ARTIKEL-29-DATENSCHUTZGRUPPE

18/DE

WP250rev.01

Leitlinien für die Meldung von Verletzungen des Schutzes personenbezogener Daten gemäß der Verordnung (EU) 2016/679

angenommen am 3. Oktober 2017

zuletzt überarbeitet und angenommen am 6. Februar 2018

DIE ARBEITSGRUPPE FÜR DEN SCHUTZ VON PERSONEN BEI DER VERARBEITUNG PERSONENBEZOGENER DATEN

eingesetzt durch die Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995,

gestützt auf die Artikel 29 und 30 dieser Richtlinie,

gestützt auf ihre Geschäftsordnung,

HAT FOLGENDE LEITLINIEN ANGENOMMEN:

INHALTSVERZEICHNIS

EINLEITUNG

Mit der Datenschutz-Grundverordnung (DSGVO) wird die Anforderung eingeführt, dass Verletzungen des Schutzes personenbezogener Daten (im Folgenden „Datenschutzverletzungen“) an die Aufsichtsbehörde[1] (bzw. im Falle grenzüberschreitender Datenschutzverletzungen an die federführende Behörde) gemeldet werden müssen und dass in bestimmten Fällen die Personen, deren personenbezogene Daten von der Datenschutzverletzung betroffen sind, von der Datenschutzverletzung benachrichtigt werden müssen.

Gegenwärtig gelten bei Datenschutzverletzungen Meldepflichten für bestimmte Organisationen, beispielsweise für die Anbieter öffentlich zugänglicher elektronischer Kommunikationsdienste (gemäß der Richtlinie 2009/136/EG und der Verordnung (EU) Nr. 611/2013[2]). Zudem sehen einige EU-Mitgliedstaaten bereits eine eigene nationale Pflicht zur Meldung von Datenschutzverletzungen vor. Hierzu kann gehören, dass Datenschutzverletzungen gemeldet werden müssen, von denen neben den Anbietern öffentlich zugänglicher elektronischer Kommunikationsdienste auch Kategorien von Verantwortlichen betroffen sind (wie in Deutschland und Italien), oder dass alle Verletzungen gemeldet werden müssen, bei denen personenbezogene Daten betroffen sind (wie in den Niederlanden). Andere Mitgliedstaaten haben unter Umständen einschlägige Verhaltensregeln eingeführt (etwa Irland[3]). Obwohl mehrere EU-Datenschutzbehörden die Verantwortlichen derzeit zur Meldung von Datenschutzverletzungen auffordern, enthält die durch die DSGVO ersetzte Datenschutzrichtlinie 95/46/EG[4] keine spezifische Pflicht zur Meldung von Datenschutzverletzungen, sodass eine solche Meldepflicht für viele Organisationen neu sein dürfte. Mit der DSGVO sind nunmehr alle Verantwortlichen zur Meldung verpflichtet, es sei denn, dass die Datenschutzverletzung voraussichtlich nicht zu einem Risiko für die Rechte und Freiheiten natürlicher Personen[5] führt. Auch die Auftragsverarbeiter, die dem Verantwortlichen jede Datenschutzverletzung melden müssen, spielen eine wichtige Rolle.[6]

Nach Ansicht der Artikel-29-Datenschutzgruppe ist die neue Meldepflicht in mehrfacher Hinsicht von Vorteil. Bei der Meldung an die Aufsichtsbehörde können sich die Verantwortlichen darüber beraten lassen, ob die betroffenen Personen informiert werden müssen. Die Aufsichtsbehörde kann den Verantwortlichen sogar anweisen, die Betroffenen über die Datenschutzverletzung zu unterrichten.[7] Im Rahmen der Benachrichtigung kann der Verantwortliche die betroffenen Personen über die durch die Datenschutzverletzung entstandenen Risiken informieren und ihnen mitteilen, wie sie sich selbst

[1] Siehe Artikel 4 Absatz 21 der DSGVO.

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

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

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

[5] Die in der Charta der Grundrechte der Europäischen Union verankerten Rechte, abrufbar unter http://eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX:12012P/TXT.

[6] Siehe Artikel 33 Absatz 2. Dies entspricht dem in Artikel 5 der Verordnung (EU) Nr. 611/2013 dargelegten Konzept, nach dem ein Betreiber, der mit der Erbringung eines Teils eines elektronischen Kommunikationsdienstes beauftragt ist (ohne in einem direkten Vertragsverhältnis zu den Teilnehmern zu stehen), den beauftragenden Betreiber im Falle einer Verletzung des Schutzes personenbezogener Daten informieren muss.

[7] Siehe Artikel 34 Absatz 4 und Artikel 58 Absatz 2 Buchstabe e.

vor den möglichen Folgen der Verletzung schützen können. Das Hauptaugenmerk eines Reaktionsplans zur Bewältigung von Datenschutzverletzungen sollte auf dem Schutz natürlicher Personen und ihrer personenbezogenen Daten liegen. Dementsprechend sollte die Meldung von Datenschutzverletzungen als Instrument betrachtet werden, das die Einhaltung der Vorschriften zum Schutz personenbezogener Daten erleichtert. Gleichzeitig ist zu beachten, dass die Nichtmeldung einer Datenschutzverletzung gegenüber einer betroffenen Person oder einer Aufsichtsbehörde unter Umständen eine mögliche Sanktion nach Artikel 83 gegen den Verantwortlichen begründen kann.

Die Verantwortlichen und Auftragsverarbeiter sollten daher vorausschauend planen und Verfahren einführen, die es ihnen ermöglichen, Datenschutzverletzungen zu erkennen und zügig einzudämmen, das Risiko für die betroffenen Personen zu bewerten[8] und anschließend festzustellen, ob die zuständige Aufsichtsbehörde informiert werden muss, und die Betroffenen gegebenenfalls von der Datenschutzverletzung zu benachrichtigen. Die Meldung an die Aufsichtsbehörde sollte Bestandteil eines solchen Vorfallreaktionsplans sein.

Die DSGVO enthält Vorschriften darüber, wann und an wen eine Datenschutzverletzung gemeldet werden muss und welche Angaben in der Meldung gemacht werden müssen. Die für die Meldung erforderlichen Informationen können schrittweise übermittelt werden, doch sollten die Verantwortlichen in jedem Fall zügig auf eine Datenschutzverletzung reagieren.

In ihrer Stellungnahme 03/2014 über die Meldung von Verletzungen des Schutzes personenbezogener Daten[9] hat die Artikel-29-Datenschutzgruppe den für die Verarbeitung Verantwortlichen Leitlinien an die Hand gegeben, um leichter entscheiden zu können, ob die betroffenen Personen im Falle einer Datenschutzverletzung benachrichtigt werden müssen. In der Stellungnahme hat sich die Gruppe mit der für die Betreiber elektronischer Kommunikationsnetze geltenden Verpflichtung gemäß der Richtlinie 2002/58/EG befasst, Fallbeispiele aus verschiedenen Bereichen vor dem Hintergrund des damaligen Entwurfs der DSGVO aufgeführt und bewährte Verfahren vorgestellt, die von allen Verantwortlichen angewendet werden können.

In den vorliegenden Leitlinien werden die verbindlichen Melde- und Benachrichtigungsanforderungen der DSGVO erläutert und einige Maßnahmen vorgestellt, die die Verantwortlichen und Auftragsverarbeiter zur Erfüllung dieser neuen Verpflichtungen ergreifen können. Außerdem werden Beispiele für verschiedene Arten von Datenschutzverletzungen beschrieben, um anhand unterschiedlicher Szenarien zu erläutern, wer jeweils unterrichtet werden muss.

I. Meldung von Verletzungen des Schutzes personenbezogener Daten nach der DSGVO

A. Grundlegende Überlegungen zum Thema Sicherheit

Eine der Anforderungen der DSGVO lautet, dass personenbezogene Daten mithilfe geeigneter technischer und organisatorischer Maßnahmen in einer Weise verarbeitet werden müssen, die eine angemessene Sicherheit der personenbezogenen Daten gewährleistet, einschließlich des Schutzes vor

[8] Dies lässt sich im Rahmen der Überwachungs- und Überprüfungsanforderung einer Datenschutz-Folgenabschätzung (DSFA) sicherstellen, die für Verarbeitungsvorgänge vorgeschrieben ist, die voraussichtlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen zur Folge haben (Artikel 35 Absätze 1 und 11).

[9] Siehe die Stellungnahme 03/2014 über die Meldung von Verletzungen des Schutzes personenbezogener Daten unter http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp213_en.pdf.

unbefugter oder unrechtmäßiger Verarbeitung und vor unbeabsichtigtem Verlust, unbeabsichtigter Zerstörung oder unbeabsichtigter Schädigung.[10]

Folglich müssen die Verantwortlichen und die Auftragsverarbeiter nach Maßgabe der DSGVO über geeignete technische und organisatorische Maßnahmen verfügen, die ein Sicherheitsniveau gewährleisten, das den für die verarbeiteten personenbezogenen Daten bestehenden Risiken angemessen ist. Sie sollten den Stand der Technik, die Implementierungskosten und die Art, den Umfang, die Umstände und die Zwecke der Verarbeitung sowie die unterschiedliche Eintrittswahrscheinlichkeit und Schwere der Risiken für die Rechte und Freiheiten natürlicher Personen berücksichtigen.[11] Darüber hinaus müssen nach der DSGVO alle geeigneten technischen Schutz- sowie organisatorischen Maßnahmen getroffen werden, um sofort feststellen zu können, ob eine Datenschutzverletzung aufgetreten ist, woraus sich dann ableitet, ob die Meldepflicht zum Tragen kommt.[12]

Eines der zentralen Komponenten jedes Datensicherheitskonzepts ist somit die Fähigkeit, Datenschutzverletzungen soweit möglich zu verhindern und, sollte eine Datenschutzverletzung dennoch auftreten, zügig darauf zu reagieren.

B. Was ist eine Verletzung des Schutzes personenbezogener Daten?

1. Begriffsbestimmung

Um gegen eine Datenschutzverletzung vorgehen zu können, müssen die Verantwortlichen zunächst in der Lage sein, eine Datenschutzverletzung zu erkennen. Der Begriff „Verletzung des Schutzes personenbezogener Daten“ wird in Artikel 4 Absatz 12 der DSGVO definiert als

> „eine Verletzung der Sicherheit, die, ob unbeabsichtigt oder unrechtmäßig, zur Vernichtung, zum Verlust, zur Veränderung, oder zur unbefugten Offenlegung von beziehungsweise zum unbefugten Zugang zu personenbezogenen Daten führt, die übermittelt, gespeichert oder auf sonstige Weise verarbeitet wurden“.

Es dürfte klar sein, was unter der „Vernichtung“ personenbezogener Daten zu verstehen ist, nämlich dass die Daten nicht mehr existieren oder nicht mehr in einer Form existieren, die für den Verantwortlichen von Nutzen ist. Auch der Begriff des „Schadens“ sollte relativ klar sein: Er bedeutet, dass personenbezogene Daten verändert oder beschädigt wurden oder nicht mehr vollständig sind. Der Begriff des „Verlusts“ personenbezogener Daten sollte dahin gehend ausgelegt werden, dass die Daten zwar unter Umständen noch vorhanden sind, der Verantwortliche aber die Kontrolle über oder den Zugang zu den Daten verloren hat, oder dass sich die Daten nicht mehr in seinem Besitz befinden. Die unrechtmäßige oder unbefugte Verarbeitung schließlich kann die Offenlegung personenbezogener Daten gegenüber (bzw. den Zugang zu personenbezogenen Daten von) Empfängern, die nicht zum Erhalt der (bzw. zum Zugang zu den) Daten befugt sind, sowie jede andere Form der Verarbeitung unter Verstoß gegen die DSGVO beinhalten.

Beispiel

[10] Siehe Artikel 5 Absatz 1 Buchstabe f und Artikel 32.

[11] Artikel 32; siehe auch Erwägungsgrund 83.

[12] Siehe Erwägungsgrund 87.

Es würde sich beispielsweise um einen Verlust personenbezogener Daten handeln, wenn ein Gerät, auf dem eine Kopie der Kundendatenbank eines Verantwortlichen gespeichert ist, verloren geht oder gestohlen wird. Ein weiteres Beispiel für Datenverlust wäre der Fall, dass die einzige Kopie eines Satzes personenbezogener Daten durch Ransomware verschlüsselt wurde oder vom Verantwortlichen durch einen Schlüssel verschlüsselt wurde, der sich nicht mehr in seinem Besitz befindet.

Es dürfte klar sein, dass es sich bei einer Datenschutzverletzung um eine Art von Sicherheitsvorfall handelt. Wie aus Artikel 4 Absatz 12 hervorgeht, ist die DSGVO jedoch nur bei Verletzungen des Schutzes *personenbezogener Daten* anwendbar. Die Folge einer solchen Datenschutzverletzung ist, dass der Verantwortliche die Einhaltung der in Artikel 5 der DSGVO dargelegten Grundsätze im Zusammenhang mit der Verarbeitung personenbezogener Daten nicht mehr gewährleisten kann. An dieser Stelle wird der Unterschied zwischen einem Sicherheitsvorfall und einer Verletzung des Schutzes personenbezogener Daten deutlich: Im Wesentlichen ist eine Verletzung des Schutzes personenbezogener Daten immer auch ein Sicherheitsvorfall, während es sich bei einem Sicherheitsvorfall nicht notwendigerweise um eine Verletzung des Schutzes personenbezogener Daten handelt.[13]

Die möglichen negativen Folgen einer Datenschutzverletzung für die betroffenen Personen werden weiter unten erörtert.

2. Formen der Verletzung des Schutzes personenbezogener Daten

Wie die Artikel-29-Datenschutzgruppe in ihrer Stellungnahme 03/2014 über die Meldung von Verletzungen des Schutzes personenbezogener Daten dargelegt hat[14], lassen sich Datenschutzverletzungen nach den folgenden drei bekannten Grundsätzen der Informationssicherheit unterteilen:

- „Verletzung der Vertraulichkeit" – die unbefugte oder unbeabsichtigte Preisgabe von oder Einsichtnahme in personenbezogene Daten
- „Verletzung der Integrität" – die unbefugte oder unbeabsichtigte Änderung personenbezogener Daten
- „Verletzung der Verfügbarkeit" – der unbefugte oder unbeabsichtigte Verlust des Zugangs[15] zu personenbezogenen Daten oder die unbeabsichtigte oder unrechtmäßige Vernichtung personenbezogener Daten

[13] Zu beachten ist, dass Sicherheitsvorfälle nicht auf Bedrohungsszenarien beschränkt sind, bei denen eine Organisation von außen angegriffen wird, sondern auch dann gegeben sind, wenn Sicherheitsgrundsätze aufgrund interner Vorgänge verletzt werden.

[14] Siehe Stellungnahme 03/2014.

[15] Nach allgemeiner Auffassung ist der „Zugang" im Wesentlichen ein Aspekt der „Verfügbarkeit". Siehe zum Beispiel NIST SP800-53rev4, wonach „Verfügbarkeit" als Sicherstellung eines zeitnahen und zuverlässigen Zugangs zu und der Nutzung von Informationen („Ensuring timely and reliable access to and use of information") definiert wird, abrufbar unter http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf. CNSSI-4009 nimmt Bezug auf den zeitnahen, zuverlässigen Zugang zu Daten und Informationsdiensten durch berechtigte Nutzer („Timely, reliable access to data and information services for authorized users"), siehe https://rmf.org/images/4-CNSS-Publications/CNSSI-4009.pdf. Auch in ISO/IEC 27000:2016 wird Verfügbarkeit in dem Sinne definiert, dass die Informationen auf Anfrage einer befugten Stelle verfügbar und nutzbar sind („The property of being accessible and useable upon demand by an authorized entity"), siehe https://www.iso.org/obp/ui/#iso:std:iso-iec:27000:ed-4:v1:en.

Zu beachten ist auch, dass eine Datenschutzverletzung je nach den Umständen die Vertraulichkeit, Integrität und Verfügbarkeit personenbezogener Daten zugleich oder eine beliebige Kombination aller Grundsätze betreffen kann.

Während sich eine Verletzung der Datenvertraulichkeit oder -integrität relativ eindeutig feststellen lässt, ist eine Verletzung der Datenverfügbarkeit unter Umständen weniger offensichtlich. Eine Datenschutzverletzung gilt immer als Verletzung der Datenverfügbarkeit, wenn personenbezogene Daten dauerhaft verloren gegangen sind oder vernichtet wurden.

Beispiel

Ein Verlust der Datenverfügbarkeit liegt zum Beispiel vor, wenn Daten unbeabsichtigt oder durch eine unbefugte Person gelöscht wurden, oder wenn im Falle sicher verschlüsselter Daten der Entschlüsselungsschlüssel verloren gegangen ist. Kann der Verantwortliche den Zugang zu den Daten etwa mithilfe einer Sicherungskopie nicht wiederherstellen, wird von einem dauerhaften Verlust der Verfügbarkeit ausgegangen.

Ein Verlust der Verfügbarkeit kann bestehen, wenn der normale Betrieb einer Organisation erheblich gestört wird, wie etwa bei einem Stromausfall oder einem Angriff in Form der gezielten Überlastung von Servern („Denial of service"-Angriff), mit der Folge, dass personenbezogene Daten nicht mehr verfügbar sind.

Unter Umständen stellt sich die Frage, ob auch ein vorübergehender Verlust der Verfügbarkeit personenbezogener Daten als Datenschutzverletzung zu werten ist, und wenn ja, ob diese gemeldet werden muss. In Artikel 32 der DSGVO („Sicherheit und Verarbeitung") wird erklärt, dass bei der Umsetzung technischer und organisatorischer Maßnahmen zur Gewährleistung eines dem Risiko angemessenen Schutzniveaus unter anderem „die Fähigkeit, die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung auf Dauer sicherzustellen" sowie „die Fähigkeit, die Verfügbarkeit der personenbezogenen Daten und den Zugang zu ihnen bei einem physischen oder technischen Zwischenfall rasch wiederherzustellen" einbezogen werden müssen.

Somit liegt auch dann eine Form der Datenschutzverletzung vor, wenn personenbezogene Daten durch einen Sicherheitsvorfall vorübergehend nicht verfügbar sind, da der fehlende Zugang zu den Daten wesentliche Folgen für die Rechte und Freiheiten natürlicher Personen haben kann. Sind personenbezogene Daten hingegen aufgrund einer geplanten Systemwartung nicht verfügbar, handelt es sich nicht um eine „Verletzung des Schutzes personenbezogener Daten" gemäß Artikel 4 Absatz 12.

Wie auch im Falle des dauerhaften Verlusts oder der dauerhaften Vernichtung personenbezogener Daten (ebenso wie bei jeder anderen Form der Datenschutzverletzung), sollte eine Datenschutzverletzung wegen vorübergehenden Verlusts der Verfügbarkeit gemäß Artikel 33 Absatz 5 dokumentiert werden. Dies hilft dem Verantwortlichen, seiner Rechenschaftspflicht gegenüber der Aufsichtsbehörde nachzukommen, die Einsicht in diese Aufzeichnungen verlangen kann.[16] Hingegen sind die Meldung an die Aufsichtsbehörde und die Benachrichtigung der betroffenen Personen je nach den Umständen der Datenschutzverletzung möglicherweise nicht erforderlich. Der Verantwortliche muss die Eintrittswahrscheinlichkeit und Schwere der Auswirkungen bewerten, die mit der mangelnden Verfügbarkeit personenbezogener Daten für die Rechte und Freiheiten natürlicher Personen verbunden sind. Der Verantwortliche muss gemäß Artikel 33 Meldung erstatten, es sei denn, dass die Datenschutzverletzung wahrscheinlich kein Risiko

[16] Siehe Artikel 33 Absatz 5.

für die Rechte und Freiheiten der betroffenen Personen zur Folge hat. Das muss natürlich fallspezifisch geprüft werden.

Beispiele

Im Falle eines Krankenhauses könnte auch dann ein Risiko für die Rechte und Freiheiten von Personen bestehen, wenn kritische medizinische Patientendaten nur vorübergehend nicht verfügbar sind; beispielsweise könnten Operationen abgesagt werden und Leben in Gefahr geraten.

Wenn dagegen die Systeme eines Medienunternehmens über mehrere Stunden nicht verfügbar sind (etwa aufgrund eines Stromausfalls), sodass das Unternehmen keine Newsletter an seine Abonnenten verschicken kann, besteht wahrscheinlich kein Risiko für die Rechte und Freiheiten von Personen.

Zu beachten ist, dass ein Verantwortlicher auch bei einer nur vorübergehenden Nichtverfügbarkeit seiner Systeme ohne zu erwartende Auswirkungen für die betroffenen Personen alle denkbaren Folgen einer Datenschutzverletzung berücksichtigen muss, da eine Meldung aus anderen Gründen dennoch erforderlich sein kann.

Beispiel

Eine Infektion durch Ransomware (ein Schadprogramm, das die Daten des Verantwortlichen bis zur Zahlung eines Lösegelds verschlüsselt) könnte einen vorübergehenden Verlust der Datenverfügbarkeit zur Folge haben, wenn die Daten mithilfe einer Sicherungskopie wiederhergestellt werden können. Trotzdem wurde in das Netzwerk eingedrungen, sodass der Vorfall unter Umständen meldepflichtig ist, wenn er als Verletzung der Datenvertraulichkeit einzustufen ist (der Angreifer also Zugang zu personenbezogenen Daten erhalten hat) und daraus ein Risiko für die Rechte und Freiheiten von Personen entsteht.

3. Mögliche Folgen von Verletzungen des Schutzes personenbezogener Daten

Datenschutzverletzungen können zahlreiche nachteilige Auswirkungen für die betroffenen Personen haben und einen physischen, materiellen oder immateriellen Schaden nach sich ziehen. Wie in der DSGVO erläutert, können hierzu der Verlust der Kontrolle über ihre personenbezogenen Daten oder Einschränkung ihrer Rechte, Diskriminierung, Identitätsdiebstahl oder -betrug, finanzielle Verluste, unbefugte Aufhebung der Pseudonymisierung, Rufschädigung und Verlust der Vertraulichkeit von dem Berufsgeheimnis unterliegenden Daten gehören. Den betroffenen Personen können auch andere erhebliche wirtschaftliche oder gesellschaftliche Nachteile entstehen.[17]

Daher verlangt die DSGVO von den Verantwortlichen, Datenschutzverletzungen an die zuständige Aufsichtsbehörde zu melden, es sei denn, dass die Datenschutzverletzung voraussichtlich nicht zu dem Risiko eines Eintritts solcher nachteiligen Auswirkungen führt. Besteht ein hohes Risiko, dass diese nachteiligen Auswirkungen eintreten, muss der Verantwortliche nach den Bestimmungen der DSGVO die betroffenen Personen so rasch wie nach allgemeinem Ermessen möglich von der Datenschutzverletzung benachrichtigen.[18]

In Erwägungsgrund 87 der DSGVO wird betont, wie wichtig es ist, eine Datenschutzverletzung feststellen, das Risiko für die betroffenen Personen einschätzen und die Datenschutzverletzung daraufhin gegebenenfalls melden zu können:

[17] Siehe auch Erwägungsgründe 85 und 75.

[18] Siehe auch Erwägungsgrund 86.

„Es sollte festgestellt werden, ob alle geeigneten technischen Schutz- sowie organisatorischen Maßnahmen getroffen wurden, um sofort feststellen zu können, ob eine Verletzung des Schutzes personenbezogener Daten aufgetreten ist, und um die Aufsichtsbehörde und die betroffene Person umgehend unterrichten zu können. Bei der Feststellung, ob die Meldung unverzüglich erfolgt ist, sollten die Art und Schwere der Verletzung des Schutzes personenbezogener Daten sowie deren Folgen und nachteilige Auswirkungen für die betroffene Person berücksichtigt werden. Die entsprechende Meldung kann zu einem Tätigwerden der Aufsichtsbehörde im Einklang mit ihren in dieser Verordnung festgelegten Aufgaben und Befugnissen führen."

Abschnitt IV enthält weiterführende Leitlinien zur Bewertung des Risikos nachteiliger Auswirkungen für die betroffenen Personen.

Versäumt es ein Verantwortlicher, eine Datenschutzverletzung an die Aufsichtsbehörde zu melden und/oder die betroffenen Personen davon zu benachrichtigen, obwohl die Voraussetzungen von Artikel 33 bzw. von Artikel 34 erfüllt sind, hat die Aufsichtsbehörde verschiedene Optionen, wobei sie alle ihr zur Verfügung stehenden Abhilfemaßnahmen berücksichtigen muss; dazu gehört unter Umständen auch die Prüfung der Verhängung einer angemessenen Geldbuße[19] entweder zusätzlich zu einer Abhilfemaßnahme gemäß Artikel 58 Absatz 2 oder als alleinige Maßnahme. Wird eine Geldbuße verhängt, kann sie gemäß Artikel 83 Absatz 4 Buchstabe a der DSGVO bis zu 10 000 000 EUR oder bis zu 2 % des gesamten weltweit erzielten Jahresumsatzes eines Unternehmens betragen. Zu beachten ist auch, dass die Nichtmeldung einer Datenschutzverletzung in manchen Fällen ein Hinweis darauf sein könnte, dass Sicherheitsmaßnahmen fehlen oder dass die vorhandenen Sicherheitsmaßnahmen unzureichend sind. Die Leitlinien der Artikel-29-Datenschutzgruppe über die Anwendung und Festsetzung von Geldbußen lauten wie folgt: „Liegen in einem bestimmten Einzelfall mehrere verschiedene Verstöße gleichzeitig vor, kann die Aufsichtsbehörde bei der Verhängung einer wirksamen, angemessenen und abschreckenden Geldbuße den Höchstbetrag für den schwerwiegendsten Verstoß zugrunde legen." In diesem Fall hat die Aufsichtsbehörde auch die Möglichkeit, Sanktionen wegen der versäumten Meldung oder Benachrichtigung (Artikel 33 und 34) einerseits sowie wegen fehlender (angemessener) Sicherheitsmaßnahmen (Artikel 32) andererseits zu verhängen, da es sich um zwei separate Verstöße handelt.

II. **Artikel 33 – Meldung an die Aufsichtsbehörde**

A. Wann muss eine Meldung erfolgen?

1. Anforderungen nach Artikel 33

Artikel 33 Absatz 1 sieht Folgendes vor:

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

[19] Weitere Informationen hierzu sind den Leitlinien der Artikel-29-Datenschutzgruppe über die Anwendung und Festsetzung von Geldbußen zu entnehmen, abrufbar unter http://ec.europa.eu/newsroom/just/document.cfm?doc_id=47889.

Erwägungsgrund 87 lautet wie folgt:[20]

„Es sollte festgestellt werden, ob alle geeigneten technischen Schutz- sowie organisatorischen Maßnahmen getroffen wurden, um sofort feststellen zu können, ob eine Verletzung des Schutzes personenbezogener Daten aufgetreten ist, und um die Aufsichtsbehörde und die betroffene Person umgehend unterrichten zu können. Bei der Feststellung, ob die Meldung unverzüglich erfolgt ist, sollten die Art und Schwere der Verletzung des Schutzes personenbezogener Daten sowie deren Folgen und nachteilige Auswirkungen für die betroffene Person berücksichtigt werden. Die entsprechende Meldung kann zu einem Tätigwerden der Aufsichtsbehörde im Einklang mit ihren in dieser Verordnung festgelegten Aufgaben und Befugnissen führen."

2. Wann wird dem Verantwortlichen eine Datenschutzverletzung „bekannt"?

Wie bereits erläutert, verlangt die DSGVO, dass der Verantwortliche eine Datenschutzverletzung unverzüglich und, falls möglich, binnen höchstens 72 Stunden meldet, nachdem ihm die Verletzung bekannt wurde. Hier könnte sich die Frage stellen, wann davon auszugehen ist, dass einem Verantwortlichen eine Datenschutzverletzung „bekannt" wurde. Nach Auffassung der Artikel-29-Datenschutzgruppe ist anzunehmen, dass einem Verantwortlichen eine Datenschutzverletzung „bekannt" wurde, wenn der betreffende Verantwortliche eine hinreichende Gewissheit darüber hat, dass ein Sicherheitsvorfall aufgetreten ist, der zu einer Beeinträchtigung des Schutzes personenbezogener Daten geführt hat.

Die DSGVO sieht jedoch wie bereits angemerkt vor, dass die Verantwortlichen alle geeigneten technischen Schutz- sowie organisatorischen Maßnahmen treffen, um sofort feststellen zu können, ob eine Datenschutzverletzung aufgetreten ist, und um die Aufsichtsbehörde und die betroffenen Personen umgehend unterrichten zu können. Ferner wird erklärt, dass bei der Feststellung, ob die Meldung unverzüglich erfolgt ist, die Art und Schwere der Datenschutzverletzung sowie deren Folgen und nachteiligen Auswirkungen für die betroffene Person berücksichtigt werden sollten.[21] Daher obliegt es den Verantwortlichen sicherzustellen, dass ihnen etwaige Datenschutzverletzungen rechtzeitig „bekannt" werden, um angemessene Maßnahmen ergreifen zu können.

Wann genau davon auszugehen ist, dass einem Verantwortlichen eine bestimmte Datenschutzverletzung „bekannt" wurde, hängt von den konkreten Umständen der Datenschutzverletzung ab. In einigen Fällen dürfte von Anfang an klar sein, dass eine Datenschutzverletzung vorliegt, in anderen hingegen kann womöglich erst nach einer gewissen Zeit festgestellt werden, ob personenbezogene Daten beeinträchtigt wurden. Der Schwerpunkt sollte jedoch auf sofortigen Maßnahmen zur Untersuchung des Vorfalls liegen, damit festgestellt wird, ob der Schutz personenbezogener Daten tatsächlich verletzt wurde, und um Abhilfemaßnahmen zu ergreifen und die Datenschutzverletzung gegebenenfalls zu melden, falls sich diese bestätigt.

Beispiele

1. Beim Verlust eines USB-Sticks, auf dem personenbezogene Daten unverschlüsselt gespeichert sind, lässt sich oft nicht feststellen, ob Unbefugte Zugang zu den betreffenden Daten hatten. Auch wenn der Verantwortliche nicht ermitteln kann, ob eine Verletzung der Vertraulichkeit vorliegt, muss ein solcher Fall dennoch gemeldet werden, weil mit hinreichender Gewissheit eine Verletzung der Datenverfügbarkeit stattgefunden hat; dem Verantwortlichen wurde der Vorfall in dem Moment „bekannt", als er den Verlust des USB-Stick bemerkt hat.

[20] Wichtig ist in diesem Zusammenhang auch Erwägungsgrund 85.

[21] Siehe Erwägungsgrund 87.

2. Ein Dritter teilt einem Verantwortlichen mit, dass er versehentlich die personenbezogenen Daten eines Kunden des Verantwortlichen erhalten hat, und legt Belege für die unbefugte Offenlegung vor. Da der Verantwortliche den eindeutigen Nachweis einer Datenschutzverletzung erhalten hat, wurde ihm der Vorfall zweifelsfrei „bekannt".

3. Ein Verantwortlicher bemerkt, dass möglicherweise in sein Netzwerk eingedrungen wurde. Der Verantwortliche prüft seine Systeme auf eine eventuelle Beeinträchtigung der darin gespeicherten Daten und stellt fest, dass dies der Fall ist. Auch in diesem Fall hat der Verantwortliche nun den eindeutigen Nachweis einer Datenschutzverletzung, sodass ihm der Vorfall zweifelsfrei „bekannt" wurde.

4. Ein Cyberkrimineller hackt das System eines Verantwortlichen und kontaktiert ihn anschließend mit einer Lösegeldforderung. In diesem Fall hat der Verantwortliche den eindeutigen Nachweis einer Datenschutzverletzung, nachdem er sein System geprüft und den Angriff bestätigt hat; die Datenschutzverletzung wurde ihm zweifelsfrei bekannt.

Nachdem der Verantwortliche erstmals durch eine Einzelperson, ein Medienunternehmen oder eine andere Stelle auf eine mögliche Datenschutzverletzung hingewiesen wurde oder selbst einen Sicherheitsvorfall aufgedeckt hat, kann er eine kurze Untersuchung durchführen, um festzustellen, ob tatsächlich eine Datenschutzverletzung aufgetreten ist. Während dieses Untersuchungszeitraums kann nicht davon ausgegangen werden, dass dem Verantwortlichen die Datenschutzverletzung „bekannt" ist. Es wird aber erwartet, dass die erste Untersuchung schnellstmöglich beginnt und dass dabei mit hinreichender Gewissheit festgestellt wird, ob eine Datenschutzverletzung stattgefunden hat; anschließend kann der Vorfall eingehender untersucht werden.

Sobald dem Verantwortlichen eine Datenschutzverletzung bekannt wird, muss eine meldepflichtige Verletzung unverzüglich und, falls möglich, binnen höchstens 72 Stunden gemeldet werden. In dieser Zeit sollte der Verantwortliche das wahrscheinliche Risiko für die betroffenen Personen prüfen, um festzustellen, ob die Meldepflicht ausgelöst wurde und welche Maßnahme(n) zur Behebung der Datenschutzverletzung getroffen werden muss/müssen. Möglicherweise hat der Verantwortliche jedoch im Rahmen einer im Vorfeld des betreffenden Verarbeitungsvorgangs durchgeführten Datenschutz-Folgenabschätzung (DSFA)[22] bereits eine erste Einschätzung der möglichen Risiken vorgenommen, die eine Datenschutzverletzung mit sich bringen könnte. Da allerdings die DSFA gegenüber den spezifischen Umständen einer tatsächlich erfolgten Datenschutzverletzung vergleichsweise allgemein gehalten ist, muss in jedem Fall eine zusätzliche Bewertung unter Berücksichtigung der konkreten Umstände des Vorfalls vorgenommen werden. Abschnitt IV enthält ausführliche Informationen zur Risikobewertung.

In den meisten Fällen sollten diese ersten Maßnahmen kurz nach dem ersten Warnhinweis (d. h. wenn der Verantwortliche oder Auftragsverarbeiter vermutet, dass ein Sicherheitsvorfall mit möglicher Beeinträchtigung personenbezogener Daten aufgetreten ist) abgeschlossen sein und sollten nur in Ausnahmefällen mehr Zeit beanspruchen.

Beispiel

Eine Person teilt dem Verantwortlichen mit, dass sie unter der Identität des Verantwortlichen eine E-Mail mit personenbezogenen Daten erhalten hat, die mit der (tatsächlichen) Nutzung der Dienste des Verantwortlichen zusammenhängen, was darauf hindeutet, dass die Sicherheit des Verantwortlichen beeinträchtigt wurde. Der Verantwortliche führt eine kurze Untersuchung durch. Dabei stellt er fest,

[22] Siehe die Leitlinien der Artikel-29-Datenschutzgruppe zur DSFA unter http://ec.europa.eu/newsroom/document.cfm?doc_id=44137.

dass in sein Netzwerk eingedrungen wurde, und findet Belege für eine unbefugte Einsichtnahme in personenbezogene Daten. Jetzt wäre davon auszugehen, dass die Datenschutzverletzung dem Verantwortlichen „bekannt“ ist und an die Aufsichtsbehörde gemeldet werden muss, es sei denn, dass sie voraussichtlich nicht zu einem Risiko für die Rechte und Freiheiten natürlicher Personen führt. Der Verantwortliche muss nun geeignete Abhilfemaßnahmen zur Behebung der Datenschutzverletzung ergreifen.

Deshalb sollte der Verantwortliche intern Vorkehrungen getroffen haben, um eine Datenschutzverletzung erkennen und beheben zu können. Der Verantwortliche könnte beispielsweise bestimmte technische Maßnahmen zur Erkennung von Unregelmäßigkeiten bei der Datenverarbeitung einsetzen, wie Programme zur Datenfluss- oder Protokollanalyse, mit denen per Korrelation von Protokolldaten Ereignisse und Warnmeldungen festgelegt werden können.[23] Wenn eine Datenschutzverletzung aufgedeckt wird, sollte sie unbedingt an die geeignete Managementebene weitergeleitet werden, damit sie behoben und gegebenenfalls gemäß Artikel 33 gemeldet werden kann und damit falls erforderlich die Benachrichtigung gemäß Artikel 34 erfolgen kann. Die Verantwortlichen könnten entsprechende Maßnahmen und Mechanismen zur Berichterstattung in ihren Vorfallreaktionsplänen und/oder Governance-Regeln konkretisieren. Sie helfen dem Verantwortlichen bei der wirksamen Planung, der Bestimmung der im Unternehmen für die Steuerung von Datenschutzverletzungen zuständigen Stelle und der Entscheidung darüber, wie und ob ein Vorfall den Umständen entsprechend weitergeleitet werden muss.

Der Verantwortliche sollte auch Vereinbarungen mit den von ihm eingesetzten Auftragsverarbeitern treffen, die selbst verpflichtet sind, den Verantwortlichen im Falle einer Datenschutzverletzung zu unterrichten (siehe unten).

Zwar sind die Verantwortlichen und Auftragsverarbeiter selbst dafür verantwortlich, geeignete Vorkehrungen zu treffen, damit sie gegen Datenschutzverletzungen vorbeugen, auf sie reagieren und sie beheben können, doch einige praktische Schritte sollten in jedem Fall unternommen werden.

- Informationen über sicherheitsrelevante Ereignisse sollten immer an die verantwortliche(n) Person(en) weitergeleitet werden, die mit der Behebung von Vorfällen, der Feststellung des Vorliegens einer Datenschutzverletzung und der Risikobewertung betraut ist bzw. sind.
- Anschließend sollte das infolge einer Datenschutzverletzung bestehende Risiko für die betroffenen Personen bewertet werden (d. h. mit welcher Wahrscheinlichkeit kein Risiko, ein Risiko oder ein hohes Risiko besteht), und die betroffenen Abteilungen sollten entsprechend informiert werden.
- Falls erforderlich sollte die Meldung an die Aufsichtsbehörde erfolgen, gegebenenfalls sollten auch die betroffenen Personen von der Datenschutzverletzung benachrichtigt werden.
- Gleichzeitig sollte der Verantwortliche Maßnahmen zur Eindämmung und Bewältigung der Datenschutzverletzung ergreifen.
- Die Datenschutzverletzung sollte während des gesamten Prozesses dokumentiert werden.

Dementsprechend sollte klar sein, dass der Verantwortliche verpflichtet ist, jedem ersten Hinweis nachzugehen und zu ermitteln, ob tatsächlich eine Datenschutzverletzung vorliegt. In diesem kurzen Zeitraum kann der Verantwortliche in gewissem Umfang Untersuchungen durchführen sowie Belege und andere relevante Details zusammentragen. Sobald aber der Verantwortliche mit hinreichender Gewissheit das Vorliegen einer Datenschutzverletzung festgestellt hat, muss er sie, wenn die Voraussetzungen von Artikel 33 Absatz 1 erfüllt sind, unverzüglich und, falls möglich, binnen

[23] Zu beachten ist, dass Protokolldaten, die die Nachvollziehbarkeit z. B. der Speicherung, Änderung oder Löschung von Daten ermöglichen, auch als personenbezogene Daten desjenigen gelten können, der den jeweiligen Verarbeitungsvorgang veranlasst hat.

höchstens 72 Stunden an die Aufsichtsbehörde melden.[24] Handelt der Verantwortliche nicht zeitnah und sollte sich herausstellen, dass tatsächlich eine Datenschutzverletzung aufgetreten ist, könnte dies als versäumte Meldung gemäß Artikel 33 gewertet werden.

In Artikel 32 wird klargestellt, dass die Verantwortlichen und Auftragsverarbeiter geeignete technische und organisatorische Maßnahmen treffen sollten, um ein angemessenes Schutzniveau für personenbezogene Daten zu gewährleisten: Die Fähigkeit zur frühzeitigen Erkennung, Behebung und Meldung einer Datenschutzverletzung sollte als wesentliches Element dieser Maßnahmen betrachtet werden.

3. Gemeinsam für die Verarbeitung Verantwortliche

Artikel 26 befasst sich mit gemeinsam für die Verarbeitung Verantwortlichen und sieht vor, dass gemeinsam für die Verarbeitung Verantwortliche festlegen, wer von ihnen welche Verpflichtung gemäß der DSGVO erfüllt.[25] Dabei muss auch die für die Einhaltung der Verpflichtungen aus den Artikeln 33 und 34 verantwortliche Partei benannt werden. Die Artikel-29-Datenschutzgruppe empfiehlt, in den vertraglichen Vereinbarungen zwischen gemeinsam für die Verarbeitung Verantwortlichen ausdrücklich zu regeln, welcher Verantwortliche in Bezug auf die Einhaltung der Pflicht zur Meldung von Datenschutzverletzungen die führende Rolle übernimmt bzw. die Verantwortung trägt.

4. Pflichten des Auftragsverarbeiters

Der Verantwortliche trägt zwar stets die Gesamtverantwortung für den Schutz personenbezogener Daten, doch der Auftragsverarbeiter hat insofern eine wichtige Rolle, als er den Verantwortlichen dabei unterstützt, seinen Verpflichtungen nachzukommen – dazu gehört auch die Meldung von Datenschutzverletzungen. In Artikel 28 Absatz 3 ist festgelegt, dass die Verarbeitung durch einen Auftragsverarbeiter auf der Grundlage eines Vertrags oder eines anderen Rechtsinstruments zu erfolgen hat. Nach Artikel 28 Absatz 3 Buchstabe f muss ein solcher Vertrag bzw. ein solches anderes Rechtsinstrument vorsehen, dass der Auftragsverarbeiter „unter Berücksichtigung der Art der Verarbeitung und der ihm zur Verfügung stehenden Informationen den Verantwortlichen bei der Einhaltung der in den Artikeln 32 bis 36 genannten Pflichten unterstützt".

Artikel 33 Absatz 2 besagt eindeutig, dass der vom Verantwortlichen eingesetzte Auftragsverarbeiter eine ihm bekannt gewordene Verletzung des Schutzes der personenbezogenen Daten, die er im Auftrag des Verantwortlichen verarbeitetet, „unverzüglich" an den Verantwortlichen melden muss. Der Auftragsverarbeiter ist dabei nicht verpflichtet, die Wahrscheinlichkeit eines mit einer Datenschutzverletzung verbundenen Risikos vor der Meldung an den Verantwortlichen zu prüfen; es ist Sache des Verantwortlichen, dies zu prüfen, sobald ihm die Datenschutzverletzung bekannt wird. Der Auftragsverarbeiter muss lediglich feststellen, ob eine Datenschutzverletzung aufgetreten ist, und diese dann an den Verantwortlichen melden. Der Verantwortliche nutzt den Auftragsverarbeiter, um seine Ziele zu erreichen; deshalb gilt grundsätzlich, dass dem Verantwortlichen die Datenschutzverletzung „bekannt" wurde, sobald ihn der Auftragsverarbeiter davon in Kenntnis gesetzt hat. Die Pflicht des Auftragsverarbeiters zur Meldung an den Verantwortlichen versetzt den Verantwortlichen in die Lage, die Verletzung zu beheben und festzustellen, ob eine Meldung an die Aufsichtsbehörde gemäß Artikel 33 Absatz 1 und eine Benachrichtigung der betroffenen Personen gemäß Artikel 34 Absatz 1 erfolgen muss. Gegebenenfalls möchte der Verantwortliche die Datenschutzverletzung auch untersuchen, weil der Auftragsverarbeiter unter Umständen nicht über

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

[25] Siehe auch Erwägungsgrund 79.

alle einschlägigen Fakten informiert ist und beispielsweise nicht wissen kann, ob der Verantwortliche eine Kopie oder Sicherung der vom Auftragsverarbeiter vernichteten oder verlorenen personenbezogenen Daten hat. Davon kann wiederum abhängen, ob der Verantwortliche den Vorfall melden muss.

Die DSGVO nennt keine konkrete Frist, innerhalb der der Auftragsverarbeiter den Verantwortlichen informieren muss. Sie sieht nur vor, dass die Benachrichtigung „unverzüglich" zu erfolgen hat. Deshalb empfiehlt die Artikel-29-Datenschutzgruppe, dass der Auftragsverarbeiter den Verantwortlichen umgehend unterrichtet und schrittweise zusätzliche Angaben zu der Datenschutzverletzung nachreicht, sobald weitere Details verfügbar werden. Dies ist wichtig, um den Verantwortlichen dabei zu unterstützen, seiner Pflicht zur Meldung der Datenschutzverletzung binnen 72 Stunden nachzukommen.

Wie bereits erläutert, sollten im Vertrag zwischen Verantwortlichem und Auftragsverarbeiter die Modalitäten festgelegt werden, nach denen die in Artikel 33 Absatz 2 genannten Verpflichtungen zusätzlich zu anderen Bestimmungen in der DSGVO zu erfüllen sind. Dazu können etwa Verpflichtungen des Auftragsverarbeiters zur frühzeitigen Meldung gehören, was wiederum dem Verantwortlichen hilft, seiner Pflicht zur Meldung an die Aufsichtsbehörde binnen 72 Stunden nachzukommen.

Erbringt der Auftragsverarbeiter Dienste für mehrere vom selben Vorfall betroffene Verantwortliche, muss er jeden Verantwortlichen einzeln über die Details des Vorfalls informieren.

Der Auftragsverarbeiter könnte im Namen des Verantwortlichen Meldung erstatten, sofern er vom Verantwortlichen eine ordnungsgemäße Genehmigung erhalten hat und dies in den vertraglichen Vereinbarungen zwischen Verantwortlichem und Auftragsverarbeiter geregelt ist. Diese Meldung muss im Einklang mit den Artikel 33 und 34 erfolgen. Dabei ist jedoch unbedingt zu beachten, dass die rechtliche Verantwortung für die Meldung beim Verantwortlichen bleibt.

B. Übermittlung von Informationen an die Aufsichtsbehörde

1. Bereitzustellende Informationen

Bei der Meldung einer Datenschutzverletzung an die Aufsichtsbehörde muss der Verantwortliche nach Maßgabe von Artikel 33 Absatz 3 zumindest folgende Informationen übermitteln:

> „a) eine Beschreibung der Art der Verletzung des Schutzes personenbezogener Daten, soweit möglich mit Angabe der Kategorien und der ungefähren Zahl der betroffenen Personen, der betroffenen Kategorien und der ungefähren Zahl der betroffenen personenbezogenen Datensätze;
>
> b) den Namen und die Kontaktdaten des Datenschutzbeauftragten oder einer sonstigen Anlaufstelle für weitere Informationen;
>
> c) eine Beschreibung der wahrscheinlichen Folgen der Verletzung des Schutzes personenbezogener Daten;
>
> d) eine Beschreibung der von dem Verantwortlichen ergriffenen oder vorgeschlagenen Maßnahmen zur Behebung der Verletzung des Schutzes personenbezogener Daten und gegebenenfalls Maßnahmen zur Abmilderung ihrer möglichen nachteiligen Auswirkungen."

In der DSGVO werden keine Kategorien von betroffenen Personen oder personenbezogenen Datensätzen definiert. Die Artikel-29-Datenschutzgruppe schlägt jedoch vor, dass die Kategorien von betroffenen Personen auf die verschiedenen Arten von Personen Bezug nehmen, deren personenbezogene Daten durch eine Datenschutzverletzung beeinträchtigt wurden. Je nach verwendeten Deskriptoren könnten dazu unter anderem Kinder und andere schutzbedürftige Gruppen,

Menschen mit Behinderungen, Beschäftige oder Kunden gehören. In ähnlicher Weise können sich die Kategorien personenbezogener Datensätze auf die unterschiedlichen Arten von Datensätzen beziehen, die ein Verantwortlicher besitzt, zum Beispiel Gesundheitsdaten, Ausbildungsunterlagen, Informationen zur Sozialfürsorge, Finanzdaten, Kontonummern, Reisepassnummern usw.

Erwägungsgrund 85 macht deutlich, dass die Meldung unter anderem dazu dienen soll, den Schaden für natürliche Personen zu begrenzen. Wenn sich also aus den Arten von betroffenen Personen oder den Arten von personenbezogenen Daten ableiten lässt, dass eine Datenschutzverletzung einen bestimmten Schaden zur Folge haben könnte (z. B. Identitätsdiebstahl, Betrug, finanzielle Verluste, Gefährdung des Berufsgeheimnisses), ist es wichtig, diese Kategorien bei der Meldung anzugeben. Damit wird eine Verknüpfung mit der Pflicht zur Beschreibung der wahrscheinlichen Folgen der Datenschutzverletzung hergestellt.

Das Fehlen genauer Informationen (z. B. die genaue Zahl der betroffenen Personen) sollte kein Hindernis für die frühzeitige Meldung einer Datenschutzverletzung sein. Nach der DSGVO dürfen ungefähre Zahlen der betroffenen Personen und der betroffenen personenbezogenen Datensätze angegeben werden. Der Fokus sollte auf der Behebung der nachteiligen Auswirkungen der Datenschutzverletzung liegen und weniger auf genauen Zahlenangaben. Daher kann, wenn eine Datenschutzverletzung eindeutig festgestellt wurde, deren genaues Ausmaß aber noch nicht bekannt ist, die Meldung schrittweise erfolgen (siehe unten), um der Meldepflicht dennoch ordnungsgemäß nachzukommen.

Nach Artikel 33 Absatz 3 hat der Verantwortliche „zumindest“ diese Informationen bei der Meldung mitzuteilen. Es steht ihm also frei, falls erforderlich zusätzliche Angaben zu machen. Bei bestimmten Datenschutzverletzungen (Vertraulichkeit, Integrität oder Verfügbarkeit) werden zur vollständigen Erklärung des Einzelfalls möglicherweise weitere Informationen benötigt.

Beispiel

Im Rahmen der Meldung an die Aufsichtsbehörde ist es für einen Verantwortlichen unter Umständen hilfreich, den Auftragsverarbeiter zu benennen, wenn dieser für die Datenschutzverletzung ursächlich ist; dies gilt insbesondere dann, wenn die personenbezogenen Daten zahlreicher anderer Verantwortlicher von dem Vorfall betroffen sind, die den gleichen Auftragsverarbeiter in Anspruch nehmen.

In jedem Fall kann die Aufsichtsbehörde im Rahmen ihrer Untersuchung einer Datenschutzverletzung weitere Details verlangen.

2. Schrittweise Meldung

Je nach Art einer Datenschutzverletzung muss der Verantwortliche zur Ermittlung aller für einen Vorfall relevanten Fakten eventuell zusätzliche Untersuchungen durchführen. In Artikel 33 Absatz 4 ist daher Folgendes festgelegt:

„Wenn und soweit die Informationen nicht zur gleichen Zeit bereitgestellt werden können, kann der Verantwortliche diese Informationen ohne unangemessene weitere Verzögerung schrittweise zur Verfügung stellen.“

Die DSGVO trägt somit der Tatsache Rechnung, dass einem Verantwortlichen nicht immer binnen 72 Stunden, nachdem ihm eine Datenschutzverletzung bekannt wurde, alle erforderlichen Informationen vorliegen, da vollständige und umfassende Details eines Vorfalls nicht immer schon innerhalb dieses ersten Zeitraums verfügbar sind. Deshalb darf die Meldung schrittweise erfolgen. Die schrittweise Meldung wird wahrscheinlich eher bei komplexeren Datenschutzverletzungen zum Tragen kommen, etwa bei bestimmten Cybersicherheitsvorfällen, die beispielsweise eingehende

forensische Ermittlungen erfordern, um alle Aspekte der Datenschutzverletzung aufzuklären und festzustellen, in welchem Umfang personenbezogene Daten beeinträchtigt wurden. In vielen Fällen wird der Verantwortliche daher weitere Untersuchungen durchführen und zu einem späteren Zeitpunkt zusätzliche Informationen nachreichen müssen. Dies ist zulässig, sofern der Verantwortliche die Verzögerung gemäß Artikel 33 Absatz 1 begründet. Die Artikel-29-Datenschutzgruppe empfiehlt, dass der Verantwortliche die Aufsichtsbehörde bei seiner ersten Meldung an die Aufsichtsbehörde auch darüber informiert, dass ihm noch nicht alle geforderten Informationen vorliegen und dass er weitere Angaben zu einem späteren Zeitpunkt nachreichen wird. Die Aufsichtsbehörde sollte dem Zeitpunkt und den Modalitäten der Übermittlung zusätzlicher Informationen zustimmen. Dies hindert den Verantwortlichen nicht daran, zu einem beliebigen anderen späteren Zeitpunkt zusätzliche Informationen bereitzustellen, wenn ihm weitere relevante Details zu der Datenschutzverletzung bekannt werden, die an die Aufsichtsbehörde weitergegeben werden müssen.

Durch die Meldepflicht sollen die Verantwortlichen insbesondere dazu angehalten werden, bei Datenschutzverletzungen umgehend tätig zu werden und sie einzudämmen, die beeinträchtigten personenbezogenen Daten nach Möglichkeit wiederherzustellen und sich von der Aufsichtsbehörde beraten zu lassen. Wenn der Verantwortliche die Aufsichtsbehörde innerhalb der ersten 72 Stunden benachrichtigt, kann er sicherstellen, dass er im Hinblick auf die Benachrichtigung der betroffenen Personen korrekt entscheidet.

Zweck der Meldung an die Aufsichtsbehörde ist es jedoch nicht nur, sich zu der Frage beraten zu lassen, ob die betroffenen Personen benachrichtigt werden müssen. In manchen Fällen wird es aufgrund der Art der Datenschutzverletzung und der Schwere des Risikos sofort offensichtlich sein, dass die betroffenen Personen unverzüglich durch den Verantwortlichen benachrichtigt werden müssen. Wenn beispielsweise die unmittelbare Gefahr von Identitätsdiebstahl besteht oder wenn besondere Kategorien personenbezogener Daten[26] online veröffentlicht wurden, sollten die Verantwortlichen unverzüglich handeln, um die Datenschutzverletzung einzudämmen und die betroffenen Personen zu benachrichtigen (siehe Abschnitt III). In Ausnahmefällen kann die Benachrichtigung sogar vor der Meldung an die Aufsichtsbehörde geschehen. Generell darf die Meldung an die Aufsichtsbehörde nicht als Rechtfertigung dafür dienen, dass die betroffenen Personen nicht wie erforderlich von der Datenschutzverletzung benachrichtigt werden.

Ferner sollte klar sein, dass der Verantwortliche die Aufsichtsbehörde nach der ersten Meldung informieren könnte, wenn sich bei Folgeuntersuchungen herausstellt, dass der Sicherheitsvorfall eingedämmt wurde und letztlich keine Datenschutzverletzung aufgetreten ist. Die neuen Erkenntnisse könnten dann den bereits an die Aufsichtsbehörde übermittelten Informationen hinzugefügt werden, sodass der Vorfall nicht als Datenschutzverletzung verzeichnet wird. Es gibt keine Strafe für die Meldung eines Vorfalls, der sich letztlich nicht als Datenschutzverletzung erweist.

Beispiel

Ein Verantwortlicher meldet der Aufsichtsbehörde binnen 72 Stunden, nachdem ihm eine Datenschutzverletzung bekannt wurde, den Verlust eines USB-Stick, auf dem eine Kopie der personenbezogenen Daten einiger seiner Kunden gespeichert ist. Später stellt sich heraus, dass der USB-Schüssel in den Räumlichkeiten des Verantwortlichen falsch abgelegt war und wiedergefunden wurde. Der Verantwortliche setzt die Aufsichtsbehörde über die Neuentwicklung in Kenntnis und bittet um Änderung der Meldung.

[26] Siehe Artikel 9.

Es wird darauf hingewiesen, dass ein schrittweises Vorgehen bei der Meldung bereits im Rahmen der bestehenden Verpflichtungen gemäß der Richtlinie 2002/58/EG, der Verordnung 611/2013 und anderer selbst gemeldeter Vorfälle vorgesehen ist.

3. Verzögerte Meldung

Erfolgt die Meldung an die Aufsichtsbehörde nicht binnen 72 Stunden, so ist nach Artikel 33 Absatz 1 eine Begründung für die Verzögerung beizufügen. Mit dieser Vorgabe sowie mit dem Konzept der schrittweisen Meldung wird zugestanden, dass die Verantwortlichen möglicherweise nicht immer in der Lage sind, eine Datenschutzverletzung innerhalb dieses Zeitraums zu melden, und dass eine verzögerte Meldung zulässig sein kann.

Ein solches Szenario wäre beispielsweise denkbar, wenn bei einem Verantwortlichen in einem kurzen Zeitraum mehrere vergleichbare Verletzungen der Datenvertraulichkeit auftreten, von denen sehr viele Personen in gleicher Weise betroffen sind. Einem Verantwortlichen könnte eine Datenschutzverletzung bekannt werden, und zu Beginn seiner Untersuchungen sowie vor der Meldung könnte er feststellen, dass weitere ähnliche Verletzungen mit unterschiedlichen Ursachen aufgetreten sind. Je nach den Umständen kann der Verantwortliche das Ausmaß der Datenschutzverletzungen vielleicht erst nach einer gewissen Zeit feststellen; anstatt jede Verletzung einzeln zu melden, erstellt er eine aussagekräftige Meldung, in der mehrere sehr ähnlich gelagerte Verletzungen mit verschiedenen möglichen Ursachen wiedergegeben werden. Dadurch könnte sich die Meldung an die Aufsichtsbehörde um mehr als 72 Stunden, nachdem dem Verantwortlichen die Datenschutzverletzungen bekannt wurden, verzögern.

Streng genommen gilt jede einzelne Datenschutzverletzung als meldepflichtiger Vorfall. Um aber einen übermäßigen Aufwand zu vermeiden, kann der Verantwortliche alle Datenschutzverletzungen in einer Meldung „bündeln“, sofern dabei dieselben Arten von personenbezogenen Daten auf dieselbe Weise in einem relativ kurzen Zeitraum beeinträchtigt wurden. Kommt es zu einer Reihe von Datenschutzverletzungen, bei denen unterschiedliche Arten von personenbezogenen Daten auf unterschiedliche Weise verletzt werden, sollte die Meldung wie gewohnt erfolgen und jede Datenschutzverletzung einzeln gemäß Artikel 33 gemeldet werden.

Auch wenn die DSGVO in gewissem Umfang verzögerte Meldungen zulässt, darf dies nicht als regelmäßige Vorgehensweise betrachtet werden. Erwähnenswert ist, dass die gebündelte Meldung auch für mehrere ähnliche Datenschutzverletzungen innerhalb der 72-Stunden-Frist genutzt werden kann.

C. Grenzüberschreitende Datenschutzverletzungen und Datenschutzverletzungen bei Niederlassungen außerhalb der EU

1. Grenzüberschreitende Datenschutzverletzungen

Wenn personenbezogene Daten grenzüberschreitend verarbeitet werden[27], können Personen in mehr als einem Mitgliedstaat von einer Datenschutzverletzung betroffen sein. In Artikel 33 Absatz 1 wird klargestellt, dass die Verantwortlichen Datenschutzverletzungen an die gemäß Artikel 55 der DSGVO zuständige Aufsichtsbehörde melden sollten.[28] Artikel 55 Absatz 1 lautet wie folgt:

> „Jede Aufsichtsbehörde ist für die Erfüllung der Aufgaben und die Ausübung der Befugnisse, die ihr mit dieser Verordnung übertragen wurden, im Hoheitsgebiet ihres eigenen Mitgliedstaats zuständig.“

[27] Siehe Artikel 4 Absatz 23.

[28] Siehe auch Erwägungsgrund 122.

Artikel 56 Absatz 1 besagt jedoch Folgendes:

> „Unbeschadet des Artikels 55 ist die Aufsichtsbehörde der Hauptniederlassung oder der einzigen Niederlassung des Verantwortlichen oder des Auftragsverarbeiters gemäß dem Verfahren nach Artikel 60 die zuständige federführende Aufsichtsbehörde für die von diesem Verantwortlichen oder diesem Auftragsverarbeiter durchgeführte grenzüberschreitende Verarbeitung."

Darüber hinaus sieht Artikel 56 Absatz 6 Folgendes vor:

> „Die federführende Aufsichtsbehörde ist der einzige Ansprechpartner der Verantwortlichen oder der Auftragsverarbeiter für Fragen der von diesem Verantwortlichen oder diesem Auftragsverarbeiter durchgeführten grenzüberschreitenden Verarbeitung."

Danach muss der Verantwortliche meldepflichtige Datenschutzverletzungen, die im Rahmen einer grenzüberschreitenden Verarbeitung auftreten, an die federführende Aufsichtsbehörde melden.[29] Daher muss der Verantwortliche bei der Ausarbeitung des Reaktionsplans zur Bewältigung von Datenschutzverletzungen prüfen, bei welcher federführenden Aufsichtsbehörde etwaige Vorfälle gemeldet werden müssen.[30] So ist der Verantwortliche in der Lage, zügig auf eine Datenschutzverletzung zu reagieren und seine Verpflichtungen gemäß Artikel 33 zu erfüllen. Es dürfte klar sein, dass sich die federführende Aufsichtsbehörde, an die Datenschutzverletzungen im Rahmen der grenzüberschreitenden Verarbeitung gemeldet werden müssen, nicht notwendigerweise an dem Ort befindet, an dem die betroffenen Personen ansässig sind oder an dem sich die Datenschutzverletzung ereignet hat. Bei der Meldung an die federführende Behörde sollte der Verantwortliche gegebenenfalls angeben, ob die Datenschutzverletzung Niederlassungen in anderen Mitgliedstaaten betrifft und in welchen Mitgliedstaaten Personen durch die Datenschutzverletzung beeinträchtigt worden sein könnten. Ist der Verantwortliche nicht sicher, welche Aufsichtsbehörde federführend ist, sollte er die Datenschutzverletzung zumindest an die lokale Aufsichtsbehörde des Ortes melden, an dem sich der Vorfall ereignet hat.

2. Datenschutzverletzungen bei Niederlassungen außerhalb der EU

Artikel 3 betrifft den räumlichen Anwendungsbereich der DSGVO. Darin ist unter anderem geregelt, wann die DSGVO für die Verarbeitung personenbezogener Daten durch einen nicht in der EU niedergelassenen Verantwortlichen oder Auftragsverarbeiter anwendbar ist. Konkret sieht Artikel 3 Absatz 2 Folgendes vor:[31]

> „Diese Verordnung findet Anwendung auf die Verarbeitung personenbezogener Daten von betroffenen Personen, die sich in der Union befinden, durch einen nicht in der Union niedergelassenen Verantwortlichen oder Auftragsverarbeiter, wenn die Datenverarbeitung im Zusammenhang damit steht

---

[29] Siehe die Leitlinien der Artikel-29-Datenschutzgruppe für die Bestimmung der federführenden Aufsichtsbehörde eines Verantwortlichen oder Auftragsverarbeiters, abrufbar unter http://ec.europa.eu/newsroom/document.cfm?doc_id=44102http://ec.europa.eu/newsroom/document.cfm?doc_id=44102

[30] Eine Liste mit den Kontaktdaten aller europäischen nationalen Datenschutzbehörden ist erhältlich unter http://ec.europa.eu/justice/data-protection/bodies/authorities/index_en.htm.

[31] Siehe auch Erwägungsgründe 23 und 24.

a) betroffenen Personen in der Union Waren oder Dienstleistungen anzubieten, unabhängig davon, ob von diesen betroffenen Personen eine Zahlung zu leisten ist;

b) das Verhalten betroffener Personen zu beobachten, soweit ihr Verhalten in der Union erfolgt."

Relevant ist auch Artikel 3 Absatz 3:[32]

„Diese Verordnung findet Anwendung auf die Verarbeitung personenbezogener Daten durch einen nicht in der Union niedergelassenen Verantwortlichen an einem Ort, der aufgrund Völkerrechts dem Recht eines Mitgliedstaats unterliegt."

Ein nicht in der EU niedergelassener Verantwortlicher, der Artikel 3 Absatz 2 oder Artikel 3 Absatz 3 unterliegt und bei sich eine Datenschutzverletzung feststellt, ist daher immer noch an die Meldepflichten gemäß Artikel 33 und 34 gebunden. Nach Artikel 27 müssen die Verantwortlichen (und Auftragsverarbeiter) in Fällen gemäß Artikel 3 Absatz 2 einen Vertreter in der EU benennen. Die Artikel-29-Datenschutzgruppe empfiehlt, dass Datenschutzverletzungen in solchen Fällen an die Aufsichtsbehörde in dem Mitgliedstaat gemeldet werden, in dem der Vertreter des Verantwortlichen in der EU niedergelassen ist.[33] Desgleichen sind Auftragsverarbeiter im Sinne des Artikels 3 Absatz 2 an die Verpflichtungen für Auftragsverarbeiter gebunden und somit – was in diesem Zusammenhang besonders relevant ist – an die Pflicht zur Meldung von Datenschutzverletzungen an den Verantwortlichen gemäß Artikel 33 Absatz 2.

D. Nicht meldepflichtige Bedingungen

Aus Artikel 33 Absatz 1 geht hervor, dass eine Datenschutzverletzung, die „voraussichtlich nicht zu einem Risiko für die Rechte und Freiheiten natürlicher Personen führt", nicht an die Aufsichtsbehörde gemeldet werden muss. Ein mögliches Beispiel wäre, wenn personenbezogene Daten bereits öffentlich verfügbar sind und die Offenlegung dieser Daten voraussichtlich kein Risiko für die betroffenen Personen darstellt. Im Gegensatz dazu stehen die Meldepflichten der Anbieter öffentlich verfügbarer elektronischer Kommunikationsdienste gemäß Richtlinie 2009/136/EG, wonach alle relevanten Datenschutzverletzungen an die zuständige Behörde gemeldet werden müssen.

Wie von der Artikel-29-Datenschutzgruppe in ihrer Stellungnahme 03/2014 über die Meldung von Verletzungen des Schutzes personenbezogener Daten[34] dargelegt, stellt auch eine Verletzung der Vertraulichkeit personenbezogener Daten, die durch einen dem Stand der Technik entsprechenden Algorithmus verschlüsselt wurden, eine Verletzung des Schutzes personenbezogener Daten dar und muss der zuständigen Behörde gemeldet werden. Ist jedoch die Vertraulichkeit des Schlüssels gewahrt – ist der Schlüssel also durch keine Sicherheitsverletzung beeinträchtigt und wurde er so generiert, dass er von Personen, die zum Zugriff auf den Schlüssel nicht befugt sind, mit derzeit verfügbaren technischen Mitteln nicht ermittelt werden kann –, sind die Daten grundsätzlich unzugänglich. Folglich haben die betroffenen Personen von der Datenschutzverletzung voraussichtlich keine nachteiligen Auswirkungen zu erwarten, sodass sie nicht benachrichtigt werden müssen.[35] Doch selbst bei verschlüsselten Daten können der Verlust oder die Änderung der Daten

[32] Siehe auch Erwägungsgrund 25.

[33] Siehe Erwägungsgrund 80 und Artikel 27.

[34] Artikel-29-Datenschutzgruppe, Stellungnahme 03/2014 über die Meldung von Verletzungen des Schutzes personenbezogener Daten, http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp213_en.pdf.

[35] Siehe auch Artikel 4 Absätze 1 und 2 der Verordnung (EG) Nr. 611/2013.

nachteilige Folgen für die betroffenen Personen haben, wenn der Verantwortliche über keine angemessenen Sicherungskopien verfügt. In diesem Fall sollten die betroffenen Personen auch dann benachrichtigt werden, wenn die Daten durch angemessene Maßnahmen verschlüsselt wurden.

Wie die Artikel-29-Datenschutzgruppe zudem erklärt hat, wäre dies auch dann der Fall, wenn personenbezogene Daten, wie etwa Passwörter, unter Verwendung einer Hash-Funktion und eines Salt-Werts sicher verschlüsselt wurden, der Hash-Wert mithilfe einer dem Stand der Technik entsprechenden kryptografischen verschlüsselten Hash-Funktion berechnet wurde, der zum Daten-Hashing verwendete Schlüssel durch keine Sicherheitsverletzung beeinträchtigt wurde und der zum Daten-Hashing verwendete Schlüssel so generiert wurde, dass er von Personen, die zum Zugriff auf den Schlüssel nicht befugt sind, mit derzeit verfügbaren technischen Mitteln nicht ermittelt werden kann.

Wenn folglich personenbezogene Daten für Unbefugte grundsätzlich unverständlich gemacht wurden und es sich bei den Daten um eine Kopie handelt oder eine Datensicherung existiert, muss eine Verletzung der Vertraulichkeit ordnungsgemäß verschlüsselter personenbezogener Daten möglicherweise nicht an die Aufsichtsbehörde gemeldet werden. Das liegt daran, dass eine solche Datenschutzverletzung voraussichtlich nicht mit einem Risiko für die Rechte und Freiheiten der betroffenen Personen verbunden ist. Insofern müssen die betroffenen Personen natürlich auch nicht benachrichtigt werden, da voraussichtlich kein hohes Risiko besteht. Dabei gilt es jedoch zu beachten, dass auch, wenn zunächst auf die Meldung verzichtet werden kann, weil kein hohes Risiko für die Rechte und Freiheiten der betroffenen Personen besteht, sich die Umstände mit der Zeit ändern können, sodass das Risiko erneut bewertet werden muss. Wenn sich etwa später herausstellt, dass der Schlüssel beeinträchtigt wurde, oder wenn eine Sicherheitslücke in der Verschlüsselungssoftware entdeckt wird, kann die Meldung doch erforderlich werden.

Darüber hinaus ist zu berücksichtigen, dass im Falle von Datenschutzverletzungen, bei denen keine Sicherungskopie der verschlüsselten personenbezogenen Daten existiert, die Datenverfügbarkeit beeinträchtigt ist, was wiederum Risiken für die betroffenen Personen bergen könnte, sodass der Vorfall möglicherweise meldepflichtig ist. Desgleichen kann die Meldung im Falle des Verlusts verschlüsselter Daten selbst dann erforderlich sein, wenn eine Sicherungskopie der personenbezogenen Daten existiert, je nachdem, wie viel Zeit die Wiederherstellung der Daten von der Sicherungskopie beansprucht und welche Folgen die mangelnde Verfügbarkeit der Daten für die betroffenen Personen hat. Wie in Artikel 32 Absatz 1 Buchstabe c dargelegt, ist „die Fähigkeit, die Verfügbarkeit der personenbezogenen Daten und den Zugang zu ihnen bei einem physischen oder technischen Zwischenfall rasch wiederherzustellen“ ein wichtiger Datensicherheitsfaktor.

Beispiel

Eine Datenschutzverletzung, bei der auf die Meldung an die Aufsichtsbehörde verzichtet werden könnte, wäre beispielsweise der Verlust eines sicher verschlüsselten, vom Verantwortlichen und seinen Mitarbeitern verwendeten mobilen Endgeräts. Sofern der für die Verschlüsselung verwendete Schlüssel im Besitz des Verantwortlichen bleibt und es sich nicht um die einzige Kopie der personenbezogenen Daten handelt, wären die personenbezogenen Daten für einen Angreifer unzugänglich. Folglich würde die Datenschutzverletzung voraussichtlich nicht zu einem Risiko für die Rechte und Freiheiten der betroffenen Personen führen. Falls sich später herausstellt, dass der für die Verschlüsselung verwendete Schlüssel beeinträchtigt wurde oder die Verschlüsselungssoftware bzw. der Verschlüsselungsalgorithmus angreifbar sind, wäre das Risiko für die Rechte und Freiheiten der betroffenen Personen anders zu bewerten, sodass eine Meldung nun erforderlich sein könnte.

Versäumt es jedoch der Verantwortliche, eine Datenschutzverletzung an die Aufsichtsbehörde zu melden, wenn die Daten nicht tatsächlich sicher verschlüsselt waren, liegt eine Missachtung von Artikel 33 vor. Bei der Auswahl der Verschlüsselungssoftware sollten die Verantwortlichen daher die Qualität und die ordnungsgemäße Umsetzung der angebotenen Verschlüsselung sorgfältig prüfen und

genau wissen, welches Schutzniveau damit tatsächlich geboten wird und ob das Schutzniveau für die bestehenden Risiken angemessen ist. Außerdem sollten die Verantwortlichen mit der Funktionswiese der von ihnen eingesetzten Verschlüsselungstechnologie vertraut sein. Ein Gerät könnte zum Beispiel beim Ausschalten verschlüsselt werden, nicht jedoch im Stand-by-Modus. Manche Produkte mit Verschlüsselungstechnologie verwenden „Standardschlüssel", die vom Kunden geändert werden müssen, um wirksam zu sein. Auch könnte eine von Sicherheitsexperten zum gegenwärtigen Zeitpunkt als angemessen eingestufte Verschlüsselungstechnologie einige Jahre später überholt sein, wodurch fraglich wird, ob das Produkt eine ausreichende Verschlüsselung der Daten und ein angemessenes Schutzniveau bietet.

III. **Artikel 34 – Benachrichtigung der betroffenen Person**

A. Unterrichtung der betroffenen Personen

In bestimmten Fällen muss der Verantwortliche zusätzlich zur Meldung an die Aufsichtsbehörde auch die betroffenen Personen von der Datenschutzverletzung benachrichtigen.

In Artikel 34 Absatz 1 ist Folgendes festgelegt:

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

Die Verantwortlichen sollten daran denken, dass die Meldung an die Aufsichtsbehörde obligatorisch ist, es sei denn, dass die Datenschutzverletzung voraussichtlich nicht zu einem Risiko für die Rechte und Freiheiten von natürlichen Personen führt. Darüber hinaus müssen auch die betroffenen Personen benachrichtigt werden, wenn die Datenschutzverletzung voraussichtlich ein hohes Risiko für die Rechte und Freiheiten der betroffenen Personen birgt. Für die Benachrichtigung der betroffenen Personen gilt demnach eine höhere Schwelle als für die Meldung an die Aufsichtsbehörden – die betroffenen Personen müssen also nicht in allen Fällen von Datenschutzverletzungen benachrichtigt werden, damit sie nicht mit unnötigen Benachrichtigungen überfrachtet werden.

Nach der DSGVO müssen die betroffenen Personen „unverzüglich", das heißt so schnell wie möglich, von einer Datenschutzverletzung benachrichtigt werden. Wichtigstes Ziel der Benachrichtigung ist es, dass die betroffenen Personen gezielt über Vorkehrungen informiert werden, die sie zu ihrem eigenen Schutz treffen können.[36] Wie bereits angemerkt, hilft eine frühzeitige Benachrichtigung den betroffenen Personen je nach Art der Datenschutzverletzung und der damit verbundenen Risiken, die nötigen Schritte einzuleiten, um sich selbst vor den negativen Folgen der Verletzung zu schützen.

Anhang B dieser Leitlinien enthält eine nicht erschöpfende Liste mit Fallbeispielen, in denen eine Datenschutzverletzung voraussichtlich zu einem hohen Risiko für die betroffenen Personen führt und in denen der Verantwortliche daher verpflichtet ist, die Betroffenen von der Datenschutzverletzung zu benachrichtigen.

B. Bereitzustellende Informationen

In Bezug auf die Benachrichtigung betroffener Personen sieht Artikel 34 Absatz 2 Folgendes vor:

[36] Siehe auch Erwägungsgrund 86.

„Die in Absatz 1 genannte Benachrichtigung der betroffenen Person beschreibt in klarer und einfacher Sprache die Art der Verletzung des Schutzes personenbezogener Daten und enthält zumindest die in Artikel 33 Absatz 3 Buchstaben b, c und d genannten Informationen und Maßnahmen."

Nach dieser Vorschrift sollten die Verantwortlichen zumindest die folgenden Informationen bereitstellen:

- eine Beschreibung der Art der Datenschutzverletzung;
- den Namen und die Kontaktdaten des Datenschutzbeauftragten oder einer sonstigen Anlaufstelle;
- eine Beschreibung der wahrscheinlichen Folgen der Datenschutzverletzung; und
- eine Beschreibung der vom Verantwortlichen ergriffenen oder vorgeschlagenen Maßnahmen zur Behebung der Datenschutzverletzung, gegebenenfalls einschließlich der Maßnahmen zur Abmilderung ihrer möglichen nachteiligen Auswirkungen.

Der Verantwortliche könnte als Beispiel für die Maßnahmen, die er zur Behebung der Datenschutzverletzung und zur Abmilderung ihrer möglichen nachteiligen Auswirkungen ergriffen hat, anführen, dass er von der zuständigen Aufsichtsbehörde nach Meldung der Datenschutzverletzung über den Umgang mit dem Vorfall und die Abmilderung seiner Auswirkungen beraten wurde. Er könnte den betroffenen Personen gegebenenfalls auch besondere Maßnahmen empfehlen, die sie zu ihrem eigenen Schutz vor möglichen nachteiligen Auswirkungen der Datenschutzverletzung treffen können, wie etwa das Zurücksetzen der Passwörter im Falle der Beeinträchtigung von Zugangsdaten. Auch hier steht es den Verantwortlichen frei, über die genannten Anforderungen hinaus weitere Informationen bereitzustellen.

C. Kontaktaufnahme mit den betroffenen Personen

Grundsätzlich sollten die betroffenen Personen direkt über eine Datenschutzverletzung benachrichtigt werden, sofern dies nicht mit einem unverhältnismäßig hohen Aufwand verbunden ist. In dem Fall hat stattdessen eine öffentliche Bekanntmachung oder eine ähnliche Maßnahme zu erfolgen, durch die die betroffenen Personen vergleichbar wirksam informiert werden (Artikel 34 Absatz 3 Buchstabe c).

Die betroffenen Personen sollten durch eine eigens für den Zweck erstellte Mitteilung von der Datenschutzverletzung benachrichtigt werden. Die Mitteilung sollte nicht zusammen mit anderen Informationen, etwa mit regelmäßigen Updates, Newslettern oder Standardmitteilungen, verschickt werden. Dies trägt zur Klarheit und Transparenz der Benachrichtigung bei.

Transparente Benachrichtigungsmethoden sind zum Beispiel die direkte Kommunikation per E-Mail, SMS oder Instant-Messaging-Dienste, an herausragender Stelle platzierte Banner oder Meldungen auf der Website, postalische Mitteilungen und aufmerksamkeitsstarke Anzeigen in den Printmedien. Die ausschließliche Benachrichtigung durch eine Pressemitteilung oder in einem Unternehmensblog wäre kein wirksames Mittel, um die betroffenen Personen von einer Datenschutzverletzung in Kenntnis zu setzen. Die Artikel-29-Datenschutzgruppe empfiehlt den Verantwortlichen, Kommunikationsmittel zu wählen, die eine optimale Vermittlung der Informationen an alle betroffenen Personen gewährleisten. Dazu muss der Verantwortliche den Umständen entsprechend möglicherweise mehrere Kommunikationswege statt nur eines Kontaktkanals nutzen.

Die Verantwortlichen müssen zudem sicherstellen, dass die Benachrichtigung in geeigneten alternativen Formaten und in den relevanten Sprachversionen erhältlich ist, damit die betroffenen Personen die vermittelten Informationen verstehen können. So dürfte etwa für die Benachrichtigung einer betroffenen Person in der Regel die bis dahin im normalen Geschäftsverkehr mit dem Empfänger verwendete Sprache geeignet sein. Wenn allerdings Personen von der Datenschutzverletzung betroffen sind, mit denen der Verantwortliche zuvor noch keinen Kontakt hatte, und insbesondere solche, die in einem anderen Mitgliedstaat oder einem anderen Drittland, in

dem der Verantwortliche niedergelassen ist, könnte eine Benachrichtigung in der lokalen Landessprache – unter Berücksichtigung der erforderlichen Ressourcen – akzeptabel sein. Entscheidend ist, dass den betroffenen Personen geholfen wird zu verstehen, welcher Art die Datenschutzverletzung ist und was sie zu ihrem Schutz tun können.

Die Verantwortlichen können am besten selbst beurteilen, welcher Kommunikationskanal für die Benachrichtigung der betroffenen Personen am geeignetsten ist, vor allem, wenn sie häufig mit ihren Kunden interagieren. Allerdings sollten die Verantwortlichen natürlich alle Kommunikationskanäle vermeiden, die durch die Datenschutzverletzung beeinträchtigt wurden, da sie von Angreifern genutzt werden könnten, die sich für den Verantwortlichen ausgeben.

Gleichzeitig wird in Erwägungsgrund 86 Folgendes erklärt:

> „Solche Benachrichtigungen der betroffenen Person sollten stets so rasch wie nach allgemeinem Ermessen möglich, in enger Absprache mit der Aufsichtsbehörde und nach Maßgabe der von dieser oder von anderen zuständigen Behörden wie beispielsweise Strafverfolgungsbehörden erteilten Weisungen erfolgen. Um beispielsweise das Risiko eines unmittelbaren Schadens mindern zu können, müssten betroffene Personen sofort benachrichtigt werden, wohingegen eine längere Benachrichtigungsfrist gerechtfertigt sein kann, wenn es darum geht, geeignete Maßnahmen gegen fortlaufende oder vergleichbare Verletzungen des Schutzes personenbezogener Daten zu treffen."

Daher könnten sich die Verantwortlichen an die Aufsichtsbehörde wenden und sich nicht nur zur Benachrichtigung der betroffenen Personen über eine Datenschutzverletzung gemäß Artikel 34 beraten lassen, sondern auch darüber, welche Inhalte die Mitteilungen an die betroffenen Personen enthalten sollten und wie die Kontaktaufnahme am besten erfolgen sollte.

Damit verbunden ist die Empfehlung in Erwägungsgrund 88, wonach „den berechtigten Interessen der Strafverfolgungsbehörden in Fällen Rechnung [getragen werden sollte], in denen die Untersuchung der Umstände einer Verletzung des Schutzes personenbezogener Daten durch eine frühzeitige Offenlegung in unnötiger Weise behindert würde". Dies kann bedeuten, dass die Verantwortlichen unter bestimmten Umständen, soweit gerechtfertigt und auf Anraten der Strafverfolgungsbehörden die Benachrichtigung der betroffenen Personen von der Datenschutzverletzung so lange hinauszögern können, bis entsprechende Ermittlungen dadurch nicht mehr beeinträchtigt werden. Anschließend müssten die betroffenen Personen aber umgehend benachrichtigt werden.

Wenn der Verantwortliche eine betroffene Person nicht von einer Datenschutzverletzung benachrichtigen kann, weil nicht genügend Daten vorliegen, um sie kontaktieren zu können, sollte der Verantwortliche die betroffene Person in diesem besonderen Fall so rasch wie nach allgemeinem Ermessen möglich benachrichtigen (z. B. wenn eine Person ihr Recht auf Auskunft über personenbezogene Daten gemäß Artikel 15 ausübt und dabei dem Verantwortlichen die zur Kontaktaufnahme notwendigen zusätzlichen Informationen übermittelt).

D. Bedingungen, unter denen keine Benachrichtigung erforderlich ist

In Artikel 34 Absatz 3 werden die folgenden drei Bedingungen genannt, unter denen die betroffenen Personen nicht von einer Datenschutzverletzung benachrichtigt werden müssen:

- Der Verantwortliche hat vor der Datenschutzverletzung geeignete technische und organisatorische Maßnahmen zum Schutz personenbezogener Daten umgesetzt, insbesondere solche Maßnahmen, durch die die personenbezogenen Daten für alle Personen, die nicht zum Zugang zu den personenbezogenen Daten befugt sind, unzugänglich gemacht werden. Dazu könnte zum Beispiel der Schutz personenbezogener Daten durch eine dem Stand der Technik entsprechende Verschlüsselung oder durch Tokenisierung gehören.
- Der Verantwortliche hat unmittelbar nach einer Datenschutzverletzung durch Maßnahmen dafür gesorgt, dass das hohe Risiko für die Rechte und Freiheiten der betroffenen Personen

aller Wahrscheinlichkeit nach nicht mehr besteht. Je nach Sachlage wäre dies beispielsweise der Fall, wenn der Verantwortliche die Person, die Zugang zu den personenbezogenen Daten hatte, sofort ermittelt und Maßnahmen gegen sie getroffen hat, bevor sie die Daten in irgendeiner Weise verwenden konnte. Trotzdem müssen – auch hier abhängig von der Art der betroffenen Daten – die möglichen Folgen einer etwaigen Beeinträchtigung der Datenvertraulichkeit gebührend berücksichtigt werden.

- Die Kontaktaufnahme mit den betroffenen Personen würde einen unverhältnismäßigen Aufwand[37] verursachen, etwa wenn deren Kontaktdaten aufgrund der Datenschutzverletzung verloren gegangen sind oder wenn diese schon vorher nicht bekannt waren. Ein solcher Fall würde beispielsweise eintreten, wenn das Lager eines statistischen Amtes überflutet wurde und die Dokumente mit den personenbezogenen Daten nur in Papierform gelagert wurden. Der Verantwortliche muss stattdessen eine öffentliche Mitteilung machen oder mit ähnlichen Maßnahmen dafür sorgen, dass die betroffenen Personen vergleichbar wirksam informiert werden. Im Falle eines unverhältnismäßigen Aufwands könnten die Informationen über die Datenschutzverletzung unter Umständen auch mithilfe technischer Lösungen auf Anfrage abrufbar gemacht werden. Das wäre auch für betroffene Personen hilfreich, die der Verantwortliche anderweitig nicht kontaktieren kann.

Im Einklang mit dem Grundsatz der Rechenschaftspflicht sollten die Verantwortlichen gegenüber der Aufsichtsbehörde nachweisen können, dass mindestens eine dieser Bedingungen erfüllt ist.[38] Dabei gilt es zu beachten, dass auch, wenn zunächst auf die Meldung verzichtet werden kann, weil kein Risiko für die Rechte und Freiheiten natürlicher Personen besteht, sich die Umstände mit der Zeit ändern können, sodass das Risiko erneut bewertet werden muss.

Hat ein Verantwortlicher beschlossen, eine betroffene Person nicht von einer Datenschutzverletzung zu benachrichtigen, kann die Aufsichtsbehörde den Verantwortlichen gemäß Artikel 34 Absatz 4 hierzu verpflichten, wenn die Datenschutzverletzung ihrer Auffassung nach voraussichtlich zu einem hohen Risiko für die betroffenen Personen führt. Alternativ kann sie auch zu dem Schluss kommen, dass die in Artikel 34 Absatz 3 genannten Bedingungen erfüllt sind und die betroffenen Personen somit nicht benachrichtigt werden müssen. Stellt die Aufsichtsbehörde fest, dass die Entscheidung gegen die Benachrichtigung der betroffenen Personen unzureichend begründet ist, kann sie erwägen, von den ihr zur Verfügung stehenden Befugnissen und Sanktionen Gebrauch zu machen.

IV. Bewertung eines Risikos und eines hohen Risikos

A. Das Risiko als Auslöser für die Meldung

Obwohl mit der DSGVO die Pflicht zur Meldung von Datenschutzverletzungen eingeführt wird, muss eine Datenschutzverletzung nicht unter allen Umständen gemeldet werden:

- Die Meldung an die Aufsichtsbehörde ist erforderlich, es sei denn, dass die Datenschutzverletzung voraussichtlich nicht zu einem Risiko für die Rechte und Freiheiten natürlicher Personen führt.

[37] Siehe die Leitlinien der Artikel-29-Datenschutzgruppe über Transparenz, in denen das Problem des unverhältnismäßigen Aufwands thematisiert wird, abrufbar unter http://ec.europa.eu/newsroom/just/document.cfm?doc_id=48850http://ec.europa.eu/newsroom/just/document.cfm?doc_id=48850.

[38] Siehe Artikel 5 Absatz 2.

- Die Pflicht zur Benachrichtigung der betroffenen Personen wird nur ausgelöst, wenn die Datenschutzverletzung voraussichtlich zu einem hohen Risiko für ihre Rechte und Freiheiten führt.

Deshalb ist es entscheidend, dass sich der Verantwortliche unmittelbar nachdem ihm eine Datenschutzverletzung bekannt wird nicht nur um die Eindämmung des Vorfalls bemüht, sondern auch prüft, welches Risiko damit verbunden sein könnte. Hierfür gibt es zwei wichtige Gründe: Erstens kann der Verantwortliche leichter wirksame Maßnahmen zur Eindämmung und Behebung der Datenschutzverletzung ergreifen, wenn ihm die Eintrittswahrscheinlichkeit und mögliche Schwere der Folgen für die betroffenen Personen bekannt sind; zweitens kann er so besser beurteilen, ob die Meldung an die Aufsichtsbehörde erforderlich ist und ob die betroffenen Personen gegebenenfalls von der Datenschutzverletzung benachrichtigt werden müssen.

Wie bereits erläutert, muss eine Datenschutzverletzung gemeldet werden, es sei denn, dass sie voraussichtlich nicht zu einem Risiko für die Rechte und Freiheiten der betroffenen Personen führt; ferner wurde dargelegt, dass die Pflicht zur Benachrichtigung der betroffenen Personen in erster Linie dadurch ausgelöst wird, dass eine Datenschutzverletzung voraussichtlich zu einem *hohen* Risiko für die Rechte und Freiheiten natürlicher Personen führt. Ein solches Risiko besteht dann, wenn die Datenschutzverletzung zu einem physischen, materiellen oder immateriellen Schaden für die Personen führen könnte, deren personenbezogene Daten beeinträchtigt wurden. Beispiele für einen solchen Schaden sind Diskriminierung, Identitätsdiebstahl oder -betrug, finanzielle Verluste und Rufschädigung. Wenn von der Datenschutzverletzung personenbezogene Daten betroffen sind, aus denen die rassische oder ethnische Herkunft, die politische Meinung, religiöse oder weltanschauliche Überzeugungen oder die Zugehörigkeit zu einer Gewerkschaft hervorgehen, oder wenn sie genetische Daten, Gesundheitsdaten oder Daten über das Sexualleben, Angaben zu strafrechtlichen Verurteilungen und Straftaten oder damit zusammenhängende Sicherungsmaßregeln betreffen, ist es wahrscheinlich, dass ein solcher Schaden eintritt.[39]

B. Im Rahmen der Risikobewertung zu berücksichtigende Faktoren

Aus den Erwägungsgründen 75 und 76 der DSGVO geht hervor, dass bei der Bewertung des Risikos grundsätzlich sowohl der Eintrittswahrscheinlichkeit als auch der Schwere des Risikos für die Rechte und Freiheiten der betroffenen Personen Rechnung zu tragen ist. Darüber hinaus sollte das Risiko anhand einer objektiven Bewertung beurteilt werden.

Es wird darauf hingewiesen, dass die Bewertung des mit einer Datenschutzverletzung verbundenen Risikos für die Rechte und Freiheiten von Menschen einen anderen Schwerpunkt hat als die Risikobewertung, die im Rahmen einer Datenschutz-Folgeabschätzung (DSFA) durchgeführt wird.[40] Bei der DSFA werden sowohl die mit der planmäßig durchgeführten Datenverarbeitung verbundenen Risiken als auch die Risiken im Falle einer Datenschutzverletzung bewertet. Bei Betrachtung einer möglichen Datenschutzverletzung werden die generelle Eintrittswahrscheinlichkeit einer solchen Verletzung sowie der potenziell daraus folgende Schaden für die betroffene Person geprüft; mit anderen Worten, es wird ein hypothetisches Ereignis bewertet. Bei einer tatsächlich eingetretenen Datenschutzverletzung hat sich der Vorfall bereits ereignet, sodass der Fokus ausschließlich auf dem Risiko der Folgen liegt, die die Datenschutzverletzung für die betroffenen Personen hat.

---

[39] Siehe Erwägungsgrund 75 und Erwägungsgrund 85.

[40] Siehe die Leitlinien der Artikel-29-Datenschutzgruppe zur DSFA, abrufbar unter http://ec.europa.eu/newsroom/document.cfm?doc_id=44137.

Beispiel

Eine DSFA ergibt, dass der vorgeschlagene Einsatz eines bestimmten Sicherheitssoftware-Produkts zum Schutz personenbezogener Daten geeignet ist, um ein Schutzniveau zu gewährleisten, das dem Risiko angemessen ist, welches andernfalls für die betroffenen Personen durch die Verarbeitung der Daten gegeben wäre. Sollte jedoch später eine Schwachstelle in der Software bekannt werden, würde sich deren Eignung zur Eindämmung des Risikos für die geschützten personenbezogenen Daten ändern, sodass das Produkt im Rahmen einer kontinuierlichen DSFA erneut bewertet werden müsste.

Später wird eine Schwachstelle des Produkts ausgenutzt, und es kommt zu einer Datenschutzverletzung. Der Verantwortliche sollte die spezifischen Umstände der Datenschutzverletzung, die beeinträchtigten Daten und das potenzielle Ausmaß der Folgen für die betroffenen Personen sowie die Eintrittswahrscheinlichkeit dieses Risikos bewerten.

Dementsprechend sollte der Verantwortliche bei der Bewertung des mit der Datenschutzverletzung verbundenen Risikos für die betroffenen Personen den spezifischen Umständen der Datenschutzverletzung Rechnung tragen, einschließlich der Schwere der potenziellen Folgen und der Wahrscheinlichkeit, dass diese Folgen eintreten. Daher empfiehlt die Artikel-29-Datenschutzgruppe, folgende Kriterien in die Bewertung einzubeziehen:[41]

- Art der Datenschutzverletzung

Die Art einer aufgetretenen Datenschutzverletzung kann sich auf die Höhe des damit verbundenen Risikos für die betroffenen Personen auswirken. So kann eine Verletzung der Vertraulichkeit medizinischer Daten durch Offenlegung gegenüber Unbefugten andere Konsequenzen für den Einzelnen haben als eine Datenschutzverletzung, bei der medizinische Unterlagen einer betroffenen Person verloren gegangen und nicht mehr verfügbar sind.

- Art, Sensibilität und Umfang personenbezogener Daten

Art und Sensibilität der durch eine Datenschutzverletzung beeinträchtigten personenbezogenen Daten sind für die Bewertung der Risiken natürlich von entscheidender Bedeutung. In der Regel steigt das Risiko, dass die betroffenen Personen zu Schaden kommen, je sensibler die Daten sind, wobei auch andere personenbezogene Daten berücksichtigt werden müssen, die eventuell bereits zu der betroffenen Person vorliegen. So wird etwa die Offenlegung des Namens und der Anschrift einer Person unter normalen Umständen wahrscheinlich keinen ernsthaften Schaden verursachen. Hingegen kann die Offenlegung der Namen und der Anschrift von Adoptiveltern gegenüber den leiblichen Eltern eines Kindes äußerst schwerwiegende Folgen sowohl für die Adoptiveltern als auch für das Kind haben.

Datenschutzverletzungen, die Gesundheitsdaten, Ausweisdokumente oder finanzielle Daten wie Kreditkarteninformationen betreffen, können alle unabhängig voneinander Schäden verursachen, doch in Kombination können solche Daten zum Identitätsdiebstahl genutzt werden. Eine Kombination aus personenbezogenen Daten ist üblicherweise sensibler als ein einzelnes Element personenbezogener Daten.

[41] Artikel 3 Absatz 2 der Verordnung (EU) Nr. 611/2013 enthält Hinweise zu den Faktoren, die im Zusammenhang mit der Meldung von Datenschutzverletzungen im Bereich der elektronischen Kommunikationsdienste berücksichtigt werden sollten, und die im Rahmen der Meldung nach Maßgabe der DSGVO herangezogen werden können. Siehe http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2013:173:0002:0008:de:PDF.

Manche Arten von personenbezogenen Daten können auf den ersten Blick relativ harmlos erscheinen, doch sollte sorgfältig geprüft werden, was sich daraus über die betroffene Person ableiten lässt. Eine Liste von Kunden, die regelmäßig Lieferungen annehmen, mag nicht besonders sensibel sein, doch dieselben Daten über Kunden, die aus Urlaubsgründen um Unterbrechung ihrer Lieferungen gebeten haben, wären nützliche Informationen für Straftäter.

Ferner kann eine kleine Menge hochsensibler personenbezogener Daten große Auswirkungen für eine betroffene Person haben; je mehr Einzelangaben vorliegen, desto umfassender sind die Informationen, die über die betreffende Person bekannt werden. Des Weiteren kann eine Datenschutzverletzung, bei der große Datenmengen über viele betroffene Personen beeinträchtigt werden, Folgen für eine entsprechend große Zahl an Einzelpersonen haben.

- Identifizierbarkeit betroffener Personen

Ein wichtiger Faktor ist die Frage, wie leicht eine Partei, die Zugang zu beeinträchtigten personenbezogenen Daten erhält, bestimmte Einzelpersonen identifizieren oder die Daten mit anderen Informationen zwecks Identifizierung Einzelner abgleichen kann. Je nach den Umständen könnte die Identifizierung ohne besondere Nachforschungen direkt anhand der beeinträchtigten personenbezogenen Daten möglich sein – oder es könnte zwar äußerst schwierig, aber unter bestimmten Voraussetzungen dennoch möglich sein, personenbezogene Daten bestimmten Einzelpersonen zuzuordnen. Die Identifizierung kann sich direkt oder indirekt aus den beeinträchtigten Daten ergeben, kann aber auch von den spezifischen Rahmenbedingungen der Datenschutzverletzung und der öffentlichen Verfügbarkeit zugehöriger personenbezogener Einzelinformationen abhängen. Diese Faktoren fallen bei Verletzungen der Vertraulichkeit und Verfügbarkeit möglicherweise stärker ins Gewicht.

Wie bereits dargelegt, sind durch eine angemessene Verschlüsselung geschützte personenbezogene Daten für Unbefugte ohne den Verschlüsselungsschlüssel unzugänglich. Darüber hinaus kann auch durch eine angemessen umgesetzte Pseudonymisierung (in Artikel 4 Absatz 5 definiert 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“) die Wahrscheinlichkeit der Identifizierung natürlicher Personen im Falle einer Datenschutzverletzung verringert werden. Allerdings darf nicht davon ausgegangen werden, dass die Daten durch Pseudonymisierungstechniken allein unzugänglich gemacht werden.

- Schwere der Folgen für die betroffenen Personen

Je nach Art der von einer Datenschutzverletzung betroffenen Daten – zum Beispiel bei besonderen Datenkategorien – kann die Datenschutzverletzung zu einem besonders schwerwiegenden potenziellen Schaden für die betroffenen Personen führen, nämlich insbesondere dann, wenn die Datenschutzverletzung Identitätsdiebstahl oder -betrug, Verletzungen, psychische Belastungen, Demütigung oder Rufschädigung zur Folge haben könnte. Sind von der Datenschutzverletzung personenbezogene Daten über schutzbedürftige Menschen betroffen, könnte das Gefährdungsrisiko für die Betroffenen steigen.

Es kann für die Höhe des möglichen Risikos relevant sein, ob der Verantwortliche weiß, dass personenbezogene Daten in die Hände von Personen mit unbekannter oder möglicherweise böser Absicht gelangt sind. Möglicherweise liegt eine Vertraulichkeitsverletzung vor, bei der personenbezogene Daten versehentlich an Dritte im Sinne von Artikel 4 Absatz 10 oder gegenüber einem anderen Empfänger weitergegeben wurden. Das wäre etwa der Fall, wenn personenbezogene Daten aus Versehen an eine falsche interne Abteilung oder an einen häufig beauftragten Lieferanten geschickt wurden. Der Verantwortliche kann den Empfänger bitten, die erhaltenen Daten

zurückzusenden oder sicher zu vernichten. Da zwischen Verantwortlichem und Empfänger eine kontinuierliche Beziehung besteht, der Verantwortliche vielleicht auch mit den Verfahrensweisen und der Historie des Empfängers vertraut ist und andere einschlägige Details über ihn kennt, kann der Empfänger in beiden Fällen als „vertrauenswürdig“ betrachtet werden. Mit anderen Worten, aufgrund des bestehenden Vertrauensverhältnisses zwischen Verantwortlichem und Empfänger könnte der Verantwortliche nach vernünftigem Ermessen davon ausgehen, dass der Empfänger die versehentlich erhaltenen Daten nicht liest oder auf sie zugreift und seine Anweisungen zur Rücksendung der Daten befolgt. Selbst wenn Einsicht in die Daten genommen wurde, könnte der Verantwortliche noch darauf vertrauen, dass der Empfänger die Daten nicht weiter nutzt, dass er sie dem Verantwortlichen unverzüglich zurückschickt und dass er bei der Wiederherstellung der Daten mitarbeitet. In solchen Fällen kann dieser Faktor in der Risikobewertung berücksichtigt werden, die der Verantwortliche nach der Datenschutzverletzung durchführt – der Umstand, dass der Empfänger vertrauenswürdig ist, kann die Schwere der Folgen der Datenschutzverletzung beseitigen, bedeutet aber nicht, dass keine Datenschutzverletzung stattgefunden hat. Das wiederum könnte bedeuten, dass die Wahrscheinlichkeit des Risikos für die betroffenen Personen nicht mehr gegeben ist, sodass sich die Meldung an die Aufsichtsbehörde oder die Benachrichtigung der betroffenen Personen erübrigen. Ob dem so ist, hängt wieder vom konkreten Einzelfall ab. Dessen ungeachtet muss der Verantwortliche die Datenschutzverletzung im Rahmen seiner allgemeinen Pflicht zur Dokumentation von Datenschutzverletzungen (siehe unten, Abschnitt V) verzeichnen.

Auch die Dauerhaftigkeit der Folgen für die betroffenen Personen sollte berücksichtigt werden, wenn die Möglichkeit besteht, dass die Folgen bei langfristigen Auswirkungen schwerwiegender werden.

- Besondere Eigenschaften der betroffenen Person

Eine Datenschutzverletzung kann personenbezogene Daten über Kinder oder andere schutzbedürftige Personen betreffen, die aufgrund des Vorfalls stärker gefährdet werden können. Es kann auch andere personenbezogene Faktoren geben, die beeinflussen, wie stark sich die Datenschutzverletzung auf die betroffene Person auswirkt.

- Besondere Eigenschaften des Verantwortlichen

Die Art und Rolle des Verantwortlichen und seiner Tätigkeiten kann sich auf die Höhe des mit einer Datenschutzverletzung verbundenen Risikos für die betroffenen Personen auswirken. Eine medizinische Einrichtung zum Beispiel verarbeitet besondere Kategorien personenbezogener Daten, sodass eine Datenschutzverletzung in ihrem Fall eine größere Gefahr für die betroffenen Personen darstellen würde als etwa einer der Mailingliste einer Zeitung.

- Die Zahl der betroffenen Personen

Datenschutzverletzungen können Auswirkungen für nur eine oder wenige Personen, aber auch für mehrere Tausend oder eine noch weit größere Zahl von Personen haben. Im Allgemeinen sind die möglichen Folgen einer Datenschutzverletzung umso weitreichender, je mehr Personen davon betroffen sind. Eine Datenschutzverletzung kann, je nach Art der personenbezogenen Daten und des Zusammenhangs, in dem diese Daten beeinträchtigt wurden, sogar für eine einzelne Person schwerwiegende Folgen haben. Entscheidend ist auch hier, dass die Wahrscheinlichkeit und Schwere der Folgen für die Betroffenen geprüft werden.

- Allgemeine Aspekte

Daher sollte der Verantwortliche bei der Bewertung des voraussichtlich von einer Datenschutzverletzung ausgehenden Risikos die Schwere der möglichen Folgen für die Rechte und Freiheiten der betroffenen Personen in Verbindung mit der Eintrittswahrscheinlichkeit dieser Folgen prüfen. Das Risiko steigt natürlich zum einen mit zunehmender Schwere und zum anderen mit steigender Eintrittswahrscheinlichkeit der Folgen einer Datenschutzverletzung. Im Zweifelsfall sollte

der Verantwortliche die Datenschutzverletzung sicherheitshalber melden. Anhang B enthält einige hilfreiche Beispiele unterschiedlicher Arten von Datenschutzverletzungen, die ein Risiko oder hohes Risiko für die betroffenen Personen bergen.

Die Agentur der Europäischen Union für Netz- und Informationssicherheit (ENISA) hat Empfehlungen für eine Methodik zur Bewertung der Schwere einer Datenschutzverletzung herausgegeben, die die Verantwortlichen und Auftragsverarbeiter bei der Ausarbeitung ihrer Reaktionspläne zur Bewältigung von Datenschutzverletzungen heranziehen können.[42]

V. Rechenschaftspflicht und Aufzeichnung

A. Dokumentation von Datenschutzverletzungen

Die Verantwortlichen sind verpflichtet, alle Datenschutzverletzungen zu dokumentieren, und zwar unabhängig davon, ob der Aufsichtsbehörde eine Verletzung gemeldet werden muss oder nicht. Artikel 33 Absatz 5 lautet dazu wie folgt:

> „Der Verantwortliche dokumentiert Verletzungen des Schutzes personenbezogener Daten einschließlich aller im Zusammenhang mit der Verletzung des Schutzes personenbezogener Daten stehenden Fakten, von deren Auswirkungen und der ergriffenen Abhilfemaßnahmen. Diese Dokumentation muss der Aufsichtsbehörde die Überprüfung der Einhaltung der Bestimmungen dieses Artikels ermöglichen."

Dies steht in Zusammenhang mit dem in Artikel 5 Absatz 2 der DSGVO verankerten Grundsatz der Rechenschaftspflicht. Mit der Protokollierung sowohl nicht meldepflichtiger als auch meldepflichtiger Datenschutzverletzungen kommen die Verantwortlichen auch ihren Verpflichtungen gemäß Artikel 24 nach, und die Aufsichtsbehörde kann Einsicht in die entsprechenden Aufzeichnungen verlangen. Daher sollten die Verantwortlichen nach Möglichkeit ein internes Verzeichnis für Datenschutzverletzungen anlegen, unabhängig davon, ob diese meldepflichtig sind oder nicht.[43]

Während die Verantwortlichen selbst über Verfahren und Struktur der Dokumentation von Datenschutzverletzungen entscheiden, sollten inhaltlich in jedem Fall bestimmte wichtige Elemente erfasst werden. Nach Artikel 33 Absatz 5 muss der Verantwortliche Details zur Datenschutzverletzung dokumentieren und sollte dabei unter anderem die Ursachen und Vorkommnisse beschreiben und angeben, welche personenbezogenen Daten beeinträchtigt wurden. Außerdem sollten die Auswirkungen und Konsequenzen der Datenschutzverletzung sowie die vom Verantwortlichen getroffenen Abhilfemaßnahmen dokumentiert werden.

Die DSGVO sieht keine Aufbewahrungsfrist für diese Dokumentation vor. Wenn die Aufzeichnungen personenbezogene Daten enthalten, obliegt es dem Verantwortlichen, die angemessene Aufbewahrungsfrist entsprechend den Grundsätzen für die Verarbeitung personenbezogener Daten[44]

---

[42] ENISA, Recommendations for a methodology of the assessment of severity of personal data breaches (Empfehlungen für eine Methodik zur Bewertung der Schwere von Verletzungen des Schutzes personenbezogener Daten), https://www.enisa.europa.eu/publications/dbn-severity.

[43] Die Verantwortlichen dürfen Datenschutzverletzungen auch im Rahmen des Verzeichnisses von Verarbeitungstätigkeiten gemäß Artikel 30 dokumentieren. Ein separates Verzeichnis ist nicht erforderlich, sofern die für Datenschutzverletzungen relevanten Informationen klar als solche erkennbar sind und auf Anforderung extrahiert werden können.

[44] Siehe Artikel 5.

zu bestimmen und die gesetzlichen Vorgaben für die Verarbeitung[45] einzuhalten. Der Verantwortliche muss die Dokumentation insofern im Einklang mit Artikel 33 Absatz 5 verwahren, als er aufgefordert werden kann, die Einhaltung dieses Artikels oder des Grundsatzes der Rechenschaftspflicht im Allgemeinen gegenüber der Aufsichtsbehörde nachzuweisen. Enthalten die Aufzeichnungen selbst keine personenbezogenen Daten, ist der in der DSGVO vorgesehene Grundsatz der Speicherbegrenzung[46] natürlich nicht anwendbar.

Die Artikel-29-Datenschutzgruppe empfiehlt Verantwortlichen zusätzlich zu dokumentieren, wie sie ihre in Reaktion auf eine Datenschutzverletzung getroffenen Entscheidungen begründen. Die Entscheidungsbegründung sollte insbesondere dann dokumentiert werden, wenn eine Datenschutzverletzung nicht gemeldet wird. Dabei sollte begründet werden, weshalb der Verantwortliche zu dem Schluss gekommen ist, dass die Datenschutzverletzung voraussichtlich nicht zu einem Risiko für die Rechte und Freiheiten natürlicher Personen führt.[47] Ist der Verantwortliche hingegen der Auffassung, dass eine oder mehrere der Bedingungen von Artikel 34 Absatz 3 erfüllt sind, sollte er dies angemessen belegen können.

Wenn der Verantwortliche eine Datenschutzverletzung an die Aufsichtsbehörde meldet, die Meldung jedoch verzögert erfolgt, muss er diese Verzögerung begründen können; eine diesbezügliche Dokumentation könnte als Beleg dafür dienen, dass die verzögerte Meldung gerechtfertigt und nicht übermäßig war.

Benachrichtigt der Verantwortliche die betroffenen Personen von einer Datenschutzverletzung, dann sollte er auf transparente Weise über die Datenschutzverletzung informieren und die Informationen wirksam und zeitnah kommunizieren. Der Verantwortliche könnte Nachweise zu diesen Kommunikationsmaßnahmen verwahren, um damit zu zeigen, dass er seiner Rechenschaftspflicht nachgekommen ist und die gesetzlichen Vorgaben eingehalten hat.

Im Hinblick auf die Einhaltung von Artikel 33 und 34 wäre es für die Verantwortlichen und Auftragsverarbeiter von Vorteil, ein dokumentiertes Meldeverfahren einzurichten, in dem festgelegt wird, welche Schritte nach Feststellung einer Datenschutzverletzung zu befolgen sind, wie Vorfälle eingedämmt, gesteuert und behoben werden und wie bei der Risikobewertung und der Meldung der Datenschutzverletzung vorzugehen ist. In diesem Zusammenhang wäre es als Nachweis der Einhaltung der DSGVO eventuell hilfreich zu zeigen, dass die Beschäftigten über die Existenz solcher Verfahren und Mechanismen informiert wurden und wissen, wie sie auf Datenschutzverletzungen reagieren müssen.

Zu beachten ist, dass Versäumnisse bei der ordnungsgemäßen Dokumentation einer Datenschutzverletzung zur Folge haben können, dass die Aufsichtsbehörde ihre Befugnisse gemäß Artikel 58 ausübt bzw. eine Geldbuße gemäß Artikel 83 verhängt.

B. Die Rolle des Datenschutzbeauftragten

Die Verantwortlichen oder Auftragsverarbeiter können entweder gemäß Artikel 37 oder freiwillig als bewährtes Verfahren einen Datenschutzbeauftragten (DSB)[48] benennen. In Artikel 39 der DSGVO ist eine Reihe von obligatorischen Aufgaben des Datenschutzbeauftragten festgelegt, wobei es dem

[45] Siehe Artikel 6 sowie Artikel 9.

[46] Siehe Artikel 5 Absatz 1 Buchstabe e.

[47] Siehe Erwägungsgrund 85.

[48] Siehe die Leitlinien der Artikel-29-Datenschutzgruppe in Bezug auf Datenschutzbeauftragte, abrufbar unter http://ec.europa.eu/newsroom/just/item-detail.cfm?item_id=50083.

Verantwortlichen freisteht, dem Datenschutzbeauftragten gegebenenfalls weitere Aufgaben zu übertragen.

Der DSB hat verschiedene für die Meldung von Datenschutzverletzungen besonders relevante obligatorische Aufgaben. Er muss unter anderem den Verantwortlichen bzw. den Auftragsverarbeiter in Datenschutzfragen beraten und informieren, die Einhaltung der DSGVO überwachen und im Zusammenhang mit DSFA Beratungsarbeit leisten. Ferner muss der DSB mit der Aufsichtsbehörde zusammenarbeiten und als Ansprechpartner für die Aufsichtsbehörde sowie für die betroffenen Personen fungieren. Zu beachten ist auch, dass der Verantwortliche bei der Meldung einer Datenschutzverletzung an die Aufsichtsbehörde gemäß Artikel 33 Absatz 3 Buchstabe b verpflichtet ist, den Namen und die Kontaktdaten seines DSB oder eines anderen Ansprechpartners mitzuteilen.

Im Zusammenhang mit der Dokumentation von Datenschutzverletzungen könnten die Verantwortlichen und Auftragsverarbeiter den DSB bei Fragen zur Struktur, zur Einrichtung und zur Verwaltung dieser Dokumentation hinzuzuziehen. Der DSB könnte zusätzlich auch mit der Führung dieser Unterlagen betraut werden.

Diese Punkte bedeuten, dass der DSB durch seine Beratungs- und Überwachungsfunktion bei der Vermeidung von und der Vorbereitung auf Datenschutzverletzungen, während einer Datenschutzverletzung (d. h. bei der Meldung an die Aufsichtsbehörde) sowie bei allen anschließenden Ermittlungen der Aufsichtsbehörde eine zentrale Rolle spielen sollte. Vor diesem Hintergrund empfiehlt die Artikel-29-Datenschutzgruppe, dass der DSB unverzüglich über Datenschutzverletzungen in Kenntnis gesetzt wird und in den gesamten Prozess der Bearbeitung und Meldung von Datenschutzverletzungen einbezogen wird.

VI. In anderen Rechtsinstrumenten festgelegte Meldepflichten

Zusätzlich zu und unabhängig von der Meldung von Datenschutzverletzungen und der Benachrichtigung der betroffenen Personen nach Maßgabe der DSGVO sollten die Verantwortlichen wissen, welchen anderen Pflichten zur Meldung von Sicherheitsvorfällen sie gegebenenfalls nach anderen zugehörigen Rechtsvorschriften unterliegen und ob sie danach auch verpflichtet sind, gleichzeitig eine Verletzung des Schutzes personenbezogener Daten an die Aufsichtsbehörde zu melden. Solche Anforderungen können je nach Mitgliedstaat variieren, doch exemplarisch seien hier die folgenden in anderen Rechtsinstrumenten vorgesehenen Meldepflichten und ihr jeweiliger Zusammenhang mit der DSGVO aufgeführt:

- Verordnung (EU) Nr. 910/2014 über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt (eIDAS-Verordnung).[49]

Gemäß Artikel 19 Absatz 2 der eIDAS-Verordnung müssen Vertrauensdiensteanbieter die zuständige Aufsichtsstelle über jede Sicherheitsverletzung oder jeden Integritätsverlust informieren, die bzw. der sich erheblich auf den erbrachten Vertrauensdienst oder die darin vorhandenen personenbezogenen Daten auswirkt. Gegebenenfalls – d. h. wenn es sich bei einer solchen Verletzung bzw. einem solchen Verlust auch um eine Verletzung des Schutzes personenbezogener Daten im Sinne der DSGVO handelt – muss der Vertrauensdiensteanbieter auch die Aufsichtsbehörde unterrichten.

- Richtlinie (EU) 2016/1148 über Maßnahmen zur Gewährleistung eines hohen gemeinsamen Sicherheitsniveaus von Netz- und Informationssystemen in der Union (NIS-Richtlinie).[50]

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

[50] Siehe http://eur-lex.europa.eu/legal-content/DE/TXT/?uri=uriserv:OJ.L_.2016.194.01.0001.01.DEU

Gemäß Artikel 14 und 16 der NIS-Richtlinie müssen die Betreiber wesentlicher Dienste und die Anbieter digitaler Dienste Sicherheitsvorfälle an die zuständige Behörde melden. Wie in Erwägungsgrund 63 der NIS-Richtlinie[51] bestätigt, gehen Sicherheitsvorfälle oft auch mit einer Beeinträchtigung des Schutzes personenbezogener Daten einher. Während die NIS-Richtlinie verlangt, dass die zuständigen Behörden und die Aufsichtsbehörden diesbezüglich zusammenarbeiten und Informationen austauschen, sind die betreffenden Betreiber bzw. Anbieter in dem Fall, dass ein Vorfall auch eine Verletzung des Schutzes personenbezogener Daten im Sinne der DSGVO darstellt oder sich zu einer solchen Verletzung entwickelt, verpflichtet, unabhängig von der Pflicht zur Meldung des Vorfalls im Rahmen der NIS-Richtlinie Meldung an die Aufsichtsbehörde zu erstatten.

Beispiel

Ein Anbieter von Cloud-Diensten, der eine Sicherheitsverletzung gemäß der NIS-Richtlinie meldet, muss den Vorfall möglicherweise auch an einen Verantwortlichen melden, wenn dabei auch der Schutz personenbezogener Daten verletzt wurde. Ebenso könnte ein Vertrauensdiensteanbieter, der nach der eIDAS-Verordnung Meldung erstattet, im Falle einer Datenschutzverletzung auch zur Meldung an die zuständige Datenschutzbehörde verpflichtet sein.

- Richtlinie 2009/136/EG (Richtlinie „Rechte der Bürger“) und Verordnung (EU) Nr. 611/2013 (Verordnung über die Maßnahmen für die Benachrichtigung von Verletzungen des Schutzes personenbezogener Daten).

Die Anbieter öffentlich zugänglicher elektronischer Kommunikationsdienste sind im Rahmen der Richtlinie 2002/58/EG[52] verpflichtet, Verletzungen an die zuständigen nationalen Behörden zu melden.

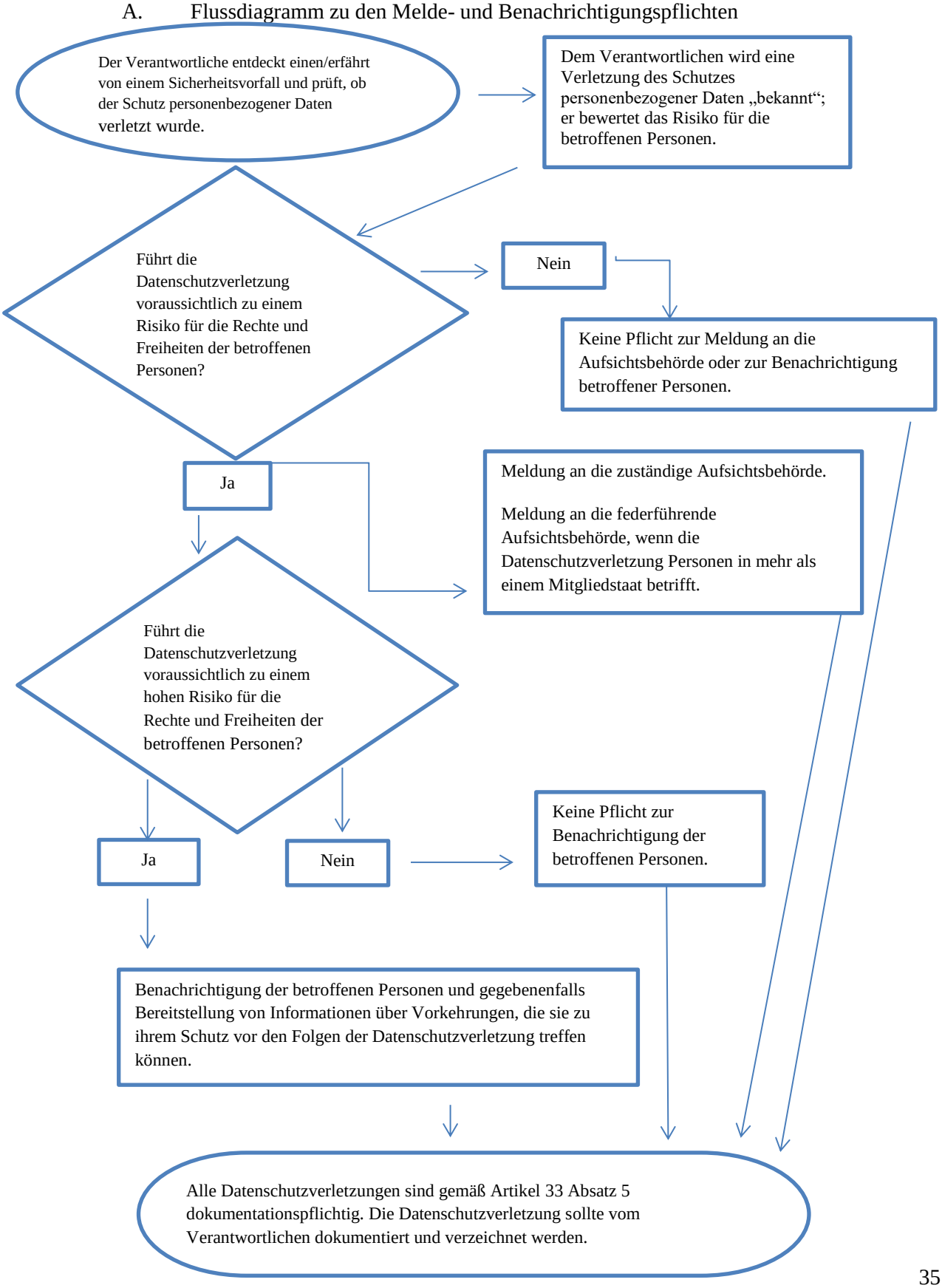
Die Verantwortlichen sollten auch wissen, ob sie aufgrund anderer anwendbarer Regelungen sonstigen rechtlichen, medizinischen oder beruflichen Meldepflichten unterliegen.

51 Erwägungsgrund 63: *„Häufig ist bei Sicherheitsvorfällen der Schutz personenbezogener Daten nicht mehr gewährleistet. Deshalb sollten die zuständigen Behörden und die Datenschutzbehörden zusammenarbeiten und Informationen zu allen einschlägigen Fragen austauschen, um Verletzungen des Schutzes personenbezogener Daten aufgrund von Sicherheitsvorfällen zu begegnen.“*

52 Am 10. Januar 2017 hat die Kommission eine Verordnung über Privatsphäre und elektronische Kommunikation vorgeschlagen, die die Richtlinie 2009/136/EG ersetzen soll und mit der Meldepflichten abgeschafft werden sollen. Allerdings bleibt die geltende Meldepflicht bis zur Annahme des Vorschlags durch das Europäische Parlament in Kraft, siehe https://ec.europa.eu/digital-single-market/en/news/proposal-regulation-privacy-and-electronic-communications.

VII. **Anhang**

A. Flussdiagramm zu den Melde- und Benachrichtigungspflichten



B. Beispiele für Verletzungen des Schutzes personenbezogener Daten und zu unterrichtende Stellen

Die folgenden nicht erschöpfenden Beispiele sollen den Verantwortlichen dabei helfen zu entscheiden, ob Datenschutzverletzungen in unterschiedlichen Szenarien melde- bzw. benachrichtigungspflichtig sind. Die Beispiele können auch als Orientierungshilfe für die Unterscheidung zwischen einem Risiko und einem hohen Risiko für die Rechte und Freiheiten der betroffenen Personen dienen.

Beispiel	**Meldung an die zuständige Aufsichtsbehörde?**	**Benachrichtigung der betroffenen Person?**	**Anmerkungen/ Empfehlungen**
i. Ein Verantwortlicher hat die Sicherungskopie eines Archivs mit personenbezogenen Daten in verschlüsselter Form auf einem USB-Stick gespeichert. Bei einem Einbruch wird der USB-Stick entwendet.	Nein.	Nein.	Solange die Daten durch einen dem Stand der Technik entsprechenden Algorithmus verschlüsselt sind, Datensicherungen existieren, der eindeutige Schlüssel nicht beeinträchtigt wurde und sich die Daten zeitnah wiederherstellen lassen, handelt es sich vermutlich nicht um eine meldepflichtige Datenschutzverletzung. Kommt es später aber doch zu einer Beeinträchtigung, ist die Meldung erforderlich.
ii. Ein Verantwortlicher betreibt einen Onlinedienst. Der Dienst wird Opfer eines Cyberangriffs und dabei werden personenbezogene Daten abgeschöpft. Der Verantwortliche hat nur in einem Mitgliedstaat Kunden.	Ja, der Vorfall muss an die Aufsichtsbehörde gemeldet werden, wenn Folgen für die betroffenen Personen zu erwarten sind.	Ja, die betroffenen Personen müssen, abhängig von der Art der beeinträchtigten personenbezogenen Daten und wenn schwerwiegende Folgen für die betroffenen Personen zu erwarten sind, benachrichtigt werden.	
iii. Im Callcenter eines Verantwortlichen kommt es zu einem kurzen, mehrere Minuten andauernden	Nein.	Nein.	Dies ist keine meldepflichtige Datenschutzverletzung, allerdings ist der Vorfall trotzdem gemäß

Stromausfall, sodass die Kunden den Verantwortlichen nicht erreichen und nicht auf ihre Unterlagen zugreifen können.			Artikel 33 Absatz 5 dokumentationspflichtig. Der Verantwortliche sollte entsprechende Aufzeichnungen führen.
iv. Ein Verantwortlicher wird Opfer eines Ransomware-Angriffs, bei dem sämtliche Daten verschlüsselt werden. Es sind keine Sicherungskopien vorhanden und die Daten können nicht wiederhergestellt werden. Bei einer Untersuchung stellt sich heraus, dass die Ransomware ausschließlich der Datenverschlüsselung diente und dass keine weiter Schadsoftware im System präsent war.	Ja, der Vorfall muss an die Aufsichtsbehörde gemeldet werden, wenn Folgen für die betroffenen Personen zu erwarten sind, da es sich um einen Verlust der Datenverfügbarkeit handelt.	Ja, die betroffenen Personen müssen, abhängig von der Art der beeinträchtigten personenbezogenen Daten, den möglichen Auswirkungen der Nichtverfügbarkeit der Daten sowie anderen wahrscheinlichen Folgen, benachrichtigt werden.	Wenn eine Datensicherung vorhanden gewesen wäre und sich die Daten zeitnah hätten wiederherstellen lassen, wären die Meldung an die Aufsichtsbehörde und die Benachrichtigung der betroffenen Personen nicht erforderlich gewesen, da kein dauerhafter Verlust der Datenverfügbarkeit oder -vertraulichkeit vorgelegen hätte. Sollte die Aufsichtsbehörde jedoch auf andere Weise Kenntnis von dem Vorfall erlangen, könnte sie eine Untersuchung in Betracht ziehen, um die Einhaltung der allgemeineren Sicherheitsanforderungen des Artikels 32 zu überprüfen.
v. Eine Person ruft im Callcenter einer Bank an, um eine Datenschutzverletzung zu melden. Die Person hat einen für jemand anderes bestimmten monatlichen Kontoauszug erhalten. Der Verantwortliche führt eine kurze (d. h. nach 24 Stunden abgeschlossene) Untersuchung durch und stellt mit hinreichender Gewissheit fest, dass eine Verletzung des Schutzes	Ja.	Nur die betroffenen Personen werden benachrichtigt, wenn ein hohes Risiko besteht und klar ist, dass keine anderen Personen betroffen sind.	Wird nach weitergehenden Untersuchungen festgestellt, dass mehr Personen betroffen sind, muss die Aufsichtsbehörde über die neue Sachlage informiert werden; zusätzlich benachrichtigt der Verantwortliche die anderen betroffenen Personen, wenn für sie ein hohes Risiko besteht.

personenbezogener Daten aufgetreten ist und ob ein systembedingter Fehler vorliegt, der bedeuten könnte, dass auch andere Personen betroffen sind oder sein können.			
vi. Ein Verantwortlicher betreibt einen Online-Marktplatz mit Kunden in mehreren Mitgliedstaaten. Nach einem Cyberangriff auf den Marktplatz veröffentlicht der Angreifer Benutzernamen, Passwörter und Kaufhistorie im Internet.	Ja, Vorfälle mit grenzüberschreitender Verarbeitung müssen an die federführende Aufsichtsbehörde gemeldet werden.	Ja, denn der Vorfall könnte zu einem hohen Risiko führen.	Der Verantwortliche sollte Maßnahmen ergreifen – indem er z. B. das Zurücksetzen der Passwörter für die betroffenen Konten erzwingt – und andere Schritte zur Eindämmung des Risikos unternehmen. Der Verantwortliche sollte auch andere Meldepflichten berücksichtigen, z. B. eine Meldepflicht als Anbieter digitaler Dienste im Sinne der NIS-Richtlinie.
vii. Ein als Auftragsdatenverarbeiter fungierendes Webhosting-Unternehmen stellt fest, dass der Code zur Steuerung der Benutzerautorisierung einen Fehler enthält. Aufgrund des Fehlers kann jeder Benutzer die Kontodaten aller anderen Benutzer einsehen.	Als Auftragsverarbeiter muss das Webhosting-Unternehmen seine betroffenen Kunden (die Verantwortlichen) unverzüglich benachrichtigen. In der Annahme, dass das Webhosting-Unternehmen eine eigene Untersuchung durchgeführt hat, sollten die betroffenen Verantwortlichen hinreichende Gewissheit darüber haben, ob in ihrem konkreten Fall eine Datenschutzverletzung aufgetreten ist, sodass wahrscheinlich davon ausgegangen werden	Wenn voraussichtlich kein hohes Risiko für die betroffenen Personen besteht, müssen diese nicht benachrichtigt werden.	Das Webhosting-Unternehmen (der Auftragsverarbeiter) muss auch etwaige andere Meldepflichten berücksichtigen (z. B. eine Meldepflicht als Anbieter digitaler Dienste im Sinne der NIS-Richtlinie). Sofern keine Anhaltspunkte dafür vorliegen, dass die Schwachstelle bei einem der Verantwortlichen ausgenutzt wurde, ist möglicherweise keine meldepflichtige Datenschutzverletzung aufgetreten. Wahrscheinlich ist der Vorfall aber dokumentationspflichtig

	kann, dass ihnen die Datenschutzverletzung mit der Benachrichtigung durch das Webhosting-Unternehmen (den Auftragsverarbeiter) „bekannt“ geworden ist. Dann muss der Verantwortliche die Datenschutzverletzung an die Aufsichtsbehörde melden.		oder als Missachtung von Artikel 32 einzustufen.
viii. Aufgrund eines Cyberangriffs sind in einem Krankenhaus medizinische Unterlagen 30 Stunden lang unzugänglich.	Ja, das Krankenhaus ist zur Meldung verpflichtet, da ein hohes Risiko für das Wohlergehen und die Privatsphäre der Patienten bestehen kann.	Ja, die betroffenen Personen müssen benachrichtigt werden.	
ix. Die personenbezogenen Daten einer großen Zahl von Studenten wurden versehentlich an eine falsche Mailingliste mit gut 1000 Empfängern geschickt.	Ja, die Meldung an die Aufsichtsbehörde ist erforderlich.	Ja, die betroffenen Personen müssen, je nach Umfang und Art der betroffenen personenbezogenen Daten und der Schwere der möglichen Folgen, benachrichtigt werden.	
x. Eine E-Mail für Direktwerbezwecke wird an Empfänger in den Feldern „An...“ oder „Cc...“ geschickt, sodass die E-Mail-Adressen der Empfänger für alle Empfänger sichtbar sind.	Ja, die Meldung an die Aufsichtsbehörde kann obligatorisch sein, wenn sehr viele Personen betroffen sind, sensible Daten offengelegt werden (z. B. die Mailingliste eines Psychotherapeuten) oder wenn andere Faktoren ein hohes Risiko bergen (z. B. wenn die E-Mail die ursprünglichen	Ja, die betroffenen Personen müssen, je nach Umfang und Art der betroffenen personenbezogenen Daten und der Schwere der möglichen Folgen, benachrichtigt werden.	Die Benachrichtigung ist unter Umständen nicht erforderlich, wenn keine sensiblen Daten offengelegt werden und nur eine kleine Anzahl von E-Mail-Adressen sichtbar ist.

	Passwörter enthält).		