang zu den Kundendaten erhalten können und der berechtigte Verantwortliche die Daten

1 Artikel 33 Datenschutz-Grundverordnung (DS-GVO).
2 Artikel 34 DS-GVO.
3 Siehe Leitlinien 9/2022 für die Meldung von Verletzungen des Schutzes personenbezogener Daten gemäß der DSGVO, Version 2.0, zuletzt überarbeitet und angenommen am 28. März 2023, Seite 9.

verloren hat. Außerdem kann eine Verletzung der Integrität vorliegen, da eine unbefugte Änderung von personenbezogenen Daten nicht verhindert oder ausgeschlossen werden kann.

Um auf eine Datenschutzverletzung zu reagieren, müssen die Verantwortlichen zunächst in der Lage sein, diese zu erkennen. Es gehört daher zu den notwendigen Vorsorgemaßnahmen eines Verantwortlichen, ein Verfahren zur Erkennung und Behandlung von Datenpannen zu etablieren. Ziel dieser Maßnahmen sollte der Schutz natürlicher Personen und ihrer personenbezogenen Daten sein. In diesem Zusammenhang ist die von der Datenschutz-Grundverordnung vorgeschriebene Meldung an die Aufsichtsbehörde und eine mögliche Information der Betroffenen als Instrument zu sehen, das die Einhaltung der Vorschriften zum Schutz personenbezogener Daten erleichtert und das Risiko nachteiliger Auswirkungen auf die betroffenen Personen abmildert. Eine Nichtbeachtung der Meldepflicht durch den Verantwortlichen stellt eine Ordnungswidrigkeit dar, die durch die Aufsichtsbehörde geahndet werden kann.[4]

Kommt es bei einem Verantwortlichen zu einer Datenschutzverletzung, weist dies grundsätzlich auf Lücken im Sicherheitskonzept hin. Zu den Aufgaben gehört es daher auch, nach aufgetretenen Datenpannen die entsprechenden Lücken in den technischen und organisatorischen Maßnahmen zu identifizieren und zu schließen.[5]

2 Meldung an die Aufsichtsbehörde

Artikel 33 Absatz 1 DS-GVO sieht Folgendes vor:

„Im Falle einer Verletzung des Schutzes personenbezogener Daten meldet der Verantwortliche unverzüglich und möglichst binnen 72 Stunden, nachdem ihm die Verletzung bekannt wurde, diese der gemäß Artikel 55 zuständigen Aufsichtsbehörde, es sei denn, dass die Verletzung des Schutzes personenbezogener Daten voraussichtlich nicht zu einem Risiko für die Rechte und Freiheiten natürlicher Personen führt. Erfolgt die Meldung an die Aufsichtsbehörde nicht binnen 72 Stunden, so ist ihr eine Begründung für die Verzögerung beizufügen."

Exkurs: Risikobewertung

Die Bewertung des mit einer Datenschutzverletzung verbundenen Risikos für die Rechte und Freiheiten von Menschen hat hier ausschließlich den Fokus auf mögliche Folgen, die die entsprechende Schutzverletzung für die betroffenen Personen haben. Bei der Einschätzung des Risikos ist sowohl die generelle Eintrittswahrscheinlichkeit als auch der potenziell daraus folgende Schaden für die Betroffenen zu beurteilen.

Die Meldepflicht bei der Aufsichtsbehörde wird bereits bei einem geringen Risiko ausgelöst. Ist das Risiko nachteiliger Auswirkungen hoch, sind auch die Betroffenen zu benachrichtigen. Ein solches Risiko besteht dann, wenn die Datenschutzverletzung zu einem physischen, materiellen oder

4 Artikel 83 Absatz 4 Buchstabe a DS-GVO.

5 Siehe Leitlinien 01/2021 zu Beispielen für die Meldung von Verletzungen des Schutzes personenbezogener Daten, Version 2.0, zuletzt überarbeitet und angenommen am 14. Dezember 2021.

immateriellen Schaden für die Personen führen könnte. Beispiele für einen solchen Schaden sind Diskriminierung, Identitätsdiebstahl oder -betrug, finanzielle Verluste und Rufschädigung. Wenn von der Datenschutzverletzung personenbezogene Daten betroffen sind, aus denen die ethnische Herkunft, die politische Meinung, religiöse oder weltanschauliche Überzeugungen oder die Zugehörigkeit zu einer Gewerkschaft hervorgeht, oder wenn sie genetische Daten, Gesundheitsdaten oder Daten über das Sexualleben, Angaben zu strafrechtlichen Verurteilungen und Straftaten oder damit zusammenhängende Sicherungsmaßregeln betreffen, ist es wahrscheinlich, dass ein solcher Schaden eintritt.[6]

- Folgende Kriterien sollten mindestens bei der Risikobewertung einbezogen werden:
- Art der Datenschutzverletzung
- Art, Sensibilität und Umfang personenbezogener Daten
- Identifizierbarkeit betroffener Personen
- Schwere der Folgen für die betroffenen Personen
- Zahl der betroffenen Personen

Weitere Aspekte können je nach den konkreten Gegebenheiten und Eigenschaften der Betroffenen bzw. des Verantwortlichen dazukommen. Generell gilt, dass je höher die Eintrittswahrscheinlichkeit und je höher der mögliche Schaden für die betroffene Person ist, desto höher ist das Risiko zu bewerten. Im Zweifel sollten Verantwortliche bzw. Auftragsverarbeiter eher von einem zu hohen als einem zu niedrigen Risiko ausgehen.

2.1 Wann wird einem Verantwortlichen eine Datenschutzverletzung „bekannt“?

Es ist davon auszugehen, dass einem Verantwortlichen ein Sicherheitsvorfall dann bekannt geworden ist, wenn er eine hinreichende Gewissheit darüber erlangt hat, dass ein Vorfall eingetreten ist, z. B. wenn eine Mitarbeiterin das Auftauchen einer Erpressernachricht nach einem Ransomware-Angriff meldet oder der Verlust eines Smartphones mit Kundendaten auffällt.

In anderen Fällen muss der Verantwortliche zunächst eine kurze Untersuchung vornehmen, um mit hinreichender Gewissheit von einer Datenschutzverletzung auszugehen. Dies könnte der Fall sein, wenn sich ein Kunde an den Verantwortlichen wendet und mitteilt, verdächtige E-Mails unter der Identität des

6 Siehe Leitlinien 9/2022 für die Meldung von Verletzungen des Schutzes personenbezogener Daten gemäß der DSGVO, Version 2.0, zuletzt überarbeitet und angenommen am 28. März 2023, Seite 27.

Verantwortlichen mit personenbezogenen Daten erhalten zu haben. Nachdem der Verantwortliche aufgrund dieser Meldung festgestellt hat, dass Unbefugte in das Netzwerk eingedrungen sind, ist zu diesem Zeitpunkt vom Bekanntwerden des Vorfalls auszugehen.

Der Verantwortliche muss ab dann unverzüglich und möglichst innerhalb von 72 Stunden eine Meldung der Datenschutzverletzung an die Aufsichtsbehörde abgeben, wenn ein Risiko für die Rechte und Freiheiten der betroffenen Personen besteht. Das bedeutet, dass er zuvor die Art und Schwere des Vorfalls und die möglichen Folgen und nachteiligen Auswirkungen auf die Betroffenen einschätzen muss.

Sollte der Verantwortliche die 72-Stunden-Frist überschreiten, so muss er die Verzögerung begründen. Zu beachten ist, dass Nacht-, Wochenend- oder Feiertagszeiten die Frist nicht verlängern können.[7]

In vielen Fällen wird der Verantwortliche zur Aufklärung eines Datenschutzvorfalls einen über die 72-Stunden-Frist hinausgehenden Zeitraum benötigen. Er kann dann zur Fristwahrung eine vorläufige Meldung machen und die erforderlichen Informationen schrittweise zur Verfügung stellen.[8]

Zudem empfiehlt es sich, eine vorsorgliche Meldung zu tätigen, wenn bislang nur eine gewisse Wahrscheinlichkeit für einen Datenschutzvorfall angenommen werden kann, dieser aber noch nicht ausreichend bestätigt ist. Gleiches gilt auch bei Unsicherheiten bezüglich des Risikos für die betroffenen Personen.

Bei mehreren gemeinsam für die Datenverarbeitung Verantwortlichen[9] sollte bereits in der Vereinbarung zur gemeinsamen Verantwortlichkeit festgelegt werden, wer welche Verpflichtungen bei eintretenden Datenschutzverletzungen hat. Sollte ein Auftragsverarbeiter[10] eine Datenschutzverletzung feststellen, so ist er verpflichtet, diese unverzüglich dem Verantwortlichen zu melden.[11] Die entsprechenden Verpflichtungen des Auftragsverarbeiters sollten in den Auftragsverarbeitungsvertrag aufgenommen werden. Der Verantwortliche hat dann die Artikel-33-Meldung an die Aufsichtsbehörde vorzunehmen.

2.2 Welche Informationen muss eine Meldung an die Aufsichtsbehörde enthalten?

Artikel 33 Absatz 3 DS-GVO sagt dazu Folgendes:

„Die Meldung gemäß Absatz 1 enthält zumindest folgende Informationen:

7 Siehe Verordnung (EWG, Euratom) Nr. 1182/71 des Rates vom 3. Juni 1971 zur Festlegung der Regeln für die Fristen, Daten und Termine (Fristen-VO).
8 Artikel 33 Absatz 4 DS-GVO.
9 Artikel 26 DS-GVO.
10 Artikel 28 DS-GVO.
11 Artikel 33 Absatz 2 DS-GVO.

a) eine Beschreibung der Art der Verletzung des Schutzes personenbezogener Daten, soweit möglich mit Angabe der Kategorien und der ungefähren Zahl der betroffenen Personen, der betroffenen Kategorien und der ungefähren Zahl der betroffenen personenbezogenen Datensätze;

b) den Namen und die Kontaktdaten des Datenschutzbeauftragten oder einer sonstigen Anlaufstelle für weitere Informationen;

c) eine Beschreibung der wahrscheinlichen Folgen der Verletzung des Schutzes personenbezogener Daten;

d) eine Beschreibung der von dem Verantwortlichen ergriffenen oder vorgeschlagenen Maßnahmen zur Behebung der Verletzung des Schutzes personenbezogener Daten und gegebenenfalls Maßnahmen zur Abmilderung ihrer möglichen nachteiligen Auswirkungen."

Als Arten von Datenschutzverletzungen kommen z. B. Cyberangriff (Hacking), Befall mit Schadsoftware sowie Diebstahl, Verlust, Fehlversand und Fehlentsorgung personenbezogener Daten in Betracht. Kategorien von Personen können Kundinnen und Kunden, Beschäftigte oder Kinder sein. Unter Kategorien von betroffenen Datensätzen könnten z. B. Gesundheitsdaten, Ausbildungsunterlagen, Sozialdaten, Finanzdaten, Kontonummern und Personaldaten fallen.

Weitere Hinweise hierzu – auch zu möglichen nachteiligen Auswirkungen für die Betroffenen – finden Sie in unserem Formular zur Meldung von Datenschutzverletzungen.

Es ist nicht zwingend erforderlich, zu Punkt a) genaue Zahlen mitzuteilen, wenn diese nicht oder noch nicht zu ermitteln sind. Zudem sind, wie oben bereits ausgeführt, eine vorläufige Meldung und die schrittweise Zurverfügungstellung der notwendigen Informationen möglich. Es empfiehlt sich, den internen Datenschutzbeauftragten in den gesamten Prozess der Aufklärung und Meldung der Datenschutzverletzung beratend mit einzubeziehen.

In vielen Fällen wird die Aufsichtsbehörde nach einer Meldung weitere Informationen nachfragen, um den Vorfall, die Auswirkungen und die erforderlichen Maßnahmen vollständig einschätzen zu können.

3 Benachrichtigung der Betroffenen

In Artikel 34 Absatz 1 DS-GVO ist Folgendes festgelegt:

„Hat die Verletzung des Schutzes personenbezogener Daten voraussichtlich ein hohes Risiko für die persönlichen Rechte und Freiheiten natürlicher Personen zur Folge, so benachrichtigt der Verantwortliche die betroffene Person unverzüglich von der Verletzung."

Die Pflicht zur Benachrichtigung tritt daher erst ein, wenn das mögliche Risiko für nachteilige Auswirkungen auf Betroffene hoch ist, während die Meldepflicht bei der Aufsichtsbehörde bereits bei einem geringen Risiko gilt. Wenn klar ist, dass die Betroffenen zu informieren sind, hat dies so schnell wie möglich zu geschehen. Wichtigstes Ziel der Benachrichtigung ist es, dass die betroffenen Personen je nach Art der Datenschutzverletzung und der damit verbundenen Risiken gezielt über Vorkehrungen informiert werden, die sie zu ihrem eigenen Schutz treffen können (z. B. Passwortänderungen, Kontenbeobachtung).

Die Verantwortlichen müssen der betroffenen Person mindestens folgende Informationen mitteilen:[12]

- Beschreibung der Art der Datenschutzverletzung,
- Name und Kontaktdaten des/der Datenschutzbeauftragten oder einer sonstigen Anlaufstelle,
- Beschreibung der möglichen Folgen der Datenschutzverletzung,
- Beschreibung der vom Verantwortlichen ergriffenen Maßnahmen zur Behebung der Datenpanne,
- Beschreibung der Maßnahmen, die der Betroffene zur Abmilderung des Risikos von nachteiligen Auswirkungen ergreifen kann.

Eine Benachrichtigung darf nur unterbleiben, wenn eine der in Artikel 34 Absatz 3 DS-GVO genannten Bedingungen eintritt. Dazu könnten z. B. vom Verantwortlichen eine im Vorfeld der Datenschutzverletzung angewandte Verschlüsselung der personenbezogenen Daten oder nach der Datenschutzverletzung durchgeführte Maßnahmen gehören, die das Risiko der Betroffenen senken (z. B. Fernlöschung von Mobilgeräten). Eine individuelle Benachrichtigung darf auch unterbleiben, soweit dies mit einem unverhältnismäßigen Aufwand verbunden wäre. In diesem Fall muss der Verantwortliche die Betroffenen durch öffentliche Bekanntmachungen oder ähnliche Maßnahmen wirksam informieren. Der Verantwortliche sollte gegenüber der Aufsichtsbehörde nachweisen können, dass mindestens eine der Bedingungen erfüllt ist, falls er deshalb auf eine Benachrichtigung verzichtet. Die Aufsichtsbehörde darf einen Verantwortlichen verpflichten, die betroffenen Personen zu benachrichtigen.[13]

4 Interne Dokumentation

In allen Fällen ist der Verantwortliche verpflichtet, eine aufgetretene Datenschutzverletzung zu dokumentieren, also auch dann, wenn er kein Risiko für Betroffene sieht und entsprechend keine Meldung an die Aufsichtsbehörde macht.[14] Die Dokumentation muss alle mit dem Vorfall in Zusammenhang stehenden Fakten, möglichen Auswirkungen und die ergriffenen Abhilfemaßnahmen umfassen. Die Aufsichtsbehörde darf die Dokumentation anfordern und muss anhand dessen erkennen können, ob die Vorgaben des Artikels 33 DS-GVO vom Verantwortlichen eingehalten worden sind.

Es ist sinnvoll, die betrieblichen oder behördlichen Datenschutzbeauftragten bei Fragen zur Struktur, zur Einrichtung und zur Verwaltung der internen Dokumentation sowie bei jedem Vorfall beratend mit einzubeziehen. Der Datenschutzbeauftragte könnte auch zusätzlich mit der Führung dieser Unterlagen betraut werden.

Die Dokumentation von Datenschutzverletzungen ist Teil der Rechenschaftspflicht[15] von Verantwortlichen, die sie gegenüber der Aufsichtsbehörde erfüllen müssen.

12 Artikel 34 Absatz 2 DS-GVO.
13 Artikel 34 Absatz 4 DS-GVO.
14 Artikel 33 Absatz 5 DS-GVO.
15 Artikel 5 Absatz 2 DS-GVO.

Die Landesbeauftragte für den Datenschutz und für das Recht auf Akteneinsicht stellt ein Formular zur Meldung von Datenschutzverletzungen auf ihrer Webseite zur Verfügung. Die Formularinhalte werden verschlüsselt an die Landesbeauftragte übertragen.

5 Weitergehende Informationen

- Formular zur Meldung von Datenschutzverletzungen
- Leitlinien 9/2022 für die Meldung von Verletzungen des Schutzes personenbezogener Daten gemäß der DSGVO, Version 2.0, zuletzt überarbeitet und angenommen am 28. März 2023
- Leitlinien 01/2021 zu Beispielen für die Meldung von Verletzungen des Schutzes personenbezogener Daten, Version 2.0, zuletzt überarbeitet und angenommen am 14. Dezember 2021

Empfehlungen für eine Methodik zur Bewertung der Schwere von Verletzungen des Schutzes personenbezogener Daten:

- ENISA, Recommendations for a methodology of the assessment of severity of personal data breaches

Zur Problematik des unverhältnismäßigen Aufwands:

- Artikel 29-Arbeitsgruppe, Leitlinien für Transparenz gemäß der Verordnung 2016/679, zuletzt geändert und angenommen am 11. April 2018

Hilfestellungen für präventive technische und organisatorische Maßnahmen:

- Das Standard-Datenschutzmodell – Eine Methode zur Datenschutzberatung und -prüfung auf der Basis einheitlicher Gewährleistungsziele, Version 3.1
- IT-Grundschutz – Informationssicherheit mit System, Bundesamt für Sicherheit in der Informationstechnik (BSI)