

EUROPEAN DATA PROTECTION SUPERVISOR

# Leitlinien zur Meldung von Verletzungen des Schutzes personenbezogener Daten

Für die Organe und  
Einrichtungen der  
Europäischen Union



21. November 2018

## INHALTSVERZEICHNIS

<b>1. Einleitung</b> .....	<b>4</b>
<b>2. Anwendungsbereich und Gliederung der Leitlinien</b> .....	<b>6</b>
2.1. ANWENDUNGSBEREICH.....	6
2.2. GLIEDERUNG.....	6
<b>3. Verletzung des Schutzes personenbezogener Daten gemäß der Verordnung über die Verarbeitung personenbezogener Daten durch EU-Institutionen</b> .....	<b>8</b>
3.1. HINTERGRUND .....	8
3.2. DEFINITION EINER VERLETZUNG DES SCHUTZES PERSONENBEZOGENER DATEN.....	10
<b>4. Bewertung einer Verletzung des Schutzes personenbezogener Daten (Bewertung eines Risikos und eines hohen Risikos)</b> .....	<b>13</b>
4.1. BEWERTUNG EINES RISIKOS UND EINES HOHEN RISIKOS .....	15
<b>5. Vornahme der Meldung einer Verletzung des Schutzes personenbezogener Daten an den EDSB (Meldung an den EDSB)</b> .....	<b>17</b>
5.1. MELDEPFLICHTEN .....	18
5.2. SCHRITTWEISE MELDUNG.....	20
<b>6. Benachrichtigung einer betroffenen Person von einer Verletzung des Schutzes personenbezogener Daten</b> .....	<b>22</b>
<b>7. Dokumentation einer Verletzung des Schutzes personenbezogener Daten (Rechenschaftspflicht und Dokumentationspflichten)</b> .....	<b>24</b>
<b>Anhang 1. Formularvorlage für die Meldung</b> .....	<b>26</b>
<b>Anhang 2. Praktische Beispiele</b> .....	<b>29</b>
<b>Anhang 3. Referenzen und hilfreiche Texte</b> .....	<b>35</b>
<b>Anhang 4. Glossar</b> .....	<b>37</b>
<b>Anhang 5. Kurze Zusammenfassung</b> .....	<b>39</b>

Die Leitlinien bieten den EU-Institutionen **praktische Hinweise** zur Einhaltung der Bestimmungen über Verletzungen des Schutzes personenbezogener Daten gemäß den Artikeln 34 und 35 der Verordnung über die Verarbeitung personenbezogener Daten durch die EU-Institutionen.

Durch die Verordnung werden die Grundsätze der Datenschutz-Grundverordnung (Verordnung (EU) 2016/679, nachfolgend „DSGVO“), einschließlich der Grundsätze bezüglich Verletzungen des Schutzes personenbezogener Daten, in die Datenschutzvorschriften für EU-Institutionen einbezogen.

Die Leitlinien enthalten Empfehlungen und bewährte Verfahren zur Umsetzung der Rechenschaftspflicht in Bezug auf den Schutz personenbezogener Daten, indem sie **helfen, die Risiken für den Schutz personenbezogener Daten, für die Privatsphäre und sonstige Grundrechte natürlicher Personen im Falle einer Verletzung des Schutzes personenbezogener Daten zu bewerten und zu verwalten**. Zudem wurden in den Leitlinien die Ratschläge gesammelt und zusammengefasst, die der Europäische Datenschutzbeauftragte (EDSB) den EU-Institutionen in den letzten Jahren gegeben hat, z. B. hinsichtlich der ersten interinstitutionellen Ausschreibungen.

In diesen Leitlinien ist der Ansatz dargestellt, den die EU-Institutionen anwenden sollten, um angemessen auf eine Verletzung des Schutzes personenbezogener Daten zu reagieren.

Bei der Bewertung der Einhaltung der Verordnung zieht der EDSB die im Folgenden aufgeführten bewährten Verfahren als **Referenz** heran. Die EU-Institutionen können sich unter Berücksichtigung ihres spezifischen Bedarfs auch für andere, nicht in diesem Dokument aufgeführte Maßnahmen entscheiden, die gleichermaßen wirksam sind. In diesem Fall müssen sie nachweisen, auf welche Weise diese Maßnahmen einen gleichwertigen Schutz personenbezogener Daten bieten.

Die EU-Institutionen sollten regelmäßig eine Bewertung ihrer Verfahren, die für den Fall einer Verletzung des Schutzes personenbezogener Daten angewandt werden, durchführen. Durch die Bewertung sollte nachgewiesen werden, dass die EU-Institutionen grundsätzlich wirksam reagieren können, um dem Risiko einer Verletzung des Schutzes personenbezogener Daten vorzubeugen oder dieses auf ein vertretbares Maß zu reduzieren.

Die Leitlinien beschreiben:

- wann eine Verletzung des Schutzes personenbezogener Daten vorliegt;
- wie eine Verletzung des Schutzes personenbezogener Daten bewertet wird;
- wie dem EDSB eine Verletzung des Schutzes personenbezogener Daten gemeldet wird;
- wie die betroffene Person von einer Verletzung des Schutzes personenbezogener Daten benachrichtigt wird;
- wie eine Verletzung des Schutzes personenbezogener Daten dokumentiert wird.

Des Weiteren enthalten die Leitlinien eine Formularvorlage für die von den EU-Institutionen vorzunehmende Meldung einer Verletzung des Schutzes personenbezogener Daten an den EDSB.

# 1. Einleitung

- 1 Diese Leitlinien sollen den Organen und Einrichtungen der EU (nachfolgend „EU-Institutionen“) praktische Hinweise zur Einhaltung der Verordnung (EU) 2018/1725 („die Verordnung“)<sup>1</sup>, welche die Verordnung (EG) Nr. 45/2001<sup>2</sup> ersetzt, liefern, indem sie ihnen helfen, wirksam auf Verletzungen des Schutzes personenbezogener Daten zu reagieren. Durch die Verordnung wird für EU-Institutionen die Pflicht eingeführt, den EDSB zu benachrichtigen, wenn eine Verletzung des Schutzes personenbezogener Daten auftritt, die ein Risiko für die Rechte und Freiheiten natürlicher Personen darstellt. Für den Fall eines hohen Risikos müssen zudem die natürlichen Personen benachrichtigt werden, deren Daten von der Verletzung betroffen sind. Durch die Verordnung werden die Datenschutzvorschriften für EU-Institutionen an die Datenschutz-Grundverordnung (Verordnung (EU) 2016/679, nachfolgend „DSGVO“)<sup>3</sup> angepasst, die in den Mitgliedstaaten der EU und des EWR auf juristische Personen des privaten und öffentlichen Sektors anwendbar sind.
- 2 Als unabhängige Aufsichtsbehörde mit Zuständigkeit für die Verarbeitung personenbezogener Daten durch die EU-Institutionen kann der EDSB unter anderem Leitlinien zu bestimmten Aspekten im Zusammenhang mit der Verarbeitung personenbezogener Daten herausgeben.
- 3 Diese Leitlinien sollten von Datenschutzbeauftragten (DSB) und Datenschutzkoordinatoren oder Kontaktpersonen sowie von den IT-Mitarbeitern und den sonstigen mit der IT-Sicherheit und der physischen Sicherheit befassten Diensten, z. B. vor Ort für die Datensicherheit zuständige Beamte und örtliche Sicherheitsbeauftragte, sowie von allen Personen, die im Rahmen ihrer Tätigkeit als für die Verarbeitung Mitverantwortliche und Auftragsverarbeiter Verantwortung für die EU-Institutionen tragen, beachtet werden. Sie helfen der oberen Führungsebene zudem dabei, von höchster Stelle der Organisation aus eine Datenschutzkultur zu fördern und den Grundsatz der Rechenschaftspflicht umzusetzen.
- 4 Der Zweck dieser Leitlinien besteht darin, den EU-Institutionen die Erfüllung ihrer Pflichten bei der Verwaltung von Verletzungen des Schutzes personenbezogener Daten zu erleichtern. Sie bleiben jedoch für die Erfüllung ihrer Pflichten gemäß dem Grundsatz der Rechenschaftspflicht verantwortlich. Die in diesen Leitlinien empfohlenen Maßnahmen ermöglichen es den EU-Institutionen, ihre Prozesse für die Verwaltung von Verletzungen des Schutzes personenbezogener Daten zu entwickeln oder anzupassen und die Pflichten zur Benachrichtigung des EDSB und der natürlichen Personen zu erfüllen. Die EU-Institutionen können sich unter Berücksichtigung ihres spezifischen Bedarfs auch für andere, nicht in

---

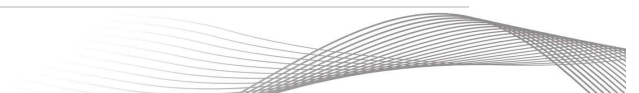
<sup>1</sup> Verordnung (EU) 2018/1725 des Europäischen Parlaments und des Rates vom 23. Oktober 2018 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die Organe, Einrichtungen und sonstigen Stellen der Union, zum freien Datenverkehr und zur Aufhebung der Verordnung (EG) Nr. 45/2001 und des Beschlusses Nr. 1247/2002/EG, ABl. L 295 vom 21.11.2018, S. 39; abrufbar unter: [https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L\\_.2018.295.01.0039.01.ENG](https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2018.295.01.0039.01.ENG).

<sup>2</sup> Verordnung (EG) Nr. 45/2001 des Europäischen Parlaments und des Rates vom 18. Dezember 2000 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die Organe und Einrichtungen der Gemeinschaft und zum freien Datenverkehr, ABl. L 8 vom 12.1.2001, S. 1.

<sup>3</sup> Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung), ABl. L 119 vom 4.5.2016, S. 1, abrufbar unter: <http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=OJ:L:2016:119:FULL>.

diesen Leitlinien aufgeführte Maßnahmen entscheiden, die gleichermaßen wirksam sind. In diesem Fall müssen sie nachweisen, auf welche Weise sie durch diese anderen Maßnahmen einen gleichwertigen Schutz erreichen wollen.

- 5 Mit fortschreitender Erfahrung und Praxis der EU-Institutionen und des EDSB bezüglich der Meldung und Mitteilung von Verletzungen des Schutzes personenbezogener Daten gemäß der Verordnung werden diese Leitlinien aktualisiert. Bei der Aktualisierung werden auch ein in Zusammenarbeit mit den Datenschutzbehörden der Mitgliedstaaten entwickeltes gemeinsames Verständnis bezüglich der Schwere von Verletzungen des Schutzes personenbezogener Daten und bezüglich der Risiken für die Personen, deren Daten von der Verletzung betroffen sind, sowie die Gewährleistung der Vereinbarkeit mit den Verfahren der Datenschutzbehörden der Mitgliedstaaten für die Durchsetzung der Bestimmungen bezüglich Verletzungen des Schutzes personenbezogener Daten gemäß der DSGVO berücksichtigt.



## 2. Anwendungsbereich und Gliederung der Leitlinien

### 2.1. Anwendungsbereich

- 6 Die Verordnung definiert die Pflichten der in den EU-Institutionen für die Verarbeitung Verantwortlichen mit Blick auf die in ihrer Verantwortung durchgeführte Verarbeitung personenbezogener Daten, und sie gewährt natürlichen Personen auf dem Rechtsweg durchsetzbare Datenschutzrechte.
- 7 Bei der Verarbeitung personenbezogener Daten in den Informationssystemen der EU-Institutionen müssen die Bestimmungen der Verordnung in vollem Umfang eingehalten werden.
- 8 In den Leitlinien ist angegeben, wie auf eine Verletzung des Schutzes personenbezogener Daten zu reagieren ist, um Artikel 34 und 35 der Verordnung einzuhalten.
- 9 In den Leitlinien werden die obligatorische Meldung von Verletzungen des Schutzes personenbezogener Daten und die Informationsanforderungen gemäß der Verordnung sowie die grundlegenden Maßnahmen erläutert, welche die EU-Institutionen als für die Verarbeitung Verantwortliche und/oder Auftragsverarbeiter ergreifen müssen, um diese neuen Pflichten zu erfüllen.
- 10 Der Schwerpunkt der Leitlinien liegt auf Verletzungen des Schutzes personenbezogener Daten und darauf, inwieweit die EU-Institutionen nicht nur darauf vorbereitet sein müssen, wirksam und gemäß ihren rechtlichen Pflichten auf diese Vorfälle zu reagieren, sondern diesen auch proaktiv vorzubeugen.
- 11 Verfahren in Bezug auf Datenschutzverletzungen dürfen Prozesse oder Verfahren zur Behandlung von Sicherheitsvorfällen nicht ersetzen oder aufheben, vielmehr sollten sie in einen solchen Prozess oder ein solches Verfahren zur Behandlung von Sicherheitsvorfällen integriert werden.

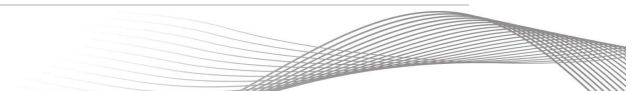
### 2.2. Gliederung

- 12 Die Leitlinien sind wie folgt gegliedert:
  - In Kapitel 1 wird der Zweck der Leitlinien erörtert.
  - In Kapitel 2 sind Anwendungsbereich und Gliederung des Dokuments beschrieben.
  - In Kapitel 3 wird eine Verletzung des Schutzes personenbezogener Daten beschrieben.
  - In Kapitel 4 wird erläutert, wie eine Verletzung des Schutzes personenbezogener Daten sowie die Risiken bewertet werden.
  - In Kapitel 5 wird erläutert, wie dem EDSB eine Verletzung des Schutzes personenbezogener Daten gemeldet wird.
  - In Kapitel 6 wird erläutert, wie die betroffenen Personen von einer Verletzung des Schutzes personenbezogener Daten benachrichtigt werden.
  - In Kapitel 7 wird erläutert, wie eine Verletzung des Schutzes personenbezogener Daten dokumentiert wird.
  - Anhang 1 enthält das Formular für die Meldung.

- In Anhang 2 werden praktische Beispiele beschrieben.
- Anhang 3 enthält Verweise auf andere nützliche Dokumente (Stellungnahmen, technische Standards, bewährte Verfahren usw.).
- Anhang 4 enthält ein Glossar.
- Anhang 5 enthält ein Flussdiagramm zu den Meldepflichten der EU-Institutionen bei Datenschutzverletzungen sowie eine Zusammenfassung der einschlägigen Erwägungen bezüglich einer Verletzung des Schutzes personenbezogener Daten.

13 Nicht Gegenstand dieses Dokuments sind:

- Eine umfassende Darstellung der einschlägigen IT-Sicherheitsmaßnahmen zur Erkennung und Begrenzung einer Verletzung des Schutzes personenbezogener Daten.
- Die technischen und funktionalen Merkmale der IT-Infrastruktur zur Vermeidung einer Verletzung des Schutzes personenbezogener Daten, wie Art der Server, Softwareplattformen und -anwendungen, Netzwerkgeräte usw.



### 3. Verletzung des Schutzes personenbezogener Daten gemäß der Verordnung über die Verarbeitung personenbezogener Daten durch EU-Institutionen

#### 3.1. Hintergrund

- 14 Bei der Meldung einer Verletzung des Schutzes personenbezogener Daten handelt es sich um eine neue Pflicht für die EU-Institutionen, die einer ähnlichen durch die DSGVO eingeführten Pflicht entspricht. Das Konzept wurde erstmals im Rahmen der e-Datenschutz-Richtlinie eingeführt. Eine Verletzung des Schutzes personenbezogener Daten kann, wenn nicht rechtzeitig und angemessen reagiert wird, einen physischen, materiellen oder immateriellen Schaden für natürliche Personen nach sich ziehen.
- 15 In allen Fällen hat der für die Verarbeitung Verantwortliche die Auswirkungen einer Verletzung des Schutzes personenbezogener Daten und insbesondere die Auswirkungen auf die betroffenen Personen zu minimieren. Die für die Verarbeitung Verantwortlichen müssen ein Verfahren für den Umgang mit Verletzungen des Schutzes personenbezogener Daten anwenden, das auch die Meldung an den EDSB sowie gegebenenfalls die Benachrichtigung der betroffenen Personen umfasst. Durch das Verfahren für den Umgang mit Verletzungen des Schutzes personenbezogener Daten werden andere Prozesse oder Verfahren für den Umgang mit Vorfällen nicht ersetzt oder aufgehoben. In der Tat wären die für die Verarbeitung Verantwortlichen gut beraten, Verfahren für den Umgang mit Verletzungen des Schutzes personenbezogener Daten in ihre Verfahren zur Verwaltung von Informationssicherheitsvorfällen zu integrieren. Des Weiteren sollte das Verfahren für den Umgang mit Verletzungen des Schutzes personenbezogener Daten mit dem Notfallplan des für die Verarbeitung Verantwortlichen sowie gegebenenfalls mit den Tätigkeiten, die von den Kommunikationsteams des für die Verarbeitung Verantwortlichen durchgeführt werden, verknüpft sein.
- 16 Zur Einhaltung der in der Verordnung festgelegten Zeitrahmen für die Meldung und Mitteilung von Verletzungen des Schutzes personenbezogener Daten wird dringend empfohlen, dass die für die Verarbeitung Verantwortlichen ein Verfahren für Verletzungen des Schutzes personenbezogener Daten anwenden, das Abhilfestrategien umfasst. Dieses Verfahren könnte bestehende IT-Sicherheitsverfahren/-handbücher ergänzen. Alle Mitarbeiter sollten über diese Pflicht und die damit verbundenen Verfahren informiert werden (z. B. Schulung für Neueinsteiger, Übung für alle Mitarbeiter).
- 17 Eine Verletzung des Schutzes personenbezogener Daten kann möglicherweise eine Reihe erheblicher negativer Auswirkungen auf die natürlichen Personen haben und einen physischen, materiellen oder immateriellen Schaden nach sich ziehen. Gemäß der DSGVO und der Verordnung kann dies den Verlust der Kontrolle über ihre personenbezogenen Daten oder die Einschränkung ihrer Rechte, Diskriminierung, Identitätsdiebstahl oder -betrug, finanzielle Verluste, die unbefugte Aufhebung der Pseudonymisierung, Rufschädigung, den Verlust der Vertraulichkeit von dem Berufsgeheimnis unterliegenden Daten oder andere erhebliche wirtschaftliche oder gesellschaftliche Nachteile für diese natürlichen Personen umfassen<sup>4</sup>.

---

<sup>4</sup> Erwägungsgrund 85 der DSGVO, Erwägungsgrund 46 der Verordnung.

- 18 Die Meldung von Datenschutzverletzungen an die Aufsichtsbehörde sowie die Benachrichtigung der betroffenen Personen sind gemäß Artikel 33 und 34 der DSGVO sowie gemäß Artikel 34 und 35 der Verordnung zu rechtlichen Pflichten geworden. Bei Meldungen von Verletzungen des Schutzes personenbezogener Daten handelt es sich um Maßnahmen zur Stärkung der betroffenen Personen, die gleichzeitig die Rechenschaftspflicht der für die Verarbeitung Verantwortlichen (und der Auftragsverarbeiter) untermauern. Durch die Meldungen von Verletzungen des Schutzes personenbezogener Daten soll die Datensicherheit in Europa gewährleistet werden.
- 19 Gleichzeitig sollten die Umstände der Verletzung hinreichend berücksichtigt werden, beispielsweise ob personenbezogene Daten durch geeignete technische Sicherheitsvorkehrungen geschützt waren, die die Wahrscheinlichkeit eines Identitätsbetrugs oder anderer Formen des Datenmissbrauchs wirksam verringern (Erwägungsgrund 88 der DSGVO).
- 20 Auch wenn dieser Aspekt in der Richtlinie 95/46/EG sowie in der Verordnung 45/2001 nicht behandelt wird, ist das Konzept der Meldung von Datenschutzverletzungen in der Gesetzgebung der EU nicht neu. Betreiber öffentlich zugänglicher elektronischer Kommunikationsdienste sind beispielsweise verpflichtet, den zuständigen nationalen Behörden eine Verletzung des Schutzes personenbezogener Daten zu melden und ein Verzeichnis der Datenschutzverletzungen zu führen, das Angaben zu den Umständen der Verletzungen, zu deren Auswirkungen und zu den ergriffenen Abhilfemaßnahmen enthält (Artikel 4 der e-Datenschutz-Richtlinie)<sup>5</sup>.
- 21 Auf nationaler Ebene haben einige Mitgliedstaaten bereits vor dem Inkrafttreten der DSGVO Maßnahmen zur Verwaltung von Datenschutzverletzungen eingeführt. Durch das Bundesdatenschutzgesetz wurde im Jahr 2009 eine Pflicht zur Meldung von Verletzungen der Vertraulichkeit eingeführt<sup>6</sup>. Im Jahr 2011 hat Irland einen Personal Data Security Breach Code of Practice [Verhaltenskodex für Datenschutzverletzungen] eingeführt<sup>7</sup>. Zwischen 2014 und 2015 hat Italien verschiedene Dokumentvorlagen für die Meldung von Datenschutzverletzungen, abhängig von der Art der betroffenen Daten, ausgearbeitet<sup>8</sup>.
- 22 Unter Berücksichtigung der Bedeutung der Meldung und Mitteilung einer Verletzung des Schutzes personenbezogener Daten für die Stärkung der Rechte der betroffenen Personen, die Förderung der Rechenschaftspflicht von für die Verarbeitung Verantwortlichen (und Auftragsverarbeitern) sowie für die Verbesserung der Datensicherheit in Europa wird den für die Verarbeitung Verantwortlichen durch die Verordnung eine Pflicht auferlegt, falls

---

<sup>5</sup> Richtlinie 2002/58/EG des Europäischen Parlaments und des Rates vom 12. Juli 2002 über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation (Datenschutzrichtlinie für elektronische Kommunikation), ABl. L 201 vom 31.7.2002, S. 37, in der durch die Richtlinie 2009/136/EG vom 25. November 2009, ABl. L 337 vom 18.12.2009, geänderten Fassung, konsolidierte Fassung abrufbar unter: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:02002L0058-20091219>.

<sup>6</sup> Gesetz zur Änderung datenschutzrechtlicher Vorschriften vom 14.8.2009, BGBl. 2009 Teil I Nr. 54, S. 2814, abrufbar unter: [http://www.bgbl.de/xaver/bgbl/start.xav?startbk=Bundesanzeiger\\_BGBI&jumpTo=bgbl109s2814.pdf](http://www.bgbl.de/xaver/bgbl/start.xav?startbk=Bundesanzeiger_BGBI&jumpTo=bgbl109s2814.pdf)

<sup>7</sup> [https://www.dataprotection.ie/docs/Data\\_Security\\_Breach\\_Code\\_of\\_Practice/1082.htm](https://www.dataprotection.ie/docs/Data_Security_Breach_Code_of_Practice/1082.htm)

<sup>8</sup> Für Gesundheitsdaten und biometrische Daten: <http://194.242.234.211/documents/10160/0/Linee+guida+in+materia+di+dossier+sanitario+-+Allegato+B.pdf>; <https://www.garantepriacy.it/documents/10160/0/All+B+al+Prov.+513+del+12+novembre+2014+Mod.+segnal+azione+data+breach.pdf>

Verletzungen des Schutzes personenbezogener Daten in EU-Institutionen (oder bei ihren Auftragsverarbeitern) eintreten.

### 3.2. Definition einer Verletzung des Schutzes personenbezogener Daten

- 23 **Gemäß Artikel 3 Absatz 16 der Verordnung** handelt es sich bei einer „Verletzung des Schutzes personenbezogener Daten“ um 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 unter der Verantwortung der EU-Institutionen als für die Verarbeitung Verantwortliche verarbeitet wurden.
- 24 Diese Definition einer Verletzung des Schutzes personenbezogener Daten gemäß der Verordnung ist an die DSGVO angepasst<sup>9</sup>.
- 25 Wenn anderweitig gegen die Verordnung verstoßen wird (z. B. keine angemessene Rechtsgrundlage für einen Verarbeitungsvorgang, unzureichende Unterrichtung der betroffenen Personen usw.), fällt dies nicht unter die Pflichten im Zusammenhang mit einer Verletzung des Schutzes personenbezogener Daten, während dennoch ein Verstoß gegen die Verordnung vorliegt. Eine Verletzung der Informationssicherheit, die nicht zur Beeinträchtigung personenbezogener Daten führt, fällt ebenfalls nicht in den Anwendungsbereich dieser Pflicht. Dabei ist es unerheblich, ob die Verletzung vorsätzlich erfolgte oder nicht.
- 26 Nicht jeder Informationssicherheitsvorfall stellt eine Verletzung des Schutzes personenbezogener Daten dar, jede Verletzung des Schutzes personenbezogener Daten stellt jedoch einen Informationssicherheitsvorfall dar.
- 27 In ihren Leitlinien, die vom EDSB bestätigt wurden, hat die Artikel-29-Datenschutzgruppe („WP29“)<sup>10</sup> entsprechend den folgenden drei bekannten Grundsätzen der Informationssicherheit drei Arten von Verletzungen des Schutzes personenbezogener Daten definiert:
- „Verletzung der Vertraulichkeit“ – die unbefugte oder unbeabsichtigte Preisgabe von oder Einsichtnahme in personenbezogene Daten, bei der ein Rechtssubjekt, das nicht dazu berechtigt ist, Kenntnis von personenbezogenen Daten erhält,
  - „Verletzung der Verfügbarkeit“ – der unbefugte oder unbeabsichtigte Verlust des Zugangs zu personenbezogenen Daten oder die unbeabsichtigte oder unrechtmäßige Vernichtung personenbezogener Daten, wobei es zum Verlust der Kontrolle des Zugangs zu personenbezogenen Daten oder zu einer unangemessenen Löschung von personenbezogenen Daten kommt, und

---

<sup>9</sup> DSGVO, Artikel 4 Absatz 12

<sup>10</sup> Leitlinien der WP29 für die Meldung von Verletzungen des Schutzes personenbezogener Daten gemäß der Verordnung (EU) 2016/679, angenommen am 3. Oktober 2017, zuletzt überarbeitet und angenommen am 6. Februar 2018; abrufbar unter: [http://ec.europa.eu/newsroom/article29/item-detail.cfm?item\\_id=612052](http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612052). Diese Leitlinien wurden vom Europäischen Datenschutzausschuss bestätigt.

- „Verletzung der Integrität“ – die unbefugte oder unbeabsichtigte Änderung personenbezogener Daten, bei der es zu unangemessenen Änderungen von personenbezogenen Daten kommt.
- 28 Eine Datenschutzverletzung kann aus verschiedenen Gründen eintreten, wie:
- a. aufgrund von Fahrlässigkeit,
  - b. infolge eines zufälligen Ereignisses oder
  - c. aufgrund von vorsätzlichen Handlungen interner oder externer Personen.
- 29 Zusammenfassend ist festzuhalten, dass es sich bei jeder Verletzung des Schutzes personenbezogener Daten um einen Sicherheitsvorfall handelt<sup>11</sup>, der abhängig von den Umständen eine Verletzung der Vertraulichkeit, der Integrität oder der Verfügbarkeit von personenbezogenen Daten sowie eine Kombination davon darstellen kann. Bei den Ursachen von Datenschutzverletzungen kann es sich unter anderem um Fahrlässigkeit, zufällige Ereignisse oder technisches Versagen sowie um vorsätzliche Handlungen interner oder externer Akteure handeln.
- 30 Einige Beispiele für Datenschutzverletzungen<sup>12</sup>:
- a. Mitarbeiter stellen personenbezogene Daten irrtümlich den falschen Empfängern zur Verfügung (z. B. Versand von E-Mails an die falschen Personen oder Verwendung der falschen Verteilerliste);
  - b. Nutzung unzulässiger Kanäle für den Austausch personenbezogener Daten;
  - c. Mitarbeiter speichern Informationen auf einem nicht zulässigen Medium;
  - d. Auftragnehmer greift ohne vorherige Genehmigung oder unter Verletzung von technischen Kontrollen auf personenbezogene Daten (z. B. Personaldaten) zu;
  - e. Papierunterlagen, die personenbezogene Daten enthalten, werden aus nicht gesicherten Recycling- oder Mülltonnen gestohlen oder darin vergessen;
  - f. Mitarbeiter greifen auf personenbezogene Daten zu oder legen personenbezogene Daten offen, ohne dass dies durch die Berechtigung im Rahmen ihrer beruflichen Tätigkeit abgedeckt ist;
  - g. Datenbanken, die personenbezogene Daten enthalten, werden gehackt oder Dritte, die nicht dem für die Verarbeitung Verantwortlichen angehören, verschaffen sich anderweitig unrechtmäßigen Zugang zu solchen Datenbanken;
  - h. Verlust oder Diebstahl von Laptops, Mobiltelefonen, Wechseldatenträgern oder Papierunterlagen, die personenbezogene Daten enthalten.
- 31 Durch das Verfahren für den Umgang mit Verletzungen des Schutzes personenbezogener Daten werden sonstige Prozesse oder Verfahren für den Umgang mit Vorfällen nicht ersetzt oder aufgehoben. In der Tat könnten EU-Institutionen möglicherweise Verfahren für den Umgang mit Verletzungen des Schutzes personenbezogener Daten in ihre Verfahren zur Verwaltung von Informationssicherheitsvorfällen integrieren. Des Weiteren würde das

---

<sup>11</sup> Nicht jeder Informationssicherheitsvorfall stellt eine Verletzung des Schutzes personenbezogener Daten dar, jede Verletzung des Schutzes personenbezogener Daten stellt jedoch einen Informationssicherheitsvorfall dar.

<sup>12</sup> Weitere Beispiele in Anhang 2.

Verfahren für den Umgang mit Verletzungen des Schutzes personenbezogener Daten mit den Sicherheitsplänen des für die Verarbeitung Verantwortlichen sowie gegebenenfalls mit den Tätigkeiten, die von den Kommunikationsteams des für die Verarbeitung Verantwortlichen durchgeführt werden, verknüpft.

## 4. Bewertung einer Verletzung des Schutzes personenbezogener Daten (Bewertung eines Risikos und eines hohen Risikos)

- 32 Artikel 34 der Verordnung folgt dem durch die DSGVO übernommenen risikobasierten Ansatz. Die Schwere der Verletzungen muss im Einzelfall bewertet werden. Das „Risiko für die Rechte und Freiheiten natürlicher Personen“ wird als Erwägungsgrundlage für die Reaktion herangezogen. Die im Rahmen einer vorherigen Datenschutz-Folgenabschätzung (DSFA) ermittelten Risiken können als Ausgangspunkt dienen.
- 33 Die Bewertung, welche Datenschutzverletzungen ein Risiko und welche Datenschutzverletzungen ein hohes Risiko mit sich bringen, ist wichtig, da nur im zweiten Fall die Pflicht zur Benachrichtigung der betroffenen Personen besteht.
- 34 Bei der Bewertung eines Risikos sollten sowohl die Eintrittswahrscheinlichkeit als auch die Schwere der negativen Auswirkungen auf die Rechte und Freiheiten der betroffenen Personen berücksichtigt werden. Anschließend sollte das Risiko auf der Grundlage einer objektiven Bewertung beurteilt werden. Bei einer tatsächlichen Verletzung ist das nachteilige Ereignis bereits eingetreten. Daher liegt der Schwerpunkt der Bewertung ausschließlich auf den möglichen Auswirkungen der Verletzung auf die Rechte und Freiheiten der natürlichen Personen. Einige Auswirkungen sind zum Zeitpunkt der Feststellung der Verletzung möglicherweise bereits eingetreten, während andere erst zu einem späteren Zeitpunkt eintreten (z. B. für den Fall eines Diebstahls von Berechtigungsnachweisen, wurden einige dieser Berechtigungsnachweise möglicherweise bereits verwendet, während andere zu einem späteren Zeitpunkt verwendet werden).
- 35 Wie bereits erwähnt, handelt es sich bei einer Verletzung des Schutzes personenbezogener Daten um einen Sicherheitsvorfall. Es kann jedoch nicht jeder Sicherheitsvorfall als Verletzung des Schutzes personenbezogener Daten betrachtet werden. Als notwendige Voraussetzung dafür, dass ein Sicherheitsvorfall als Verletzung des Schutzes personenbezogener Daten betrachtet wird, müssen personenbezogene Daten betroffen sein.
- 36 In diesen Leitlinien wird davon ausgegangen, dass die EU-Institutionen über einen bewährten Prozess zur Verwaltung von Informationssicherheitsvorfällen, einschließlich Berichterstattung, verfügen. Es ist unbedingt erforderlich, dass eine Verletzung des Schutzes personenbezogener Daten erkannt werden kann.

Nicht jeder Informationssicherheitsvorfall stellt eine Verletzung des Schutzes personenbezogener Daten dar, jede Verletzung des Schutzes personenbezogener Daten stellt jedoch einen Informationssicherheitsvorfall dar.

Bei der Bewertung jedes gemeldeten Vorfalls sollte ermittelt werden, ob personenbezogene Daten betroffen sind.

Wenn personenbezogene Daten betroffen sind, wird der Sicherheitsvorfall als Verletzung des Schutzes personenbezogener Daten betrachtet.

- 37 Wenn ein Anhaltspunkt dafür vorliegt, dass ein Sicherheitsvorfall personenbezogene Daten betreffen könnte, wird unverzüglich der Datenschutzbeauftragte (DSB) hinzugezogen.

Wenn der Sicherheitsvorfall als Verletzung des Schutzes personenbezogener Daten betrachtet wird, sollte im nächsten Schritt bewertet werden, welche Auswirkungen der Vorfall auf die Rechte und Freiheiten natürlicher Personen hätte.

- 38 Wenn der Sicherheitsvorfall als Verletzung des Schutzes personenbezogener Daten betrachtet wird, bewerten die EU-Institutionen die Auswirkungen der Verletzung auf die Rechte und Freiheiten der betroffenen Personen. Diese Bewertung sollte so objektiv wie möglich sein. Dieser Schritt ist sehr wichtig, da hier die Meldepflichten der EU-Institutionen als für die Verarbeitung Verantwortliche bestimmt werden.

Eine EU-Institution setzt ihr eigenes Verfahren für die Verwaltung von Verletzungen des Schutzes personenbezogener Daten oder ihre eigenen Richtlinien um, die auf die Folgenabschätzung für jede gemeldete Verletzung des Schutzes personenbezogener Daten sowie auf die Auswahl des angemessenen Verfahrens für die Meldung an den EDSB und die betroffenen Personen ausgerichtet sind. Rollen und Zuständigkeiten müssen eindeutig festgelegt sein.

- 39 Es ist äußerst wichtig, dass die EU-Institution eine richtige Bewertung der Risiken gewährleistet, die den Auslöser für die Meldung an den EDSB und für die mögliche Benachrichtigung einer betroffenen Person darstellt.

In Fällen, in denen durch eine gemeldete Verletzung des Schutzes personenbezogener Daten nachweislich kein Risiko für die Rechte und Freiheiten von betroffenen Personen entsteht, muss der für die Verarbeitung Verantwortliche weder den EDSB noch die betroffenen Personen benachrichtigen. Diese Entscheidung sollte jedoch auf der geeigneten Ebene getroffen und gut dokumentiert werden, um es dem EDSB zu ermöglichen, die Einhaltung der Vorschriften durch die EU-Institutionen auch für nicht gemeldete Datenschutzverletzungen zu überprüfen.

- 40 Die EU-Institutionen werden eine schrittweise Anleitung oder eine Methode, die auf die objektive Bewertung der Höhe des Risikos einer Verletzung des Schutzes personenbezogener Daten abzielt, in ihr Verfahren zur Verwaltung von Datenschutzverletzungen oder in ein separates Verfahren integrieren.

Gemäß Artikel 34 der Verordnung meldet eine EU-Institution dem Europäischen Datenschutzbeauftragten eine Verletzung des Schutzes personenbezogener Daten innerhalb von **72 Stunden**, es sei denn, die Verletzung führt voraussichtlich nicht zu einem **Risiko** für die Rechte und Freiheiten natürlicher Personen.

Gemäß Artikel 35 Absatz 1 der Verordnung sollten die EU-Institutionen zudem auch die betroffenen Personen von der Verletzung benachrichtigen, falls die Verletzung des Schutzes personenbezogener Daten zu einem „**hohen Risiko**“ für die Rechte und Freiheiten natürlicher Personen führt.

- 41 In allen Fällen hat der für die Verarbeitung Verantwortliche die Auswirkungen einer Verletzung des Schutzes personenbezogener Daten und insbesondere die Auswirkungen auf die betroffenen Personen zu minimieren.

#### 4.1. Bewertung eines Risikos und eines hohen Risikos

- 42 Die Pflicht zur Meldung von Datenschutzverletzungen spiegelt einen risikobasierten Ansatz wider.

Die Schwere der Verletzungen muss im Einzelfall bewertet werden. Das „Risiko für die Rechte und Freiheiten natürlicher Personen“ sollte bei der Durchführung der Bewertung als Erwägungsgrundlage herangezogen werden. Die im Rahmen einer Datenschutz-Folgenabschätzung ermittelten Risiken können als Ausgangspunkt dienen<sup>13</sup>.

- 43 Die Bewertung, welche Datenschutzverletzungen ein Risiko und welche Datenschutzverletzungen ein hohes Risiko mit sich bringen, ist für die Melde- und Benachrichtigungspflicht relevant. Für den Fall eines Risikos, bei dem es sich nicht um ein hohes Risiko handelt, nehmen die EU-Institutionen lediglich eine Meldung an den EDSB als Aufsichtsbehörde vor, während in Fällen eines hohen Risikos auch die Pflicht zur Benachrichtigung der betroffenen Personen besteht.
- 44 In den Erwägungsgründen 46<sup>14</sup> und 47<sup>15</sup> der Verordnung ist bestimmt, dass bei der Bewertung eines Risikos sowohl die Eintrittswahrscheinlichkeit als auch die Schwere des Risikos für die Rechte und Freiheiten der betroffenen Personen berücksichtigt werden sollten. Anschließend sollte das Risiko auf der Grundlage einer objektiven Bewertung beurteilt werden. Bei einer tatsächlichen Datenschutzverletzung ist das Ereignis bereits eingetreten. Daher konzentriert sich der für die Verarbeitung Verantwortliche ausschließlich auf die Auswirkungen der Verletzung auf natürliche Personen<sup>16</sup>.

---

<sup>13</sup> Artikel 39 der Verordnung.

<sup>14</sup> „Die Risiken für die Rechte und Freiheiten natürlicher Personen - mit unterschiedlicher Eintrittswahrscheinlichkeit und Schwere - können aus einer Verarbeitung personenbezogener Daten hervorgehen, die zu einem physischen, materiellen oder immateriellen Schaden führen könnte, insbesondere wenn die Verarbeitung zu einer Diskriminierung, einem Identitätsdiebstahl oder -betrug, einem finanziellen Verlust, einer Rufschädigung, einem Verlust der Vertraulichkeit von dem Berufsgeheimnis unterliegenden personenbezogenen Daten, der unbefugten Aufhebung der Pseudonymisierung oder anderen erheblichen wirtschaftlichen oder gesellschaftlichen Beeinträchtigungen führen kann, wenn die betroffenen Personen um ihre Rechte und Freiheiten gebracht oder daran gehindert werden, die sie betreffenden personenbezogenen Daten zu kontrollieren, wenn personenbezogene Daten, aus denen die rassische oder ethnische Herkunft, politische Auffassungen, religiöse oder weltanschauliche Überzeugungen oder die Zugehörigkeit zu einer Gewerkschaft hervorgehen, und genetische Daten, Gesundheitsdaten oder das Sexualleben oder strafrechtliche Verurteilungen und Straftaten oder damit zusammenhängende Sicherungsmaßnahmen betreffende Daten verarbeitet werden, wenn persönliche Aspekte bewertet werden, insbesondere wenn Aspekte, die die Arbeitsleistung, wirtschaftliche Lage, Gesundheit, persönliche Vorlieben oder Interessen, die Zuverlässigkeit oder das Verhalten, den Aufenthaltsort oder Ortswechsel betreffen, analysiert oder prognostiziert werden, um persönliche Profile zu erstellen oder zu nutzen, wenn personenbezogene Daten schutzbedürftiger natürlicher Personen, insbesondere Daten von Kindern, verarbeitet werden oder wenn die Verarbeitung eine große Menge personenbezogener Daten und eine große Anzahl von betroffenen Personen betrifft.“

<sup>15</sup> „Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten der betroffenen Person sollten in Bezug auf die Art, den Umfang, die Umstände und die Zwecke der Verarbeitung bestimmt werden. Das Risiko sollte anhand einer objektiven Bewertung beurteilt werden, bei der festgestellt wird, ob die Datenverarbeitung ein Risiko oder ein hohes Risiko birgt.“

<sup>16</sup> Es ist darauf hinzuweisen, dass sich diese objektive Bewertung für den Fall einer Datenschutzverletzung von der Bewertung im Rahmen der Datenschutz-Folgenabschätzung unterscheidet. Bei der Datenschutz-Folgenabschätzung werden sowohl die Risiken der planmäßig durchgeführten Datenverarbeitung als auch die Risiken für den Fall einer Datenschutzverletzung berücksichtigt, letztere jedoch hypothetisch. Siehe auch Leitlinien der WP29 für die Meldung von Verletzungen des Schutzes personenbezogener Daten gemäß der Verordnung (EU) 2016/679.

- 45 Die Bewertung der Auswirkungen einer Datenschutzverletzung auf die betroffene Person ist wichtig, da sie den EU-Institutionen ebenfalls helfen wird, die geeigneten Maßnahmen zur Begrenzung und Behandlung der Verletzung zu ergreifen.
- 46 Wie von der WP29 in ihren Leitlinien empfohlen, sind bei der Bewertung der Risiken die folgenden Faktoren zu berücksichtigen:
1. Art der Datenschutzverletzung;
  2. Art, Sensibilität und Umfang personenbezogener Daten;
  3. Identifizierbarkeit betroffener Personen;
  4. Schwere der Folgen für die betroffenen Personen;
  5. besondere Eigenschaften der betroffenen Person;
  6. besondere Eigenschaften des für die Verarbeitung Verantwortlichen;
  7. Zahl der betroffenen Personen.
- 47 Alle oben genannten Faktoren müssen jeweils einzeln oder in Kombination mit den anderen sorgfältig bewertet werden, um die Höhe der Risiken für die natürlichen Personen anzugeben.

Die im Rahmen der Datenschutz-Folgenabschätzung ermittelten Risiken können den für die Verarbeitung Verantwortlichen bei der Bewertung des Risikos helfen. Es ist sehr wahrscheinlich, dass Datenschutzverletzungen bei Verarbeitungstätigkeiten, für die vorab eine Datenschutz-Folgenabschätzung gemäß Artikel 39 der Verordnung durchgeführt werden musste, zu einem höheren Risiko für die Rechte natürlicher Personen führen können und stärkere Auswirkungen auf die natürlichen Personen haben können.

- 48 In den in Anhang 2 dargestellten praktischen Beispielen für Verletzungen des Schutzes personenbezogener Daten ist die Höhe des Risikos angegeben. Weitere Hinweise zur Bewertung des Risikos finden sich in Anhang 3.

## 5. Vornahme der Meldung einer Verletzung des Schutzes personenbezogener Daten an den EDSB (Meldung an den EDSB)

**FUNKTIONALES POSTFACH DES EDSB FÜR MELDUNGEN VON VERLETZUNGEN DES SCHUTZES PERSONENBEZOGENER DATEN**

[data-breach-notification@edps.europa.eu](mailto:data-breach-notification@edps.europa.eu)

**ALLE MITTEILUNGEN SOLLTEN VERSCHLÜSSELT WERDEN**

Eine EU-Institution sollte dem Europäischen Datenschutzbeauftragten eine Verletzung des Schutzes personenbezogener Daten innerhalb von 72 Stunden melden, es sei denn, die Verletzung führt voraussichtlich nicht zu einem Risiko für die Rechte und Freiheiten natürlicher Personen. Wenn die Verletzung des Schutzes personenbezogener Daten zu einem „hohen Risiko“ für die Rechte und Freiheiten natürlicher Personen führt, sollte eine EU-Institution auch die betroffenen Personen von der Verletzung benachrichtigen.

- 49 Artikel 34 der Verordnung enthält die Pflicht zur Meldung von Verletzungen des Schutzes personenbezogener Daten an den EDSB. Der für die Verarbeitung Verantwortliche sollte dem EDSB die Datenschutzverletzung innerhalb von 72 Stunden, nachdem ihm die Verletzung bekannt wurde, melden. Es wird davon ausgegangen, dass dem für die Verarbeitung Verantwortlichen die Verletzung „bekannt“ geworden ist, wenn die hinreichende Sicherheit besteht, dass eine Verletzung des Schutzes personenbezogener Daten eingetreten ist.
- 50 In das Verfahren zur Meldung an den EDSB sind einbezogen: einerseits der für die Verarbeitung Verantwortliche (ein Vertreter) und andererseits die für Datenschutzangelegenheiten zuständige Person, z. B. der Datenschutzbeauftragte (DSB).
- 51 Der Auftragsverarbeiter spielt ebenfalls eine wichtige Rolle, da er die Aufgabe hat, den für die Verarbeitung Verantwortlichen über Datenschutzverletzungen zu informieren.
- 52 Die EU-Institutionen können bei verschiedenen Datenverarbeitungstätigkeiten gemäß der Verordnung sowohl für die Verarbeitung Verantwortliche als auch Auftragsverarbeiter sein. Sie können zudem externe Auftragsverarbeiter (z. B. Auftragnehmer) einsetzen, die für einige Tätigkeiten im Rahmen der Verarbeitung personenbezogener Daten verantwortlich sind.
- 53 Der für die Verarbeitung Verantwortliche bleibt vollständig für den Schutz personenbezogener Daten verantwortlich. Der Auftragsverarbeiter kann den für die Verarbeitung Verantwortlichen bei der Erfüllung seiner Pflichten unterstützen; dies umfasst die Meldung von Datenschutzverletzungen.
- 54 Wenn ein Auftragsverarbeiter bei der Verarbeitung im Auftrag des für die Verarbeitung Verantwortlichen Kenntnis von einer Verletzung des Schutzes personenbezogener Daten erhält, muss er dem für die Verarbeitung Verantwortlichen die Verletzung „unverzüglich“, d. h. schnellstmöglich, melden. Es ist zu beachten, dass der Auftragsverarbeiter nicht erst die sich aus einer Verletzung ergebenden Risiken bewerten muss, bevor er die Meldung an den für die Verarbeitung Verantwortlichen vornimmt; der für die Verarbeitung Verantwortliche hat diese Bewertung durchzuführen, wenn ihm die Verletzung bekannt wird. Der Auftragsverarbeiter muss lediglich feststellen, ob eine Verletzung eingetreten ist

und diese dann dem für die Verarbeitung Verantwortlichen melden. Der für die Verarbeitung Verantwortliche bedient sich des Auftragsverarbeiters, um seine Zwecke zu erreichen; daher sollte grundsätzlich davon ausgegangen werden, dass die Verletzung dem für die Verarbeitung Verantwortlichen „bekannt“ geworden ist, wenn der Auftragsverarbeiter ihn darüber informiert hat.

Es ist wichtig, dass ein **für die Verarbeitung Verantwortlicher** Klauseln bezüglich der Verletzung des Schutzes personenbezogener Daten in die Verträge mit Auftragnehmern, die als Auftragsverarbeiter tätig werden, aufnimmt, gemäß denen diese verpflichtet sind, den für die Verarbeitung Verantwortlichen unverzüglich über eine Verletzung des Schutzes personenbezogener Daten zu informieren und alle mit dieser Verletzung verbundenen Informationen zur Verfügung zu stellen.

Als Auftragsverarbeiter sind Sie verpflichtet, den bzw. die zuständigen für die Verarbeitung Verantwortlichen unverzüglich zu informieren, wenn Sie eine Verletzung des Schutzes personenbezogener Daten feststellen, und alle notwendigen Informationen zu dem Vorfall zur Verfügung zu stellen.

- 55 Der Vertreter des für die Verarbeitung Verantwortlichen sollte die Meldung an den EDSB senden und, mit der Unterstützung aller sonstigen Bearbeiter des Falls, alle Umstände im Zusammenhang mit der Verletzung des Schutzes personenbezogener Daten, deren Auswirkungen und die ergriffenen Abhilfemaßnahmen nachverfolgen, wie in Kapitel 7 beschrieben. Der für die Verarbeitung Verantwortliche muss den DSB in den gesamten Prozess für die Verwaltung und Meldung von Verletzungen des Schutzes personenbezogener Daten (sowohl Meldung an den EDSB als auch Benachrichtigung der betroffenen Person) einbeziehen.
- 56 Bei der Meldung der Datenschutzverletzung an den EDSB hat der für die Verarbeitung Verantwortliche den Namen und die Kontaktdaten seines DSB anzugeben.

Der für die Verarbeitung Verantwortliche informiert den DSB unverzüglich über den Eintritt einer Verletzung des Schutzes personenbezogener Daten und stellt sicher, dass der DSB in den gesamten Prozess für die Verwaltung und Meldung von Datenschutzverletzungen (sowohl an den EDSB als auch an die betroffene Person) einbezogen wird.

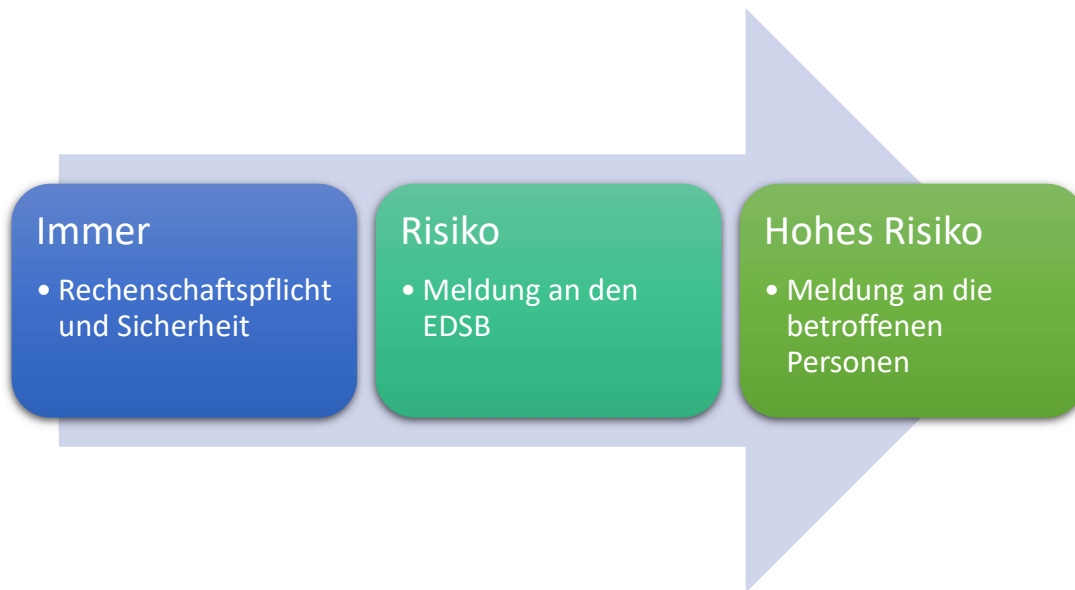
- 57 Auf Anfrage sollte der DSB im Zusammenhang mit der Notwendigkeit einer Meldung oder Benachrichtigung im Falle einer Verletzung des Schutzes personenbezogener Daten beratend tätig werden, und er sollte die Einhaltung der Bestimmungen, auch während einer Datenschutzverletzung (d. h. bei der Meldung), sowie die Nachverfolgung, auch während anschließender Untersuchungen durch den EDSB, überwachen.

Die EU-Institutionen müssen die Verfahren umsetzen, welche die wirksame Benachrichtigung im Falle einer Datenschutzverletzung ermöglichen, von: dem Auftragsverarbeiter an den für die Verarbeitung Verantwortlichen; dem für die Verarbeitung Verantwortlichen an die Aufsichtsbehörde-EDSB; und dem für die Verarbeitung Verantwortlichen an die betroffene Person.

### 5.1. Meldepflichten

- 58 Der für die Verarbeitung Verantwortliche sollte die Meldung innerhalb von 72 Stunden, nachdem ihm die Datenschutzverletzung bekannt wurde, versenden.

- 59 Falls der für die Verarbeitung Verantwortliche die Frist von 72 Stunden nicht einhält, hat er der Meldung eine Begründung für die Verzögerung beizufügen.
- 60 Die Meldepflicht ist von der Höhe des Risikos für die Person(en), deren Daten von der Verletzung betroffen sind, abhängig:
- Für den Fall eines unwahrscheinlichen Risikos besteht keine Pflicht zur Meldung an den EDSB; der für die Verarbeitung Verantwortliche sollte jedoch seinen DSB informieren und die Verletzung dokumentieren.
  - Wenn ein Risiko besteht, sollte der für die Verarbeitung Verantwortliche dem EDSB die Verletzung innerhalb von 72 Stunden melden. Für den Fall, dass der Zeitrahmen von 72 Stunden nicht eingehalten wird, sollte eine Begründung beigefügt werden.
  - Wenn ein hohes Risiko besteht, gilt neben der Pflicht zur Information des EDSB auch die Pflicht gemäß Artikel 35, die betroffene Person von der Verletzung des Schutzes personenbezogener Daten zu benachrichtigen.



**Abbildung 1. Übersicht über die sukzessiven Pflichten der für die Verarbeitung Verantwortlichen**

- 61 Die Meldung einer Verletzung des Schutzes personenbezogener Daten an den EDSB sollte mindestens enthalten<sup>17</sup>:
- eine Beschreibung der Art der Verletzung des Schutzes personenbezogener Daten, soweit möglich mit Angabe der Kategorien und der ungefähren Zahl der betroffenen Personen sowie der Kategorien und der ungefähren Zahl der betroffenen personenbezogenen Datensätze;
  - Name und Kontaktdaten des DSB;

---

<sup>17</sup> Siehe auch Kapitel 6

3. eine Beschreibung der wahrscheinlichen Folgen der Verletzung des Schutzes personenbezogener Daten<sup>18</sup>;
  4. eine Beschreibung der von dem für die Verarbeitung Verantwortlichen ergriffenen oder vorgeschlagenen Maßnahmen<sup>19</sup> zur Behebung der Verletzung des Schutzes personenbezogener Daten und gegebenenfalls der Maßnahmen zur Abmilderung ihrer möglichen nachteiligen Auswirkungen auf natürliche Personen.
- 62 In Anhang 1 stellt der EDSB ein Formular für die Meldung von Verletzungen des Schutzes personenbezogener Daten zur Verfügung, das die EU-Institutionen verwenden können.

## 5.2. Schrittweise Meldung

- 63 Abhängig von der Art der Datenschutzverletzung benötigen die EU-Institutionen als für die Verarbeitung Verantwortliche möglicherweise weitere Informationen und Ermittlungen sowie mehr Zeit, um die Umstände der Datenschutzverletzung festzustellen. Dies wird in Artikel 34 Absatz 5 der Verordnung berücksichtigt, gemäß dem es gestattet ist, dass dem EDSB die Informationen schrittweise zur Verfügung gestellt werden.
- 64 Den für die Verarbeitung Verantwortlichen werden nicht immer innerhalb des Zeitrahmens von 72 Stunden, nachdem ihnen eine Verletzung des Schutzes personenbezogener Daten bekannt wurde, alle erforderlichen Informationen vorliegen. Folglich sind vollständige und umfassende Angaben zu dem Vorfall möglicherweise nicht immer innerhalb dieses ersten Zeitraums verfügbar.
- 65 Dies kann für komplexe Datenschutzverletzungen gelten, etwa bei bestimmten Arten von Cybersicherheitsvorfällen, die möglicherweise eine eingehende forensische Untersuchung erfordern, um die Art der Datenschutzverletzung vollständig zu ermitteln und festzustellen, in welchem Umfang personenbezogene Daten beeinträchtigt wurden. In vielen Fällen wird der für die Verarbeitung Verantwortliche daher weitere Untersuchungen durchführen und zu einem späteren Zeitpunkt zusätzliche Informationen nachreichen müssen. In diesen Fällen müssen die für die Verarbeitung Verantwortlichen dem EDSB die Gründe für die Verzögerung der vollständigen Berichterstattung mitteilen.
- 66 Durch die Meldepflicht soll es den EU-Institutionen insbesondere ermöglicht werden, bei Datenschutzverletzungen umgehend tätig zu werden und sie einzudämmen, die

---

<sup>18</sup> Artikel 34 der Verordnung bezieht sich auf wahrscheinliche Folgen. Die für die Verarbeitung Verantwortlichen tun möglicherweise gut daran, nicht nur die wahrscheinlichen Folgen, sondern auch mögliche Folgen zu berücksichtigen und zu beschreiben, da sich die Wahrscheinlichkeit, dass sich das Risiko für den Eintritt bestimmter Folgen realisiert, im Verlauf der Zeit erhöhen kann (z. B. waren personenbezogene Daten zum Zeitpunkt der Verletzung durch eine dem Stand der Technik entsprechende Verschlüsselung gesichert, so dass wahrscheinlich keine Folgen eintreten; wenn jedoch zu einem späteren Zeitpunkt eine gravierende Schwachstelle der verwendeten Verschlüsselung festgestellt wird, ist die Wahrscheinlichkeit für den Eintritt der Folgen höher). Siehe diesbezüglich Beispiel 1 in Anhang 2.

<sup>19</sup> Eindämmungsmaßnahmen können umfassen: Abschalten des Systems, wenn die Datenschutzverletzung durch einen Systemfehler verursacht wird; Änderung des Benutzerpassworts und des Systems; Konfigurationen zur Zugangs- und Nutzungskontrolle; Prüfung, ob unverzüglich interne oder externe fachliche Beratung oder Unterstützung eingeholt wurde, um die Lücken des Systems zu beheben und/oder die Hacker-Tätigkeiten zu beenden; Beendigung oder Änderung der Zugangsrechte von Personen, die verdächtigt werden, eine Datenschutzverletzung begangen zu haben oder daran beteiligt gewesen zu sein; Benachrichtigung der zuständigen Strafverfolgungsbehörden, wenn ein Identitätsdiebstahl oder sonstige Straftaten begangen oder wahrscheinlich begangen wurden.

beeinträchtigten Daten nach Möglichkeit wiederherzustellen und sich vom EDSB beraten zu lassen.

- 67 Der für die Verarbeitung Verantwortliche sollte den EDSB informieren, wenn er noch nicht über alle erforderlichen Informationen verfügt, und er stellt zu einem späteren Zeitpunkt weitere Angaben zur Verfügung und vereinbart, wie und wann zusätzliche Informationen bereitgestellt werden sollten. Dies hindert den für die Verarbeitung Verantwortlichen nicht daran, zu einem beliebigen anderen Zeitpunkt zusätzliche Informationen bereitzustellen, wenn ihm weitere relevante Details zu der Datenschutzverletzung bekannt werden, die an den EDSB weitergegeben werden müssen.
- 68 Für die schrittweise Meldung kann ebenfalls das in Anhang 1 bereitgestellte Formular für die Meldung verwendet werden.

## 6. Benachrichtigung einer betroffenen Person von einer Verletzung des Schutzes personenbezogener Daten

- 69 Gemäß Artikel 35 der Verordnung benachrichtigt der für die Verarbeitung Verantwortliche die betroffene Person unverzüglich von einer Verletzung des Schutzes personenbezogener Daten, wenn die Verletzung voraussichtlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen zur Folge hat.
- 70 Daher besteht in diesem Fall keine festgesetzte Frist für den Versand der Benachrichtigung, diese ist jedoch unverzüglich, d. h. schnellstmöglich, vorzunehmen. Unter Berücksichtigung des hohen Risikos wird es der Person, deren personenbezogene Daten von der Verletzung betroffen sind, durch die sofortige Information jedoch ermöglicht, alle notwendigen Vorkehrungen zu treffen.
- 71 Die Benachrichtigung sollte eine Beschreibung der Art der Verletzung des Schutzes personenbezogener Daten sowie an die betroffene natürliche Person gerichtete Empfehlungen zur Minderung etwaiger nachteiliger Auswirkungen dieser Verletzung enthalten. Solche Benachrichtigungen an die betroffenen Personen sollten so rasch wie nach allgemeinem Ermessen möglich in enger Absprache mit dem EDSB und nach Maßgabe der von ihm erteilten Weisungen erfolgen.
- 72 Die betroffenen Personen sollten direkt von einer Datenschutzverletzung benachrichtigt werden, sofern dies nicht mit einem unverhältnismäßig hohen Aufwand verbunden ist.
- 73 Die Benachrichtigung enthält die Kontaktdaten des DSB und beschreibt in klarer und einfacher Sprache mindestens:
- die Art der Verletzung des Schutzes personenbezogener Daten;
  - die wahrscheinlichen Folgen der Verletzung des Schutzes personenbezogener Daten<sup>20</sup>;
  - die von dem für die Verarbeitung Verantwortlichen ergriffenen oder vorgeschlagenen Maßnahmen zur Behebung der Verletzung des Schutzes personenbezogener Daten und gegebenenfalls Maßnahmen zur Abmilderung ihrer möglichen nachteiligen Auswirkungen auf natürliche Personen.
- 74 Die EU-Institutionen sollten natürlichen Personen gegebenenfalls auch besondere Maßnahmen empfehlen, die sie zu ihrem eigenen Schutz vor möglichen nachteiligen Auswirkungen der Datenschutzverletzung treffen können, wie etwa das Zurücksetzen der Passwörter im Falle der Beeinträchtigung ihrer Zugangsdaten. Auch hier steht es einem für die Verarbeitung Verantwortlichen frei, über die genannten Anforderungen hinaus weitere Informationen bereitzustellen.
- 75 Die EU-Institutionen kommunizieren direkt mit den betroffenen Personen, sofern dies nicht mit einem unverhältnismäßig hohen Aufwand verbunden ist (Artikel 35 Buchstabe c).

---

<sup>20</sup> Artikel 35 der Verordnung bezieht sich auf wahrscheinliche Folgen. Die für die Verarbeitung Verantwortlichen tun möglicherweise gut daran, nicht nur die wahrscheinlichen Folgen, sondern auch mögliche Folgen zu berücksichtigen. Wenn eine Datenschutzverletzung kein hohes Risiko für die betroffenen Personen darstellt, da wahrscheinlich keine Folgen eintreten (z. B. sensible Gesundheitsdaten waren zum Zeitpunkt der Verletzung durch eine dem Stand der Technik entsprechende Verschlüsselung gesichert), muss die betroffene Person nicht informiert werden. Wenn sich die Wahrscheinlichkeit, dass sich das Risiko für den Eintritt bestimmter Folgen realisiert, im Verlauf der Zeit erhöht, sollten die betroffenen Personen jedoch über die Datenschutzverletzung informiert werden. Siehe diesbezüglich Beispiel 1 in Anhang 2.

Direkte Kommunikationswege umfassen beispielsweise E-Mail, SMS, Direktnachrichten oder postalische Mitteilungen.

- 76 Es gibt Ausnahmen von der Pflicht der EU-Institutionen, betroffene Personen von einer Verletzung des Schutzes personenbezogener Daten zu benachrichtigen (einige praktische Beispiele für Fälle, in denen die Benachrichtigung betroffener Personen nicht erforderlich ist, finden sich in Anhang 2):
- wenn der für die Verarbeitung Verantwortliche geeignete technische und organisatorische Sicherheitsvorkehrungen getroffen hat und diese Vorkehrungen auf die von der Verletzung betroffenen personenbezogenen Daten angewandt wurden (z. B. Verschlüsselung);
  - wenn der für die Verarbeitung Verantwortliche durch nachfolgende Maßnahmen sichergestellt hat, dass das hohe Risiko für die Rechte und Freiheiten der betroffenen Personen aller Wahrscheinlichkeit nach nicht mehr besteht.
- 77 Für den Fall, dass die individuelle Kommunikation mit einem unverhältnismäßig hohen Aufwand verbunden wäre (z. B. Verlust der Kontaktdaten aufgrund der Datenschutzverletzung), kann der für die Verarbeitung Verantwortliche die betroffenen Personen durch öffentliche Bekanntmachung oder eine ähnliche Maßnahme, durch die die betroffenen Personen vergleichbar wirksam informiert werden, benachrichtigen.
- 78 Gemäß dem Grundsatz der Rechenschaftspflicht müssen die für die Verarbeitung Verantwortlichen gegenüber dem EDSB nachweisen können, dass sie mindestens eine der oben genannten Bedingungen erfüllen, wenn sie beschließen, die betroffenen Personen nicht von einer Datenschutzverletzung zu benachrichtigen. Es ist möglich, dass eine Benachrichtigung zunächst nicht erforderlich ist, wenn kein Risiko für Personen besteht. Dies kann sich jedoch im Verlauf der Zeit ändern, und das Risiko müsste neu bewertet werden.
- 79 Stellt der EDSB fest, dass die Entscheidung, die betroffenen Personen nicht über eine Verletzung des Schutzes personenbezogener Daten zu informieren, unter Berücksichtigung der Wahrscheinlichkeit, dass die Verletzung des Schutzes personenbezogener zu einem hohen Risiko führt, nicht begründet ist, kann er den für die Verarbeitung Verantwortlichen anweisen, eine entsprechende Benachrichtigung vorzunehmen. Die Nichterfüllung einer solchen Anweisung kann zur Anwendung von Vollstreckungsmaßnahmen führen.

## 7. Dokumentation einer Verletzung des Schutzes personenbezogener Daten (Rechenschaftspflicht und Dokumentationspflichten)

- 80 Gemäß Artikel 34 Absatz 6 der Verordnung dokumentiert der für die Verarbeitung Verantwortliche alle Verletzungen des Schutzes personenbezogener Daten, einschließlich der im Zusammenhang mit der Verletzung des Schutzes personenbezogener Daten stehenden Fakten, deren Auswirkungen und der ergriffenen Abhilfemaßnahmen. Diese Dokumentation muss dem Europäischen Datenschutzbeauftragten die Überprüfung der Einhaltung der Bestimmungen der Verordnung ermöglichen.
- 81 Die Aufbewahrung der Nachweise für die Datenschutzverletzung ist auch wichtig, um die Untersuchung zu erleichtern und über Abhilfemaßnahmen zu entscheiden.
- 82 Rechenschaftspflicht bedeutet, dass der für die Verarbeitung Verantwortliche für die Einhaltung der sonstigen im Zusammenhang mit der Verarbeitung personenbezogener Daten stehenden Grundsätze verantwortlich ist und in der Lage sein muss, deren Einhaltung nachzuweisen. Zu diesen Grundsätzen gehören auch die Integrität und Vertraulichkeit, die für den Fall von Datenschutzverletzungen beeinträchtigt werden. Mit anderen Worten müssen Daten in einer Weise verarbeitet werden, bei der durch geeignete technische und organisatorische Maßnahmen der Schutz vor unbefugter oder unrechtmäßiger Verarbeitung oder vor unbeabsichtigtem Verlust, unbeabsichtigter Zerstörung oder unbeabsichtigter Schädigung gewährleistet wird.

Die EU-Institutionen müssen ein internes Verzeichnis für Verletzungen einrichten, in dem alle Umstände im Zusammenhang mit der Verletzung des Schutzes personenbezogener Daten, deren Auswirkungen und die ergriffenen Abhilfemaßnahmen erfasst sind. Dieses Verzeichnis könnte das bestehende Register für IT-Sicherheitsvorfälle ergänzen.

Die EU-Institutionen können ihren DSB um eine Stellungnahme hinsichtlich der Struktur, der Einrichtung und Verwaltung dieses internen Verzeichnisses für Datenschutzverletzungen ersuchen. Der DSB könnte zudem mit der Aufbewahrung dieser Unterlagen betraut werden.

- 83 Die Nachverfolgung von Datenschutzverletzungen ist notwendig, damit der für die Verarbeitung Verantwortliche nachweisen kann, dass er seine Pflichten gemäß der Verordnung einhält. Zudem würde der für die Verarbeitung Verantwortliche sowohl über ein Verzeichnis der bewährten Verfahren, die für den Fall von Datenschutzverletzungen zu befolgen sind, als auch über eine Liste der damit im Zusammenhang stehenden Sicherheitsvorfälle verfügen, durch welche die Umsetzung von Strategien zur Verbesserung der Sicherheit der Datenverarbeitung ermöglicht werden könnte.
- 84 Alle im Rahmen des Verfahrens für Verletzungen des Schutzes personenbezogener Daten gesammelten oder durch dieses Verfahren generierten Informationen sollten streng nach dem Grundsatz „Kenntnis nur, wenn nötig“ behandelt werden. Die Mitteilung von Datenschutzverletzungen sollte nicht über Systeme/Infrastruktur erfolgen, die möglicherweise durch ein Ereignis beeinträchtigt wurden.

Für den Fall von Ermittlungen oder einer Untersuchung oder falls diese Informationen anderweitig erforderlich sind, erwartet der EDSB, dass der DSB der EU-Institutionen in der

Lage ist, Informationen aus dem Verzeichnis für Verletzungen bereitzustellen und/oder dem EDSB das Verzeichnis zugänglich zu machen.

# Anhang 1. Formularvorlage für die Meldung



## EUROPÄISCHER DATENSCHUTZBEAUFTRAGTER

### FORMULAR FÜR DIE MELDUNG VON VERLETZUNGEN DES SCHUTZES PERSONENBEZOGENER DATEN (ARTIKEL 34 DER VERORDNUNG 2018/1725)

#### DATUM:

#### A. ART DER MELDUNG

A.1 UMFASSEND<sup>21</sup>

A.2 SCHRITTWEISE<sup>22</sup>: ERSTE:  ERGÄNZENDE<sup>23</sup>  ABSCHLIESSENDE MELDUNG<sup>24</sup>

Aktenzeichen<sup>25</sup>:

A.3 REGISTRIERUNGSNUMMER<sup>26</sup> DER DATENSCHUTZVERLETZUNG IN IHREM VERZEICHNIS:

JA  REG-NR.: NO

#### B. EU-INSTITUTION ALS FÜR DIE VERARBEITUNG VERANTWORTLICHE:

B.1 NAME DER ORGANISATION (EU-INSTITUTION):

B.2 ANSCHRIFT:

B.3 ANSPRECHPARTNER:

B.4 TELEFON:

B.5 E-MAIL:

B.6 DATENSCHUTZBEAUFTRAGTER:

B.7 TELEFON:

B.8 E-MAIL:

#### C. AUFTRAGSVERARBEITER: (bitte angeben, wenn die Datenschutzverletzung vom Auftragsverarbeiter gemeldet wurde)

C.1 NAME DER ORGANISATION:

C.2 ANSCHRIFT:

C.3 ANSPRECHPARTNER:

C.4 TELEFON:

C.5 E-MAIL:

C.6 DATENSCHUTZBEAUFTRAGTER:

C.7 TELEFON:

C.8 E-MAIL:

<sup>21</sup> Bitte auswählen, wenn es sich um eine umfassende Meldung handelt.

<sup>22</sup> Bitte auswählen, wenn es sich um eine erste, unvollständige Meldung handelt, der weitere Informationen folgen (Artikel 34 Absatz 4 der Verordnung).

<sup>23</sup> Es handelt sich um eine Ergänzung der ersten Meldung.

<sup>24</sup> Es handelt sich um die abschließenden Informationen zu dem Vorfall.

<sup>25</sup> Für den Fall einer ergänzenden oder abschließenden Meldung geben Sie, soweit vorhanden, bitte das von dem EDSB zugewiesene Aktenzeichen an.

<sup>26</sup> Artikel 34 Absatz 6 der Verordnung 2018/1725.

## D. ABSCHNITT DATENSCHUTZVERLETZUNG

D.1 Beschreiben Sie kurz den Vorfall und wie die Datenschutzverletzung festgestellt wurde:

D.2 Betroffene Sicherheitskriterien (ein oder mehrere Kästchen ankreuzen)

- I. VERTRAULICHKEIT  (möglicherweise) unbefugte Offenlegung oder unbefugter Zugang
- II. INTEGRITÄT  unbeabsichtigte oder unrechtmäßige Änderung
- III. VERFÜGBARKEIT  unbeabsichtigte oder unrechtmäßige Vernichtung oder unbeabsichtigter oder unrechtmäßiger Verlust

D.3 GENAUES DATUM ODER GENAUER ZEITRAUM DER DATENSCHUTZVERLETZUNG:

D.4 DATUM DER FESTSTELLUNG<sup>27</sup>: UHRZEIT:

D.5 DATUM DER MELDUNG<sup>28</sup>: UHRZEIT:

D.6 Wenn zwischen der Feststellung und der Meldung mehr als 72 Stunden vergangen sind, erklären Sie bitte, warum Sie die Meldung nicht fristgerecht vorgenommen haben:

D.7 WER WURDE INFORMIERT/ZU DEM VORFALL HINZUGEZOGEN<sup>29</sup>:

D.8 KATEGORIEN VON BETROFFENEN PERSONENBEZOGENEN DATEN<sup>30</sup>

D.9 UNGEFÄHRE ZAHL DER BETROFFENEN PERSONENBEZOGENEN DATEN:

Geben Sie nach Möglichkeit bitte die genaue Zahl an:

D.10 KATEGORIEN VON BETROFFENEN PERSONEN<sup>31</sup>:

D.11 UNGEFÄHRE ZAHL DER BETROFFENEN PERSONEN:

D.12 WAHRSCHEINLICHE oder TATSÄCHLICHE FOLGEN DER DATENSCHUTZVERLETZUNG FÜR DIE BETROFFENEN PERSONEN:

D.13 ABSCHÄTZUNG DES RISIKOS FÜR DIE RECHTE UND FREIHEITEN NATÜRLICHER PERSONEN:

RISIKO  HOHES RISIKO

D.14 Erläutern Sie kurz, wie die Bewertung des Risikos für die Rechte und Freiheiten natürlicher Personen vorgenommen wurde.

D.15 Haben Sie die betroffenen Personen über die Verletzung informiert? JA<sup>32</sup>  wenn ja, WANN:

NEIN , wenn nein, erläutern Sie bitte, warum (noch) nicht

D.16 MASSNAHMEN ZUR BEWÄLTIGUNG DES RISIKOS UND ZUR BEGRENZUNG SEINER AUSWIRKUNGEN<sup>33</sup>:

D.17 EINFÜHRUNG EINES FORMELLEN PROZESSES FÜR DIE BEARBEITUNG VON SICHERHEITSVORFÄLLEN: JA  NEIN  wenn nein, begründen Sie bitte, warum nicht:

---

<sup>27</sup> Geben Sie bitte das Datum an, an dem Sie Kenntnis von der Verletzung des Schutzes personenbezogener Daten erlangt haben.

<sup>28</sup> Die Meldung sollte innerhalb von 72 Stunden, nachdem Ihnen die Datenschutzverletzung bekannt wurde, erfolgen. Ist dies nicht der Fall, ist eine Begründung für die Verzögerung vorzulegen.

<sup>29</sup> Geben Sie bitte die Personen an, die an der Bearbeitung des Vorfalls durch die EU-Institution (intern und extern) beteiligt sind.

<sup>30</sup> Listen Sie bitte alle Elemente/Datenfelder auf, die beeinträchtigt wurden, z. B. Vor- und Nachnamen, Geburtsdatum, finanzielle Daten, Gesundheitsdaten usw.

<sup>31</sup> Listen Sie bitte alle Kategorien von betroffenen Personen auf, z. B. Beamte der EU, MEP, europäische Bürger, Kinder, schutzbedürftige Gruppen, wie Menschen mit Behinderung, usw.

<sup>32</sup> Wenn ja, fügen Sie bitte eine Kopie der an die betroffene Person gesandten Benachrichtigung bei.

<sup>33</sup> Geben Sie bitte die Sicherheitsmaßnahmen sowie die Maßnahmen zur Risikominderung an, z. B. Daten wurden verschlüsselt, ein redundantes System hat es der Organisation ermöglicht, zum Zweck der Geschäftskontinuität auf die Daten zuzugreifen.

Basic Model

---

<sup>34</sup> Erläutern Sie bitte die Grundursache für den Sicherheitsvorfall, der zu der Datenschutzverletzung geführt hat.

## Anhang 2. Praktische Beispiele

Die folgenden Beispiele können den EU-Institutionen bei der Feststellung helfen, ob Verletzungen des Schutzes personenbezogener Daten in unterschiedlichen Szenarien melde- bzw. benachrichtigungspflichtig sind. Die Liste der Beispiele ist nicht erschöpfend.

Zudem können diese Beispiele bei der Unterscheidung zwischen einem Risiko und einem hohen Risiko für die Rechte und Freiheiten natürlicher Personen helfen.

Beachten Sie bitte, dass eine Verletzung der Informationssicherheit, die nicht zur Beeinträchtigung personenbezogener Daten führt, nicht in den Anwendungsbereich dieses Verfahrens fällt. Wenn beispielsweise eine Datenbank, die anonyme Daten enthält, ein Datenleck aufweist, würde dies einen Sicherheitsvorfall, jedoch keine Verletzung des Schutzes personenbezogener Daten darstellen.

Zudem stellt die Tatsache, dass die EU-Institutionen den betroffenen Personen keine angemessenen Informationen über eine Verarbeitung zur Verfügung stellen, keine Datenschutzverletzung im Sinne von Artikel 35 der Verordnung dar.

Es ist unerheblich, ob die Verletzung vorsätzlich erfolgte oder nicht.

Nicht jeder Informationssicherheitsvorfall stellt eine Verletzung des Schutzes personenbezogener Daten dar, jede Verletzung des Schutzes personenbezogener Daten stellt jedoch einen Informationssicherheitsvorfall dar.

Es ist wichtig, zu verstehen, dass es sich bei dem Kriterium für die Entscheidungen über eine Meldung und Benachrichtigung um **das Risiko für jede betroffene Person** und **nicht um die Schwere des Vorfalls** handelt, die im Sicherheitsmanagement üblicherweise als Kriterium herangezogen wird.

Der Unterschied zwischen den beiden Kriterien kann durch eine Betrachtung der berücksichtigten Elemente veranschaulicht werden:

Für die Bewertung der **Schwere des Vorfalls** können die folgenden Elemente herangezogen werden:

- Geringer Schweregrad: beeinträchtigte Daten im Rahmen der Verarbeitung recht gewöhnlich (z. B. nur Vor- und Nachnamen); es bestehen Sicherheitsmaßnahmen zur Begrenzung der Auswirkungen (z. B. Verlust von Daten, diese sind jedoch durch eine starke Verschlüsselung gesichert), geringe Zahl an betroffenen Personen.
- Mittlerer Schweregrad: beeinträchtigte Daten etwas umfassender (z. B. Vor- und Nachnamen sowie Geburtsdatum, Lohngruppe und Familienzulage sowie sonstige Bereiche), in Anbetracht der Umstände bedeutende Zahl an betroffenen Personen (z. B. alle natürlichen Personen, die für die GD XX arbeiten, die meisten natürlichen Personen, die an einem bestimmten sensiblen Projekt arbeiten, usw.).
- Hoher Schweregrad: sensible Daten (z. B. Gesundheitszeugnis) und/oder sehr hohe Zahl an betroffenen Personen (z. B. alle Beamten der EU) und/oder betroffenen Politikern und/oder in den Medien wurde über die Datenschutzverletzung berichtet (Rufschädigung für die EU-Institutionen).

Das **Risiko für die natürliche Person** stellt ein in Bezug auf die Schwere des Vorfalls zu berücksichtigendes Element dar; es ist jedoch von spezifischen Elementen abhängig:

- die betroffenen Datenkategorien, z. B. kann die Offenlegung bestimmter Kategorien, finanzieller Daten oder sonstiger Datenelemente, die üblicherweise vertraulich behandelt werden, zu einem hohen Risiko führen,

- die Datenmenge für eine natürliche Person, z. B. kann ein hohes Risiko angezeigt sein, wenn viele Unterlagen zu bestimmten Transaktionen offengelegt werden, wie eine Liste der Telefongespräche mit den verbundenen Parteien, Listen der Aufgabenverteilungen usw., aber auch wenn die Daten verschiedene Aspekte einer natürlichen Person betreffen, auch wenn keine besonderen Kategorien betroffen sind, wie Daten über die Privatanschrift, die Familienzusammensetzung im Verlauf der Zeit, den Karriereverlauf, Reiseunterlagen, die Aktivität in sozialen Medien, Online-Transaktionen oder vergleichbare Kombinationen verschiedener Aspekte des Lebens,
- die einfache oder schwere Identifizierbarkeit natürlicher Personen, z. B. kann generell angenommen werden, dass das Risiko bei pseudonymisierten Daten geringer ist als bei Daten, die durch identifizierende Merkmale vollständig qualifiziert sind, wobei die Wirksamkeit der Pseudonymisierung bewertet werden muss. Es ist beispielsweise möglich, dass die Identifizierung anhand der Daten auch ohne solche Merkmale möglich ist (wie eine Liste der Arbeitsaufgaben, die unter allen Mitarbeitern einer Organisation einzigartig ist und die möglicherweise über HR-Instrumente zugänglich ist),
- die Merkmale der betroffenen natürlichen Personen, z. B. besteht bei Personen, deren Schutzbedürftigkeit bereits bekannt ist, wie Opfer von Belästigung oder Straftaten, mit größerer Wahrscheinlichkeit ein hohes Risiko infolge einer Datenschutzverletzung, als bei anderen Personen,
- die Merkmale des für die Verarbeitung Verantwortlichen, z. B. kann die reine Tatsache, dass eine natürliche Person in der Datenbank einer Organisation registriert wurde, die sich mit familiären Problemen befasst, für die natürliche Person ein höheres Risiko bergen, als dies bei einer Datenbank der Teilnehmer an einer Fachkonferenz der Fall ist,
- Eigenschaften der Verletzung, z. B. entsteht durch eine Verletzung aufgrund von gezielten Handlungen eines böswilligen Akteurs, der Zugang zu vertraulichen Daten erhalten hat, mit größerer Wahrscheinlichkeit ein hohes Risiko für die natürlichen Personen, als bei einer versehentlichen Offenlegung ähnlicher Daten gegenüber einer begrenzten Gruppe bekannter Empfänger.

Die Zahl der betroffenen natürlichen Personen stellt einen wichtigen Faktor für die Schwere eines Vorfalls dar. Eine höhere Zahl führt jedoch nicht notwendigerweise zu einem höheren Risiko für die betroffenen natürlichen Personen; wenn beispielsweise ein böswillig handelnder Akteur nur zu wenigen Kreditkartendaten Zugang erhält, kann die Wahrscheinlichkeit der unrechtmäßigen Nutzung für jede dieser Kreditkarten höher sein, als wenn eine große Datenbank gestohlen wird.

Für die Pflicht zur Meldung der Datenschutzverletzung an den EDSB oder für die Pflicht zur Benachrichtigung der betroffenen Personen stellt die Höhe des Risikos das entscheidende Kriterium dar. Die Schwere des Vorfalls ist für die Reaktion der Organisation sowie für die zu ergreifenden Minderungs- und Abhilfemaßnahmen von Bedeutung.

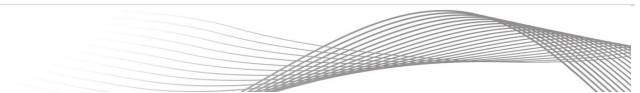
Beispiel	Art der Datenschutzverletzung	Meldung an den EDSB	Benachrichtigung der betroffenen Person	Erläuterung
<p>Eine GD zieht in ein anderes Gebäude um. Die Möbelpacker stellen fest, dass der Schrank des HR-Archivs offen ist und mehrere Ordner fehlen. Die Ordner enthalten Gesundheitsdaten. Es ist eine digitale Sicherungskopie verfügbar.</p>	<p>Vertraulichkeit Integrität</p>	<p>Ja</p>	<p>Ja</p>	<p>Da die Ordner sensible Daten enthalten, besteht ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen.</p>
<p>Eine Einrichtung, die über ein Netzwerk-Dateisystem für Patienten mit seltenen Krankheiten in der EU verfügt, betreibt ihre eigene Infrastruktur. Ein Kollege entdeckt Ransomware, nachdem ein privater USB-Stick verwendet wurde, und nach einer Weile kann niemand auf Daten von den Dateiservern zugreifen.</p>	<p>Verfügbarkeit Vertraulichkeit</p>	<p>Ja</p>	<p>Ja</p>	<p>Aufgrund der Sensibilität der Daten besteht ein hohes Risiko für die betroffenen natürlichen Personen.</p>
<p>Ein hochrangiges Mitglied einer EU-Institution verliert einen USB-Stick, der Kopien von Beschlussentwürfen und Materialien aus den Akten enthält, einschließlich personenbezogener Daten. Der USB-Stick ist mit einem dem Stand der Technik entsprechenden Algorithmus verschlüsselt. Es existieren Sicherungskopien der Daten.</p>	<p>Vertraulichkeit</p>	<p>NEIN</p>	<p>NEIN</p>	<p>Da die Daten mit einem dem Stand der Technik entsprechenden Algorithmus verschlüsselt sind, Sicherungskopien der Daten existieren, der eindeutige Schlüssel nicht beeinträchtigt wurde und sich die Daten zeitnah wiederherstellen lassen, sind eine Meldung an den EDSB sowie die Benachrichtigung der betroffenen Person nicht erforderlich.</p> <p>Kommt es zu einem späteren Zeitpunkt jedoch zu einer Beeinträchtigung des USB-Sticks,</p>



				sind die Meldung an den EDSB und die Benachrichtigung der betroffenen Person erforderlich. Dies gilt auch, wenn zu einem späteren Zeitpunkt eine gravierende Schwachstelle in dem Algorithmus festgestellt wird, der für die Verschlüsselung der Daten auf dem verloren gegangenen USB-Stick verwendet wurde, da dies dazu führt, dass sich die Wahrscheinlichkeit für eine Beeinträchtigung der Vertraulichkeit der Daten erhöht. In diesem Fall muss die Verletzung des Schutzes personenbezogener Daten neu bewertet werden.
Die Liste der Benutzernamen und Passwörter für das jeweilige Arbeitskonto der Mitarbeiter einer GD weist ein Datenleck auf. Dieses Datenleck wurde unverzüglich von der IT-Sicherheit festgestellt, und die Institution hat sofort die Benutzernamen geändert und die Passwörter zurückgesetzt.	Vertraulichkeit	NEIN	NEIN	Da die GD Sofortmaßnahmen zur Beseitigung des Risikos und der negativen Auswirkungen der Verletzung des Schutzes personenbezogener Daten ergriffen hat, besteht kein Risiko für die natürlichen Personen.
Ein Mitglied der Personalabteilung sendet versehentlich eine E-Mail an alle abgelehnten Bewerber für eine Stelle, wobei die E-Mail-Adressen im Cc-Feld und nicht im Bcc-Feld eingegeben werden.	Vertraulichkeit	JA	NEIN	Ungeachtet der Tatsache, dass persönliche E-Mail-Adressen mitgeteilt werden und erkennbar ist, wer sich um die Stelle beworben hat, besteht in diesem Fall ein Risiko für die Rechte und Freiheiten der natürlichen Personen, die nicht möchten, dass diese Informationen



				weitergegeben werden. In diesem Fall besteht kein hohes Risiko.
Ein Beamter einer EU-Institution sendet versehentlich eine Datei, die den Namen, die Nachnamen, die Kontaktdaten oder die Amtsposition einer gesamten GD enthält, an Mitarbeiter in einer anderen GD oder EU-Einrichtung.	Vertraulichkeit	NEIN	NEIN	In diesem Fall ist eine Meldung nicht erforderlich, da die oben genannten Informationen über die Mitarbeiter bereits in interinstitutionellen offenen Verzeichnissen bezüglich der Mitarbeiter der EU-Institutionen öffentlich zugänglich sind.
Eine Datenbank, die Informationen über Whistleblowing-Verfahren in EU-Institutionen enthält, wurde gehackt, und die Informationen wurden im Internet veröffentlicht. Die Namen der Whistleblower und der betroffenen Personen wurden veröffentlicht.	Vertraulichkeit	JA	JA	In diesem Fall besteht ein hohes Risiko für die Rechte und Freiheiten betroffener Personen. Aus diesem Grund muss eine Meldung an den EDSB vorgenommen werden, und es sollten sowohl die Whistleblower als auch sonstige betroffene Personen benachrichtigt werden.
Eine EU-Einrichtung wird Opfer eines Ransomware-Angriffs, der dazu führt, dass alle personenbezogenen Daten von EU-Bürgern, die in einem speziellen Förderprogramm registriert sind, verschlüsselt werden. Sicherungskopien sind nicht verfügbar, und die Daten können nicht wiederhergestellt werden.	Integrität Verfügbarkeit Vertraulichkeit	JA	JA	Eine Datenschutzverletzung, die die Integrität, Verfügbarkeit und möglicherweise die Vertraulichkeit betrifft. In diesem Fall besteht ein hohes Risiko für die Rechte und Freiheiten der betroffenen Person. Aus diesem Grund muss eine Meldung an den EDSB vorgenommen werden, und die natürlichen Personen sollten benachrichtigt werden.
Gesundheitszeugnisse der Mitarbeiter einer GD wurden versehentlich gelöscht oder, für den Fall von sicher	Verfügbarkeit Integrität	JA	JA	Da keine Sicherungskopie der Daten existiert und die Daten nicht wiederhergestellt werden können,



verschlüsselten Daten, ist der Entschlüsselungsschlüssel verloren gegangen. Es existieren weder eine Sicherungskopie der Daten der Gesundheitszeugnisse noch physische Dateien.				stellt der Verlust der Gesundheitszeugnisse der Mitarbeiter ein hohes Risiko für deren Rechte und Freiheiten dar. Daher müssen der EDSB und die betroffenen Personen benachrichtigt werden.
Ein Laptop, auf dem sich die Kopie einer Liste der Mitarbeiter befindet, gegen die Disziplinarmaßnahmen verhängt wurden, wurde gestohlen.	Vertraulichkeit	JA	JA	Aufgrund der Sensibilität der Daten besteht ein hohes Risiko für die Rechte und Freiheiten dieser Mitarbeiter, wenn unbefugte Personen Zugang zu diesen Daten haben.
Tausende Datensätze, die personenbezogene Daten enthalten, werden unverschlüsselt auf der Plattform der Cloud-Service-Anbieter (CSP) gespeichert. Der Cloud-Service-Anbieter wird nach einem Jahr gehackt.	Integrität Vertraulichkeit	JA	JA	Unter Berücksichtigung der großen Zahl der betroffenen natürlichen Personen sollten diese von dem Vorfall benachrichtigt werden.
Personenbezogene Daten von Steuerpflichtigen in der EU, die hohe Steuern zahlen, werden mit dem AES-512-Algorithmus verschlüsselt gespeichert, und der Schlüssel befindet sich auf dem lokalen Dateisystem. Der vor Ort für die Datensicherheit zuständige Beamte informiert nach einem Jahr über einen Einbruch in das Netzwerk. Es wurde auf den Verschlüsselungsschlüssel zugegriffen.	Integrität Vertraulichkeit	JA	JA	Unter Berücksichtigung der Art der Datenschutzverletzung und des potenziellen Risikos für die betroffenen natürlichen Personen sollte eine Meldung versandt werden.



## Anhang 3. Referenzen und hilfreiche Texte

### Strategiepapiere des EDSB, Artikel-29-Datenschutzgruppe:

1. **Stellungnahme 03/2014 der Artikel-29-Datenschutzgruppe über die Meldung von Verletzungen des Schutzes personenbezogener Daten**

<http://ec.europa.eu/newsroom/article29/news-overview.cfm>

2. **Leitlinien für die Meldung von Verletzungen des Schutzes personenbezogener Daten gemäß der Verordnung (EU) 2016/679, angenommen am 3. Oktober 2017, zuletzt überarbeitet und angenommen am 6. Februar 2018, Artikel-29-Datenschutzgruppe**

[http://ec.europa.eu/newsroom/article29/item-detail.cfm?item\\_id=612052](http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612052)

### Strategiepapiere anderer EU-Datenschutzbehörden,

1. **Irland:**

Personal Data Security Breach Code of Practice [Verhaltenskodex für Datenschutzverletzungen], 9. Juli 2011

[https://www.dataprotection.ie/docs/Data\\_Security\\_Breach\\_Code\\_of\\_Practice/1082.htm](https://www.dataprotection.ie/docs/Data_Security_Breach_Code_of_Practice/1082.htm)

2. **Vereinigtes Königreich:**

a. **Berichterstattung über Verletzungen des Schutzes personenbezogener Daten**

<https://ico.org.uk/for-organisations/resources-and-support/getting-ready-for-the-gdpr-resources/pdb/>

3. **Leitlinien zur Verwaltung von Datenschutzverletzungen:**

[https://ico.org.uk/media/for-organisations/documents/1562/guidance\\_on\\_data\\_security\\_breach\\_management.pdf](https://ico.org.uk/media/for-organisations/documents/1562/guidance_on_data_security_breach_management.pdf)

#### **Italien**

Datenschutzverletzung gemäß der DSGVO

<http://www.garanteprivacy.it/regolamentoue/approccio-basato-sul-rischio-e-misure-di-accountability-responsabilizzazione-di-titolari-e-responsabili>

### Dokumente und Referenzen der Agentur der Europäischen Union für Netz- und Informationssicherheit (ENISA):

4. **Empfehlungen für eine Methodik zur Bewertung der Schwere von Verletzungen des Schutzes personenbezogener Daten**

<https://www.enisa.europa.eu/publications/dbn-severity>

5. **Empfehlungen für die technische Umsetzung von Artikel 4**

[https://www.enisa.europa.eu/publications/art4\\_tech](https://www.enisa.europa.eu/publications/art4_tech)

6. **Instrument für die Meldung von Verletzungen des Schutzes personenbezogener Daten**

<https://www.enisa.europa.eu/topics/data-protection/personal-data-breaches/personal-data-breach-notification-tool>

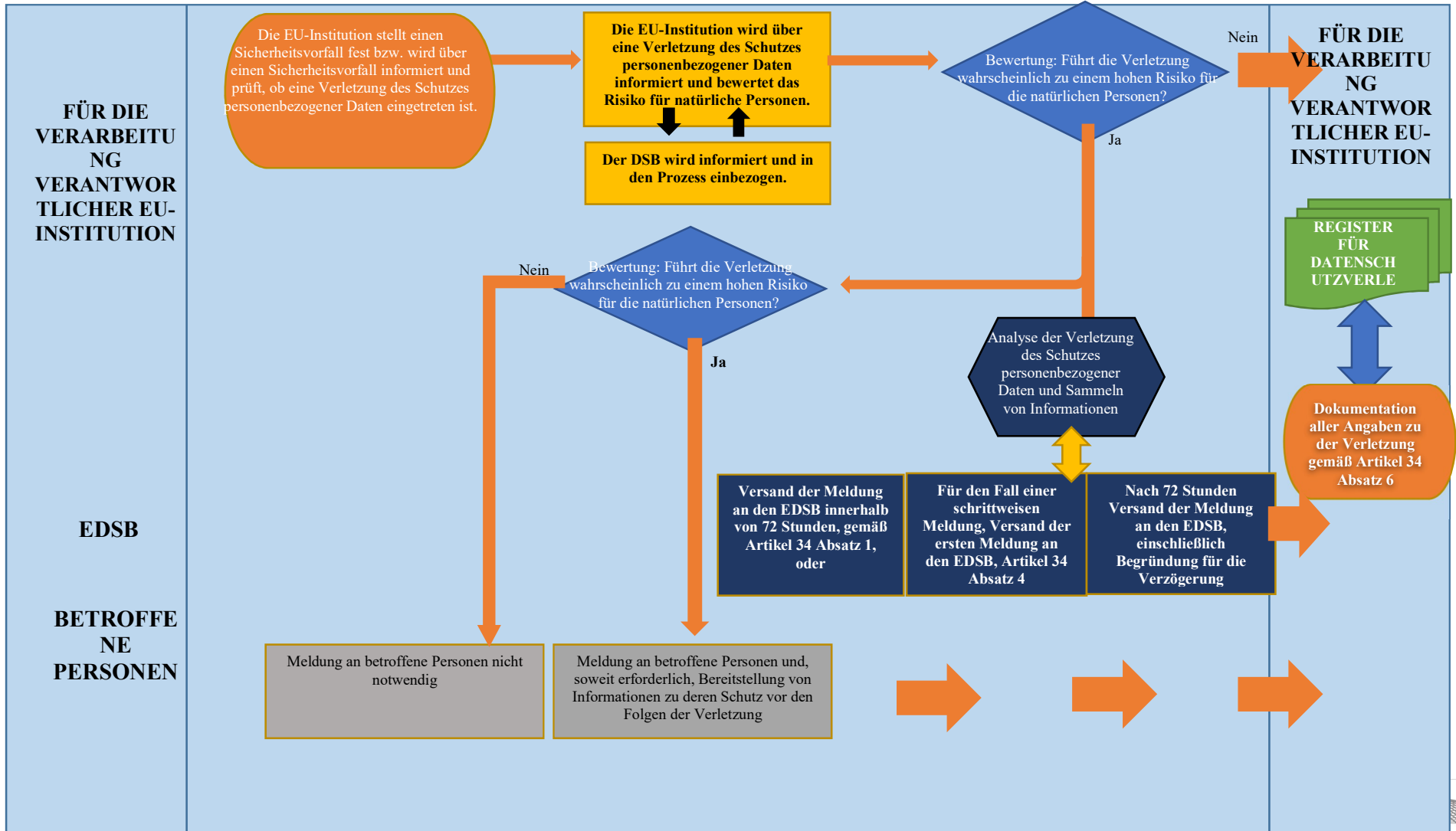
## Anhang 4. Glossar

Begriff	Beschreibung
<b>Authentifizierung</b>	Der Prozess zur Sicherstellung und Bestätigung der Identität eines Benutzers oder einer Maschine, die einen Vorgang durchführt (in der Regel über ein IT-System).
<b>Personenbezogene Daten</b>	Alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person (im Folgenden „betroffene Person“) beziehen; als identifizierbar wird eine natürliche Person angesehen, die direkt oder indirekt, insbesondere mittels Zuordnung zu einer Kennung wie einem Namen, zu einer Kennnummer, zu Standortdaten, zu einer Online-Kennung oder zu einem oder mehreren besonderen Merkmalen, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind, identifiziert werden kann.
<b>Verletzung des Schutzes personenbezogener Daten</b>	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.
<b>Besondere Kategorien (personenbezogener Daten)</b>	Gemäß der geltenden Verordnung die Daten, aus denen die rassische oder ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen oder die Gewerkschaftszugehörigkeit hervorgehen, sowie Gesundheitsdaten oder Daten zum Sexualleben. In dem Vorschlag für eine neue Verordnung werden genetische Daten und biometrische Daten zur eindeutigen Identifizierung einer natürlichen Person hinzugefügt.  Diese Kategorien unterliegen besonderen Vorschriften.
<b>Für die Verarbeitung Verantwortlicher</b>	Das Organ oder die Einrichtung der Gemeinschaft, die Generaldirektion, das Referat oder jede andere Verwaltungseinheit, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung personenbezogener Daten entscheidet.
<b>Auftragsverarbeiter</b>	Eine natürliche oder juristische Person, Behörde, Einrichtung oder jede andere Stelle, die personenbezogene Daten im Auftrag des für die Verarbeitung Verantwortlichen verarbeitet.
<b>Unterauftragsverarbeiter</b>	Eine natürliche oder juristische Person, Behörde, Einrichtung oder jede andere Stelle, die im Auftrag eines Auftragsverarbeiters personenbezogene Daten verarbeitet.
<b>Datenschutzbeauftragter (DSB)</b>	Ein Mitarbeiter einer Organisation, der mit der Unterstützung der Organisation bei der Einhaltung des

	geltenden Datenschutzrechts betraut ist. Ernennung, Aufgaben und Befugnisse sind in der Verordnung (und der neuen Verordnung) geregelt. Es kann sich um eine externe oder eine von verschiedenen Instituten gemeinsam eingesetzte Person handeln.
<b><i>Betroffene Person</i></b>	Natürliche Person, deren personenbezogene Daten verarbeitet werden.
<b><i>Datenschutz-Folgenabschätzung (DSFA)</i></b>	Bewertung der Risiken für die Rechte und Freiheiten natürlicher Personen aufgrund der Verarbeitung ihrer personenbezogenen Daten. In der neuen Verordnung sind Elemente und Umstände vorgesehen, bei deren Vorliegen eine Datenschutz-Folgenabschätzung obligatorisch ist. Dennoch können die für die Verarbeitung Verantwortlichen auch über diese Umstände hinaus eine solche Bewertung durchführen und den entsprechenden Nutzen daraus ziehen.
<b><i>Risiko</i></b>	Im Rahmen des Datenschutzes kann ein Risiko als die Auswirkungen möglicher Ereignisse auf personenbezogene Daten, die der Privatsphäre des Auftraggebers angehören, definiert werden, und es ist durch das Ausmaß der Folgen und ihre Eintrittswahrscheinlichkeit gekennzeichnet.
<b><i>Risikobewertung</i></b>	Gesamtprozess der Risikoidentifikation, Risikoanalyse und Risikobeurteilung.
<b><i>Informationssicherheits-Risikomanagement (ISRM)</i></b>	Der Risikomanagementprozess zur Sicherstellung, dass die Vertraulichkeit, Integrität und Verfügbarkeit von Vermögenswerten einer Organisation den Zielen der Organisation entsprechen.
<b><i>Vertraulichkeit</i></b>	Die Informationen werden weder unbefugten Personen oder Stellen noch im Rahmen unrechtmäßiger Verarbeitungsprozesse zugänglich gemacht oder mitgeteilt.
<b><i>Integrität</i></b>	Genauigkeit und Vollständigkeit.
<b><i>Verfügbarkeit</i></b>	Die Informationen sind auf Anfrage einer befugten Stelle verfügbar und nutzbar.
<b><i>Meldung von Verletzungen des Schutzes personenbezogener Daten (von Datenschutzverletzungen)</i></b>	Obligatorische Meldung von Verletzungen des Schutzes personenbezogener Daten (von Datenschutzverletzungen) an die Datenschutzbehörde.
<b><i>Höhe des Risikos</i></b>	Ausmaß eines Risikos im Hinblick auf seine Folgen und deren Wahrscheinlichkeit.

# Anhang 5. Kurze Zusammenfassung

## A. Flussdiagramm zu den Meldepflichten der EU-Institutionen bei Datenschutzverletzungen



**Zu beachten:**

**FUNKTIONALES POSTFACH DES EDSB FÜR MELDUNGEN VON VERLETZUNGEN DES SCHUTZES PERSONENBEZOGENER DATEN**

[data-breach-notification@edps.europa.eu](mailto:data-breach-notification@edps.europa.eu)

Nicht jeder Informationssicherheitsvorfall stellt eine Verletzung des Schutzes personenbezogener Daten dar, jede Verletzung des Schutzes personenbezogener Daten stellt jedoch einen Informationssicherheitsvorfall dar.

Bei der Bewertung jedes gemeldeten Vorfalls sollte ermittelt werden, ob personenbezogene Daten betroffen sind.

Wenn personenbezogene Daten betroffen sind, wird der Sicherheitsvorfall als Verletzung des Schutzes personenbezogener Daten betrachtet.

Wenn der Sicherheitsvorfall als Verletzung des Schutzes personenbezogener Daten betrachtet wird, sollte im nächsten Schritt bewertet werden, welche Auswirkungen der Vorfall auf die Rechte und Freiheiten natürlicher Personen hätte.

Eine EU-Institution sollte einen notwendigen Schritt in ihren Prozess zur Verwaltung von Sicherheitsvorfällen einführen, bei dem für jeden gemeldeten Sicherheitsvorfall geprüft wird, ob personenbezogene Daten betroffen sind, um auf diese Weise den Eintritt einer Verletzung des Schutzes personenbezogener Daten festzustellen, die den Prozess zur Verwaltung von Datenschutzverletzungen auslöst.

Eine EU-Institution setzt ihr eigenes Verfahren für die Verwaltung von Verletzungen des Schutzes personenbezogener Daten oder ihre eigenen Richtlinien um, die auf die Folgenabschätzung für jede gemeldete Verletzung des Schutzes personenbezogener Daten sowie auf die Auswahl des angemessenen Verfahrens für die Meldung an den EDSB und die betroffenen Personen ausgerichtet sind. Rollen und Zuständigkeiten müssen eindeutig festgelegt sein.

In Fällen, in denen durch eine gemeldete Verletzung des Schutzes personenbezogener Daten nachweislich kein Risiko für die betroffenen Personen entsteht, muss der für die Verarbeitung Verantwortliche weder den EDSB noch die betroffenen Personen benachrichtigen. Diese Entscheidung sollte jedoch gut dokumentiert werden.

Gemäß Artikel 34 der Verordnung sollte eine EU-Institution dem Europäischen Datenschutzbeauftragten eine Verletzung des Schutzes personenbezogener Daten innerhalb von **72 Stunden** melden, es sei denn, die Verletzung führt voraussichtlich nicht zu einem **Risiko** für die Rechte und Freiheiten natürlicher Personen.

Gemäß Artikel 35 Absatz 1 sollten die EU-Institutionen zudem auch die betroffenen Personen von der Verletzung benachrichtigen, falls die Verletzung des Schutzes personenbezogener Daten zu einem „**hohen Risiko**“ für die Rechte und Freiheiten natürlicher Personen führt.

Die Schwere der Verletzungen muss im Einzelfall bewertet werden. Das „Risiko für die Rechte und Freiheiten natürlicher Personen“ sollte als Erwägungsgrundlage herangezogen werden.

Die im Rahmen der Datenschutz-Folgenabschätzung ermittelten Risiken können den für die Verarbeitung Verantwortlichen bei der Bewertung des Risikos helfen. Es ist sehr wahrscheinlich, dass Datenschutzverletzungen bei Verarbeitungstätigkeiten, für die vorab eine Datenschutz-Folgenabschätzung gemäß Artikel 39 der Verordnung durchgeführt werden musste, zu einem höheren Risiko für die Rechte natürlicher Personen führen können und stärkere Auswirkungen auf die natürlichen Personen haben können.

Eine EU-Institution sollte dem Europäischen Datenschutzbeauftragten eine Verletzung des Schutzes personenbezogener Daten innerhalb von 72 Stunden melden, es sei denn, die Verletzung führt voraussichtlich nicht zu einem Risiko für die Rechte und Freiheiten natürlicher Personen. Wenn die Verletzung des Schutzes personenbezogener Daten zu einem „hohen Risiko“ für die Rechte und Freiheiten natürlicher Personen führt, sollte eine EU-Institution auch die betroffenen Personen von der Verletzung benachrichtigen.

Wenn keine Sicherungskopie der Daten existiert und Dienste nicht wiederhergestellt werden können, könnte dies als Verletzung des Schutzes personenbezogener Daten betrachtet werden.

Wenn personenbezogene Daten bereits öffentlich zugänglich sind, stellt die Freigabe der gleichen Daten durch Dritte kein Risiko für natürliche Personen dar und wird nicht als Verletzung des Schutzes personenbezogener Daten betrachtet.

Die EU-Institutionen müssen ein internes Verzeichnis für Verletzungen einrichten, in dem alle Umstände im Zusammenhang mit der Verletzung des Schutzes personenbezogener Daten, deren Auswirkungen und die ergriffenen Abhilfemaßnahmen erfasst sind. Dieses Verzeichnis könnte das bestehende Register für IT-Sicherheitsvorfälle ergänzen.

