edpb
European Data Protection Board

Guidelines

AUTOMATISIERT VON www.DeepL.com, daher keine Garantie für die Richtigkeit!

Leitlinien 9/2022 zur Meldung von Verletzungen des Schutzes personenbezogener Daten nach der DSGVO

Version 2.0

Verabschiedet am 28. März 2023

• Dieses Dokument ersetzt das WP 250.01 der Artikel-29-Gruppe vom 06.02.2018.
• Am 10.10.2022 wurde die Tatsache hinzugefügt, dass der One-Stop-Shop nicht anwendbar ist, wenn es um die Meldung von Datenschutzverletzungen geht.
• Am 28.03.2023 gibt es eine neue Fassung nach Abschluss der Konsultationsphase.

Versionsgeschichte

Version 1.0	10. Oktober 2022	Verabschiedung der Leitlinien (aktualisierte Fassung der vorherigen Leitlinien WP250 (rev.01), die von der Arbeitsgruppe 29 angenommen und vom EDPB am 25. Mai 2018 gebilligt wurden) für eine gezielte öffentliche Konsultation.
Version 2.0	28. März 2023	Verabschiedung der Leitlinien im Anschluss an die gezielte öffentliche Konsultation zum Thema Meldung von Datenschutzverletzungen bei für die Verarbeitung Verantwortlichen, die nicht im EWR ansässig sind.

INHALTSVERZEICHNIS

Der Europäische Datenschutzausschuss

gestützt auf Artikel 70 Absatz 1 Buchstaben e und l der 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 (im Folgenden "DSGVO"),

gestützt auf das EWR-Abkommen, insbesondere auf Anhang XI und Protokoll 37, geändert durch den Beschluss des Gemeinsamen EWR-Ausschusses Nr. 154/2018 vom 6. Juli 2018[1],

gestützt auf Artikel 12 und Artikel 22 seiner Geschäftsordnung,

gestützt auf die Leitlinien der Artikel-29-Datenschutzgruppe für die Meldung von Verletzungen des Schutzes personenbezogener Daten gemäß der Verordnung (EU) 2016/679, WP250 rev.01,

HAT DIE FOLGENDEN LEITLINIEN ANGENOMMEN

0 VORWORT

1. Am 3. Oktober 2017 nahm die Datenschutzgruppe 29 (nachstehend "WP29") ihre Leitlinien zur Meldung von Verletzungen des Schutzes personenbezogener Daten nach der Verordnung (EU) 2016/679 (WP250 rev.01)[2]angenommen, die vom Europäischen Datenschutzausschuss (im Folgenden "EDPB") in seiner ersten Plenarsitzung gebilligt wurden[3]. Das vorliegende Dokument ist eine leicht aktualisierte Fassung dieser Leitlinien. Jede Bezugnahme auf die WP29-Leitlinien zur Meldung von Verletzungen des Schutzes personenbezogener Daten gemäß der Verordnung (EU) 2016/679 (WP250 rev.01) sollte von nun an als Bezugnahme auf die vorliegenden EDSB-Leitlinien 9/2022 ausgelegt werden.

2. Der EDSB hat festgestellt, dass die Meldepflichten bei Verletzungen des Schutzes personenbezogener Daten in Nicht-EU-Betrieben geklärt werden müssen. Der diesbezügliche Absatz wurde überarbeitet und aktualisiert, während der Rest des Dokuments, abgesehen von redaktionellen Änderungen, unverändert geblieben ist. Die Überarbeitung betrifft insbesondere den Absatz 73 in Abschnitt II.C.2 dieses Dokuments.

EINFÜHRUNG

3. Mit der Datenschutz-Grundverordnung wurde die Anforderung eingeführt, dass eine Verletzung des Schutzes personenbezogener Daten (im Folgenden "Verletzung") der zuständigen nationalen Aufsichtsbehörde gemeldet werden muss[4] (oder im Falle einer grenzüberschreitenden Verletzung der federführenden Behörde) zu benachrichtigen und in bestimmten Fällen die Personen, deren personenbezogene Daten von der Verletzung betroffen sind, über die Verletzung zu informieren.

4. Für bestimmte Organisationen, wie z. B. Anbieter von öffentlich zugänglichen elektronischen Kommunikationsdiensten (gemäß der Richtlinie 2009/136/EG und der Verordnung (EU) Nr. 611/2013), bestand eine Meldepflicht bei Verstößen[5]. Es gab auch einige Mitgliedstaaten, die bereits ihre eigenen

[1] Die in diesem Dokument enthaltenen Verweise auf "Mitgliedstaaten" sind als Verweise auf "EWR-Mitgliedstaaten" zu verstehen.
[2] WP29 Guidelines on Personal data breach notification under Regulation 2016/679 (WP250 rev.01) (zuletzt

überarbeitet und aktualisiert am 6. Februar 2018), verfügbar unter https://ec.europa.eu/newsroom/article29/items/612052.

[3] Siehe https://edpb.europa.eu/news/news/2018/endorsement-gdpr-wp29-guidelines-edpb_en.

[4] Siehe Artikel 4(21) der Datenschutz-Grundverordnung.

[5] Siehe http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:32009L0136 und http://eur-lex.europa.eu/legalcontent/EN/TXT/?uri=CELEX%3A32013R0611

nationale Verpflichtung zur Meldung von Verstößen. Dazu könnte die Verpflichtung gehören, Verstöße zu melden, die neben den Anbietern öffentlich zugänglicher elektronischer Kommunikationsdienste auch Kategorien von für die Verarbeitung Verantwortlichen betreffen (z. B. in Deutschland und Italien), oder eine Verpflichtung, alle Verstöße zu melden, die personenbezogene Daten betreffen (z. B. in den Niederlanden). In anderen Mitgliedstaaten gibt es möglicherweise einschlägige Verhaltenskodizes (z. B. in Irland[6]). Während eine Reihe von EU-Datenschutzbehörden die für die Verarbeitung Verantwortlichen aufforderten, Verstöße zu melden, sah die Datenschutzrichtlinie 95/46/EG[7]die durch die Datenschutz-Grundverordnung ersetzt wurde, enthielt keine spezifische Verpflichtung zur Meldung von Datenschutzverletzungen, so dass eine solche Anforderung für viele Organisationen neu war. Die Datenschutz-Grundverordnung schreibt allen für die Verarbeitung Verantwortlichen eine Meldepflicht vor, es sei denn, es ist unwahrscheinlich, dass eine Datenschutzverletzung zu einem Risiko für die Rechte und Freiheiten von Personen führt[8]. Auch Auftragsverarbeitern kommt eine wichtige Rolle zu, und sie müssen ihren für die Verarbeitung Verantwortlichen über jede Datenschutzverletzung informieren[9].

5. Der EDSB ist der Ansicht, dass die Meldepflicht eine Reihe von Vorteilen hat. Bei der Benachrichtigung der Aufsichtsbehörde können die für die Verarbeitung Verantwortlichen Ratschläge darüber einholen, ob die betroffenen Personen informiert werden müssen. Die Aufsichtsbehörde kann nämlich anordnen, dass der für die Verarbeitung Verantwortliche diese Personen über die Verletzung informiert[10]. Die Unterrichtung der betroffenen Personen über eine Sicherheitsverletzung ermöglicht es dem für die Verarbeitung Verantwortlichen, sie über die Risiken zu informieren, die sich aus der Sicherheitsverletzung ergeben, sowie über die Schritte, die die betroffenen Personen unternehmen können, um sich vor den möglichen Folgen zu schützen. Der Schwerpunkt eines jeden Plans zur Reaktion auf eine Datenschutzverletzung sollte auf dem Schutz der Personen und ihrer personenbezogenen Daten liegen. Folglich sollte die Meldung von Datenschutzverletzungen als ein Instrument zur Verbesserung der Einhaltung der Vorschriften zum Schutz personenbezogener Daten betrachtet werden. Gleichzeitig ist zu beachten, dass das Versäumnis, eine Datenschutzverletzung entweder einer Person oder einer Aufsichtsbehörde zu melden, gemäß Artikel 83 DSGVO eine mögliche Sanktion gegen den für die Verarbeitung Verantwortlichen nach sich ziehen kann.

6. Die für die Verarbeitung Verantwortlichen und die Auftragsverarbeiter werden daher ermutigt, im Voraus zu planen und Verfahren einzurichten, mit denen sie in der Lage sind, eine Datenschutzverletzung zu erkennen und unverzüglich einzudämmen, das Risiko für den Einzelnen zu bewerten [11]zu bewerten und dann zu entscheiden, ob es notwendig ist, die zuständige Aufsichtsbehörde zu benachrichtigen und die betroffenen Personen erforderlichenfalls über die Verletzung zu informieren. Die Benachrichtigung der Aufsichtsbehörde sollte Teil dieses Notfallplans sein.

7. Die Datenschutz-Grundverordnung enthält Bestimmungen darüber, wann und wem eine Datenschutzverletzung gemeldet werden muss und welche Informationen im Rahmen der Meldung bereitgestellt werden sollten. Die für die Benachrichtigung erforderlichen Informationen können schrittweise bereitgestellt werden, doch sollten die für die Verarbeitung Verantwortlichen in jedem Fall rechtzeitig auf eine Verletzung reagieren.

8. In ihrer Stellungnahme 03/2014 zur Meldung von Verletzungen des Schutzes personenbezogener Daten[12]gab die WP29 den für die Verarbeitung Verantwortlichen Leitlinien an die Hand, um ihnen bei der Entscheidung zu helfen, ob sie betroffene Personen im Falle einer Datenschutzverletzung benachrichtigen sollen. Die Stellungnahme befasste sich mit der Verpflichtung von Anbietern elektronischer Kommunikation im Rahmen der Richtlinie 2002/58/EG und enthielt Beispiele aus verschiedenen Sektoren im Kontext des damaligen Entwurfs der Datenschutz-Grundverordnung und stellte bewährte Verfahren für alle für die Verarbeitung Verantwortlichen vor.

9. In den aktuellen Leitlinien werden die Anforderungen der DSGVO an die Benachrichtigung bei Datenschutzverletzungen und an die Kommunikation erläutert sowie einige der Schritte, die für die Verarbeitung Verantwortliche und Auftragsverarbeiter unternehmen können, um diesen Verpflichtungen nachzukommen. Sie

[6] Siehe https://www.dataprotection.ie/docs/Data_Security_Breach_Code_of_Practice/1082.htm

[7] Siehe http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:31995L0046

[8] Die in der Charta der Grundrechte der EU verankerten Rechte, verfügbar unter http://eurlex.europa.eu/legal-content/EN/TXT/?uri=CELEX:12012P/TXT

[9] Siehe Artikel 33 Absatz 2 der Datenschutz-Grundverordnung. Das Konzept ähnelt Artikel 5 der Verordnung (EU) Nr. 611/2013, der besagt, dass ein Anbieter, der vertraglich verpflichtet ist, einen Teil eines elektronischen Kommunikationsdienstes bereitzustellen (ohne eine direkte vertragliche Beziehung zu den Teilnehmern zu haben), verpflichtet ist, den vertragsschließenden Anbieter im Falle einer Verletzung des Schutzes personenbezogener Daten zu benachrichtigen.

[10] Siehe Artikel 34 Absatz 4 und Artikel 58 Absatz 2 Buchstabe e der Datenschutz-Grundverordnung.

[11] Dies kann im Rahmen der Überwachungs- und Überprüfungsanforderung einer Datenschutzfolgenabschätzung sichergestellt werden, die für Verarbeitungen erforderlich ist, die wahrscheinlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen mit sich bringen (Artikel 35 Absätze 1 und 11).

[12] Siehe Stellungnahme der WP29 03/2014 zur Meldung von Verletzungen des Schutzes personenbezogener Daten http://ec.europa.eu/justice/data-protection/article29/documentation/opinion-recommendation/files/2014/wp213_en.pdf

auch Beispiele für verschiedene Arten von Verstößen und wer in den verschiedenen Szenarien benachrichtigt werden müsste.

I. BENACHRICHTIGUNG ÜBER VERLETZUNGEN DES DATENSCHUTZES NACH DER GDPR

A. Grundlegende Sicherheitsüberlegungen

10. Eine der Anforderungen der DSGVO besteht darin, dass personenbezogene Daten durch geeignete technische und organisatorische Maßnahmen so zu verarbeiten sind, dass eine angemessene Sicherheit der personenbezogenen Daten gewährleistet ist, einschließlich des Schutzes vor unbefugter oder unrechtmäßiger Verarbeitung und vor unbeabsichtigtem Verlust, unbeabsichtigter Zerstörung oder Beschädigung[13].

11. Dementsprechend verlangt die Datenschutz-Grundverordnung sowohl von den für die Verarbeitung Verantwortlichen als auch von den Auftragsverarbeitern, dass sie geeignete technische und organisatorische Maßnahmen ergreifen, um ein Sicherheitsniveau zu gewährleisten, das dem Risiko für die verarbeiteten personenbezogenen Daten angemessen ist. Sie sollten dem Stand der Technik, den Kosten der Umsetzung und der Art, dem Umfang, dem Kontext und den Zwecken der Verarbeitung sowie der unterschiedlichen Wahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen Rechnung tragen[14]. Die Datenschutz-Grundverordnung schreibt außerdem vor, dass alle geeigneten technischen Schutzmaßnahmen und organisatorischen Vorkehrungen getroffen werden müssen, um unverzüglich feststellen zu können, ob eine Datenschutzverletzung stattgefunden hat, was wiederum ausschlaggebend dafür ist, ob die Meldepflicht erfüllt wird [15].

12. Ein Schlüsselelement jeder Datensicherheitspolitik ist daher die Fähigkeit, eine Datenschutzverletzung nach Möglichkeit zu verhindern und, falls sie dennoch eintritt, rechtzeitig darauf zu reagieren.

B. Was ist eine Verletzung des Schutzes personenbezogener Daten?

1. Definition

13. Bei jedem Versuch, eine Datenschutzverletzung zu beheben, sollte der für die Verarbeitung Verantwortliche zunächst in der Lage sein, eine solche zu erkennen. Die Datenschutz-Grundverordnung definiert eine "Verletzung des Schutzes personenbezogener Daten" in Artikel 4(12) als:

> "*eine Verletzung der Sicherheit, die zur zufälligen oder unrechtmäßigen Zerstörung, zum Verlust, zur Veränderung, zur unbefugten Weitergabe oder zum Zugriff auf übermittelte, gespeicherte oder*

14. Was mit der "Vernichtung" personenbezogener Daten gemeint ist, sollte recht klar sein: Dies ist der Fall, wenn die Daten nicht mehr oder nicht mehr in einer Form vorhanden sind, die für den für die Verarbeitung Verantwortlichen von Nutzen ist. Auch die "Beschädigung" sollte relativ klar sein: Dies ist der Fall, wenn personenbezogene Daten verändert oder beschädigt wurden oder nicht mehr vollständig sind. Der Begriff "Verlust" personenbezogener Daten ist so auszulegen, dass die Daten zwar noch vorhanden sind, der für die Verarbeitung Verantwortliche aber die Kontrolle über sie verloren hat, keinen Zugang mehr zu ihnen hat oder sie nicht mehr in seinem Besitz hat. Schließlich kann eine unbefugte oder unrechtmäßige Verarbeitung die Weitergabe personenbezogener Daten an (oder den Zugriff durch) Empfänger umfassen, die nicht berechtigt sind, die Daten zu erhalten (oder darauf zuzugreifen), oder jede andere Form der Verarbeitung, die gegen die DSGVO verstößt.

> **Beispiel**
>
> Ein Beispiel für den Verlust personenbezogener Daten kann sein, dass ein Gerät mit einer Kopie der Kundendatenbank eines für die Verarbeitung Verantwortlichen verloren geht oder gestohlen wird. Ein weiteres Beispiel für einen Verlust kann sein, dass die einzige Kopie eines Satzes personenbezogener Daten durch Ransomware verschlüsselt wurde oder von dem für die

15. Es sollte klar sein, dass eine Datenschutzverletzung eine Art von Sicherheitsvorfall ist. Wie aus Artikel 4 Absatz 12 hervorgeht, gilt die Datenschutz-Grundverordnung jedoch nur, wenn eine Verletzung personenbezogener Daten vorliegt. Die Folge einer solchen Verletzung ist, dass der für die Verarbeitung Verantwortliche nicht in der Lage sein wird, die Einhaltung der Grundsätze in Bezug auf die

[13] Siehe Artikel 5 Absatz 1 Buchstabe f und Artikel 32 der Datenschutzgrundverordnung.
[14] Artikel 32; siehe auch Erwägungsgrund 83 der Datenschutz-Grundverordnung.
[15] Siehe Erwägungsgrund 87 GDPR.

die Verarbeitung personenbezogener Daten gemäß Artikel 5 der DSGVO. Dies verdeutlicht den Unterschied zwischen einem Sicherheitsvorfall und einer Verletzung des Schutzes personenbezogener Daten - im Wesentlichen sind zwar alle Verletzungen des Schutzes personenbezogener Daten Sicherheitsvorfälle, aber nicht alle Sicherheitsvorfälle sind notwendigerweise Verletzungen des Schutzes personenbezogener Daten[16].

16. Im Folgenden werden die möglichen nachteiligen Auswirkungen eines Verstoßes auf den Einzelnen betrachtet.

2. Arten von Verletzungen des Schutzes personenbezogener Daten

17. In ihrer Stellungnahme 03/2014 zur Meldung von Sicherheitsverletzungen erklärte die WP29, dass Sicherheitsverletzungen nach den folgenden drei bekannten Grundsätzen der Informationssicherheit kategorisiert werden können[17]:

    - **"Verletzung der Vertraulichkeit**" - wenn es zu einer unbefugten oder versehentlichen Offenlegung personenbezogener Daten oder zum Zugriff auf diese Daten kommt.
    - **"Verletzung der Integrität**" - wenn eine unbefugte oder versehentliche Änderung personenbezogener Daten vorliegt.
    - "**Verfügbarkeitsverletzung**" - wenn ein versehentlicher oder unbefugter Verlust des Zugangs[18] oder Vernichtung von personenbezogenen Daten.

18. Es sei auch darauf hingewiesen, dass eine Verletzung je nach den Umständen gleichzeitig die Vertraulichkeit, die Integrität und die Verfügbarkeit personenbezogener Daten sowie eine beliebige Kombination dieser Aspekte betreffen kann.

19. Während die Feststellung, ob eine Verletzung der Vertraulichkeit oder der Integrität vorliegt, relativ eindeutig ist, ist die Frage, ob eine Verletzung der Verfügbarkeit vorliegt, möglicherweise weniger klar. Eine Verletzung wird immer dann als Verfügbarkeitsverletzung angesehen, wenn es zu einem dauerhaften Verlust oder einer Zerstörung personenbezogener Daten gekommen ist.

Beispiel

Ein Verfügbarkeitsverlust liegt beispielsweise vor, wenn Daten versehentlich oder von einer unbefugten Person gelöscht wurden oder - im Falle von sicher verschlüsselten Daten - der Entschlüsselungscode verloren gegangen ist. Kann der für die Verarbeitung Verantwortliche den Zugang zu den Daten nicht wiederherstellen, z. B. anhand einer Sicherungskopie, so gilt dies als dauerhafter Verlust der Verfügbarkeit.

Ein Verfügbarkeitsverlust kann auch dann eintreten, wenn der normale Dienst einer Organisation erheblich gestört ist, z. B. durch einen Stromausfall oder einen Denial-of-Service-Angriff, so dass

20. Es kann die Frage gestellt werden, ob ein vorübergehender Verlust der Verfügbarkeit personenbezogener Daten als eine Verletzung angesehen werden sollte und, wenn ja, ob diese Verletzung gemeldet werden muss. In Artikel 32 DSGVO, "Sicherheit der Verarbeitung", wird erläutert, dass bei der Umsetzung technischer und organisatorischer Maßnahmen zur Gewährleistung eines dem Risiko angemessenen Sicherheitsniveaus unter anderem "*die Fähigkeit zur Gewährleistung der kontinuierlichen Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Verarbeitungssysteme und*

[16] Es sei darauf hingewiesen, dass ein Sicherheitsvorfall nicht auf Bedrohungsmodelle beschränkt ist, bei denen eine Organisation von außen angegriffen wird, sondern auch Vorfälle bei der internen Verarbeitung umfasst, die gegen Sicherheitsgrundsätze verstoßen.

[17] Siehe Stellungnahme der WP29 03/2014.

[18] Es ist allgemein bekannt, dass der "Zugang" ein wesentlicher Bestandteil der "Verfügbarkeit" ist. Siehe z. B. NIST SP80053rev4, das "Verfügbarkeit" definiert als: "Sicherstellung des rechtzeitigen und zuverlässigen Zugangs zu und der Nutzung von Informationen", verfügbar unter http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf. Auch CNSSI-4009 bezieht sich auf: "Rechtzeitiger, zuverlässiger Zugang zu Daten und Informationsdiensten für autorisierte Benutzer". Siehe https://rmf.org/wpcontent/uploads/2017/10/CNSSI-4009.pdf. ISO/IEC 27000:2016 definiert "Verfügbarkeit" auch als "Eigenschaft, bei Bedarf für eine autorisierte Stelle zugänglich und nutzbar zu sein": https://www.iso.org/obp/ui/#iso:std:isoiec:27000:ed-4:v1:en

Dienste" und "*die Fähigkeit, die Verfügbarkeit und den Zugang zu personenbezogenen Daten im Falle eines physischen oder technischen Zwischenfalls zeitnah wiederherzustellen*".

21. Daher ist auch ein Sicherheitsvorfall, der dazu führt, dass personenbezogene Daten für eine gewisse Zeit nicht verfügbar sind, eine Art von Sicherheitsverletzung, da der fehlende Zugang zu den Daten erhebliche Auswirkungen auf die Rechte und Freiheiten natürlicher Personen haben kann. Um es klar zu sagen: Wenn personenbezogene Daten aufgrund einer geplanten Systemwartung nicht verfügbar sind, ist dies keine "Sicherheitsverletzung" im Sinne von Artikel 4 Absatz 12 DSGVO.

22. Wie bei einem dauerhaften Verlust oder einer Zerstörung personenbezogener Daten (oder auch bei jeder anderen Art von Datenschutzverletzung) sollte eine Datenschutzverletzung, die mit einem vorübergehenden Verlust der Verfügbarkeit einhergeht, gemäß Artikel 33 Absatz 5 DSGVO dokumentiert werden. Dies hilft dem für die Verarbeitung Verantwortlichen, gegenüber der Aufsichtsbehörde, die möglicherweise Einsicht in diese Aufzeichnungen verlangt, seine Verantwortlichkeit nachzuweisen[19]. Je nach den Umständen des Verstoßes kann jedoch eine Meldung an die Aufsichtsbehörde und eine Mitteilung an die betroffenen Personen erforderlich sein oder nicht. Der für die Verarbeitung Verantwortliche muss die Wahrscheinlichkeit und Schwere der Auswirkungen auf die Rechte und Freiheiten natürlicher Personen infolge der fehlenden Verfügbarkeit personenbezogener Daten bewerten. Gemäß Artikel 33 DSGVO muss der für die Verarbeitung Verantwortliche eine Meldung machen, es sei denn, es ist unwahrscheinlich, dass die Verletzung ein Risiko für die Rechte und Freiheiten der betroffenen Personen darstellt. Natürlich muss dies von Fall zu Fall geprüft werden.

Beispiel

Wenn in einem Krankenhaus wichtige medizinische Daten über Patienten nicht verfügbar sind, selbst wenn dies nur vorübergehend der Fall ist, könnte dies ein Risiko für die Rechte und Freiheiten des Einzelnen darstellen; so könnten beispielsweise Operationen abgesagt und Leben gefährdet werden.

Umgekehrt dürfte ein mehrstündiger Ausfall der Systeme eines Medienunternehmens (z. B. aufgrund eines Stromausfalls), wenn dieses Unternehmen dann keine Newsletter mehr an seine Abonnenten versenden kann, kaum ein Risiko für die Rechte und Freiheiten des Einzelnen darstellen.

23. Es sei darauf hingewiesen, dass ein Verlust der Verfügbarkeit der Systeme eines für die Verarbeitung Verantwortlichen zwar möglicherweise nur vorübergehend ist und sich nicht auf Einzelpersonen auswirkt, dass der für die Verarbeitung Verantwortliche aber dennoch alle möglichen Folgen einer Sicherheitsverletzung bedenken muss, da eine Benachrichtigung auch aus anderen Gründen erforderlich sein kann.

Beispiel

Eine Infektion durch Ransomware (bösartige Software, die die Daten des für die Verarbeitung Verantwortlichen verschlüsselt, bis ein Lösegeld gezahlt wird) könnte zu einem vorübergehenden Verlust der Verfügbarkeit führen, wenn die Daten aus einem Backup wiederhergestellt werden können. Dennoch ist ein Eindringen in das Netzwerk erfolgt, und eine Meldung könnte erforderlich sein, wenn der Vorfall als Verletzung der Vertraulichkeit eingestuft wird (d. h. der Angreifer hat

3. Die möglichen Folgen einer Verletzung des Schutzes personenbezogener Daten

24. Eine Datenschutzverletzung kann potenziell eine Reihe von erheblichen nachteiligen Auswirkungen auf Einzelpersonen haben, die zu physischem, materiellem oder immateriellem Schaden führen können. Die DSGVO erklärt, dass dies den Verlust der Kontrolle über ihre personenbezogenen Daten, die Einschränkung ihrer Rechte, Diskriminierung, Identitätsdiebstahl oder Betrug, finanzielle Verluste, die unbefugte Aufhebung der Pseudonymisierung, Rufschädigung und den Verlust der Vertraulichkeit personenbezogener Daten, die durch das Berufsgeheimnis geschützt sind, umfassen kann. Sie kann auch jeden anderen erheblichen wirtschaftlichen oder sozialen Nachteil für diese Personen umfassen[20].

25. Dementsprechend ist der für die Verarbeitung Verantwortliche nach der Datenschutz-Grundverordnung verpflichtet, der zuständigen Aufsichtsbehörde eine Datenschutzverletzung zu melden, es sei denn, es ist unwahrscheinlich, dass die Gefahr derartiger nachteiliger Auswirkungen eintritt. Wenn es eine

[19] Siehe Artikel 33 Absatz 5 der Datenschutz-Grundverordnung.
[20] Siehe auch Erwägungsgründe 85 und 75 der Datenschutz-Grundverordnung.

Da das Risiko, dass diese nachteiligen Auswirkungen eintreten, wahrscheinlich hoch ist, verlangt die Datenschutz-Grundverordnung, dass der für die Verarbeitung Verantwortliche die betroffenen Personen so bald wie möglich über die Verletzung informiert[21].

26. In Erwägungsgrund 87 der Datenschutz-Grundverordnung wird betont, wie wichtig es ist, in der Lage zu sein, eine Datenschutzverletzung zu erkennen, das Risiko für den Einzelnen zu bewerten und ihn dann gegebenenfalls zu benachrichtigen:

> *"Es sollte geprüft werden, ob alle geeigneten technischen Schutzmaßnahmen und organisatorischen Vorkehrungen getroffen wurden, um unverzüglich festzustellen, ob eine Verletzung des Schutzes personenbezogener Daten vorliegt, und um die Aufsichtsbehörde und die betroffene Person unverzüglich zu informieren. Die Tatsache, dass die Benachrichtigung ohne unangemessene Verzögerung erfolgt ist, sollte insbesondere unter Berücksichtigung der Art und Schwere der Verletzung des Schutzes personenbezogener Daten und ihrer Folgen und nachteiligen Auswirkungen für die betroffene Person festgestellt werden. Eine solche Meldung kann dazu führen, dass die*

27. Weitere Leitlinien zur Bewertung des Risikos schädlicher Wirkungen für den Einzelnen werden in Abschnitt IV behandelt.

28. Wenn die für die Verarbeitung Verantwortlichen es versäumen, entweder die Aufsichtsbehörde oder die betroffenen Personen oder beide von einer Verletzung des Datenschutzes zu benachrichtigen, obwohl die Anforderungen der Artikel 33 und/oder 34 DSGVO erfüllt sind, hat die Aufsichtsbehörde die Wahl, alle ihr zur Verfügung stehenden Abhilfemaßnahmen zu erwägen, wozu auch die Verhängung einer angemessenen Geldstrafe gehört[22]entweder als Begleitmaßnahme zu einer Abhilfemaßnahme nach Artikel 58 Absatz 2 DSGVO oder als eigenständige Maßnahme. Wird eine Geldbuße verhängt, so kann diese bis zu 10 000 000 EUR oder bis zu 2 % des gesamten weltweiten Jahresumsatzes eines Unternehmens gemäß Artikel 83 Absatz 4 Buchstabe a der DSGVO betragen. Es ist auch wichtig zu bedenken, dass in einigen Fällen das Versäumnis, eine Datenschutzverletzung zu melden, entweder das Fehlen bestehender Sicherheitsmaßnahmen oder die Unzulänglichkeit der bestehenden Sicherheitsmaßnahmen offenbaren könnte. In den Leitlinien der WP29 für Geldbußen heißt es: "*Wenn in einem bestimmten Einzelfall mehrere verschiedene Verstöße zusammen begangen werden, kann die Aufsichtsbehörde die Geldbußen in einer Höhe festsetzen, die wirksam, verhältnismäßig und abschreckend ist und sich im Rahmen des schwerwiegendsten Verstoßes bewegt*". In diesem Fall hat die Aufsichtsbehörde auch die Möglichkeit, Sanktionen für das Versäumnis zu verhängen, die Verletzung zu melden oder mitzuteilen (Artikel 33 und 34 DSGVO), und für das Fehlen von (angemessenen) Sicherheitsmaßnahmen (Artikel 32 DSGVO), da es sich um zwei verschiedene Verstöße handelt.

II. ARTIKEL 33 - MITTEILUNG AN DIE AUFSICHTSBEHÖRDE

A. Wann ist zu melden?

1. Artikel 33 Anforderungen

29. Artikel 33 Absatz 1 der Datenschutz-Grundverordnung besagt Folgendes:

> "*Im Falle einer Verletzung des Schutzes personenbezogener Daten meldet der für die Verarbeitung Verantwortliche die Verletzung des Schutzes personenbezogener Daten unverzüglich und, soweit möglich, spätestens 72 Stunden, nachdem er davon Kenntnis erlangt hat, der gemäß Artikel 55 zuständigen Aufsichtsbehörde, es sei denn, die Verletzung des Schutzes personenbezogener Daten wird voraussichtlich nicht zu einem Risiko für die Rechte und Freiheiten natürlicher Personen führen.*

30. Erwägungsgrund 87 GDPR besagt[23]:

[21] Siehe auch Erwägungsgrund 86 der Datenschutz-Grundverordnung.

[22] Weitere Einzelheiten finden Sie in den Leitlinien der WP29 für die Anwendung und Festsetzung von Geldbußen, die Sie hier finden: http://ec.europa.eu/newsroom/just/document.cfm?doc_id=47889

[23] Erwägungsgrund 85 der Datenschutz-Grundverordnung ist hier ebenfalls von Bedeutung.

"Es sollte geprüft werden, ob alle geeigneten technischen Schutzmaßnahmen und organisatorischen Vorkehrungen getroffen wurden, um unverzüglich festzustellen, ob eine Verletzung des Schutzes personenbezogener Daten vorliegt, und um die Aufsichtsbehörde und die betroffene Person unverzüglich zu informieren. Die Tatsache, dass die Benachrichtigung ohne unangemessene Verzögerung erfolgt ist, sollte insbesondere unter Berücksichtigung der Art und Schwere der Verletzung des Schutzes personenbezogener Daten und ihrer Folgen und nachteiligen Auswirkungen für die betroffene Person festgestellt werden. Eine solche Meldung kann dazu führen, dass die

2. Wann wird ein Kontrolleur "bewusst"?

31. Wie oben ausgeführt, schreibt die DSGVO vor, dass der für die Verarbeitung Verantwortliche im Falle einer Verletzung die Verletzung unverzüglich und nach Möglichkeit spätestens 72 Stunden, nachdem er von ihr Kenntnis erlangt hat, melden muss. Dies kann die Frage aufwerfen, wann ein für die Verarbeitung Verantwortlicher von einer Verletzung "Kenntnis" erlangt hat. Der EDSB ist der Ansicht, dass ein für die Verarbeitung Verantwortlicher dann als "informiert" gelten sollte, wenn er mit hinreichender Sicherheit weiß, dass ein Sicherheitsvorfall eingetreten ist, der zu einer Gefährdung personenbezogener Daten geführt hat.

32. Wie bereits erwähnt, verpflichtet die Datenschutz-Grundverordnung den für die Verarbeitung Verantwortlichen jedoch, alle geeigneten technischen und organisatorischen Maßnahmen zu ergreifen, um unverzüglich festzustellen, ob eine Datenschutzverletzung vorliegt, und die Aufsichtsbehörde und die betroffenen Personen unverzüglich zu informieren. Ferner heißt es, dass die Tatsache, dass die Benachrichtigung ohne unangemessene Verzögerung erfolgt ist, insbesondere unter Berücksichtigung der Art und Schwere der Verletzung und ihrer Folgen und nachteiligen Auswirkungen für die betroffene Person festgestellt werden sollte[24]. Damit ist der für die Verarbeitung Verantwortliche verpflichtet, dafür zu sorgen, dass er rechtzeitig von etwaigen Verstößen "Kenntnis" erlangt, damit er geeignete Maßnahmen ergreifen kann.

33. Wann genau ein für die Verarbeitung Verantwortlicher von einer bestimmten Verletzung "Kenntnis" hat, hängt von den Umständen der jeweiligen Verletzung ab. In einigen Fällen wird es von Anfang an relativ klar sein, dass eine Verletzung vorliegt, während es in anderen Fällen einige Zeit dauern kann, bis festgestellt wird, ob personenbezogene Daten kompromittiert worden sind. Das Hauptaugenmerk sollte jedoch auf der unverzüglichen Untersuchung eines Vorfalls liegen, um festzustellen, ob es tatsächlich zu einer Verletzung des Schutzes personenbezogener Daten gekommen ist, und, falls dies der Fall ist, um Abhilfemaßnahmen zu ergreifen und gegebenenfalls eine Meldung zu machen.

Beispiele

1. Im Falle des Verlusts eines USB-Sticks mit unverschlüsselten personenbezogenen Daten ist es zu überprüfen, ob Unbefugte Zugang zu diesen Daten hatten. Dennoch, auch wenn die
Da der für die Verarbeitung Verantwortliche möglicherweise nicht feststellen kann, ob eine Verletzung der Vertraulichkeit vorliegt, muss ein solcher Fall gemeldet werden, da ein angemessener Grad an Sicherheit besteht, dass eine Verletzung der Verfügbarkeit vorliegt; der für die Verarbeitung

2. Ein Dritter teilt dem für die Verarbeitung Verantwortlichen mit, dass er versehentlich die einen seiner Kunden und legt Beweise für die unbefugte Weitergabe vor. Da der für die Verarbeitung Verantwortliche
Wenn der Kommission eindeutige Beweise für einen Verstoß gegen die Geheimhaltungspflicht

3. Ein Kontrolleur stellt fest, dass möglicherweise ein Eindringling in sein Netz eingedrungen ist. ihre Systeme überprüft, um festzustellen, ob personenbezogene Daten, die in diesem System gespeichert sind, kompromittiert wurden, und
bestätigt, dass dies der Fall ist. Noch einmal: Da der für die Verarbeitung Verantwortliche nun

[24] Siehe Erwägungsgrund 87 GDPR.

4. Ein Cyberkrimineller kontaktiert den für die Verarbeitung Verantwortlichen, nachdem er Lösegeld. In diesem Fall hat der für die Verarbeitung Verantwortliche, nachdem er sein System überprüft hat, um zu bestätigen, dass es angegriffen wurde, eine klare

34. Nachdem der für die Verarbeitung Verantwortliche zum ersten Mal von einer Person, einer Medienorganisation oder einer anderen Quelle über eine mögliche Verletzung informiert wurde oder wenn er selbst einen Sicherheitsvorfall festgestellt hat, kann er eine kurze Untersuchung durchführen, um festzustellen, ob tatsächlich eine Verletzung vorliegt oder nicht. Während dieses Zeitraums der Untersuchung kann der für die Verarbeitung Verantwortliche nicht als "wissend" angesehen werden. Es wird jedoch erwartet, dass die erste Untersuchung so schnell wie möglich beginnt und mit einem angemessenen Grad an Sicherheit feststellt, ob eine Verletzung stattgefunden hat; eine detailliertere Untersuchung kann dann folgen.

35. Sobald der für die Verarbeitung Verantwortliche Kenntnis von einer meldepflichtigen Sicherheitsverletzung erlangt hat, muss er diese unverzüglich, nach Möglichkeit jedoch spätestens innerhalb von 72 Stunden, melden. Während dieses Zeitraums sollte der für die Verarbeitung Verantwortliche das wahrscheinliche Risiko für den Einzelnen bewerten, um festzustellen, ob die Meldepflicht ausgelöst wurde und welche Maßnahmen zur Behebung der Verletzung erforderlich sind. Der für die Verarbeitung Verantwortliche kann jedoch bereits eine erste Bewertung des potenziellen Risikos, das sich aus einer Verletzung ergeben könnte, im Rahmen einer Datenschutz-Folgenabschätzung (DPIA)[25] vor der Durchführung des betreffenden Verarbeitungsvorgangs vorgenommen. Die Datenschutz-Folgenabschätzung kann jedoch im Vergleich zu den spezifischen Umständen eines tatsächlichen Verstoßes eher allgemein gehalten sein, so dass in jedem Fall eine zusätzliche Bewertung unter Berücksichtigung dieser Umstände vorgenommen werden muss. Weitere Einzelheiten zur Risikobewertung finden Sie in Abschnitt IV.

36. In den meisten Fällen sollten diese vorläufigen Maßnahmen bald nach der ersten Warnmeldung abgeschlossen sein (d.h. wenn der für die Verarbeitung Verantwortliche oder der Auftragsverarbeiter vermutet, dass ein Sicherheitsvorfall eingetreten ist, der personenbezogene Daten betreffen könnte). - Nur in Ausnahmefällen sollte es länger dauern.

Beispiel

Eine Person teilt dem für die Verarbeitung Verantwortlichen mit, dass sie eine E-Mail erhalten hat, die sich als der für die Verarbeitung Verantwortliche ausgibt und personenbezogene Daten enthält, die sich auf ihre (tatsächliche) Nutzung des Dienstes des für die Verarbeitung Verantwortlichen beziehen, was darauf schließen lässt, dass die Sicherheit des für die Verarbeitung Verantwortlichen beeinträchtigt wurde. Der für die Verarbeitung Verantwortliche führt eine kurze Untersuchung durch und stellt fest, dass in sein Netzwerk eingedrungen wurde und Beweise für einen unbefugten Zugriff auf personenbezogene Daten vorliegen. Der für die Verarbeitung Verantwortliche gilt nun als

37. Der für die Verarbeitung Verantwortliche sollte daher über interne Verfahren verfügen, die es ihm ermöglichen, einen Verstoß zu erkennen und zu beheben. Beispielsweise kann der für die Verarbeitung Verantwortliche oder der Auftragsverarbeiter zur Feststellung von Unregelmäßigkeiten bei der Datenverarbeitung bestimmte technische Maßnahmen wie Datenfluss- und Protokollanalysatoren einsetzen, mit deren Hilfe durch Korrelation von Protokolldaten Ereignisse und Warnungen definiert werden können[26]. Es ist wichtig, dass eine aufgedeckte Datenschutzverletzung der zuständigen Verwaltungsebene gemeldet wird, damit sie behandelt und gegebenenfalls gemäß Artikel 33 und erforderlichenfalls gemäß Artikel 34 gemeldet werden kann. Solche Maßnahmen und Meldeverfahren könnten in den Reaktionsplänen des für die Verarbeitung Verantwortlichen und/oder in den Governance-Regelungen detailliert beschrieben werden. Diese werden dem für die Verarbeitung Verantwortlichen helfen, wirksam zu planen und festzulegen, wer innerhalb der Organisation die operative Verantwortung für die Bewältigung eines Verstoßes trägt und wie oder ob ein Vorfall gegebenenfalls eskaliert werden soll.

38. Der für die Verarbeitung Verantwortliche sollte auch Vereinbarungen mit allen Auftragsverarbeitern

treffen, die er einsetzt und die ihrerseits verpflichtet sind, den für die Verarbeitung Verantwortlichen im Falle eines Verstoßes zu benachrichtigen (siehe unten).

[25] Siehe WP29-Leitlinien WP248 zu DPIAs hier: http://ec.europa.eu/newsroom/document.cfm?doc_id=44137

[26] Es sei darauf hingewiesen, dass Protokolldaten, die die Nachvollziehbarkeit z. B. der Speicherung, Änderung oder Löschung von Daten erleichtern, auch als personenbezogene Daten der Person gelten können, die den jeweiligen Verarbeitungsvorgang veranlasst hat.

39. Es liegt zwar in der Verantwortung der für die Verarbeitung Verantwortlichen und der Auftragsverarbeiter, geeignete Maßnahmen zu ergreifen, um eine Datenschutzverletzung zu verhindern, darauf zu reagieren und sie zu beheben, doch gibt es einige praktische Schritte, die in jedem Fall unternommen werden sollten.

    - Informationen über alle sicherheitsrelevanten Ereignisse sollten an eine oder mehrere verantwortliche Person(en) weitergeleitet werden, deren Aufgabe es ist, auf Vorfälle einzugehen, das Vorliegen einer Sicherheitsverletzung festzustellen und das Risiko zu bewerten.
    - Das Risiko für Einzelpersonen infolge eines Verstoßes sollte dann bewertet werden (Wahrscheinlichkeit, dass kein Risiko, Risiko oder hohes Risiko besteht), wobei die entsprechenden Abteilungen der Organisation informiert werden.
    - Die Aufsichtsbehörde ist zu benachrichtigen, und die betroffenen Personen sind gegebenenfalls über die Verletzung zu informieren.
    - Gleichzeitig sollte der für die Verarbeitung Verantwortliche Maßnahmen ergreifen, um die Verletzung einzudämmen und zu beheben. Die Dokumentation des Verstoßes sollte in dem Maße erfolgen, wie er sich entwickelt.

40. Dementsprechend sollte klar sein, dass der für die Verarbeitung Verantwortliche verpflichtet ist, auf eine erste Warnung zu reagieren und festzustellen, ob tatsächlich ein Verstoß vorliegt oder nicht. In dieser kurzen Zeitspanne kann der für die Verarbeitung Verantwortliche einige Nachforschungen anstellen und Beweise und andere relevante Details sammeln. Sobald der für die Verarbeitung Verantwortliche jedoch mit hinreichender Sicherheit festgestellt hat, dass eine Datenschutzverletzung vorliegt, muss er, sofern die Bedingungen in Artikel 33 Absatz 1 DSGVO erfüllt sind, die Aufsichtsbehörde unverzüglich und nach Möglichkeit spätestens innerhalb von 72 Stunden benachrichtigen[27]. Wird ein für die Verarbeitung Verantwortlicher nicht rechtzeitig tätig und stellt sich heraus, dass ein Verstoß vorliegt, könnte dies als Unterlassung der Meldung gemäß Artikel 33 DSGVO angesehen werden.

41. Artikel 32 DSGVO stellt klar, dass der für die Verarbeitung Verantwortliche und der Auftragsverarbeiter über geeignete technische und organisatorische Maßnahmen verfügen sollten, um ein angemessenes Maß an Sicherheit für personenbezogene Daten zu gewährleisten: Die Fähigkeit, eine Datenschutzverletzung rechtzeitig zu erkennen, zu beheben und zu melden, sollte als wesentlicher Bestandteil dieser Maßnahmen angesehen werden.

3. Gemeinsame Kontrolleure

42. Artikel 26 DS-GVO betrifft gemeinsam für die Verarbeitung Verantwortliche und legt fest, dass gemeinsam für die Verarbeitung Verantwortliche ihre jeweiligen Verantwortlichkeiten für die Einhaltung der DS-GVO festlegen müssen[28]. Dazu gehört auch die Festlegung, welche Partei für die Einhaltung der Verpflichtungen gemäß Artikel 33 und 34 DSGVO verantwortlich ist. Der EDSB empfiehlt, dass die vertraglichen Vereinbarungen zwischen gemeinsam für die Verarbeitung Verantwortlichen Bestimmungen enthalten, die festlegen, welcher für die Verarbeitung Verantwortliche die Führung bei der Einhaltung der Pflichten zur Meldung von Datenschutzverstößen gemäß der DSGVO übernimmt bzw. dafür verantwortlich ist.

4. Verpflichtungen des Verarbeiters

43. Der für die Verarbeitung Verantwortliche behält die Gesamtverantwortung für den Schutz personenbezogener Daten, aber der Auftragsverarbeiter spielt eine wichtige Rolle, um den für die Verarbeitung Verantwortlichen in die Lage zu versetzen, seinen Verpflichtungen nachzukommen; dazu gehört auch die Meldung von Verstößen. In Artikel 28 Absatz 3 DSGVO ist nämlich festgelegt, dass die Verarbeitung durch einen Auftragsverarbeiter durch einen Vertrag oder einen anderen Rechtsakt geregelt wird. In Artikel 28 Absatz 3 Buchstabe f heißt es, dass der Vertrag oder sonstige Rechtsakt vorsehen muss, dass der Auftragsverarbeiter "den für die Verarbeitung Verantwortlichen bei der Einhaltung der Verpflichtungen nach den Artikeln 32 bis 36 unterstützt, wobei die Art der Verarbeitung und die dem Auftragsverarbeiter zur Verfügung stehenden Informationen zu berücksichtigen sind".

44. Artikel 33 Absatz 2 DSGVO stellt klar, dass ein Auftragsverarbeiter, der von einem für die Verarbeitung Verantwortlichen eingesetzt wird und von einer Verletzung der personenbezogenen Daten erfährt, die er im Auftrag des für die Verarbeitung Verantwortlichen verarbeitet, den für die Verarbeitung Verantwortlichen "unverzüglich" benachrichtigen muss. Es sei darauf hingewiesen, dass der Auftragsverarbeiter nicht erst die Wahrscheinlichkeit eines Risikos aufgrund einer Verletzung bewerten muss, bevor er den für die Verarbeitung Verantwortlichen benachrichtigt; diese Bewertung muss der für die Verarbeitung Verantwortliche vornehmen, sobald er von der Verletzung Kenntnis erhält. Der Auftragsverarbeiter muss lediglich feststellen, ob

---

[27] Siehe Verordnung Nr. 1182/71 zur Festlegung der Regeln für die Fristen, Daten und Termine, abrufbar unter: http://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:31971R1182&from=EN

[28] Siehe auch Erwägungsgrund 79 der Datenschutz-Grundverordnung.

eine Verletzung aufgetreten ist, und benachrichtigen dann den für die Verarbeitung Verantwortlichen. Der für die Verarbeitung Verantwortliche bedient sich des Auftragsverarbeiters, um seine Zwecke zu erreichen; daher sollte der für die Verarbeitung Verantwortliche grundsätzlich als "informiert" gelten, sobald der Auftragsverarbeiter ihn über die Verletzung informiert hat. Die Verpflichtung des Auftragsverarbeiters, den für die Verarbeitung Verantwortlichen zu benachrichtigen, gibt dem für die Verarbeitung Verantwortlichen die Möglichkeit, sich mit der Verletzung zu befassen und zu entscheiden, ob er die Aufsichtsbehörde gemäß Artikel 33 Absatz 1 und die betroffenen Personen gemäß Artikel 34 Absatz 1 benachrichtigen muss oder nicht. Der für die Verarbeitung Verantwortliche wird die Verletzung möglicherweise auch untersuchen wollen, da der Auftragsverarbeiter möglicherweise nicht in der Lage ist, alle relevanten Fakten in Bezug auf die Angelegenheit zu kennen, z. B. wenn sich eine Kopie oder Sicherungskopie der vom Auftragsverarbeiter zerstörten oder verloren gegangenen personenbezogenen Daten noch im Besitz des für die Verarbeitung Verantwortlichen befindet. Dies kann sich auf die Frage auswirken, ob der für die Verarbeitung Verantwortliche dann eine Meldung machen muss.

45. Die Datenschutz-Grundverordnung sieht keine ausdrückliche Frist vor, innerhalb derer der Auftragsverarbeiter den für die Verarbeitung Verantwortlichen benachrichtigen muss, sondern nur, dass er dies "ohne unangemessene Verzögerung" tun muss. Daher empfiehlt der EDSB, dass der Auftragsverarbeiter den für die Verarbeitung Verantwortlichen unverzüglich benachrichtigt und schrittweise weitere Informationen über die Verletzung bereitstellt, sobald weitere Einzelheiten verfügbar sind. Dies ist wichtig, damit der für die Verarbeitung Verantwortliche die Verpflichtung zur Meldung an die Aufsichtsbehörde innerhalb von 72 Stunden erfüllen kann.

46. Wie oben erläutert, sollte im Vertrag zwischen dem für die Verarbeitung Verantwortlichen und dem Auftragsverarbeiter festgelegt werden, wie die in Artikel 33 Absatz 2 genannten Anforderungen zusätzlich zu anderen Bestimmungen der Datenschutz-Grundverordnung erfüllt werden sollen. Dies kann Anforderungen für eine frühzeitige Meldung durch den Auftragsverarbeiter beinhalten, die wiederum die Verpflichtung des für die Verarbeitung Verantwortlichen unterstützen, der Aufsichtsbehörde innerhalb von 72 Stunden Bericht zu erstatten.

47. Erbringt der Auftragsverarbeiter Dienstleistungen für mehrere für die Verarbeitung Verantwortliche, die alle von demselben Vorfall betroffen sind, so muss er jedem für die Verarbeitung Verantwortlichen die Einzelheiten des Vorfalls mitteilen.

48. Ein Auftragsverarbeiter könnte eine Meldung im Namen des für die Verarbeitung Verantwortlichen vornehmen, wenn der für die Verarbeitung Verantwortliche dem Auftragsverarbeiter die entsprechende Genehmigung erteilt hat und dies Teil der vertraglichen Vereinbarungen zwischen dem für die Verarbeitung Verantwortlichen und dem Auftragsverarbeiter ist. Eine solche Meldung muss im Einklang mit Artikel 33 und 34 DSGVO erfolgen. Es ist jedoch wichtig zu beachten, dass die rechtliche Verantwortung für die Meldung bei dem für die Verarbeitung Verantwortlichen verbleibt.

B. Übermittlung von Informationen an die Aufsichtsbehörde

1. Zu liefernde Informationen

49. Wenn ein für die Verarbeitung Verantwortlicher der Aufsichtsbehörde einen Verstoß meldet, muss er gemäß Artikel 33 Absatz 3 DSGVO zumindest Folgendes tun:

> *"a) eine Beschreibung der Art der Verletzung des Schutzes personenbezogener Daten, einschließlich, soweit möglich, der Kategorien und der ungefähren Zahl der betroffenen Personen sowie der Kategorien und der ungefähren Zahl der betroffenen personenbezogenen Datensätze;*
>
> (b) *den Namen und die Kontaktdaten des Datenschutzbeauftragten oder einer anderen Kontaktstelle mitteilen, bei der weitere Informationen eingeholt werden können;*
>
> (c) *die voraussichtlichen Folgen der Verletzung des Schutzes personenbezogener Daten beschreiben;*
>
> (d) *Beschreibung der Maßnahmen, die der für die Verarbeitung Verantwortliche ergriffen hat oder zu ergreifen beabsichtigt, um die Verletzung des Schutzes personenbezogener Daten zu beheben,*

50. In der Datenschutz-Grundverordnung werden keine Kategorien von betroffenen Personen oder personenbezogenen Datensätzen definiert. Der EDSB schlägt jedoch Kategorien von betroffenen Personen vor, die sich auf die verschiedenen Arten von Personen beziehen, deren personenbezogene Daten von einer Verletzung betroffen sind: Je nach den verwendeten Deskriptoren könnten dies unter anderem Kinder und andere schutzbedürftige Gruppen, Menschen mit Behinderungen, Mitarbeiter oder Kunden sein. In ähnlicher Weise können sich Kategorien personenbezogener Datensätze auf die verschiedenen Arten von Datensätzen beziehen, die der für die Verarbeitung Verantwortliche möglicherweise verarbeitet, z. B. Gesundheitsdaten, Bildungsdaten, Informationen über die Sozialfürsorge, Finanzdaten, Bankkontonummern, Reisepassnummern usw.

51. In Erwägungsgrund 85 der Datenschutz-Grundverordnung wird klargestellt, dass einer der Zwecke der Benachrichtigung die Begrenzung des Schadens für den Einzelnen ist. Wenn also die Art der betroffenen Personen oder die Art der personenbezogenen Daten auf das Risiko eines besonderen Schadens infolge einer Sicherheitsverletzung hinweisen (z. B. Identitätsdiebstahl, Betrug, finanzieller Verlust, Gefährdung des Berufsgeheimnisses), dann ist es wichtig, dass die Meldung diese Kategorien angibt. Auf diese Weise ist sie mit der Anforderung verknüpft, die wahrscheinlichen Folgen der Verletzung zu beschreiben.

52. Wenn keine genauen Informationen verfügbar sind (z. B. die genaue Anzahl der betroffenen Personen), sollte dies kein Hindernis für eine rechtzeitige Meldung der Datenschutzverletzung sein. Die Datenschutz-Grundverordnung erlaubt es, bei der Zahl der betroffenen Personen und der Zahl der betroffenen personenbezogenen Datensätze Schätzungen vorzunehmen. Der Schwerpunkt sollte darauf liegen, die nachteiligen Auswirkungen der Sicherheitsverletzung zu beheben, anstatt genaue Zahlen zu nennen.

53. Wenn also klar ist, dass eine Verletzung vorliegt, aber das Ausmaß noch nicht bekannt ist, ist eine schrittweise Benachrichtigung (siehe unten) ein sicherer Weg, um die Benachrichtigungspflichten zu erfüllen.

54. In Artikel 33 Absatz 3 DSGVO heißt es, dass der für die Verarbeitung Verantwortliche mit einer Meldung "zumindest" diese Informationen bereitstellt, so dass ein für die Verarbeitung Verantwortlicher erforderlichenfalls weitere Einzelheiten angeben kann. Bei verschiedenen Arten von Verstößen (Vertraulichkeit, Integrität oder Verfügbarkeit) kann es erforderlich sein, weitere Informationen zu übermitteln, um die Umstände des jeweiligen Falls vollständig zu erläutern.

> **Beispiel**
>
> Im Rahmen der Meldung an die Aufsichtsbehörde kann es für einen für die Verarbeitung Verantwortlichen nützlich sein, seinen Auftragsverarbeiter zu nennen, wenn dieser die Ursache für eine Datenschutzverletzung ist, insbesondere wenn diese zu einem Vorfall geführt hat, der die

55. In jedem Fall kann die Aufsichtsbehörde im Rahmen ihrer Untersuchung eines Verstoßes weitere Einzelheiten anfordern.

2. Notifizierung in Phasen

56. Je nach Art des Verstoßes kann eine weitere Untersuchung durch den für die Verarbeitung Verantwortlichen erforderlich sein, um alle relevanten Fakten im Zusammenhang mit dem Vorfall zu ermitteln. Artikel 33 Absatz 4 der Datenschutz-Grundverordnung besagt daher:

> "*Ist es nicht möglich, die Informationen gleichzeitig zu übermitteln, so können sie ohne unangemessene Verzögerung schrittweise bereitgestellt werden*."

57. Dies bedeutet, dass die Datenschutz-Grundverordnung anerkennt, dass die für die Verarbeitung Verantwortlichen nicht immer alle erforderlichen Informationen über eine Sicherheitsverletzung innerhalb von 72 Stunden nach Bekanntwerden haben werden, da vollständige und umfassende Einzelheiten des Vorfalls in dieser ersten Zeit nicht immer zur Verfügung stehen können. Daher ist eine stufenweise Meldung möglich. Dies ist eher bei komplexeren Verstößen der Fall, wie z. B. bei einigen Arten von Cybersicherheitsvorfällen, bei denen z. B. eine eingehende forensische Untersuchung erforderlich sein kann, um die Art des Verstoßes und das Ausmaß der Gefährdung personenbezogener Daten vollständig zu ermitteln. Folglich wird der für die Verarbeitung Verantwortliche in vielen Fällen zu einem späteren Zeitpunkt weitere Nachforschungen anstellen und zusätzliche Informationen nachreichen müssen. Dies ist zulässig, sofern der für die Verarbeitung Verantwortliche gemäß Artikel 33 Absatz 1 DSGVO Gründe für die Verzögerung angibt. Der EDSB empfiehlt, dass der für die Verarbeitung Verantwortliche bei der ersten Meldung an die Aufsichtsbehörde auch mitteilen sollte, wenn er noch nicht über alle erforderlichen Informationen

verfügt und zu einem späteren Zeitpunkt weitere Einzelheiten vorlegen wird. Die Aufsichtsbehörde sollte vereinbaren, wie und wann die zusätzlichen Informationen bereitgestellt werden sollen. Dies hindert den für die Verarbeitung Verantwortlichen nicht daran, zu einem anderen Zeitpunkt weitere Informationen zu übermitteln, wenn ihm zusätzliche relevante Einzelheiten über die Verletzung bekannt werden, die der Aufsichtsbehörde vorgelegt werden müssen.

58. Der Schwerpunkt der Meldepflicht liegt darin, die für die Verarbeitung Verantwortlichen zu ermutigen, unverzüglich auf eine Sicherheitsverletzung zu reagieren, sie einzudämmen und, wenn möglich, die gefährdeten personenbezogenen Daten wiederherzustellen sowie die Aufsichtsbehörde um Rat zu fragen. Durch die Benachrichtigung der Aufsichtsbehörde innerhalb der ersten 72 Stunden kann der für die Verarbeitung Verantwortliche sicherstellen, dass die Entscheidungen über die Benachrichtigung oder Nichtbenachrichtigung von Personen korrekt sind.

59. Der Zweck der Benachrichtigung der Aufsichtsbehörde besteht jedoch nicht nur darin, Hinweise zu erhalten, ob die betroffenen Personen benachrichtigt werden sollen. In einigen Fällen wird es offensichtlich sein, dass der für die Verarbeitung Verantwortliche aufgrund der Art der Verletzung und der Schwere des Risikos die betroffenen Personen unverzüglich benachrichtigen muss. Wenn beispielsweise die unmittelbare Gefahr eines Identitätsdiebstahls besteht oder wenn besondere Kategorien personenbezogener Daten[29] online offengelegt werden, sollte der für die Verarbeitung Verantwortliche unverzüglich handeln, um die Verletzung einzudämmen und die betroffenen Personen zu benachrichtigen (siehe Abschnitt III). In Ausnahmefällen kann dies sogar vor der Benachrichtigung der Aufsichtsbehörde erfolgen. Generell kann die Benachrichtigung der Aufsichtsbehörde nicht als Rechtfertigung dafür dienen, dass die betroffene Person nicht über die Verletzung informiert wurde, wenn dies erforderlich ist.

60. Es sollte auch klar sein, dass ein für die Verarbeitung Verantwortlicher nach einer ersten Meldung die Aufsichtsbehörde auf den neuesten Stand bringen kann, wenn eine Folgeuntersuchung Beweise dafür liefert, dass der Sicherheitsvorfall eingedämmt wurde und tatsächlich keine Sicherheitsverletzung vorliegt. Diese Informationen könnten dann zu den bereits an die Aufsichtsbehörde übermittelten Informationen hinzugefügt werden, und der Vorfall könnte dementsprechend als kein Verstoß gewertet werden. Es gibt keine Strafe für die Meldung eines Vorfalls, der sich letztendlich nicht als Sicherheitsverletzung herausstellt.

Beispiel

Ein für die Verarbeitung Verantwortlicher meldet der Aufsichtsbehörde innerhalb von 72 Stunden nach Feststellung einer Datenschutzverletzung, dass er einen USB-Stick mit einer Kopie der personenbezogenen Daten einiger seiner Kunden verloren hat. Der USB-Stick wird später in den Räumlichkeiten des für die Verarbeitung Verantwortlichen falsch abgelegt gefunden und

61. Es sei darauf hingewiesen, dass ein stufenweiser Ansatz für die Meldung bereits im Rahmen der bestehenden Verpflichtungen der Richtlinie 2002/58/EG, der Verordnung (EU) Nr. 611/2013 und anderer selbstgemeldeter Vorfälle gilt.

3. Verspätete Benachrichtigungen

62. In Artikel 33 Absatz 1 der Datenschutz-Grundverordnung wird klargestellt, dass eine Meldung an die Aufsichtsbehörde, die nicht innerhalb von 72 Stunden erfolgt, mit einer Begründung für die Verzögerung versehen werden muss. Damit und mit dem Konzept der schrittweisen Benachrichtigung wird anerkannt, dass ein für die Verarbeitung Verantwortlicher nicht immer in der Lage ist, eine Verletzung innerhalb dieses Zeitraums zu melden, und dass eine verspätete Meldung zulässig sein kann.

63. Ein solches Szenario könnte beispielsweise eintreten, wenn ein für die Verarbeitung Verantwortlicher innerhalb eines kurzen Zeitraums mehrere ähnliche Verstöße gegen die Vertraulichkeit feststellt, von denen eine große Zahl von betroffenen Personen in gleicher Weise betroffen ist. Ein für die Verarbeitung Verantwortlicher könnte von einer Verletzung Kenntnis erlangen und, während er seine Untersuchung einleitet und vor der Benachrichtigung, weitere ähnliche Verletzungen feststellen, die unterschiedliche Ursachen haben. Je nach den Umständen kann es einige Zeit dauern, bis der für die Verarbeitung Verantwortliche das Ausmaß der Verstöße feststellt, und anstatt jeden Verstoß einzeln zu melden, organisiert er stattdessen eine umfassende Meldung, die mehrere sehr ähnliche Verstöße mit möglicherweise unterschiedlichen Ursachen umfasst. Dies könnte dazu führen, dass sich die Meldung an die Aufsichtsbehörde um mehr als 72 Stunden verzögert, nachdem der für die Verarbeitung Verantwortliche erstmals von diesen Verstößen Kenntnis erlangt hat.

64. Streng genommen ist jede einzelne Verletzung ein meldepflichtiger Vorfall. Um jedoch eine übermäßige Belastung zu vermeiden, kann der für die Verarbeitung Verantwortliche unter Umständen eine "gebündelte" Meldung einreichen, die alle diese Verstöße umfasst, sofern sie dieselbe Art personenbezogener Daten betreffen, die innerhalb eines relativ kurzen Zeitraums auf

dieselbe Weise verletzt wurden. Bei einer Reihe von Verstößen, die verschiedene Arten personenbezogener Daten betreffen, die auf unterschiedliche Weise verletzt wurden, sollte die Benachrichtigung auf die übliche Weise erfolgen, wobei jeder Verstoß gemäß Artikel 33 zu melden ist.

[29] Siehe Artikel 9 GDPR.

65. Die Datenschutz-Grundverordnung lässt zwar in gewissem Umfang verspätete Meldungen zu, doch sollte dies nicht als etwas angesehen werden, das regelmäßig vorkommt. Es ist erwähnenswert, dass gebündelte Meldungen auch für mehrere ähnliche Verstöße erfolgen können, die innerhalb von 72 Stunden gemeldet werden.

C. Grenzüberschreitende Verstöße und Verstöße in Nicht-EU-Betrieben

1. Grenzüberschreitende Verstöße

66. Bei einer grenzüberschreitenden Verarbeitung[30] personenbezogener Daten, kann eine Verletzung betroffene Personen in mehr als einem Mitgliedstaat betreffen. In Artikel 33 Absatz 1 DSGVO wird klargestellt, dass der für die Verarbeitung Verantwortliche die gemäß Artikel 55 DSGVO zuständige Aufsichtsbehörde benachrichtigen sollte, wenn eine Verletzung aufgetreten ist[31]. Artikel 55 Absatz 1 der Datenschutz-Grundverordnung besagt Folgendes:

> "*Jede Aufsichtsbehörde ist für die Wahrnehmung der ihr nach dieser Verordnung übertragenen Aufgaben und Befugnisse im Hoheitsgebiet ihres eigenen Mitgliedstaats zuständig*."

67. In Artikel 56 Absatz 1 der Datenschutz-Grundverordnung heißt es jedoch:

> "*Unbeschadet des Artikels 55 ist die Aufsichtsbehörde der Hauptniederlassung oder der einzigen Niederlassung des für die Verarbeitung Verantwortlichen oder des Auftragsverarbeiters dafür zuständig, nach dem Verfahren des Artikels 60 als federführende Aufsichtsbehörde für die von diesem Verantwortlichen oder Auftragsverarbeiter durchgeführte grenzüberschreitende Verarbeitung zu*

68. Außerdem heißt es in Artikel 56 Absatz 6 der Datenschutz-Grundverordnung:

> "*Die federführende Aufsichtsbehörde ist der einzige Gesprächspartner des für die Verarbeitung Verantwortlichen oder des Auftragsverarbeiters für die von diesem durchgeführte*

69. Dies bedeutet, dass der für die Verarbeitung Verantwortliche die federführende Aufsichtsbehörde benachrichtigen muss, wenn im Rahmen einer grenzüberschreitenden Verarbeitung eine Verletzung vorliegt und eine Benachrichtigung erforderlich ist[32]. Daher muss ein für die Verarbeitung Verantwortlicher bei der Ausarbeitung seines Plans zur Reaktion auf eine Sicherheitsverletzung beurteilen, welche Aufsichtsbehörde die federführende Aufsichtsbehörde ist, die er benachrichtigen muss[33]. Auf diese Weise kann der für die Verarbeitung Verantwortliche unverzüglich auf eine Datenschutzverletzung reagieren und seinen Verpflichtungen gemäß Artikel 33 nachkommen. Es sollte klar sein, dass im Falle einer Verletzung, die eine grenzüberschreitende Verarbeitung beinhaltet, die federführende Aufsichtsbehörde zu benachrichtigen ist, die nicht notwendigerweise der Ort ist, an dem sich die betroffenen Personen befinden oder an dem die Verletzung stattgefunden hat. Bei der Benachrichtigung der federführenden Behörde sollte der für die Verarbeitung Verantwortliche gegebenenfalls angeben, ob die Verletzung Einrichtungen in anderen Mitgliedstaaten betrifft und in welchen Mitgliedstaaten die betroffenen Personen wahrscheinlich von der Verletzung betroffen sind. Hat der für die Verarbeitung Verantwortliche Zweifel an der Identität der federführenden Aufsichtsbehörde, sollte er zumindest die örtliche Aufsichtsbehörde benachrichtigen, in der die Verletzung stattgefunden hat.

2. Verstöße in Nicht-EU-Betrieben

70. Artikel 3 DSGVO betrifft den territorialen Anwendungsbereich der DSGVO, einschließlich der Fälle, in denen sie für die Verarbeitung personenbezogener Daten durch einen für die Verarbeitung Verantwortlichen oder einen Auftragsverarbeiter gilt, der nicht in der EU ansässig ist. Artikel 3 Absatz 2 der Datenschutz-Grundverordnung besagt im Einzelnen[34]:

[30] Siehe Artikel 4 Absatz 23 der Datenschutz-Grundverordnung.
[31] Siehe auch Erwägungsgrund 122 der Datenschutz-Grundverordnung.
[32] Siehe WP29-Leitlinien zur Ermittlung der federführenden Aufsichtsbehörde eines für die Verarbeitung Verantwortlichen oder Auftragsverarbeiters, abrufbar unter http://ec.europa.eu/newsroom/document.cfm?doc_id=44102.
[33] Eine Liste der Kontaktdaten aller europäischen nationalen Datenschutzbehörden finden Sie unter: https://edpb.europa.eu/about-edpb/about-edpb/members_en
[34] Siehe auch die Erwägungsgründe 23 und 24 der Datenschutz-Grundverordnung.

"Diese Verordnung gilt für die Verarbeitung personenbezogener Daten von betroffenen Personen, die sich in der Union aufhalten, durch einen nicht in der Union niedergelassenen für die Verarbeitung Verantwortlichen oder Auftragsverarbeiter, wenn die Verarbeitungstätigkeiten im Zusammenhang stehen mit:

(a) *das Angebot von Waren oder Dienstleistungen an die betroffenen Personen in der Union, unabhängig davon, ob eine Zahlung der betroffenen Person erforderlich ist, oder*

71. Artikel 3 Absatz 3 der Datenschutz-Grundverordnung ist ebenfalls relevant und besagt[35]:

"*Diese Verordnung gilt für die Verarbeitung personenbezogener Daten durch einen für die Verarbeitung Verantwortlichen, der nicht in der Union, sondern an einem Ort ansässig ist, an dem das*

72. Fällt ein für die Verarbeitung Verantwortlicher, der nicht in der EU niedergelassen ist, unter Artikel 3 Absatz 2 oder Artikel 3 Absatz 3 DSGVO und kommt es zu einer Datenschutzverletzung, so ist er dennoch an die Meldepflichten gemäß Artikel 33 und 34 DSGVO gebunden. Nach Artikel 27 DSGVO muss ein für die Verarbeitung Verantwortlicher (und ein Auftragsverarbeiter) einen Vertreter in der EU benennen, wenn Artikel 3 Absatz 2 der DSGVO Anwendung findet.

73. Die bloße Anwesenheit eines Vertreters in einem Mitgliedstaat löst jedoch nicht das System der einzigen Anlaufstelle aus.[36] Aus diesem Grund muss die Sicherheitsverletzung jeder Aufsichtsbehörde gemeldet werden, bei der die betroffenen Personen in ihrem Mitgliedstaat ansässig sind. Diese Meldung(en) obliegt/erfolgen dem für die Verarbeitung Verantwortlichen.[37]

74. Unterliegt ein Auftragsverarbeiter Artikel 3 Absatz 2 der Datenschutz-Grundverordnung, so ist er an die Pflichten der Auftragsverarbeiter gebunden, insbesondere an die Pflicht, dem für die Verarbeitung Verantwortlichen gemäß Artikel 33 Absatz 2 der Datenschutz-Grundverordnung einen Verstoß zu melden.

D. Bedingungen, unter denen eine Meldung nicht erforderlich ist

75. Artikel 33 Absatz 1 DSGVO stellt klar, dass Verstöße, die "wahrscheinlich nicht zu einem Risiko für die Rechte und Freiheiten natürlicher Personen führen", nicht der Aufsichtsbehörde gemeldet werden müssen. Ein Beispiel wäre, wenn personenbezogene Daten bereits öffentlich zugänglich sind und eine Offenlegung dieser Daten kein wahrscheinliches Risiko für die betroffene Person darstellt. Dies steht im Gegensatz zu den bestehenden Meldepflichten für Anbieter öffentlich zugänglicher elektronischer Kommunikationsdienste in der Richtlinie 2009/136/EG, die besagen, dass alle relevanten Verstöße der zuständigen Behörde gemeldet werden müssen.

76. In ihrer Stellungnahme 03/2014 zur Meldung von Sicherheitsverletzungen[38] erklärte die WP29, dass eine Verletzung der Vertraulichkeit personenbezogener Daten, die mit einem dem Stand der Technik entsprechenden Algorithmus verschlüsselt wurden, immer noch eine Verletzung des Schutzes personenbezogener Daten darstellt und gemeldet werden muss. Wenn jedoch die Vertraulichkeit des Schlüssels intakt ist - d.h. der Schlüssel wurde nicht durch eine Sicherheitsverletzung kompromittiert und wurde so generiert, dass er mit den verfügbaren technischen Mitteln nicht von einer Person ermittelt werden kann, die nicht zum Zugriff darauf berechtigt ist - dann sind die Daten im Prinzip unverständlich. Daher ist es unwahrscheinlich, dass die Verletzung Personen beeinträchtigt und würde daher nicht

[35] Siehe auch Erwägungsgrund 25 der Datenschutz-Grundverordnung.
[36] Siehe WP29-Leitlinien zur Ermittlung der federführenden Aufsichtsbehörde eines für die Verarbeitung Verantwortlichen oder Auftragsverarbeiters, abrufbar unter http://ec.europa.eu/newsroom/document.cfm?doc_id=44102.
[37] Im Einklang mit den Leitlinien 3/2018 zum territorialen Anwendungsbereich der DSGVO (Artikel 3), abrufbar unter https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-32018-territorial-scope-

gdpr- article-3-version_en, ist der EDSB der Ansicht, dass die Funktion eines Vertreters in der Union nicht mit der Rolle eines externen Datenschutzbeauftragten ("DSB") vereinbar ist, weshalb die Verantwortung für die Benachrichtigung der Aufsichtsbehörde im Falle einer Verletzung des Schutzes personenbezogener Daten gemäß Artikel 27 Absatz 5 DSGVO weiterhin bei dem für die Verarbeitung Verantwortlichen liegt. Ein Vertreter kann jedoch in das Meldeverfahren einbezogen werden, wenn dies ausdrücklich im schriftlichen Mandat festgelegt wurde.

[38] WP29, Stellungnahme 03/2014 zur Meldung von Sicherheitsverletzungen, http://ec.europa.eu/justice/data- protection/article29/documentation/opinion-recommendation/files/2014/wp213_en.pdf

eine Mitteilung an diese Personen erfordern [39]. Aber auch bei verschlüsselten Daten kann ein Verlust oder eine Änderung negative Folgen für die betroffenen Personen haben, wenn der für die Verarbeitung Verantwortliche keine angemessenen Sicherungskopien hat. In diesem Fall wäre eine Mitteilung an die betroffenen Personen erforderlich, selbst wenn die Daten selbst angemessenen Verschlüsselungsmaßnahmen unterlagen.

77. Die WP29 erläuterte ferner, dass dies ebenfalls der Fall wäre, wenn personenbezogene Daten wie Passwörter sicher gehasht und gesalzen würden, der Hash-Wert mit einer dem Stand der Technik entsprechenden kryptografischen Schlüssel-Hash-Funktion berechnet würde, der zum Hashing der Daten verwendete Schlüssel nicht durch eine Verletzung kompromittiert würde und der zum Hashing der Daten verwendete Schlüssel so generiert würde, dass er mit den verfügbaren technischen Mitteln von keiner Person ermittelt werden kann, die nicht zum Zugriff darauf berechtigt ist.

78. Wenn personenbezogene Daten für Unbefugte im Wesentlichen unverständlich gemacht wurden und es sich bei den Daten um eine Kopie oder eine Sicherungskopie handelt, muss eine Verletzung der Vertraulichkeit, die ordnungsgemäß verschlüsselte personenbezogene Daten betrifft, der Aufsichtsbehörde unter Umständen nicht gemeldet werden. Denn es ist unwahrscheinlich, dass eine solche Verletzung ein Risiko für die Rechte und Freiheiten des Einzelnen darstellt. Dies bedeutet natürlich, dass auch die betroffene Person nicht informiert werden muss, da wahrscheinlich kein hohes Risiko besteht. Es ist jedoch zu bedenken, dass eine Benachrichtigung zwar zunächst nicht erforderlich ist, wenn kein Risiko für die Rechte und Freiheiten des Einzelnen besteht, sich dies jedoch im Laufe der Zeit ändern kann und das Risiko neu bewertet werden muss. Wenn sich zum Beispiel herausstellt, dass der Schlüssel kompromittiert ist oder eine Schwachstelle in der Verschlüsselungssoftware aufgedeckt wird, kann eine Meldung dennoch erforderlich sein.

79. Darüber hinaus ist zu beachten, dass bei einer Sicherheitsverletzung, bei der es keine Sicherungskopien der verschlüsselten personenbezogenen Daten gibt, eine Verletzung der Verfügbarkeit vorliegt, die ein Risiko für den Einzelnen darstellen könnte und daher möglicherweise eine Meldung erfordert. Ebenso kann eine Verletzung, bei der verschlüsselte Daten verloren gehen, auch dann eine meldepflichtige Verletzung darstellen, wenn eine Sicherungskopie der personenbezogenen Daten vorhanden ist, je nachdem, wie lange es dauert, die Daten aus dieser Sicherungskopie wiederherzustellen, und welche Auswirkungen die mangelnde Verfügbarkeit für die Betroffenen hat. Wie es in Artikel 32 Absatz 1 Buchstabe c der Datenschutz-Grundverordnung heißt, ist ein wichtiger Sicherheitsfaktor "*die Fähigkeit, die Verfügbarkeit und den Zugang zu personenbezogenen Daten im Falle eines physischen oder technischen Zwischenfalls rechtzeitig wiederherzustellen*".

Beispiel

Eine Verletzung, die keine Meldung an die Aufsichtsbehörde erfordert, wäre der Verlust eines sicher verschlüsselten mobilen Geräts, das von dem für die Verarbeitung Verantwortlichen und seinen Mitarbeitern verwendet wird. Sofern der Verschlüsselungsschlüssel im sicheren Besitz des für die Verarbeitung Verantwortlichen verbleibt und dies nicht die einzige Kopie der personenbezogenen Daten ist, wären die personenbezogenen Daten für einen Angreifer unzugänglich. Dies bedeutet, dass die Verletzung wahrscheinlich nicht zu einem Risiko für die Rechte und Freiheiten der betroffenen Personen führen wird. Wenn sich später herausstellt, dass der Verschlüsselungsschlüssel kompromittiert wurde oder dass die Verschlüsselungssoftware oder der Algorithmus angreifbar sind,

80. Ein Verstoß gegen Artikel 33 DSGVO liegt jedoch vor, wenn ein für die Verarbeitung Verantwortlicher die Aufsichtsbehörde in einer Situation, in der die Daten tatsächlich nicht sicher verschlüsselt wurden, nicht benachrichtigt. Daher sollten die für die Verarbeitung Verantwortlichen bei der Auswahl von Verschlüsselungssoftware die Qualität und die ordnungsgemäße Umsetzung der angebotenen Verschlüsselung sorgfältig abwägen und verstehen, welches Schutzniveau sie tatsächlich bietet und ob dieses den bestehenden Risiken angemessen ist. Die für die Kontrolle Verantwortlichen sollten auch die Funktionsweise des Verschlüsselungsprodukts genau kennen. So kann ein Gerät beispielsweise verschlüsselt sein, wenn es ausgeschaltet ist, aber nicht, wenn es sich

im Standby-Modus befindet. Einige Verschlüsselungsprodukte haben "Standardschlüssel", die von jedem Kunden geändert werden müssen, um wirksam zu sein. Es kann auch sein, dass die Verschlüsselung von Sicherheitsexperten derzeit als ausreichend angesehen wird, aber in einigen Jahren veraltet sein könnte,

[39] Siehe auch Artikel 4 Absätze 1 und 2 der Verordnung 611/2013.

Das heißt, es ist fraglich, ob die Daten durch dieses Produkt ausreichend verschlüsselt werden und ein angemessenes Schutzniveau bieten.

III. ARTIKEL 34 - MITTEILUNG AN DIE BETROFFENE PERSON

A. Information der Bürger

81. In bestimmten Fällen ist der für die Verarbeitung Verantwortliche verpflichtet, nicht nur die Aufsichtsbehörde zu benachrichtigen, sondern auch die betroffenen Personen über die Verletzung zu informieren.

Artikel 34(1) der Datenschutzgrundverordnung besagt:

> "Führt *die Verletzung des Schutzes personenbezogener Daten wahrscheinlich zu einem hohen Risiko für die Rechte und Freiheiten natürlicher Personen, teilt der für die Verarbeitung Verantwortliche der betroffenen Person die Verletzung des Schutzes personenbezogener Daten unverzüglich mit.*"

82. Die für die Verarbeitung Verantwortlichen sollten sich daran erinnern, dass eine Benachrichtigung der Aufsichtsbehörde obligatorisch ist, es sei denn, es ist unwahrscheinlich, dass ein Risiko für die Rechte und Freiheiten natürlicher Personen als Folge einer Verletzung besteht. Wenn ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen infolge eines Verstoßes wahrscheinlich ist, müssen die Betroffenen ebenfalls informiert werden. Die Schwelle für die Benachrichtigung von Personen über eine Sicherheitsverletzung ist daher höher als für die Benachrichtigung von Aufsichtsbehörden, und nicht alle Sicherheitsverletzungen müssen den Betroffenen mitgeteilt werden, um sie vor unnötiger Benachrichtigung zu schützen.

83. Die Datenschutz-Grundverordnung besagt, dass die Benachrichtigung der Betroffenen über eine Datenschutzverletzung "ohne unangemessene Verzögerung", d. h. so schnell wie möglich, erfolgen muss. Das Hauptziel der Benachrichtigung natürlicher Personen besteht darin, spezifische Informationen über Schritte zu liefern, die sie unternehmen sollten, um sich zu schützen[40]. Wie bereits erwähnt, wird eine rechtzeitige Benachrichtigung je nach Art der Verletzung und des Risikos den Betroffenen helfen, Maßnahmen zu ergreifen, um sich vor den negativen Folgen der Verletzung zu schützen.

84. Anhang B dieser Leitlinien enthält eine nicht erschöpfende Liste von Beispielen dafür, wann eine Verletzung wahrscheinlich zu einem hohen Risiko für Einzelpersonen führt und wann ein für die Verarbeitung Verantwortlicher die Betroffenen über eine Verletzung benachrichtigen muss.

B. Zu liefernde Informationen

85. In Artikel 34 Absatz 2 der Datenschutz-Grundverordnung ist festgelegt, dass Personen benachrichtigt werden müssen:

> "*Die Mitteilung an die betroffene Person nach Absatz 1 dieses Artikels beschreibt in klarer und einfacher Sprache die Art der Verletzung des Schutzes personenbezogener Daten und enthält mindestens die in Artikel 33 Absatz 3 Buchstaben b, c und d genannten Informationen und*

86. Gemäß dieser Bestimmung sollte der für die Verarbeitung Verantwortliche zumindest die folgenden Informationen bereitstellen:

- eine Beschreibung der Art des Verstoßes;
- den Namen und die Kontaktdaten des Datenschutzbeauftragten oder einer anderen Kontaktstelle;
- eine Beschreibung der voraussichtlichen Folgen des Verstoßes; und
- eine Beschreibung der Maßnahmen, die der für die Verarbeitung Verantwortliche ergriffen hat oder zu ergreifen gedenkt, um den Verstoß zu beheben, gegebenenfalls einschließlich Maßnahmen zur Abmilderung seiner möglichen nachteiligen Auswirkungen.

87. Als Beispiel für die Maßnahmen, die zur Behebung der Verletzung und zur Abmilderung ihrer möglichen nachteiligen Auswirkungen ergriffen wurden, könnte der für die Verarbeitung Verantwortliche angeben, dass er nach der Meldung der Verletzung bei der zuständigen Aufsichtsbehörde Ratschläge zur Bewältigung der Verletzung und zur Minderung ihrer Auswirkungen erhalten hat. Der für die Verarbeitung Verantwortliche sollte gegebenenfalls auch Einzelpersonen spezifische Ratschläge erteilen, um sich zu schützen vor

[40] Siehe auch Erwägungsgrund 86 der Datenschutz-Grundverordnung.

mögliche nachteilige Folgen der Sicherheitsverletzung, wie z. B. das Zurücksetzen von Passwörtern, wenn ihre Zugangsdaten kompromittiert wurden. Auch hier kann der für die Verarbeitung Verantwortliche über die hier geforderten Angaben hinausgehende Informationen bereitstellen.

C. Kontaktaufnahme mit Einzelpersonen

88. Grundsätzlich sollte die betreffende Verletzung den betroffenen Personen direkt mitgeteilt werden, es sei denn, dies würde einen unverhältnismäßigen Aufwand bedeuten. In einem solchen Fall muss stattdessen eine öffentliche Bekanntmachung oder eine ähnliche Maßnahme erfolgen, durch die die betroffenen Personen auf ebenso wirksame Weise informiert werden (Artikel 34 Absatz 3 Buchstabe c DSGVO).

89. Bei der Mitteilung einer Datenschutzverletzung an die betroffenen Personen sollten spezielle Nachrichten verwendet werden, die nicht zusammen mit anderen Informationen, wie z. B. regelmäßigen Aktualisierungen, Newslettern oder Standardnachrichten, verschickt werden sollten. Dies trägt dazu bei, dass die Mitteilung über die Sicherheitsverletzung klar und transparent ist.

90. Beispiele für transparente Kommunikationsmethoden sind direkte Nachrichten (z. B. E-Mail, SMS, Direktnachrichten), auffällige Banner oder Benachrichtigungen auf der Website, postalische Mitteilungen und auffällige Anzeigen in Printmedien. Eine Benachrichtigung, die ausschließlich in einer Pressemitteilung oder einem Unternehmensblog enthalten ist, wäre kein wirksames Mittel, um eine Person über eine Datenschutzverletzung zu informieren. Der EDSB empfiehlt, dass die für die Verarbeitung Verantwortlichen ein Mittel wählen sollten, das die Wahrscheinlichkeit maximiert, dass alle betroffenen Personen angemessen informiert werden. Je nach den Umständen kann dies bedeuten, dass der für die Verarbeitung Verantwortliche mehrere Kommunikationsmethoden einsetzt, anstatt nur einen einzigen Kontaktkanal zu nutzen.

91. Die für die Verarbeitung Verantwortlichen müssen unter Umständen auch dafür sorgen, dass die Kommunikation in geeigneten alternativen Formaten und in den relevanten Sprachen zugänglich ist, damit die Personen die ihnen zur Verfügung gestellten Informationen verstehen können. Wenn beispielsweise einer Person eine Datenschutzverletzung mitgeteilt wird, ist die Sprache, die im normalen Geschäftsverkehr mit dem Empfänger verwendet wurde, in der Regel angemessen. Betrifft die Datenschutzverletzung jedoch betroffene Personen, mit denen der für die Verarbeitung Verantwortliche noch nie zu tun hatte, oder insbesondere solche, die in einem anderen Mitgliedstaat oder einem anderen Nicht-EU-Land als dem, in dem der für die Verarbeitung Verantwortliche niedergelassen ist, ansässig sind, könnte eine Kommunikation in der Landessprache unter Berücksichtigung der erforderlichen Ressourcen akzeptabel sein. Entscheidend ist, dass die betroffenen Personen die Art der Datenschutzverletzung und die Schritte, die sie zu ihrem eigenen Schutz unternehmen können, verstehen.

92. Die für die Verarbeitung Verantwortlichen sind am besten in der Lage, den am besten geeigneten Kontaktkanal für die Mitteilung einer Sicherheitsverletzung an Einzelpersonen zu bestimmen, insbesondere wenn sie häufig mit ihren Kunden interagieren. Ein für die Verarbeitung Verantwortlicher sollte sich jedoch davor hüten, einen Kontaktkanal zu nutzen, der durch die Sicherheitsverletzung gefährdet ist, da dieser Kanal auch von Angreifern genutzt werden könnte, die sich als der für die Verarbeitung Verantwortliche ausgeben.

93. Gleichzeitig wird in Erwägungsgrund 86 der Datenschutz-Grundverordnung erklärt, dass:

> *"Solche Mitteilungen an die betroffenen Personen sollten so schnell wie möglich und in enger Zusammenarbeit mit der Aufsichtsbehörde erfolgen, wobei die von ihr oder von anderen einschlägigen Behörden wie den Strafverfolgungsbehörden gegebenen Hinweise zu beachten sind. Beispielsweise würde die Notwendigkeit, ein unmittelbares Schadensrisiko zu mindern, eine unverzügliche Mitteilung an die betroffenen Personen erfordern, während die Notwendigkeit, geeignete Maßnahmen gegen fortgesetzte oder ähnliche Verletzungen des Schutzes*

94. Die für die Verarbeitung Verantwortlichen sollten sich daher an die Aufsichtsbehörde wenden und

diese konsultieren, nicht nur um Ratschläge für die Unterrichtung der betroffenen Personen über eine Datenschutzverletzung gemäß Artikel 34 einzuholen, sondern auch um zu erfahren, welche Nachrichten an die betroffenen Personen zu senden sind und wie sie am besten zu kontaktieren sind.

95. Damit verbunden ist der Hinweis in Erwägungsgrund 88 der Datenschutz-Grundverordnung, dass bei der Benachrichtigung über eine Verletzung "die berechtigten Interessen der Strafverfolgungsbehörden berücksichtigt werden sollten, wenn eine frühzeitige Bekanntgabe die Untersuchung der Umstände einer Verletzung des Schutzes personenbezogener Daten unnötig behindern könnte". Dies kann bedeuten, dass der für die Verarbeitung Verantwortliche unter bestimmten Umständen in begründeten Fällen und auf Anraten der Strafverfolgungsbehörden die Benachrichtigung der betroffenen Personen über die Verletzung so lange hinauszögern kann, bis sie

würde solche Untersuchungen nicht beeinträchtigen. Allerdings müssten die betroffenen Personen auch nach diesem Zeitpunkt unverzüglich informiert werden.

96. Wenn es dem für die Verarbeitung Verantwortlichen nicht möglich ist, einer Person eine Verletzung mitzuteilen, weil die gespeicherten Daten nicht ausreichen, um die Person zu kontaktieren, sollte der für die Verarbeitung Verantwortliche die Person informieren, sobald dies nach vernünftigem Ermessen möglich ist (z. B. wenn eine Person ihr Recht auf Zugang zu personenbezogenen Daten nach Artikel 15 ausübt und dem für die Verarbeitung Verantwortlichen die für die Kontaktaufnahme erforderlichen zusätzlichen Informationen zur Verfügung stellt).

D. Bedingungen, unter denen eine Kommunikation nicht erforderlich ist

97. In Artikel 34 Absatz 3 DSGVO werden drei Bedingungen genannt, die, wenn sie erfüllt sind, keine Benachrichtigung von Personen im Falle einer Datenschutzverletzung erfordern. Diese sind:

- Der für die Verarbeitung Verantwortliche hat vor der Verletzung geeignete technische und organisatorische Maßnahmen zum Schutz personenbezogener Daten ergriffen, insbesondere solche, die personenbezogene Daten für Personen, die nicht zum Zugriff auf sie berechtigt sind, unverständlich machen. Dies könnte zum Beispiel Folgendes umfassen
  Schutz personenbezogener Daten durch modernste Verschlüsselung oder durch Tokenisierung.
- Unmittelbar nach einer Verletzung hat der für die Verarbeitung Verantwortliche Maßnahmen ergriffen, um sicherzustellen, dass das hohe Risiko für die Rechte und Freiheiten der betroffenen Personen wahrscheinlich nicht mehr gegeben ist. Je nach den Umständen des Falles kann der für die Verarbeitung Verantwortliche zum Beispiel unverzüglich Folgendes festgestellt haben
  und Maßnahmen gegen die Person ergriffen, die auf die personenbezogenen Daten zugegriffen hat, bevor diese etwas damit anfangen konnte. Die möglichen Folgen einer Verletzung der Vertraulichkeit müssen auch hier je nach Art der betroffenen Daten gebührend berücksichtigt werden.
- Es wäre ein unverhältnismäßiger Aufwand[41] Einzelpersonen zu kontaktieren, vielleicht wenn deren Kontakt
  Daten infolge der Verletzung verloren gegangen sind oder gar nicht erst bekannt sind. Zum Beispiel,
  das Lager eines statistischen Amtes überflutet wurde und die Dokumente mit personenbezogenen Daten nur in Papierform aufbewahrt wurden. Stattdessen muss der für die Verarbeitung Verantwortliche eine öffentliche Bekanntmachung veröffentlichen oder eine ähnliche Maßnahme ergreifen, durch die die betroffenen Personen in gleich wirksamer Weise informiert werden. Im Falle eines unverhältnismäßigen Aufwands könnten auch technische Vorkehrungen in Betracht gezogen werden, um Informationen über die Verletzung auf Anfrage zur Verfügung zu stellen, was sich für diejenigen Personen als nützlich erweisen könnte, die von einer Verletzung betroffen sein könnten, die der für die Verarbeitung Verantwortliche aber anderweitig nicht erreichen kann.

98. Gemäß dem Grundsatz der Rechenschaftspflicht sollten die für die Verarbeitung Verantwortlichen in der Lage sein, der Aufsichtsbehörde nachzuweisen, dass sie eine oder mehrere der folgenden Bedingungen erfüllen [42]. Es ist zu bedenken, dass eine Meldung zwar zunächst nicht erforderlich sein kann, wenn kein Risiko für die Rechte und Freiheiten natürlicher Personen besteht, dass sich dies aber im Laufe der Zeit ändern kann und das Risiko neu bewertet werden muss.

99. Wenn ein für die Verarbeitung Verantwortlicher beschließt, die betroffene Person nicht zu benachrichtigen, kann die Aufsichtsbehörde gemäß Artikel 34 Absatz 4 DSGVO dies verlangen, wenn sie der Ansicht ist, dass die Verletzung wahrscheinlich ein hohes Risiko für die betroffene Person darstellt. Sie kann aber auch der Ansicht sein, dass die Voraussetzungen des Artikels 34 Absatz 3 DSGVO erfüllt sind, so dass eine Benachrichtigung der Betroffenen nicht erforderlich ist. Stellt die Aufsichtsbehörde fest, dass die Entscheidung, die betroffenen Personen nicht zu benachrichtigen, nicht gut begründet ist, kann sie erwägen, von ihren verfügbaren Befugnissen und Sanktionen Gebrauch zu machen.

[41] Siehe WP29-Leitlinien zur Transparenz, in denen die Frage des unverhältnismäßigen Aufwands behandelt wird, verfügbar unter http://ec.europa.eu/newsroom/just/document.cfm?doc_id=48850

[42] Siehe Artikel 5 Absatz 2 der Datenschutz-Grundverordnung.

IV. RISIKOBEWERTUNG UND HOHES RISIKO

A. Risiko als Auslöser für eine Meldung

100. Obwohl die Datenschutz-Grundverordnung die Verpflichtung zur Meldung einer Datenschutzverletzung einführt, ist dies nicht unter allen Umständen erforderlich:

- Die zuständige Aufsichtsbehörde ist zu benachrichtigen, es sei denn, ein Verstoß führt wahrscheinlich nicht zu einem Risiko für die Rechte und Freiheiten von Personen.
- Die Benachrichtigung der betroffenen Person erfolgt nur dann, wenn eine Verletzung wahrscheinlich zu einem hohen Risiko für ihre Rechte und Freiheiten führt.

101. Das bedeutet, dass der für die Verarbeitung Verantwortliche unmittelbar nach Bekanntwerden einer Datenschutzverletzung nicht nur versuchen sollte, den Vorfall einzudämmen, sondern auch das Risiko, das sich daraus ergeben könnte, bewerten sollte. Dafür gibt es zwei wichtige Gründe: Erstens hilft die Kenntnis der Wahrscheinlichkeit und der potenziellen Schwere der Auswirkungen auf den Einzelnen dem für die Verarbeitung Verantwortlichen, wirksame Maßnahmen zur Eindämmung und Behebung der Verletzung zu ergreifen; zweitens hilft sie ihm zu bestimmen, ob eine Benachrichtigung der Aufsichtsbehörde und gegebenenfalls der betroffenen Personen erforderlich ist.

102. Wie oben erläutert, ist die Benachrichtigung über eine Verletzung erforderlich, es sei denn, es ist unwahrscheinlich, dass sie zu einem Risiko für die Rechte und Freiheiten natürlicher Personen führt, und der wichtigste Auslöser, der die Benachrichtigung der betroffenen Personen über eine Verletzung erforderlich macht, ist, dass sie wahrscheinlich zu einem *hohen* Risiko für die Rechte und Freiheiten natürlicher Personen führt. Dieses Risiko besteht, wenn die Verletzung zu einem physischen, materiellen oder immateriellen Schaden für die Personen führen kann, deren Daten verletzt wurden. Beispiele für solche Schäden sind Diskriminierung, Identitätsdiebstahl oder Betrug, finanzielle Verluste und Rufschädigung. Wenn die Verletzung personenbezogene Daten betrifft, aus denen die rassische oder ethnische Herkunft, politische Meinungen, religiöse oder philosophische Überzeugungen oder die Mitgliedschaft in einer Gewerkschaft hervorgehen, oder wenn sie genetische Daten, Daten über die Gesundheit oder Daten über das Sexualleben oder strafrechtliche Verurteilungen und Straftaten oder damit zusammenhängende Sicherheitsmaßnahmen umfasst, sollte ein solcher Schaden als wahrscheinlich angesehen werden[43].

B. Faktoren, die bei der Risikobewertung zu berücksichtigen sind

103. In den Erwägungsgründen 75 und 76 der Datenschutz-Grundverordnung wird vorgeschlagen, dass bei der Risikobewertung generell sowohl die Wahrscheinlichkeit als auch die Schwere des Risikos für die Rechte und Freiheiten der betroffenen Personen berücksichtigt werden sollten. Ferner heißt es dort, dass das Risiko auf der Grundlage einer objektiven Bewertung beurteilt werden sollte.

104. Es ist anzumerken, dass die Bewertung des Risikos für die Rechte und Freiheiten der Menschen infolge eines Verstoßes einen anderen Schwerpunkt hat als das Risiko, das in einer Datenschutzfolgenabschätzung betrachtet wird.)[44]. Bei der Datenschutzfolgenabschätzung werden sowohl die Risiken einer planmäßigen Datenverarbeitung als auch die Risiken im Falle einer Datenschutzverletzung berücksichtigt. Bei der Betrachtung einer potenziellen Sicherheitsverletzung werden ganz allgemein die Wahrscheinlichkeit eines solchen Ereignisses und der Schaden für die betroffene Person untersucht, d. h. es handelt sich um eine Bewertung eines hypothetischen Ereignisses. Bei einer tatsächlichen Verletzung ist das Ereignis bereits eingetreten, so dass der Schwerpunkt ausschließlich auf dem daraus resultierenden Risiko und den Auswirkungen der Verletzung auf den Einzelnen liegt.

Beispiel

Eine Datenschutz-Folgenabschätzung legt nahe, dass die vorgeschlagene Verwendung einer bestimmten Sicherheitssoftware zum Schutz personenbezogener Daten eine geeignete Maßnahme ist, um ein Sicherheitsniveau zu gewährleisten, das dem Risiko angemessen ist, das die Verarbeitung ansonsten für den Einzelnen darstellen würde. Wenn jedoch später eine Schwachstelle bekannt wird, würde sich die Eignung der Software zur Eindämmung des Risikos für die geschützten

[43] Siehe Erwägungsgrund 75 und Erwägungsgrund 85 der DSGVO.
[44] Siehe WP-Leitlinien zu DPIAs hier: http://ec.europa.eu/newsroom/document.cfm?doc_id=44137

eine Verletzung auftritt. Der für die Verarbeitung Verantwortliche sollte die besonderen Umstände der Sicherheitsverletzung, die betroffenen Daten und die potenziellen Auswirkungen auf den

105. Dementsprechend sollte der für die Verarbeitung Verantwortliche bei der Bewertung des Risikos für Einzelpersonen infolge eines Verstoßes die besonderen Umstände des Verstoßes berücksichtigen, einschließlich der Schwere der potenziellen Auswirkungen und der Wahrscheinlichkeit, dass diese eintreten. Der EDPB empfiehlt daher, dass bei der Bewertung folgende Kriterien berücksichtigt werden sollten[45]:

- **Die Art des Verstoßes**

106. Die Art der Sicherheitsverletzung kann das Ausmaß des Risikos für den Einzelnen beeinflussen. So kann beispielsweise eine Verletzung der Vertraulichkeit, bei der medizinische Informationen an Unbefugte weitergegeben wurden, andere Folgen für den Einzelnen haben als eine Verletzung, bei der die medizinischen Daten einer Person verloren gegangen und nicht mehr verfügbar sind.

- **Art, Sensibilität und Umfang der personenbezogenen Daten**

107. Ein Schlüsselfaktor bei der Risikobewertung ist natürlich die Art und Sensibilität der personenbezogenen Daten, die durch die Sicherheitsverletzung gefährdet wurden. Je sensibler die Daten sind, desto größer ist in der Regel das Risiko eines Schadens für die betroffenen Personen, aber es sollten auch andere personenbezogene Daten berücksichtigt werden, die möglicherweise bereits über die betroffene Person verfügbar sind. So ist es zum Beispiel unwahrscheinlich, dass die Offenlegung des Namens und der Adresse einer Person unter normalen Umständen einen erheblichen Schaden verursacht. Wenn jedoch der Name und die Adresse eines Adoptivelternteils an ein leibliches Elternteil weitergegeben werden, könnten die Folgen sowohl für den Adoptivelternteil als auch für das Kind sehr schwerwiegend sein.

108. Verletzungen von Gesundheitsdaten, Identitätsdokumenten oder Finanzdaten wie Kreditkartendaten können alle für sich genommen Schaden anrichten, aber wenn sie zusammen verwendet werden, könnten sie zum Identitätsdiebstahl genutzt werden. Eine Kombination personenbezogener Daten ist in der Regel sensibler als ein einzelnes Stück personenbezogener Daten.

109. Einige Arten personenbezogener Daten mögen auf den ersten Blick relativ harmlos erscheinen, doch sollte sorgfältig geprüft werden, was diese Daten über die betroffene Person verraten können. Eine Liste von Kunden, die regelmäßige Lieferungen annehmen, mag nicht besonders sensibel sein, aber dieselben Daten über Kunden, die darum gebeten haben, dass ihre Lieferungen während ihres Urlaubs gestoppt werden, wären nützliche Informationen für Kriminelle.

110. Ebenso kann eine kleine Menge hochsensibler personenbezogener Daten eine große Auswirkung auf eine Person haben, und eine große Anzahl von Details kann eine größere Bandbreite von Informationen über diese Person offenbaren. Auch eine Sicherheitsverletzung, die große Mengen personenbezogener Daten über viele betroffene Personen betrifft, kann sich auf eine entsprechend große Zahl von Personen auswirken.

- **Leichte Identifizierung von Personen**

111. Ein wichtiger zu berücksichtigender Faktor ist, wie einfach es für eine Partei, die Zugang zu kompromittierten personenbezogenen Daten hat, ist, bestimmte Personen zu identifizieren oder die Daten mit anderen Informationen abzugleichen, um Personen zu identifizieren. Je nach den Umständen kann die Identifizierung direkt anhand der verletzten personenbezogenen Daten möglich sein, ohne dass besondere Nachforschungen zur Ermittlung der Identität der Person erforderlich sind, oder es kann äußerst schwierig sein, personenbezogene Daten einer bestimmten Person zuzuordnen, aber unter bestimmten Bedingungen ist es dennoch möglich. Die Identifizierung kann direkt oder indirekt anhand der verletzten Daten möglich sein, sie kann aber auch vom spezifischen Kontext der Verletzung und der öffentlichen Verfügbarkeit damit verbundener personenbezogener Daten abhängen. Dies kann bei Verstößen gegen die Vertraulichkeit und die Verfügbarkeit von Daten von

größerer Bedeutung sein.

[45] Artikel 3 Absatz 2 der Verordnung (EU) Nr. 611/2013 enthält Leitlinien zu den Faktoren, die bei der Meldung von Verstößen im Bereich der elektronischen Kommunikationsdienste zu berücksichtigen sind und die im Zusammenhang mit der Meldung nach der Datenschutz-Grundverordnung nützlich sein können. Siehe http://eur- lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2013:173:0002:0008:de:PDF

112. Wie bereits erwähnt, sind personenbezogene Daten, die durch ein angemessenes Verschlüsselungsniveau geschützt sind, für Unbefugte ohne den Entschlüsselungscode unverständlich. Darüber hinaus kann eine angemessen umgesetzte Pseudonymisierung (definiert in Artikel 4 Absatz 5 DSGVO als "*die Verarbeitung personenbezogener Daten in einer Weise, dass die personenbezogenen Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden können, sofern diese zusätzlichen Informationen gesondert aufbewahrt werden und technischen und organisatorischen Maßnahmen unterliegen, die gewährleisten, dass die personenbezogenen Daten nicht einer identifizierten oder identifizierbaren natürlichen Person zugewiesen werden*") ebenfalls die Wahrscheinlichkeit verringern, dass Personen im Falle einer Datenschutzverletzung identifiziert werden können. Pseudonymisierungstechniken allein können jedoch nicht als Mittel zur Unkenntlichmachung der Daten angesehen werden.

- **Schwere der Folgen für den Einzelnen**

113. Je nach Art der personenbezogenen Daten, die von einer Verletzung betroffen sind, z. B. besondere Datenkategorien, kann der potenzielle Schaden für Einzelpersonen besonders schwerwiegend sein, insbesondere wenn die Verletzung zu Identitätsdiebstahl oder Betrug, körperlichem Schaden, psychischem Leid, Demütigung oder Rufschädigung führen könnte. Betrifft die Datenschutzverletzung personenbezogene Daten schutzbedürftiger Personen, könnten diese einem größeren Risiko ausgesetzt sein.

114. Ob der für die Verarbeitung Verantwortliche weiß, dass sich personenbezogene Daten in den Händen von Personen befinden, deren Absichten unbekannt oder möglicherweise böswillig sind, kann einen Einfluss auf das Ausmaß des potenziellen Risikos haben. Es kann eine Verletzung der Vertraulichkeit vorliegen, bei der personenbezogene Daten irrtümlich an einen Dritten im Sinne von Artikel 4 Absatz 10 oder einen anderen Empfänger weitergegeben werden. Dies kann z. B. der Fall sein, wenn personenbezogene Daten versehentlich an die falsche Abteilung einer Organisation oder an eine häufig genutzte Lieferantenorganisation übermittelt werden. Der für die Verarbeitung Verantwortliche kann den Empfänger auffordern, die erhaltenen Daten entweder zurückzugeben oder sicher zu vernichten. In beiden Fällen kann der Empfänger als "vertrauenswürdig" eingestuft werden, da der für die Verarbeitung Verantwortliche eine laufende Beziehung zu ihm unterhält und ihm seine Verfahren, seine Geschichte und andere relevante Details bekannt sind. Mit anderen Worten: Der für die Verarbeitung Verantwortliche kann sich auf den Empfänger verlassen, so dass er vernünftigerweise erwarten kann, dass dieser die irrtümlich übermittelten Daten nicht liest oder darauf zugreift und seine Anweisungen zur Rückgabe der Daten befolgt. Selbst wenn auf die Daten zugegriffen wurde, kann der für die Verarbeitung Verantwortliche möglicherweise darauf vertrauen, dass der Empfänger keine weiteren Maßnahmen ergreift und die Daten unverzüglich an den für die Verarbeitung Verantwortlichen zurücksendet und bei ihrer Wiederherstellung mitwirkt. In solchen Fällen kann dies in die Risikobewertung einfließen, die der für die Verarbeitung Verantwortliche nach der Verletzung vornimmt - die Tatsache, dass der Empfänger Vertrauen genießt, kann die Schwere der Folgen der Verletzung mildern, bedeutet aber nicht, dass keine Verletzung vorliegt. Dies wiederum kann jedoch die Wahrscheinlichkeit eines Risikos für Einzelpersonen beseitigen, so dass keine Benachrichtigung der Aufsichtsbehörde oder der betroffenen Personen mehr erforderlich ist. Auch hier wird dies von Fall zu Fall entschieden. Dennoch muss der für die Verarbeitung Verantwortliche im Rahmen der allgemeinen Pflicht, Aufzeichnungen über Verstöße zu führen, Informationen über die Verletzung aufbewahren (siehe Abschnitt V unten).

115. Es sollte auch die Dauerhaftigkeit der Folgen für den Einzelnen berücksichtigt werden, wobei die Auswirkungen als größer angesehen werden können, wenn die Folgen langfristig sind.

- **Besondere Merkmale der Person**

116. Eine Sicherheitsverletzung kann personenbezogene Daten von Kindern oder anderen schutzbedürftigen Personen betreffen, die dadurch einer größeren Gefahr ausgesetzt sein können. Es kann andere Faktoren in Bezug auf die betreffende Person geben, die das Ausmaß der Auswirkungen der Sicherheitsverletzung auf sie beeinflussen können.

- **Besondere Merkmale des für die Datenverarbeitung Verantwortlichen**

117. Die Art und Rolle des für die Verarbeitung Verantwortlichen und seine Tätigkeiten können sich auf das Ausmaß des Risikos für Einzelpersonen infolge einer Verletzung auswirken. Eine medizinische Einrichtung wird beispielsweise besondere Kategorien personenbezogener Daten verarbeiten, was bedeutet, dass die Gefahr für Einzelpersonen größer ist, wenn ihre personenbezogenen Daten verletzt werden, als bei einer Mailingliste einer Zeitung.

- **Die Anzahl der betroffenen Personen**

118. Eine Sicherheitsverletzung kann nur eine oder einige wenige Personen betreffen, aber auch mehrere Tausend, wenn nicht sogar viel mehr. Generell gilt: Je mehr Personen betroffen sind, desto größer sind die Auswirkungen einer Sicherheitsverletzung. Je nach Art der personenbezogenen Daten und dem Kontext, in dem sie kompromittiert wurden, kann eine Sicherheitsverletzung jedoch auch für eine einzelne Person schwerwiegende Folgen haben. Auch hier kommt es darauf an, die Wahrscheinlichkeit und Schwere der Auswirkungen auf die Betroffenen zu berücksichtigen.

- **Allgemeine Punkte**

119. Daher sollte der für die Verarbeitung Verantwortliche bei der Bewertung des Risikos, das sich aus einem Verstoß ergeben könnte, eine Kombination aus der Schwere der potenziellen Auswirkungen auf die Rechte und Freiheiten von Personen und der Wahrscheinlichkeit ihres Eintretens berücksichtigen. Es liegt auf der Hand, dass das Risiko höher ist, wenn die Folgen eines Verstoßes schwerwiegender sind, und dass das Risiko ebenfalls höher ist, wenn die Wahrscheinlichkeit des Eintretens größer ist. Im Zweifelsfall sollte der für die Verarbeitung Verantwortliche auf Nummer sicher gehen und eine Meldung machen. Anhang B enthält einige nützliche Beispiele für verschiedene Arten von Verstößen, die ein Risiko oder ein hohes Risiko für Einzelpersonen darstellen.

120. Die Agentur der Europäischen Union für Netz- und Informationssicherheit (ENISA) hat Empfehlungen für eine Methodik zur Bewertung der Schwere einer Sicherheitsverletzung ausgearbeitet, die für die Verarbeitung Verantwortlichen und Auftragsverarbeitern bei der Ausarbeitung ihres Plans zur Reaktion auf Sicherheitsverletzungen nützlich sein können[46].

V. RECHENSCHAFTSPFLICHT UND FÜHRUNG VON AUFZEICHNUNGEN

A. Dokumentieren von Verstößen

121. Unabhängig davon, ob eine Datenschutzverletzung der Aufsichtsbehörde gemeldet werden muss oder nicht, muss der für die Verarbeitung Verantwortliche alle Verstöße dokumentieren, wie in Artikel 33 Absatz 5 der Datenschutz-Grundverordnung erläutert:

> "*Der für die Verarbeitung Verantwortliche dokumentiert jede Verletzung des Schutzes personenbezogener Daten, einschließlich der Fakten im Zusammenhang mit der Verletzung des Schutzes personenbezogener Daten, ihrer Auswirkungen und der getroffenen Abhilfemaßnahmen.*

122. Dies steht im Zusammenhang mit dem Grundsatz der Rechenschaftspflicht, der in Artikel 5 Absatz 2 der Datenschutz-Grundverordnung enthalten ist. Der Zweck der Aufzeichnung von nicht meldepflichtigen und meldepflichtigen Verstößen bezieht sich auch auf die Verpflichtungen des für die Verarbeitung Verantwortlichen gemäß Artikel 24 DSGVO, und die Aufsichtsbehörde kann Einsicht in diese Aufzeichnungen verlangen. Den für die Verarbeitung Verantwortlichen wird daher empfohlen, ein internes Register der Verstöße zu erstellen, unabhängig davon, ob sie meldepflichtig sind oder nicht[47].

123. Während es dem für die Verarbeitung Verantwortlichen überlassen bleibt, welche Methode und Struktur er bei der Dokumentation einer Datenschutzverletzung anwendet, gibt es im Hinblick auf die aufzeichnungspflichtigen Informationen einige Schlüsselelemente, die in jedem Fall enthalten sein sollten. Wie in Artikel 33 Absatz 5 DSGVO vorgeschrieben, muss der für die Verarbeitung Verantwortliche die Einzelheiten der Verletzung aufzeichnen, einschließlich der Ursachen, des Ablaufs und der betroffenen personenbezogenen Daten. Auch die Auswirkungen und Folgen der Verletzung sowie die von dem für die Verarbeitung Verantwortlichen ergriffenen Abhilfemaßnahmen sollten darin enthalten sein.

124. In der Datenschutz-Grundverordnung ist keine Aufbewahrungsfrist für solche Unterlagen festgelegt. Wenn solche Aufzeichnungen personenbezogene Daten enthalten, obliegt es dem für die Verarbeitung Verantwortlichen, die angemessene Aufbewahrungsfrist im Einklang mit den

Grundsätzen für die Verarbeitung personenbezogener Daten festzulegen[48] und eine rechtmäßige Grundlage für die Verarbeitung zu schaffen[49]. Er muss die Dokumentation gemäß Artikel 33 Absatz 5 aufbewahren.

---

[46] ENISA, Recommendations for a methodology of the assessment of severity of personal data breaches, https://www.enisa.europa.eu/publications/dbn-severity

[47] Der für die Verarbeitung Verantwortliche kann sich dafür entscheiden, Verstöße als Teil seines gemäß Artikel 30 DSGVO geführten Verzeichnisses der Verarbeitungstätigkeiten zu dokumentieren. Ein gesondertes Register ist nicht erforderlich, sofern die für die Datenschutzverletzung relevanten Informationen eindeutig als solche erkennbar sind und auf Anfrage entnommen werden können.

[48] Siehe Artikel 5 GDPR.

[49] Siehe Artikel 6 und auch Artikel 9 GDPR.

Datenschutz-Grundverordnung (DSGVO), sofern sie aufgefordert werden kann, der Aufsichtsbehörde die Einhaltung dieses Artikels oder des Grundsatzes der Rechenschaftspflicht im Allgemeinen nachzuweisen. Wenn die Aufzeichnungen selbst keine personenbezogenen Daten enthalten, gilt der Grundsatz der Speicherbegrenzung[50] der Datenschutz-Grundverordnung nicht anwendbar.

125. Zusätzlich zu diesen Einzelheiten empfiehlt der EDSB, dass der für die Verarbeitung Verantwortliche auch seine Gründe für die als Reaktion auf eine Verletzung getroffenen Entscheidungen dokumentiert. Insbesondere, wenn eine Verletzung nicht gemeldet wird, sollte eine Begründung für diese Entscheidung dokumentiert werden. Dabei sollte auch begründet werden, warum der für die Verarbeitung Verantwortliche der Ansicht ist, dass die Verletzung wahrscheinlich nicht zu einem Risiko für die Rechte und Freiheiten von Personen führt [51] . Wenn der für die Verarbeitung Verantwortliche der Ansicht ist, dass eine der Bedingungen in Artikel 34 Absatz 3 DSGVO erfüllt ist, sollte er in der Lage sein, geeignete Nachweise dafür zu erbringen, dass dies der Fall ist.

126. Meldet der für die Verarbeitung Verantwortliche der Aufsichtsbehörde zwar einen Verstoß, aber mit Verspätung, so muss er in der Lage sein, diese Verspätung zu begründen; entsprechende Unterlagen könnten helfen, nachzuweisen, dass die Verspätung bei der Meldung gerechtfertigt und nicht übermäßig ist.

127. Teilt der für die Verarbeitung Verantwortliche den betroffenen Personen eine Datenschutzverletzung mit, so sollte er die Verletzung transparent darstellen und die Mitteilung wirksam und rechtzeitig vornehmen. Dementsprechend würde es dem für die Verarbeitung Verantwortlichen helfen, seine Rechenschaftspflicht und die Einhaltung der Vorschriften nachzuweisen, indem er Belege für eine solche Mitteilung aufbewahrt.

128. Um die Einhaltung der Artikel 33 und 34 DSGVO zu unterstützen, wäre es sowohl für die für die Verarbeitung Verantwortlichen als auch für die Auftragsverarbeiter vorteilhaft, über ein dokumentiertes Meldeverfahren zu verfügen, in dem das Verfahren festgelegt ist, das zu befolgen ist, sobald eine Datenschutzverletzung festgestellt wurde, einschließlich der Eindämmung, Bewältigung und Wiederherstellung des Vorfalls sowie der Risikobewertung und der Meldung der Verletzung. Um die Einhaltung der DSGVO nachzuweisen, könnte es auch nützlich sein, nachzuweisen, dass die Mitarbeiter über die Existenz solcher Verfahren und Mechanismen informiert wurden und dass sie wissen, wie sie auf Datenschutzverletzungen reagieren sollen.

129. Es sei darauf hingewiesen, dass das Versäumnis, einen Verstoß ordnungsgemäß zu dokumentieren, dazu führen kann, dass die Aufsichtsbehörde ihre Befugnisse gemäß Artikel 58 DSGVO ausübt oder eine Geldstrafe gemäß Artikel 83 DSGVO verhängt.

B. Die Rolle des Datenschutzbeauftragten

130. Ein für die Verarbeitung Verantwortlicher oder ein Auftragsverarbeiter kann einen Datenschutzbeauftragten (DSB)[52]haben, entweder gemäß Artikel 37 DSGVO oder freiwillig im Rahmen der guten Praxis. Artikel 39 der Datenschutz-Grundverordnung legt eine Reihe obligatorischer Aufgaben für den DSB fest, schließt jedoch nicht aus, dass der für die Verarbeitung Verantwortliche gegebenenfalls weitere Aufgaben zuweisen kann.

131. Zu den obligatorischen Aufgaben des DSB, die für die Meldung von Datenschutzverletzungen von besonderer Bedeutung sind, gehören unter anderem die Beratung und Information des für die Verarbeitung Verantwortlichen oder des Auftragsverarbeiters über den Datenschutz, die Überwachung der Einhaltung der DSGVO und die Beratung in Bezug auf die Datenschutzfolgenabschätzung. Der DSB muss auch mit der Aufsichtsbehörde zusammenarbeiten und als Kontaktstelle für die Aufsichtsbehörde und für betroffene Personen fungieren. Zu beachten ist auch, dass der für die Verarbeitung Verantwortliche bei der Meldung der Datenschutzverletzung an die Aufsichtsbehörde gemäß Artikel 33 Absatz 3 Buchstabe b der DSGVO den Namen und die Kontaktdaten seines DSB oder einer anderen Kontaktstelle angeben muss.

132. Was die Dokumentation von Verstößen angeht, so könnte der für die Verarbeitung Verantwortliche oder der Auftragsverarbeiter die Meinung seines DSB zur Struktur, Einrichtung und Verwaltung dieser Dokumentation einholen. Der DSB könnte auch zusätzlich mit der Führung solcher Aufzeichnungen beauftragt werden.

133. Diese Faktoren bedeuten, dass der behördliche Datenschutzbeauftragte eine Schlüsselrolle bei der Vorbeugung oder Vorbereitung auf eine Sicherheitsverletzung spielen sollte, indem er beratend tätig wird und die Einhaltung der Vorschriften überwacht, aber auch während einer Sicherheitsverletzung

---

[50] Siehe Artikel 5 Absatz 1 Buchstabe e) der Datenschutz-Grundverordnung.

[51] Siehe Erwägungsgrund 85 der Datenschutz-Grundverordnung.

[52] Siehe WP-Leitlinien für behördliche Datenschutzbeauftragte hier: http://ec.europa.eu/newsroom/just/item-detail.cfm?item_id=50083

(d. h. bei der Benachrichtigung der Aufsichtsbehörde) und während der anschließenden Untersuchung durch die Aufsichtsbehörde. Vor diesem Hintergrund empfiehlt der EDSB, dass der DSB unverzüglich über das Vorliegen einer Datenschutzverletzung informiert wird und während des gesamten Verfahrens zur Bewältigung der Datenschutzverletzung und der Benachrichtigung einbezogen wird.

VI. MELDEPFLICHTEN AUS ANDEREN RECHTSINSTRUMENTEN

134. Zusätzlich und unabhängig von der Benachrichtigung und Mitteilung von Verstößen gemäß der DSGVO sollten sich die für die Verarbeitung Verantwortlichen auch darüber im Klaren sein, ob sie aufgrund anderer einschlägiger Rechtsvorschriften verpflichtet sind, Sicherheitsvorfälle zu melden, und ob sie möglicherweise gleichzeitig die Aufsichtsbehörde über einen Verstoß gegen den Schutz personenbezogener Daten informieren müssen. Solche Anforderungen können von Mitgliedstaat zu Mitgliedstaat unterschiedlich sein, aber Beispiele für Meldepflichten in anderen Rechtsinstrumenten und deren Zusammenspiel mit der DSGVO sind die folgenden:

- *Verordnung (EU) 910/2014 über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt (eIDAS-Verordnung)*[53].

135. Gemäß Artikel 19 Absatz 2 der eIDAS-Verordnung müssen Vertrauensdiensteanbieter ihre Aufsichtsbehörde über eine Sicherheitsverletzung oder einen Integritätsverlust benachrichtigen, die bzw. der erhebliche Auswirkungen auf den bereitgestellten Vertrauensdienst oder die darin gespeicherten personenbezogenen Daten hat. Gegebenenfalls - d. h. wenn eine solche Verletzung oder ein solcher Verlust auch eine Verletzung des Schutzes personenbezogener Daten nach der DSGVO darstellt - sollte der Vertrauensdiensteanbieter auch die Aufsichtsbehörde benachrichtigen.

- *Richtlinie (EU) 2016/1148 über Maßnahmen zur Gewährleistung eines hohen gemeinsamen Sicherheitsniveaus für Netz- und Informationssysteme in der Union (NIS-Richtlinie)*[54].

136. Nach Artikel 14 und 16 der NIS-Richtlinie sind Betreiber wesentlicher Dienste und Anbieter digitaler Dienste verpflichtet, ihrer zuständigen Behörde Sicherheitsvorfälle zu melden. Wie in Erwägungsgrund 63 der NIS[55]anerkannt, können Sicherheitsvorfälle oft eine Kompromittierung personenbezogener Daten beinhalten. Während die NIS von den zuständigen Behörden und den Aufsichtsbehörden verlangt, in diesem Zusammenhang zusammenzuarbeiten und Informationen auszutauschen, ist es nach wie vor so, dass in Fällen, in denen solche Vorfälle Verstöße gegen die Datenschutz-Grundverordnung darstellen oder zu solchen werden, die Betreiber und/oder Anbieter verpflichtet wären, die Aufsichtsbehörde unabhängig von den Meldepflichten für Vorfälle gemäß der NIS zu informieren.

Beispiel

Ein Cloud-Diensteanbieter, der eine Verletzung gemäß der NIS-Richtlinie meldet, muss möglicherweise auch einen für die Verarbeitung Verantwortlichen benachrichtigen, wenn dies eine Verletzung des Schutzes personenbezogener Daten beinhaltet. Ebenso kann ein

- *Richtlinie 2009/136/EG (Richtlinie über die Rechte der Bürger) und Verordnung 611/2013 (Verordnung über die Unterrichtung über Verstöße).*

137. Anbieter von öffentlich zugänglichen elektronischen Kommunikationsdiensten im Rahmen der Richtlinie 2002/58/EG[56] müssen den zuständigen nationalen Behörden Verstöße melden.

[53] Siehe http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv%3AOJ.L_.2014.257.01.0073.01.ENG

[54] Siehe http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2016.194.01.0001.01.ENG

[55] Erwägungsgrund 63: *"Personenbezogene Daten sind in vielen Fällen infolge von Zwischenfällen gefährdet. In*

diesem Zusammenhang sollten die zuständigen Behörden und die Datenschutzbehörden zusammenarbeiten und Informationen über alle relevanten Angelegenheiten austauschen, um Verletzungen des Schutzes personenbezogener Daten infolge von Zwischenfällen zu bekämpfen."

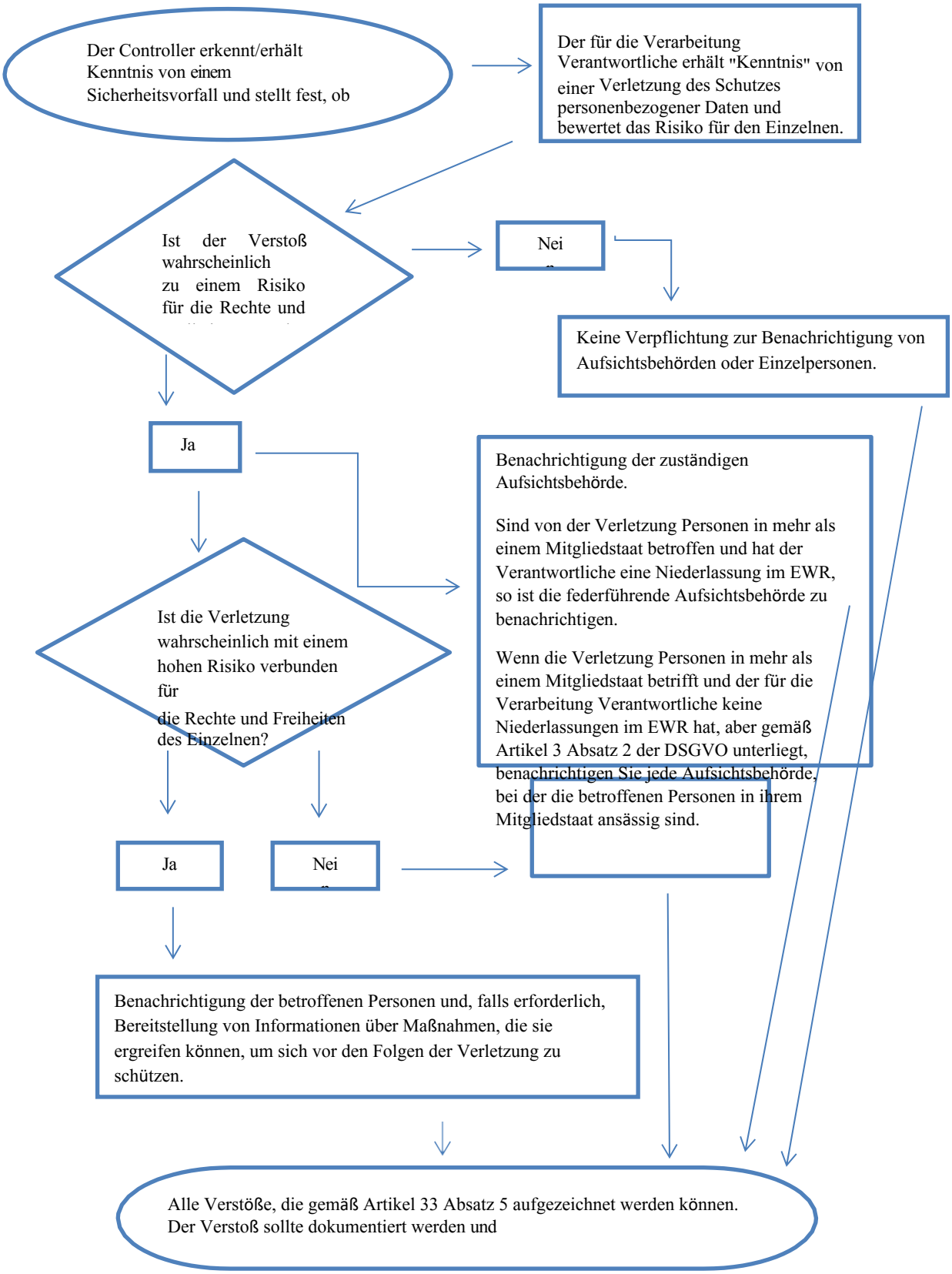
[56] Am 10. Januar 2017 schlug die Europäische Kommission eine Verordnung über den Schutz der Privatsphäre und die elektronische Kommunikation vor, die die Richtlinie 2009/136/EG ersetzen und die Meldepflicht aufheben soll. Bis dieser Vorschlag jedoch vom Europäischen Parlament gebilligt wird, bleibt die bestehende Meldepflicht bestehen

138. Die für die Verarbeitung Verantwortlichen sollten auch alle zusätzlichen rechtlichen, medizinischen oder beruflichen Meldepflichten im Rahmen anderer geltender Regelungen kennen.

Kraft, siehe https://ec.europa.eu/digital-single-market/en/news/proposal-regulation-privacy-and-elektronische Kommunikation

VII. ANHANG

A. Flussdiagramm der Meldepflichten



B. Beispiele für Verletzungen des Schutzes personenbezogener Daten und wer zu benachrichtigen ist

Die folgenden, nicht erschöpfenden Beispiele sollen den für die Verarbeitung Verantwortlichen dabei helfen, festzustellen, ob sie in verschiedenen Fällen einer Verletzung des Schutzes personenbezogener Daten eine Meldung machen müssen. Diese Beispiele können auch dabei helfen, zwischen einem Risiko und einem hohen Risiko für die Rechte und Freiheiten von Personen zu unterscheiden.

Beispiel	Benachrichtigen Sie die Aufsichtsbehörde Behörde	Benachrichtigung über die Daten Thema	Anmerkungen/Empfehlungen
i Ein Kontrolleur speicherte eine Sicherung eines Archivs von personenbezogenen Daten verschlüsselt auf einem USB Schlüssel. Der Schlüssel ist gestohlen während einer Einbruch.	Nein.	Nein.	Solange die Daten verschlüsselt mit einem Status von Algorithmus, Backups der Daten existieren die eindeutigen Schlüssel nicht gefährdet ist, und die Daten können rechtzeitig wiederhergestellt, diese darf nicht meldepflichtig sein Verstoß. Wenn es jedoch später ist gefährdet, Benachrichtigung erforderlich ist.
ii Ein Controller unterhält eine Online Dienst. Infolge eines Cyberangriffs auf diesen Dienst werden personenbezogene Daten von Einzelpersonen exfiltriert. Der für die Verarbeitung Verantwortliche hat Kunden in einem einzigen Mitgliedstaat.	Ja, Meldung an die Aufsichtsbehörde, wenn mit Folgen für den Einzelnen zu rechnen ist.	Ja, Meldung an Einzelpersonen, je nach Art der betroffenen personenbezogenen Daten und wenn die Schwere der wahrscheinlichen Folgen für Einzelpersonen hoch ist.	
iii Eine kurze Leistung Dauer des Ausfalls mehrere Minuten am Stück Anruf des Kontrolleurs	Nein.	Nein.	Es handelt sich zwar nicht um einen meldepflichtigen Verstoß, aber dennoch um ein meldepflichtiges Ereignis gemäß Artikel 33 Absatz 5.

Bedeutung von Zentrum Kunden sind nicht in der Lage, die Controller und Zugang zu ihren Aufzeichnungen.			Der für die Verarbeitung Verantwortliche sollte entsprechende Aufzeichnungen führen.
iv Ein Controller wird von einer Ransomware betroffen Angriff, der zu in allen Daten, die verschlüsselt. Nein zurück- ups sind verfügbar und die Daten können nicht wiederhergestellt werden. Auf Untersuchung wird deutlich, dass der Ransomware nur Funktionalität	Ja, melden Sie an der Aufsichtsbehörde, wenn es wahrscheinlich ist Folgen für Einzelpersonen, da dies ein Verlust ist der Verfügbarkeit.	Ja, Meldung an Einzelpersonen, je nach über die Art der betroffene personenbezogene Daten und die möglichen Auswirkungen der mangelnden Verfügbarkeit der Daten, sowie andere wahrscheinliche Folgen.	Wenn eine Sicherungskopie vorhanden war und die Daten rechtzeitig wiederhergestellt werden konnten, müsste dies der Aufsichtsbehörde oder den Betroffenen nicht gemeldet werden, da kein dauerhafter Verlust der Verfügbarkeit oder der Vertraulichkeit eingetreten wäre. Wenn die Aufsichtsbehörde jedoch wurde auf die
war die Verschlüsselung der Daten, und dass es war kein anderer Malware vorhanden in das System.			Vorfall durch andere Mittel, es kann eine Untersuchung zur Bewertung Einhaltung der breitere Sicherheit Anforderungen des Artikels 32.

v Eine Person ruft das Callcenter einer Bank an, um eine Datenverletzung zu melden. Die Person hat einen Monatsauszug für eine andere Person erhalten. Der für die Verarbeitung Verantwortliche führt eine kurze Untersuchung durch (d. h. innerhalb von 24 Stunden) und stellt mit hinreichender Sicherheit fest, dass eine Verletzung des Schutzes personenbezogener Daten stattgefunden hat und ob es sich um einen systemischen Fehler handelt, der dazu führen kann, dass andere Personen betroffen sind oder betroffen sein könnten.	Ja.	Nur die betroffenen Personen werden benachrichtigt, wenn ein hohes Risiko besteht und klar ist, dass andere nicht betroffen waren.	Stellt sich nach weiteren Untersuchungen heraus, dass mehr Personen betroffen sind, muss die Aufsichtsbehörde auf den neuesten Stand gebracht werden, und der für die Verarbeitung Verantwortliche unternimmt den zusätzlichen Schritt, andere Personen zu benachrichtigen, wenn ein hohes Risiko für sie besteht.
vi Ein für die Verarbeitung Verantwortlicher betreibt einen Online-Marktplatz und hat Kunden in mehreren Mitgliedstaaten. Der Marktplatz wird Opfer eines Cyberangriffs, und der Angreifer veröffentlicht Benutzernamen, Passwörter und Kaufdaten im Internet.	Ja, Meldung an die federführende Aufsichtsbehörde, wenn es sich um eine grenzüberschreitende Verarbeitung handelt.	Ja, das könnte zu einem hohen Risiko führen.	Der für die Verarbeitung Verantwortliche sollte Maßnahmen ergreifen, z. B. die Zurücksetzung von Passwörtern für die betroffenen Konten erzwingen, sowie andere Schritte zur Risikominderung unternehmen. Der für die Verarbeitung Verantwortliche sollte auch etwaige andere Meldepflichten berücksichtigen, z. B. gemäß der NIS-Richtlinie als Anbieter digitaler Dienste.
vii Ein Website-Hosting-Unternehmen, das als Datenverarbeiter tätig ist, stellt einen Fehler im Code fest, der die Benutzerautorisierung kontrolliert. Die Auswirkung des Fehlers	Als Auftragsverarbeiter muss das Hosting-Unternehmen der Website Folgendes mitteilen seine betroffenen Kunden (die für die Verarbeitung Verantwortlichen) ohne unangemessene	Wenn wahrscheinlich kein hohes Risiko für die Personen besteht, müssen sie nicht benachrichtigt werden.	Das Website-Hosting-Unternehmen (Auftragsverarbeiter) muss alle anderen Meldepflichten berücksichtigen (z. B. gemäß der NIS-Richtlinie als Anbieter digitaler Dienste). Wenn es keine Beweise für diese Schwachstelle gibt,

bedeutet, dass jeder Nutzer	Verzögerung zu informieren. Unter der Annahme, dass das Website-Hosting		die
auf die Kontodaten eines anderen Benutzers zugreifen kann	Wenn das für die Verarbeitung Verantwortliche Unternehmen seine eigene Untersuchung durchgeführt hat, sollten die betroffenen für die Verarbeitung Verantwortlichen hinreichend sicher sein, dass ein Verstoß vorliegt, und es ist daher wahrscheinlich, dass sie "Kenntnis erlangt" haben, sobald sie vom Hosting-Unternehmen (dem Auftragsverarbeiter) benachrichtigt worden sind. Der für die Verarbeitung Verantwortliche muss dann die Aufsichtsbehörde benachrichtigen Behörde		mit einem der für die Verarbeitung Verantwortlichen ausgebeutet wurde, liegt möglicherweise kein meldepflichtiger Verstoß vor, aber es ist wahrscheinlich, dass er aufgezeichnet werden kann oder eine Nichteinhaltung gemäß Artikel 32 darstellt.
viii Medizinische Aufzeichnungen in einem Krankenhaus sind aufgrund eines Cyberangriffs 30 Stunden lang nicht verfügbar.	Ja, das Krankenhaus ist zur Meldung verpflichtet, da eine hohe Gefahr für das Wohlbefinden und die Privatsphäre des Patienten bestehen kann.	Ja, melden Sie sich bei den betroffenen Personen.	
ix Persönliche Daten einer großen Anzahl von Studenten werden irrtümlich an eine falsche Mailingliste mit mehr als 1000 Empfängern geschickt.	Ja, Meldung an die Aufsichtsbehörde.	Ja, Meldung an Einzelpersonen je nach Umfang und Art der betroffenen personenbezogenen Daten und der Schwere der möglichen Folgen.	

x	Eine Direktmarketing-E-Mail wird an Empfänger in den Feldern "an:" oder "cc:" gesendet, so dass jeder Empfänger die E-Mail-Adresse der anderen Empfänger sehen kann.	Ja, die Benachrichtigung der Aufsichtsbehörde kann obligatorisch sein, wenn eine große Anzahl von Personen betroffen ist, wenn sensible Daten offengelegt werden (z. B. eine Mailingliste eines Psychotherapeuten) oder wenn andere Faktoren ein hohes Risiko darstellen (z. B. wenn die Mail die ursprünglichen Passwörter enthält).	Ja, Meldung an Einzelpersonen je nach Umfang und Art der betroffenen personenbezogenen Daten und der Schwere der möglichen Folgen.	Eine Benachrichtigung ist möglicherweise nicht erforderlich, wenn keine sensiblen Daten offengelegt werden und wenn nur eine geringe Anzahl von E-Mail-Adressen offengelegt wird.