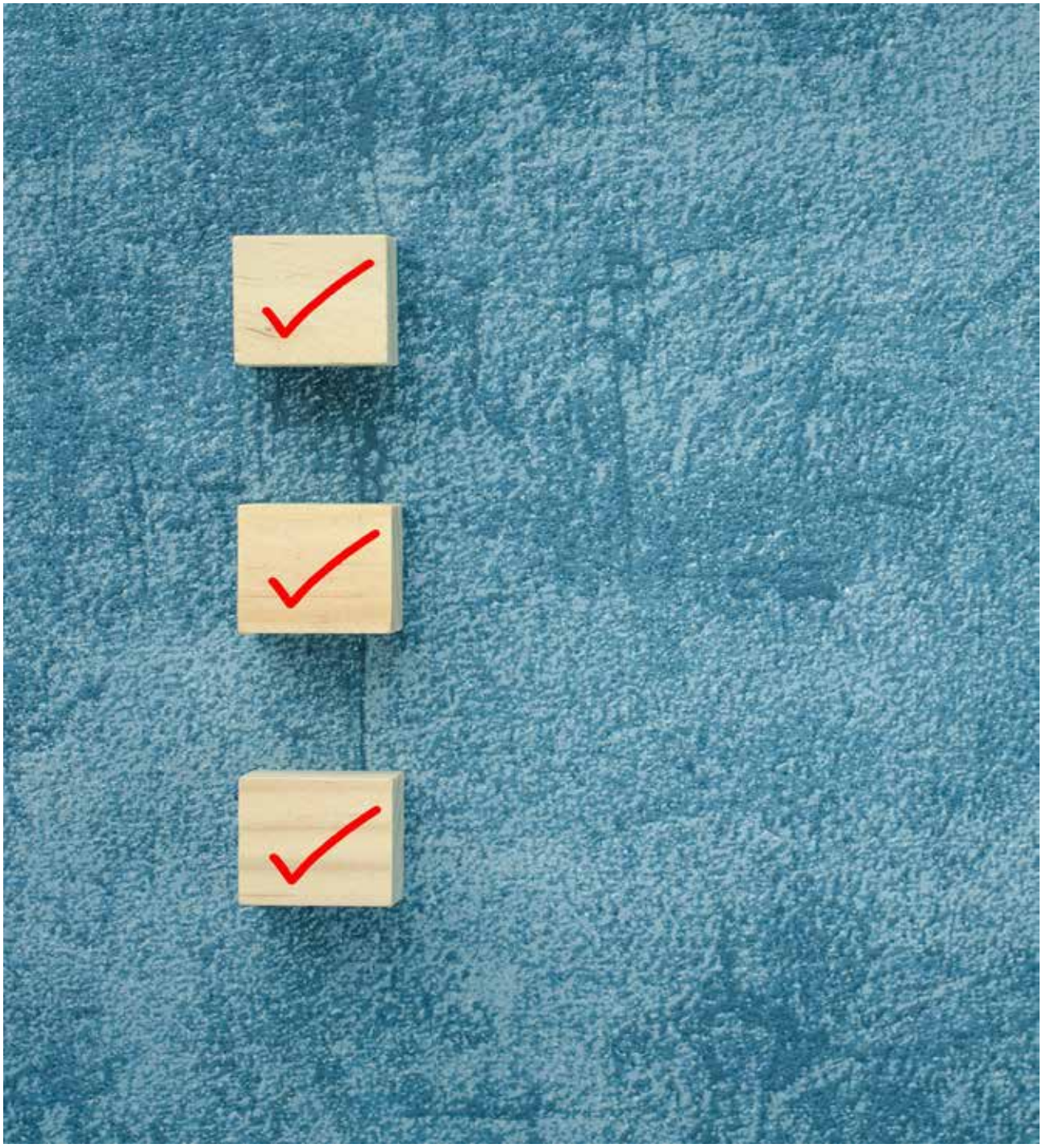
GDD-Praxishilfe

Checkliste „Meldung von Datenschutzverletzungen nach Art. 33, 34 DS-GVO“



INHALT

Vorwort 3

I. Einleitung 4

II. Meldepflichten an die Aufsichtsbehörde nach Art. 33 DS-GVO 4

1. Schutzverletzung und Risiko der Beeinträchtigung 4

2. Bestehen eines Risikos für die Rechte und Freiheiten natürlicher Personen 5

3. Inhalt, Form und Frist der Meldung 6

a. Inhalt 7

b. Form 7

c. Frist 7

4. Meldepflichtiger 8

5. Dokumentationspflicht 8

III. Benachrichtigung der betroffenen Person gem. Art. 34 DS-GVO 8

1. Schutzverletzung 9

2. Bestehen eines Risikos 9

3. Inhalt, Form und Frist der Meldung 9

a. Inhalt 9

b. Form 9

c. Frist 10

4. Meldepflichtiger 10

5. Ausnahmen 10

6. Dokumentation 11

IV. EDSA-Fallgruppen 11

1. Ransomware-Angriffe 11

2. Daten-Exfiltrations-Angriffe 12

3. Menschliches Fehlverhalten 13

4. Verlorene oder gestohlene Geräte und Papierdokumente 14

5. Fehlversand personenbezogener Informationen 14

6. Social Engineering, insb. Phishing Attacken 15

7. Zusammenfassung 15

Vorwort

Datenschutzverletzungen stellen Unternehmen und Organisationen vor immense Herausforderungen. Sie erfordern schnelles Handeln, präzise Analysen und die Einhaltung strikter gesetzlicher Vorgaben. Mit den Regelungen der Art. 33 und 34 DS-GVO gibt die Datenschutz-Grundverordnung Vorgaben für die Meldung von Datenschutzverletzungen, um die Rechte und Freiheiten der Betroffenen zu schützen.

Die GDD-Praxishilfe Checkliste „Meldung von Datenschutzverletzungen nach Art. 33, 34 DS-GVO“ bietet Verantwortlichen eine Unterstützung bei der Umsetzung dieser komplexen Anforderungen. Sie liefert praxisorientierte Erläuterungen zu den Voraussetzungen und Verfahren der Meldepflichten und ergänzt diese durch anschauliche Fallbeispiele aus der Praxis. Ziel ist es, Verantwortlichen die notwendige Orientierung zu geben, um Datenschutzvorfälle korrekt einzuordnen und geeignete Maßnahmen zu ergreifen.

I. Einleitung

Die Datenschutz-Grundverordnung (DS-GVO) stellt im europäischen Datenschutzrecht zentrale Regelungen zum Schutz personenbezogener Daten auf. In den Art. 33 und 34 der DS-GVO sind die Meldepflichten im Falle von Datenschutzverletzungen verankert. Diese Vorschriften sollen sicherstellen, dass bei einer Verletzung des Schutzes personenbezogener Daten schnell und effektiv reagiert wird, um den potenziellen Schaden für betroffene Personen zu minimieren. Art. 33 DS-GVO verpflichtet den Verantwortlichen, jede Verletzung des Schutzes personenbezogener Daten unverzüglich der zuständigen Aufsichtsbehörde zu melden, sofern die Verletzung ein Risiko für die Rechte und Freiheiten der betroffenen Personen darstellt. Art. 34 DS-GVO sieht darüber hinaus vor, dass der Verantwortliche die betroffenen Personen direkt zu informieren hat, wenn ein hohes Risiko für ihre Rechte und Freiheiten besteht. Diese Meldepflichten sind ein wichtiger Bestandteil des präventiven Datenschutzmanagements und dienen der Transparenz sowie dem Schutz der betroffenen Personen vor Missbrauch ihrer Daten.

Die nachfolgende Praxishilfe befasst sich umfassend mit den Voraussetzungen, die eine Meldepflicht auslösen. Im Anschluss wird sodann auf konkrete Beispiele des Europäischen Datenschutzausschusses (EDSA) eingegangen[1]. Diese Beispiele verdeutlichen, in welchen Situationen eine Meldepflicht besteht und wie die Risikobewertung in der Praxis erfolgen kann. Sie bieten den Verantwortlichen wertvolle Orientierungshilfen, um Datenschutzvorfälle korrekt einzuordnen und entsprechende Maßnahmen zu ergreifen.

II. Meldepflichten an die Aufsichtsbehörde nach Art. 33 DS-GVO

Nach der Vorschrift des Art. 33 Abs. 1 S. 1 DS-GVO hat der Verantwortliche eine Verletzung des Schutzes personenbezogener Daten unverzüglich und möglichst binnen 72 Stunden nach Bekanntwerden an die Aufsichtsbehörde zu melden, sofern durch diese Verletzung ein Risiko für die Rechte und Freiheiten natürlicher Personen nicht ausgeschlossen werden kann. Demnach hat eine Meldung an die Aufsichtsbehörden regelmäßig dann nicht zu erfolgen, wenn bereits keine Verletzung des Schutzes personenbezogener Daten besteht oder diese Verletzung kein Risiko der Beeinträchtigung der Rechte der Betroffenen befürchten lässt. Nachfolgend soll ein Überblick gegeben werden, in welchen Fällen eine Verletzung des Schutzes personenbezogener Daten anzunehmen ist, wann diese ein Risiko für die Rechte und Freiheiten der Betroffenen begründet, wer meldepflichtig ist und in welcher Gestalt eine Meldung an die Aufsichtsbehörde zu erfolgen hat. Während eine Leitlinie übergeordnete Zielsetzungen beschreibt, die ein Unternehmen, eine Behörde oder ein Verein im Datenschutz verfolgen, werden Datenschutz-Richtlinien konkret regelsetzend. Richtlinien geben einen konkreten Rahmen vor, der wiederum, falls erforderlich, in Arbeitsanweisungen oder Prozessbeschreibungen detailliert werden kann.

1. Schutzverletzung und Risiko der Beeinträchtigung

Die Meldung an die Aufsichtsbehörde wird zunächst durch die Verletzung des Schutzes personenbezogener Daten nebst Ergebnis einer Risikobewertung ausgelöst.[2] In Art. 4

1 EDSA-Leitlinien 01/2021 zu Beispielen für die Meldung von Verletzungen des Schutzes personenbezogener Daten, Angenommen am 14. Dezember 2021 Version 2.0.

2 Franck, GDD-Ratgeber Datenpannen, Melde- und Benachrichtigungspflichten nach der DS-GVO, 3. Aufl. 2021 (Franck, GDD-Ratgeber Datenpannen), S. 34.

Nr. 12 DS-GVO wird die „Verletzung des Schutzes personenbezogener Daten“ legaldefiniert als „eine Verletzung der Datensicherheit, die 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”. Der EDSA unterscheidet drei Gruppen von Schutzverletzungen: **„Verletzung der Verfügbarkeit“, „Verletzung der Integrität“ und „Verletzung der Vertraulichkeit“**.[3]

Die Legaldefinition aus Art. 4 Nr. 12 DS-GVO nimmt Bezug auf unterschiedliche Verletzungserfolge. Die **Vernichtung, der Verlust und die Veränderung** der personenbezogenen Daten beziehen sich unmittelbar auf die Schutzziele **Integrität und Verfügbarkeit** gem. Art. 32 Abs. 1 lit. b) und c) DS-GVO. **Vernichtung** meint dabei die Zerstörung des Datenträgers unabhängig von der Speichermethode. Unter **Verlust** fallen die Löschung sowie die Nichtauffindbarkeit, wobei die Art des Löschens nicht von Belang ist. Entscheidend ist, dass die Verfügbarkeit der Daten beeinträchtigt wurde.[4] Unter der **Veränderung** der Daten wird die Verfälschung der gespeicherten Informationen verstanden. Hierbei bleiben die Datenfelder oder Dokumente zwar bestehen, erfahren jedoch eine inhaltliche Veränderung. Sind die Daten verändert worden und sind die Ursprungsdaten nicht wiederherstellbar, ist bezüglich dieser zugleich ein Verlust eingetreten, wodurch sich ggf. Risiken addieren.[5]

Die zweite Kategorie betrifft den **Vertraulichkeitsschutz**. Nach der Legaldefinition des Art. 4 Nr. 12 DS-GVO fallen hierunter die **unbefugte Offenlegung von** sowie der **unbefugte Zugang zu personenbezogenen Daten**. Bei der unbefugten Offenlegung handelt es sich um die Weitergabe personenbezogener Daten durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung. Ein unbefugter Zugang liegt bei einer unmittelbaren Einsichtnahme oder Abrufmöglichkeit vor, unabhängig davon, ob der Zugriff bewusst durch den Verantwortlichen gewährt wurde oder dieser eigenmächtig durch den Zugreifenden erfolgt (Hacker-Angriff o.ä.).[6] Die Vorschriften der Art. 33, 34 DS-GVO setzen – anders als die Vorgängerreglung des § 42a BDSG a.F. – hinsichtlich der **Verletzung der Vertraulichkeit** keine unrechtmäßige Kenntnisnahme durch einen **Dritten** voraus. Daraus folgt, dass eine Schutzverletzung i.S.v. Art. 4 Nr. 12 DS-GVO auch dann zu bejahen sein dürfte, wenn ein Mitarbeiter des Verantwortlichen außerhalb seiner Zuständigkeiten oder zu privaten Zwecken Zugriff auf personenbezogene Daten erhält.[7]

2. Bestehen eines Risikos für die Rechte und Freiheiten natürlicher Personen

Die Meldung an die Aufsichtsbehörde hat gem. Art. 33 Abs. 1 DS-GVO bei der Verletzung des Schutzes personenbezogener Daten zu erfolgen, **es sei denn**, dass die Verletzung des Schutzes personenbezogener Daten nicht zu einem Risiko für die Rechte und Freiheiten natürlicher Personen führt. Ob ein derartiges Risiko tatsächlich droht, ist auf Grundlage einer Gefahrenprognose im konkreten Einzelfall durch den Verantwortlichen zu ermitteln. Dieser Prognoseentscheidung sind insbesondere die Art der betroffenen Daten (**abstraktes Missbrauchsrisiko**) und die konkreten potenziellen Auswirkungen der Datenschutzverlet-

3 EDSA-Leitlinien 01/2021 zu Beispielen für die Meldung von Verletzungen des Schutzes personenbezogener Daten, Angenommen am 14. Dezember 2021 Version 2.0, S. 6 f., Franck, GDD-Ratgeber Datenpannen, S. 36.
4 Franck, GDD-Ratgeber Datenpannen, S. 36.
5 Franck, GDD-Ratgeber Datenpannen, S. 36.
6 Franck, GDD-Ratgeber Datenpannen, S. 36.
7 Gola/Heckmann/Reif, 3. Aufl. 2022, DS-GVO Art. 33 Rn. 35.

zung (**konkretes Missbrauchsrisiko**) zugrunde zu legen.[8] Hinsichtlich des konkreten Risikos kann beispielsweise berücksichtigt werden, ob es sich um einen vorsätzlichen Angriff auf die Systeme des Verantwortlichen handelt oder um einen Fall, in dem ein Mitarbeiter aufgrund unachtsamen Fehlverhaltens Daten herausgibt, ob der Datenempfänger bekannt ist und den Verantwortlichen möglicherweise selbst über den Vorfall unterrichtet hat und ob sich der Verantwortliche als lohnendes Ziel derartiger Angriffe darstellt.[9] Beurteilt der Verantwortliche das Risiko fehlerhaft, droht ein Bußgeld gem. Art. 83 Abs. 4 lit. a) DS-GVO. Zur Korrektheit der Beurteilung ist ausschließlich das Wissen von Belang, welches zum Zeitpunkt der Prognose bereits vorliegt.[10] Aus ErwG 85 DS-GVO ergibt sich, dass der Verantwortliche für den Fall, dass er nicht in der Lage ist, festzustellen, ob ein Risiko vorliegt (**non liquet**), zur Meldung an die Aufsichtsbehörde verpflichtet ist.[11] Im Rahmen von Art. 33 Abs. 1 DS-GVO stellt die Meldung des Verantwortlichen an die Behörde den Regelfall dar und ist nur ausnahmsweise nicht zu tätigen. Diese Beweislastumkehr (**„es sei denn"**) kann allerdings nicht dazu führen, dass jede Verletzung unabhängig von der Beurteilung des ihr innewohnenden Risikos gemeldet wird, da Art. 33 Abs. 3 lit. c) DS-GVO die Beschreibung der wahrscheinlichen Folgen verlangt.[12] Zu berücksichtigen sind als Risiken für die Rechte und Freiheiten natürlicher Personen alle drohenden physischen, materiellen oder immateriellen Schäden. ErwG 85 DS-GVO nennt hier insbesondere den Verlust der Kontrolle über die personenbezogenen Daten oder die Einschränkung der Rechte, Diskriminierung, Identitätsdiebstahl oder -betrug, finanzielle Verluste, unbefugte Aufhebung der Pseudonymisierung, Rufschädigung, Verlust der Vertraulichkeit von Daten, die dem Berufsgeheimnis unterliegen, oder andere erhebliche wirtschaftliche oder gesellschaftliche Nachteile. Nach dem EDSA ist die Schwere der möglichen Folgen für die Rechte und Freiheiten der betroffenen Personen verbunden mit der Wahrscheinlichkeit des Eintritts dieser Folgen zu prüfen. Mit zunehmender Schwere sowie mit steigender Eintrittswahrscheinlichkeit steige dabei das Risiko einer Datenschutzverletzung.[13] In Zweifelsfällen ist nach dem EDSA sicherheitshalber eine Meldung an die Aufsichtsbehörde vorzunehmen.[14] Die Meldepflicht aus Art. 33 DS-GVO bezieht sich schließlich auch auf irreversible Schäden, die bei der betroffenen Person aufgrund einer Datenschutzverletzung eingetreten ist.[15] Denn Ziel der Meldepflicht ist die Vermeidung bzw. Minimierung von aus der Datenschutzverletzung resultierenden Folgeschäden.[16] Bei bereits eingetretenen Schäden bleibt eine Vertiefung des Schadens denkbar. Außerdem ist nicht einleuchtend, wieso eine Aufsichtsbehörde über Fälle noch nicht eingetretener Beeinträchtigungen zu unterrichten wäre, während tatsächliche Schadensfälle der Behörde vorenthalten werden dürften.[17]

3. Inhalt, Form und Frist der Meldung

Hinsichtlich des Inhalts und der Form der Meldung gibt es für die Verantwortlichen einige wesentliche Aspekte zu beachten.

8 Gola/Heckmann/Reif, 3. Aufl. 2022, DS-GVO Art. 33 Rn. 45.
9 Gola/Heckmann/Reif, 3. Aufl. 2022, DS-GVO Art. 33 Rn. 45.
10 Franck, GDD-Ratgeber Datenpannen, S. 42.
11 Franck, GDD-Ratgeber Datenpannen, S. 41 f.
12 Franck, GDD-Ratgeber Datenpannen, S. 42.
13 Vgl. auch die Risikomatrix der DSK im Kurzpapier Nr. 18: Risiko für die Rechte und Freiheiten natürlicher Personen (Stand 26.04.2018), S. 5; Gola/Heckmann/Reif DS-GVO Art. 33 Rn. 49.
14 Artikel-29-Datenschutzgruppe, WP 250 rev.01 (Stand 06.02.2018), S. 30 f., bestätigt durch den EDSA am 25.05.2018; Gola/Heckmann/Reif, 3. Aufl. 2022, DS-GVO Art. 33 Rn. 49.
15 Franck, GDD-Ratgeber Datenpannen, S. 41.
16 Gola/Heckmann/Reif, 3. Aufl. 2022, DS-GVO Art. 33 Rn. 2.
17 Franck, GDD-Ratgeber Datenpannen, S. 41.

a. Inhalt

Aus Art. 33 Abs. 3 lit. a) – d) DS-GVO ergibt sich der Mindestinhalt für Meldungen an die Aufsichtsbehörde. Demnach hat die Meldung zumindest folgende Informationen zu enthalten:

- eine Beschreibung der Art der Verletzung des Schutzes personenbezogener Daten (soweit möglich auch mit Angabe der Kategorien und der ungefähren Zahl der betroffenen Personen, der betroffenen Kategorien und der ungefähren Zahl der betroffenen personenbezogenen Datensätze);
- den Namen und die Kontaktdaten des Datenschutzbeauftragten oder einer sonstigen Anlaufstelle für weitere Informationen;
- eine Beschreibung der wahrscheinlichen Folgen der Verletzung des Schutzes personenbezogener Daten;
- 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.

b. Form

Eine konkrete Vorgabe hinsichtlich der Form der Meldung trifft Art. 33 DS-GVO im Gegensatz zu Art. 34 i.V.m. Art. 12 Abs. 1 S. 2 und 3 DS-GVO nicht. Die Aufsichtsbehörden sind demnach nicht verpflichtet, gesicherte elektronische Mittel für die Zustellung der Meldungen zur Verfügung zu stellen.[18] In Anbetracht der 72-Stunden-Frist dürfte sich der Postweg allerdings als ungeeignet darstellen.[19] Die Aufsichtsbehörden bieten Online-Meldeformulare an, über die eine entsprechende Meldung erfolgen kann.[20] Die Meldung hat regelmäßig in der Amtssprache der Aufsichtsbehörde zu erfolgen, an die gemeldet wird.

c. Frist

Die Meldefrist von 72 Stunden beginnt gem. Art. 33 Abs. 1 S. 1 DS-GVO mit Bekanntwerden der Datenschutzverletzung durch den Verantwortlichen. Hierfür ist zumindest erforderlich, dass Informationen hinsichtlich der Verletzung in die Sphäre des Verantwortlichen gelangen, wobei hier die Grundsätze der Wissensvertretung i.S.v. § 166 Abs. 1 BGB analog anzuwenden sind. Auftragsverarbeiter zählen nicht zu den Wissensvertretern des Verantwortlichen, was sich unmittelbar aus Art. 33 Abs. 2 DS-GVO ergibt, da der Auftragsverarbeiter bei Bekanntwerden einer Datenschutzverletzung an den Verantwortlichen meldet.[21] Bei Bekanntwerden einer unbefugten Offenlegung dürften sich keine großen Probleme ergeben. Bei einem unbefugten Zugang ist der Zeitpunkt des Bekanntwerdens hingegen nicht ohne Weiteres zweifelsfrei feststellbar, da nicht feststeht, ob Dritte unbefugten Zugang zu personenbezogenen Daten erhalten. Bei einem begründeten Verdacht treffen den Verantwortlichen Nachforschungspflichten. Eine Meldepflicht nach Art. 33 Abs. 1 DS-GVO soll dann ausgelöst werden, wenn eine hohe Wahrscheinlichkeit einer Kenntnisnahme durch Dritte besteht, da im Falle geschickter Angreifer, die ihre Spuren bereits verwischt haben, andernfalls eine Meldung trotz hoher Wahrscheinlichkeit der miss-

18 Franck, GDD-Ratgeber Datenpannen, S. 49.

19 Franck, GDD-Ratgeber Datenpannen, S. 49.
20 Eine Übersicht zu den Meldeformularen der einzelnen Aufsichtsbehörden findet sich bei Franck GDD-Ratgeber Datenpannen, S. 100 f.
21 Franck, GDD-Ratgeber Datenpannen, S. 50.

bräuchlichen Verwendung der personenbezogenen Daten ausbliebe.[22]

Die Meldung hat gem. Art. 33 Abs. 1 S. 1 DS-GVO **unverzüglich und möglichst binnen 72 Stunden** zu erfolgen. „Unverzüglich" ist als Hinweis auf § 121 Abs. 1 S. 1 BGB zu verstehen, sodass eine Meldung „ohne schuldhaftes Zögern" zu erfolgen hat. Aufgrund des Wortlauts der Vorschrift des Art. 33 Abs. 1 S. 1 DS-GVO („möglichst") ist in begründeten Ausnahmen eine Überschreitung der 72-Stunden-Frist möglich, vgl. Art. 33 Abs. 1 S. 2 DS-GVO. Hierbei ist jedoch zu beachten, dass eine länger andauernden Sachverhaltsaufklärung nicht ohne Weiteres ein ausreichender Grund für ein Hinauszögern der Meldung, da Art. 33 Abs. 4 DS-GVO die Möglichkeit der schrittweisen Unterrichtung der Aufsichtsbehörde über eine Datenschutzverletzung vorsieht.[23]

4. Meldepflichtiger

Die Meldepflicht kann nur denjenigen treffen, bei dem die Verletzung aufgetreten ist. Demnach muss der Pflichtige die Daten selbst übermittelt, gespeichert oder auf sonstige Weise verarbeitet haben.[24] Adressat der Meldepflicht ist daher regelmäßig der Verantwortliche. In einem Konzern ist die Legaleinheit meldepflichtig, bei der die Datenschutzverletzung aufgetreten ist.[25] Sofern zwei oder mehr Verantwortliche als gemeinsam Verantwortliche i.S.v. Art. 26 DS-GVO handeln, ist jeder von ihnen im Außenverhältnis meldepflichtig. Vertragliche Regelungen über die Zuweisung der Meldepflichten an einen Beteiligten entfalten ausschließlich im Innenverhältnis ihre Wirkung.[26] Die Verpflichtung zur Meldung trifft öffentliche wie private Stellen gleichermaßen. Nicht zur Meldung an die Aufsichtsbehörde verpflichtet sind hingegen die Auftragsverarbeiter. Für diese ergibt sich aus Art. 33 Abs. 2 DS-GVO lediglich eine Pflicht zur Meldung an den Verantwortlichen, der dann wiederum die Meldung an die Aufsichtsbehörde vornimmt.

5. Dokumentationspflicht

Unabhängig von dem mit der Verletzung des Schutzes personenbezogener Daten einhergehenden Risiko ist jede derartige Verletzung intern zu dokumentieren, auch wenn nach einer entsprechenden Abwägung der Risiken eine Meldung an die Aufsichtsbehörde i.S.v. Art. 33 Abs. 1 DS-GVO bzw. die betroffene Person nach Art. 34 Abs. 1 DS-GVO entbehrlich ist.[27]

III. Benachrichtigung der betroffenen Person gem. Art. 34 DS-GVO

Die Vorschrift des Art. 34 DS-GVO regelt die Information der betroffenen Person bei einer Datenschutzverletzung und bildet mit Art. 33 DS-GVO einen Normenkomplex. An die Meldepflicht gegenüber der betroffenen Person sind erhöhte Anforderungen geknüpft, sodass eine derartige Pflicht seltener ausgelöst wird als die Meldepflicht gegenüber der Aufsichtsbehörde nach Art. 33 DS-GVO. Erforderlich für das Auslösen der Meldepflicht an die betroffene Person ist, dass die Verletzung des Schutzes der personenbezogenen Daten voraussichtlich ein **hohes Risiko für persönliche Rechte und Freiheiten** der Betroffenen mit sich bringt. Hierdurch sollen Folgeschäden verhindert bzw. minimiert werden und Unternehmen Anreize gesetzt wer-

22 Franck, GDD-Ratgeber Datenpannen, S. 50 f.
23 Franck, GDD-Ratgeber Datenpannen, S. 51 ff.
24 Franck, GDD-Ratgeber Datenpannen, S. 34.
25 Gola/Heckmann/Reif, 3. Aufl. 2022, DS-GVO Art. 33 Rn. 19.
26 Gola/Heckmann/Reif, 3. Aufl. 2022, DS-GVO Art. 33 Rn. 20.
27 EDSA-Leitlinien 01/2021 zu Beispielen für die Meldung von Verletzungen des Schutzes personenbezogener Daten, Angenommen am 14. Dezember 2021 Version 2.0 (EDSA-Leitlinien zu Meldepflichten), Rn. 1023, Franck GDD-Ratgeber Datenpannen, S. 51 ff.

den, die Datensicherheit voranzutreiben und so präventiv Datenschutzverletzungen vorzubeugen.[28] Zu benachrichtigen ist die betroffene Person i.S.v. Art. 4 Nr. 1 DS-GVO. Im Falle von Minderjährigen wird der gesetzliche Vertreter und im Falle von Betreuungsverhältnissen deren Betreuer benachrichtigt. Bei einem Cyber-Angriff auf ein Online-Banking-Portal kann sich die Meldepflicht zudem auf Kunden beziehen, die von dem Angriff nicht betroffen waren, um ihnen so die Möglichkeit zu eröffnen, ihren Kontoschutz zu überprüfen.[29]

1. Schutzverletzung

Der Begriff der Schutzverletzung deckt sich mit dem aus Art. 33 Abs. 1 DS-GVO.[30] Auslöser der Meldepflicht ist das konkrete Ergebnis der Risikobewertung und nicht bereits das Bekanntwerden einer Schutzverletzung.

2. Bestehen eines Risikos

Hinsichtlich der Einschätzung des Risikos kann auf die Vorgehensweise bei Art. 33 Abs. 1 DS-GVO verwiesen werden.[31] Die Meldepflicht nach Art. 34 Abs. 1 DS-GVO wird allerdings nur bei Bestehen eines „hohen Risikos" für die persönlichen Rechte und Freiheiten natürlicher Personen ausgelöst. Ein solches hohes Risiko soll nach dem EDSA immer dann vorliegen, wenn der Schadenseintritt wahrscheinlich ist.[32] Hingegen sei eine bloß abstrakte Möglichkeit des Schadenseintritts nicht ausreichend.[33] Die Informationspflicht entfällt nicht, sofern ein Schaden bereits eingetreten ist oder die betroffene Person bereits Kenntnis über die Datenschutzverletzung erlangt hat.

3. Inhalt, Form und Frist der Meldung

Grundsätzlich deckt sich die Meldung an die betroffene Person in Art und Umfang der Meldung an die Aufsichtsbehörde nach Art. 33 Abs. 1 DS-GVO.[34]

a. Inhalt

Anzugeben ist insbesondere die **Art der Schutzverletzung**, wobei hier im Gegensatz zur Meldung an die Aufsichtsbehörde nicht allzu tief ins technische Detail gegangen werden muss, da hierunter vor allem die Verständlichkeit für die betroffene Person leiden könnte. Auf die Angabe der Personenkategorien und Zahl der betroffenen Personen i.S.v. Art. 33 Abs. 3 lit. a) DS-GVO kann grds. verzichtet werden, die konkreten Datenkategorien und die Zahl der Datensätze dürften für die jeweilige Risikoeinschätzungen der betroffenen Personen allerdings von Relevanz sein. Im Gegensatz zur Meldung an die Aufsichtsbehörde könnte bei Veränderung, unbefugter Offenlegung oder unbefugtem Zugang die Übermittlung der tatsächlichen inhaltlichen Daten erforderlich sein.[35] Die Empfänger der unbefugten Offenlegung sind nicht von einer Meldung umfasst, könnten im Nachhinein aber von den betroffenen Personen erfragt werden, vgl. Art. 15 Abs. 2 lit. c) DS-GVO.[36] Im Übrigen sind die mitzuteilenden Informationen mit Art. 33 Abs. 3 lit. b), c) und d) DS-GVO identisch.[37]

b. Form

Die Meldung an die betroffene Person hat gem. Art. 12 Abs. 1 S. 2 DS-GVO schriftlich oder in anderer Form (z.B.: elektronisch) zu erfolgen. In Eilfällen ist gem. Art. 12 Abs. 1 S. 2 und 3

28 Gola/Heckmann/Reif, 3. Aufl. 2022, DS-GVO Art. 34 Rn. 1.
29 Franck, GDD-Ratgeber Datenpannen, S. 55 f.
30 Vgl. oben II.1.
31 Vgl. oben II.2.
32 Artikel-29-Datenschutzgruppe, WP 250 Rev. 1 v. 06.02.2018, S. 23.
33 Franck, GDD-Ratgeber Datenpannen, S. 56 f.
34 Vgl. oben II.3.a.
35 Franck, GDD-Ratgeber Datenpannen, S. 61 f.
36 Franck, GDD-Ratgeber Datenpannen, S. 6231, Vgl. oben II.2.
37 Vgl. oben II.3.a.

DS-GVO eine mündliche Unterrichtung möglich, die sodann aber zu dokumentieren ist.[38] Mit der Benachrichtigung der betroffenen Personen darf keine Werbung o.ä. verbunden werden. Briefe sind entsprechend ihrer inhaltlichen Bedeutung, also in einem offiziellen Design, zu halten und nicht wie Werbebriefe auszugestalten, sodass der Empfänger den Charakter der rechtlich erheblichen Information, die dem Brief innewohnt, erkennen kann.[39]

Unter Umständen greift wegen unverhältnismäßigen Aufwands eine Ausnahme nach Art. 34 Abs. 3 lit. c) DS-GVO, wonach eine Benachrichtigung durch öffentliche Bekanntmachung eine ähnliche Maßnahme vorzunehmen ist, z.B. durch Anzeigen in zwei bundesweit erscheinenden Tageszeitungen, die jeweils mindestens eine halbe Seite umfassen, wobei auch regionale Zeitschriften ausreichend sind, wenn sich der Betroffenenkreis entsprechend lokal eingrenzen lässt. Amts- und Verkündigungsblätter sind allerdings regelmäßig mangels einschlägigen Leserkreises ungeeignet.[40] Bei grenzüberschreitenden Verarbeitungen können die nationalen oder regionalen Medien der entsprechenden Mitgliedstaaten bewusst unterrichtet werden, eine Berichterstattung von sich aus reicht nicht aus. Auch die **sozialen Netzwerke/Medien** können genutzt werden, um Datenschutzvorfälle bekannt zu machen. Häufig ist es sinnvoll, die oben genannten Möglichkeiten zu kombinieren, um so möglichst flächendeckend zu informieren.[41]

Die Meldung hat gem. Art. 34 Abs. 2 DS-GVO in klarer und einfacher Sprache zu erfolgen, wobei der Meldepflichtige die Landessprache des Betroffenen, die in der vorherigen Kommunikation mit ihm bereits verwendet wurde, zu wählen hat.[42]

c. Frist

Gem. Art. 34 Abs. 1 DS-GVO hat die Meldung an den Betroffenen **unverzüglich** zu erfolgen, sodass die starre 72-Stunden-Frist aus Art. 33 Abs. 1 DS-GVO keine Anwendung findet. Die Frist beginnt ebenso wie bei Art. 33 Abs. 1 DS-GVO mit Bekanntwerden der Schutzverletzung. Im Sinne eines effektiven Betroffenenschutzes und unter Betrachtung des ErwG 86 DS-GVO ist der Betroffene zwecks Vermeidung größerer Nachteile möglichst frühzeitig zu informieren, auch wenn der Sachverhalt noch nicht in Gänze ausermittelt ist. Es bedarf damit eines gestrafften Risikobewertungsprozesses.[43]

4. Meldepflichtiger

Die Benachrichtigungspflicht trifft ebenso wie bei Art. 33 Abs. 1 DS-GVO den Verantwortlichen. Auch hier bleibt der Auftragsverarbeiter außen vor. Gemeinsam Verantwortliche i.S.v. Art. 26 DS-GVO können intern festlegen, wer die Benachrichtigung vornimmt, im Außenverhältnis sind allerdings beide meldepflichtig. Der Vertreter in der Union i.S.v. Art. 27 DS-GVO kann die Meldung für den Verantwortlichen vornehmen.

5. Ausnahmen

Für bestimmte Konstellationen sieht Art. 34 Abs. 3 DS-GVO Ausnahmen vor, die den Verantwortlichen von einer Meldepflicht an die betroffene Person befreien.

So hat zunächst gem. **Art. 34 Abs. 3 lit. a) DS-GVO** eine Benachrichtigung wegen unbefugter Offenbarung oder unbefugten Zugangs

38 Vgl. oben II.3.a.
39 Franck, GDD-Ratgeber Datenpannen, S. 61 f.
40 Franck, GDD-Ratgeber Datenpannen, S. 63.
41 Franck, GDD-Ratgeber Datenpannen, S. 63 f.
42 Franck, GDD-Ratgeber Datenpannen, S. 64.
43 Franck, GDD-Ratgeber Datenpannen, S. 65 f.

nicht zu erfolgen, wenn der Verantwortliche die Daten durch geeignete technische und organisatorische Maßnahmen für unbefugte unzugänglich gemacht hat, beispielsweise durch Verschlüsselung. Gleichermaßen entfällt gem. **Art. 34 Abs. 3 lit. b) DS-GVO** die Benachrichtigungspflicht des Verantwortlichen, wenn der Verantwortliche durch nachträgliche Maßnahmen sicherstellt, dass ein Risiko aller Wahrscheinlichkeit nach nicht mehr besteht und mit dem Eintritt eines Schadens normalerweise nicht mehr zu rechnen ist, z.B. beim Sperren von Kreditkarten und deren Neuvergabe.[44] Eine Meldung an die Aufsichtsbehörde kann hingegen nicht die Benachrichtigungspflicht an die betroffene Person ersetzen.[45] Zuletzt kann eine individuelle Meldung des Verantwortlichen an die betroffene Person gem. **Art. 34 Abs. 3 lit. c) DS-GVO** unterbleiben, sofern diese mit einem unverhältnismäßigen Aufwand verbunden wäre. Stattdessen kann der Verantwortliche mittels öffentlicher Bekanntmachung seiner Benachrichtigungspflicht gerecht werden. Ob eine individuelle Benachrichtigung unverhältnismäßig ist, kann sich zwar aufgrund einer unbestimmten Personenzahl ergeben. Allerdings sind, sofern ungewiss ist, wer genau von einem Datenschutz betroffen ist, alle potenziell betroffenen Personen zu benachrichtigen.[46] Die ordnungsgem.e öffentliche Bekanntmachung befreit den Verantwortlichen endgültig von seiner Benachrichtigungspflicht in Bezug auf das konkrete meldepflichtige Ereignis.[47]

6. Dokumentation

Wie bereits bei der Meldepflicht nach Art. 33 Abs. 1 DS-GVO ausgeführt, ist jede Verletzung personenbezogener Daten intern zu dokumentieren, unabhängig von dem mit der Verletzung des Schutzes personenbezogener Daten einhergehenden Risikos für die Rechte und Freiheiten der Betroffenen.[48]

IV. EDSA-Fallgruppen

In seinen „Leitlinien 01/2021 zu Beispielen für die Meldung von Verletzungen des Schutzes personenbezogener Daten“ unterscheidet der EDSA zwischen sechs unterschiedlichen Fällen von Datenschutzvorfällen, namentlich Ransomware-Angriffen, Angriffen mit Datenabfluss, Risiken durch internes Personal, Verlust oder Diebstahl von Geräten oder Dokumenten, Datenschutzverletzungen im Zusammenhang mit postalischen Versendungen und „Social Engineering“-Attacken. Insgesamt bildet der EDSA in diesen Leitlinien 18 Fallbeispiele zu den jeweiligen Datenschutzvorfällen.[49] Der EDSA beurteilt nach Schilderung der Sachverhalte, ob Meldungen zu erfolgen haben.

1. Ransomware-Angriffe

Nach Ausführungen des EDSA handelt es sich bei den Ransomware-Angriffen auf datenschutzrechtlich Verantwortliche um eine immer häufigere Ursache für die Meldung von Datenschutzverletzungen. Bei diesen Angriffen verschlüsselt der Angreifer mithilfe einer Schadsoftware personenbezogene Daten und verlangt anschließend ein Lösegeld vom Verantwortlichen im Austausch gegen den Entschlüsselungs-Code. Bei dieser Art von Angriffen werden Daten im Regelfall nicht exfiltriert.[50]

44 Franck, GDD-Ratgeber Datenpannen, S. 58.
45 Franck, GDD-Ratgeber Datenpannen, S. 59.
46 Franck, GDD-Ratgeber Datenpannen, S. 60.
47 Franck, GDD-Ratgeber Datenpannen, S. 60.

48 Vgl. unter II.5.
49 Gola/Heckmann/Reif, 3. Aufl. 2022, DS-GVO Art. 33 Rn. 31; weitere Beispiele aus den Tätigkeitsberichten der nationalen Aufsichtsbehörden finden sich in Franck GDD-Ratgeber Datenpanne, S. 34 ff.
50 EDSA-Leitlinien zu Meldepflichten, Rn. 16.

In seinen **Fällen Nr. 01 – 04** geht der EDSA im Rahmen seiner Leitlinien auf unterschiedliche Fallgestaltungen von Ransomware-Angriffen ein.

Im **Fall Nr. 01** wurde ein Fertigungsunternehmen Opfer eines Angriffs, bei dem Daten verschlüsselt wurden, eine Exfilftration hingegen nicht stattfand. Dank moderner Verschlüsselung und verfügbarer Sicherungskopien (Backups) konnten die Daten schnell wiederhergestellt werden, sodass keine Meldung, sondern lediglich eine interne Dokumentation erforderlich war.[51]

Anders im **Fall Nr. 02**: Dort wurden auf dem Computer eines landwirtschaftlichen Unternehmens die Daten von dem Angreifer ebenfalls nur verschlüsselt, nicht hingegen exfiltriert. Allerdings fehlten dem Verantwortlichen entsprechende Backups, was zu einer fünftägigen Wiederherstellung und damit zu betrieblichen Beeinträchtigungen führte, wodurch aufgrund des festgestellten (mittleren) Risikos für die Rechte und Freiheiten natürlicher Personen – neben der internen Dokumentation – eine Meldung an die Aufsichtsbehörde erforderlich war.[52]

Fall Nr. 03 betrifft ein Krankenhaus, in dem Patientendaten bei einem Ransomware-Angriff zwar verschlüsselt, nicht hingegen exfiltriert wurden. Trotz Backups führte allerdings eine zweitägige Systemwiederherstellung zu erheblichen Verzögerungen in der Patientenversorgung, weshalb sowohl eine Meldung an die Aufsichtsbehörde als auch eine Benachrichtigung an die betroffenen Personen notwendig waren.[53]

Noch schwerwiegender liegt es in **Fall Nr. 04**, bei dem auf den Server eines öffentlichen Verkehrsunternehmens zugegriffen wurde und personenbezogene Daten von Kunden und Mitarbeitern sowie von mehreren Tausend Personen, die die Dienste des Unternehmens in Anspruch nahmen, verschlüsselt und zudem exfiltriert wurden, was sowohl eine Meldung als auch eine Benachrichtigung erforderte, da ein hohes Risiko für Identitätsdiebstahl bestand.[54]

2. Daten-Exfiltrations-Angriffe

Die sog. Daten-Exfiltrations-Angriffe ähneln den Ransomware-Angriffen. Bei diesen nutzt ein dritter ebenfalls Schwachstellen von Diensten aus, die der Verantwortliche über das Internet anbietet. Im Gegensatz zu Ransomware-Angriffen, bei denen der Angreifer kein Interesse an den Daten hat, kommt es ihm bei Daten-Exfiltrations-Angriffen gerade auf das Kopieren, Exfiltrieren und Missbrauchen der entsprechenden persönlichen Informationen zu einem böswilligen Zweck an. Betroffen ist bei dieser Art von Angriffen vordergründig die **Vertraulichkeit** und unter Umständen auch die **Integrität** der betroffenen Daten.[55]

Auf die **Exfiltration von Daten** wird in den **Fällen Nr. 05 – 07** im Rahmen der Leitlinien des EDSA gesondert eingegangen.

So erhielt ein Angreifer in dem unter **Fall Nr. 05** geschilderten Sachverhalt durch die Installation eines Schadcodes auf der Website einer Arbeitsvermittlungsstelle Zugang zu 213 Bewerbungsformularen. Da diese Daten für Identitätsdiebstahl oder gezielte Angriffe genutzt werden könnten und so ein hohes Risiko für die Rechte und Freiheiten der betroffenen Personen bestand, war eine Meldung an die Aufsichtsbehörde sowie eine Benachrichtigung an die Betroffenen notwendig.[56]

51 EDSA-Leitlinien zu Meldepflichten, Rn. 16 ff.
52 EDSA-Leitlinien zu Meldepflichten, Rn. 26 ff.
53 EDSA-Leitlinien zu Meldepflichten, Rn. 36 ff.
54 EDSA-Leitlinien zu Meldepflichten, Rn. 41 ff.
55 EDSA-Leitlinien zu Meldepflichten, Rn. 50.
56 EDSA-Leitlinien zu Meldepflichten, Rn. 51 ff.

Bei **Fall Nr. 06** wurden gehashte Passwörter von 1.200 Nutzern einer Kochwebsite exfiltriert, wobei das Salt[57] nicht beeinträchtigt wurde. Der Verantwortliche informierte vorsichtshalber die Nutzer, die nur beliebige Pseudonyme als Benutzernamen wählen durften, und forderte sie auf, ihre Passwörter zu ändern. Hier sah der EDSA jedoch kein (erhebliches) Risiko für die Rechte und Freiheiten der Betroffenen, sodass weder eine Meldung an die Aufsichtsbehörde noch eine Benachrichtigung der Betroffenen zu erfolgen hatte und eine interne Dokumentation ausreichend war.[58]

Im Gegensatz dazu betrifft **Fall Nr. 07** eine Bank, die Opfer eines Cyber-Angriffs (sog. Credential-Stuffing) wurde. Hierbei waren rund 100.000 Datensubjekte betroffen und der Angreifer verschaffte sich Zugang zu ca. 2.000 Konten, die triviale Passwörter nutzten. Dies stellte ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen dar, sodass eine Meldung an die Aufsichtsbehörde sowie eine Benachrichtigung aller Betroffenen – und nicht nur der 2.000 gehackten Kontoinhaber – erforderlich war.[59]

3. Menschliches Fehlverhalten

Nach Einschätzung des EDSA ist menschlichem Fehlverhalten in Bezug auf Datenschutzverletzungen besondere Bedeutung zuzumessen, da es sehr häufig vorkommt. Für den Verantwortlichen ist derartiges Verhalten schwer zu erkennen und zu verhindern, da es sowohl beabsichtigt als auch unbeabsichtigt vorkommen kann. Hinsichtlich der Rolle menschlichen Versagens verweist der EDSA auf ein Papier der International Conference of Data Protection and Privacy Commissioners (ICDPPC), der heutigen Global Privacy Assembly (GPA), vom Oktober 2019. Dieses enthält eine nicht abschließende Liste von Schutzmaßnahmen, welche ergriffen werden sollten, um menschlichem Versagen weitestgehend vorzubeugen und dieses zu verhindern.[60]

Bei **Fall Nr. 08** kopierte ein Mitarbeiter gezielt Geschäftsdaten, die er nach seiner Kündigung zu eigenen Akquisezwecken nutzte, wovon der Verantwortliche später erfuhr. Der EDSA sah hier zwar ein – wenn auch nur geringes – Risiko für die Rechte und Freiheiten der Betroffenen, hielt jedoch neben der erforderlichen Meldung an die Aufsichtsbehörde eine Benachrichtigung der Betroffenen nicht für erforderlich, da außer der Kontaktaufnahme zu der betroffenen Person kein weiterer Missbrauch der Daten zu befürchten ist.[61]

In Fall **Nr. 09** wurden Kundendaten versehentlich an einen nicht zuständigen Versicherungsvermittler übermittelt, der nicht dem Unternehmen des Verantwortlichen angehörte. Da der Versicherungsvermittler allerdings ein Berufsgeheimnisträger war und die Verletzung aufgrund einer entsprechenden Vereinbarung unmittelbar dem Verantwortlichen meldete sowie die Löschung der Daten vornahm und diese schriftlich bestätigte, lag nach Ansicht des EDSA kein Risiko für die Rechte und Freiheiten natürlicher Personen vor, sodass die bloße interne Dokumentation ausreichend war und keine Meldung an die Aufsichtsbehörde zu erfolgen hatte.[62] Dies wäre unter Umständen anders zu beurteilen, wenn der Empfänger der Daten kein Berufsgeheimnisträger ist.

57 Ein Salt bezeichnet eine zufällige Zeichenfolge, die dem Passwort vor dem Hashing-Prozess zugefügt wird, wodurch der dem jeweiligen Passwort zugeordnete Hash einzigartig ist und eine Entschlüsselung erschwert wird.
58 EDSA-Leitlinien zu Meldepflichten, Rn. 56 ff.
59 EDSA-Leitlinien zu Meldepflichten, Rn. 63 ff.
60 EDSA-Leitlinien zu Meldepflichten, Rn. 71; Gola/Heckmann/Reif, 3. Aufl. 2022, DS-GVO Art. 33 Rn. 4158, EDSA-Leitlinien zu Meldepflichten, Rn. 56 ff.
61 EDSA-Leitlinien zu Meldepflichten, Rn. 71 ff.
62 EDSA-Leitlinien zu Meldepflichten, Rn. 78 ff.

4. Verlorene oder gestohlene Geräte und Papierdokumente

Der Verlust beziehungsweise der Diebstahl von Geräten und Papierdokumenten, auf denen sich personenbezogene Daten befinden, kommt nach Angaben des EDSA sehr häufig vor. Kleinere Datenträger wie USB-Sticks oder Festplatten gehen schnell verloren, Laptops, Handys oder andere EDV-Geräte sind oftmals Gegenstand eines Diebstahls.[63]

Wird, wie in **Fall Nr. 10** geschildert, ein technisches Gerät, auf dem sich personenbezogene Daten befinden, gestohlen, ist eine Meldung sowohl an die Aufsichtsbehörde als auch eine Benachrichtigung der betroffenen Personen mangels bestehenden Risikos entbehrlich, wenn sowohl das Gerät bzw. die App, auf dem/der sich die Daten befinden, als auch die Daten selbst mit einem starken Passwort geschützt sind und darüber hinaus eine Sicherungskopie der Daten vorliegt.[64]

Anders ist es zu beurteilen, wenn, wie in **Fall Nr. 11** dargestellt, das Notebook eines Mitarbeiters eines Dienstleistungsunternehmens gestohlen wird, auf dem sich personenbezogene Daten von über 100.000 Kunden befinden und die Festplatte nicht mit einem Passwort geschützt ist. Hier besteht aufgrund der Verletzung des Schutzes der personenbezogenen Daten ein hohes Risiko für die Rechte und Freiheiten der Betroffenen, sodass sowohl eine Meldung an die Aufsichtsbehörde als auch eine Benachrichtigung der Betroffenen zu erfolgen hat.[65]

Genauso ist bei dem unter **Fall Nr. 12** geschilderten Sachverhalt zu verfahren, wenn aus einer Rehabilitationseinrichtung für Drogenabhängige ein Patientenbuch in Papierform[66], das grundlegende Identitäts- und Gesundheitsdaten der Patienten enthält und von dem keine Sicherungskopie existiert, gestohlen wird.[67]

5. Fehlversand personenbezogener Informationen

Beim Fehlversand personenbezogener Informationen handelt es sich ebenfalls um internes menschliches Versagen, das zur Verletzung des Schutzes personenbezogener Daten führt, wobei diese nicht auf einer böswilligen Handlung des Verletzers beruht. Derartiges Versagen kann im Nachhinein selten rückgängig gemacht werden, sodass in diesen Fällen eine Vorbeugung von immenser Bedeutung ist.[68]

Werden, wie in **Fall Nr. 13** dargestellt, zwei Bestellungen von Schuhen vertauscht und erhalten die beiden Personen jeweils die Bestellung sowie die dazugehörigen Packzettel mit den entsprechenden personenbezogenen Daten des anderen, wird das Risiko für die Rechte und Freiheiten der Betroffenen durch den EDSA als gering eingestuft, sodass keine Meldepflichten für den Verantwortlichen bestehen.[69]

Werden hingegen mittels einer E-Mail höchstpersönliche Daten versehentlich an Dritte versandt, ist eine Meldung an die Aufsichtsbehörde sowie eine Benachrichtigung der Betroffenen durch den Verantwortlichen unerlässlich. Dieser unter **Fall Nr. 14** geschilderte Sachverhalt, bei dem der Verantwortliche eine Liste persönlicher Daten von ca. 60.000 Arbeitssuchenden an jeden dieser Arbeitssuchenden selbst versandte, löste die entsprechenden Pflichten aus.

Eine Melde- und Benachrichtigungspflicht lehnte der EDSA hingegen bei **Fall Nr. 15** ab.

63 EDSA-Leitlinien zu Meldepflichten, Rn. 85 ff.
64 EDSA-Leitlinien zu Meldepflichten, Rn. 88 ff.
65 EDSA-Leitlinien zu Meldepflichten, Rn. 93 ff.
66 Ein papierenes Verzeichnis mit strukturierten Informationen über die Patienten einer Rehabilitationsklinik kann Gegenstand einer Schutzverletzung sein, wohingegen der Verlust von oder der Zugang zu unstrukturierten Akten zwar eine Verarbeitung im Sinne des Art. 4 Nr. 12 DS-GVO darstellt, auf die die DS-GVO insgesamt aber keine Anwendung findet (Art. 2 Abs. 1 DS-GVO), vgl. Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht, DS-GVO Art. 4 Nr. 12 Rn. 6.
67 EDSA-Leitlinien zu Meldepflichten, Rn. 99 ff.
68 EDSA-Leitlinien zu Meldepflichten, Rn. 106.
69 EDSA-Leitlinien zu Meldepflichten, Rn. 106 f.

Hier wurde eine Teilnehmerliste für einen Kurs in englischer Rechtssprache, die Namen, E-Mail-Adressen und Ernährungsvorlieben der Teilnehmer enthielt, versehentlich an 15 ehemalige Teilnehmer gesandt. Auf der Liste hatten zwei Teilnehmer angegeben, dass sie eine Laktoseintoleranz haben. Der Verantwortliche entdeckte den Fehler, informierte die Empfänger und forderte sie auf, die Liste zu löschen. Der EDSA sieht hier nur ein geringes Risiko für die Rechte und Freiheiten der Betroffenen.[70]

Bei **Fall Nr. 16** verschickte eine Versicherungsgruppe durch einen Fehler bei der automatischen Kuvertierung zwei Briefe unterschiedlicher Versicherungsnehmer in einem Umschlag, sodass der Empfänger die Daten eines Dritten (Name, Adresse, Geburtsdatum, Kfz-Kennzeichen und Versicherungstarife) erhält. Der EDSA erachtet das Risiko für die Rechte und Freiheiten des Betroffenen hier als Mittel bis gering ein, da der Missbrauch der Daten zwar unwahrscheinlich ist, dieser aber auch nicht gänzlich ausgeschlossen werden kann, sodass jedenfalls eine Meldung an die Aufsichtsbehörde zu erfolgen hat.[71]

6. Social Engineering, insbes. Phishing Attacken

Das Social Engineering bezeichnet eine moderne Angriffsmethode, bei der neben einem Schadcode, mit dem die Daten verschlüsselt werden, zusätzliche soziale Komponenten ausgenutzt werden, um das Opfer zu einer ungewollten Handlung zu verleiten, die im Sinne des Angreifers durchgeführt wird. Ein Beispiel sind die sog. Phishing-Attacken.[72]

In den **Fällen Nr. 17 und Nr. 18** stellt der EDSA klar, dass Angriffe mittels Social Engineering in der Regel mit einem hohen Risiko für die Rechte und Freiheiten natürlicher Personen einhergehen und die entsprechenden Meldepflichten auslösen.

In **Fall Nr. 17** wurden Rechnungsdaten von einem Mitarbeiter des Verantwortlichen mittels einer E-Mail an eine nicht berechtigte Person weitergegeben, die sich am Telefon unter Verwendung korrekter Daten als die berechtigte Person ausgegeben hatte. Hier waren sowohl eine Meldung an die Aufsichtsbehörde als auch eine Benachrichtigung an die betroffene Person erforderlich.[73]

Gleiches gilt für den **Fall Nr. 18**, bei dem ein Angreifer E-Mail-Konten einer Supermarktkette veränderte und eine schlagwortbasierte Mailweiterleitung an eine externe Mail-Adresse einrichtete. Dadurch erhielt der Angreifer u.a. Zugriff auf Lohndaten von 89 Mitarbeitern.[74]

7. Zusammenfassung

Die Leitlinien des EDSA verdeutlichen, dass jede Datenschutzverletzung sorgfältig anhand der potenziellen Risiken für die Rechte und Freiheiten betroffener Personen bewertet werden muss, um die geeigneten Maßnahmen einzuleiten. Eine pauschale Beurteilung ist – wie so häufig im Datenschutz – nicht möglich. Die – nicht abschließende – Auflistung der Fallgruppen soll dem Verantwortlichen eine grobe Orientierung bieten, die für den konkreten Einzelfall richtigen Entscheidungen zu treffen und so seinen Pflichten aus der DS-GVO gerecht zu werden. Die Fälle der Verantwortlichen werden sich in Zukunft aller Voraussicht nach von denen der Leitlinien unterscheiden, allerdings ist zumindest die grobe Art des jeweiligen Angriffs anhand der Leitlinien nachzuvollziehen.

Hegt der Verantwortliche Zweifel hinsichtlich des Bestehens eines Risikos i.S.d. Art. 33,

70 EDSA-Leitlinien zu Meldepflichten, Rn. 114 ff.
71 EDSA-Leitlinien zu Meldepflichten, Rn. 119 ff.
72 Gola/Heckmann/Reif, 3. Aufl. 2022, DS-GVO Art. 33 Rn. 41
73 EDSA-Leitlinien zu Meldepflichten, Rn. 124 ff.
74 EDSA-Leitlinien zu Meldepflichten, Rn. 129 ff.

34 DS-GVO, sollte er sicherheitshalber eine entsprechende Meldung abgeben.

Am Ende jeder Fallgruppe erfolgt eine nicht abschließende Auflistung von Maßnahmen, die der Verantwortliche je nach Besonderheit des Einzelfalles prüfen und sodann ergreifen sollte, um die Wahrscheinlichkeit einer Verletzung des Schutzes personenbezogener Daten zu verringern.[75]

Hinweis:
Diese Praxishilfe dient der Übersicht zur Meldung von Datenpannen. Weiterführende Informationen enthält der **GDD-Ratgeber „Datenpannen – Melde- und Benachrichtigungspflichten nach DS-GVO und BDSG“**, dessen 4. Auflage sich derzeit in der Vorbereitung befindet.

75 Vgl. z.B. EDSA-Leitlinien zu Meldepflichten, Rn. 48 f., 69 f., 83 f., 104 f., 122 f.

Mitglied werden? Mehr Informationen?

https://www.gdd.de/service/mitglied-werden oder eine E-Mail an: info@gdd.de

Eine Mitgliedschaft bietet wesentliche Vorteile:

>> Mitglieder-Nachrichten mit aktuellen Fachinformationen in Form eines monatlichen Newsletters
>> Bezug der Fachzeitschrift RDV (Recht der Datenverarbeitung)
>> Beratung bei konkreten Einzelfragen
>> Zugriff auf Rechtsprechungs- und Literaturarchiv
>> Online-Service „DataAgenda Plus“ (Muster, Checklisten, RDV ONLINE Archiv, Arbeitspapiere etc.)
>> Mitarbeit in Erfahrungsaustausch- und Arbeitskreisen
>> Teilnahme an den kostenfreien GDD-Informationstagen sowie Vergünstigungen bei Seminaren u.v.m.

Schließen Sie sich unseren mehr als 3.600 Mitgliedern an. Eine Mitgliedschaft erhalten Sie schon ab 150,- EUR/Jahr für Privatpersonen und ab 300,- EUR/Jahr für Firmen.

Diese Praxishilfe wurde erstellt durch:

Maximilian Olker
Referent und Doktorand, GDD e.V., Bonn

Sie basiert auf Ausführungen des umfassenderen GDD-Ratgebers „Datenpannen“, 3. Aufl. (2021) von Prof. Dr. Lorenz Franck.

Satz: C. Wengenroth, GDD-Geschäftsstelle, Bonn
Stand: Version 1.0 (Januar 2025)

Herausgeber:
Gesellschaft für Datenschutz und Datensicherheit (GDD e.V.)
Heinrich-Böll-Ring 10
53119 Bonn

Tel.: +49 2 28 96 96 75-00
www.gdd.de
info@gdd.de