BRANDI
RECHTSANWÄLTE

VORGEHEN BEI DATENSCHUTZVORFÄLLEN

Informationen zum Datenschutz I Februar 2023

English version

Einleitung

Datenschutzverstöße sowie Datenverlust und Datendiebstähle sind bedeutsame Risikofaktoren für alle Unternehmen, die personenbezogene Daten verarbeiten, da es keinen absoluten Schutz gespeicherter Daten geben kann. Solange personenbezogene Daten unternehmensseitig erfasst, gespeichert oder auf andere Weise verarbeitet werden, besteht grundsätzlich die Möglichkeit und somit auch das Risiko, dass die Daten durch ein Versehen oder eine kriminelle Handlung unberechtigten Dritten gegenüber offengelegt werden oder abhandenkommen. Für den Fall, dass es zu einem solchen Abfluss von Daten oder einer solchen unberechtigten Kenntnisnahme kommt, sieht die Datenschutzgrundverordnung (DSGVO) verschiedene Handlungspflichten – insbesondere Informations- und Meldepflichten – zulasten des für die Datenverarbeitung Verantwortlichen vor. Die entsprechenden Vorgaben sind unter anderem auf den datenschutzrechtlichen Transparenzgrundsatz zurückzuführen, aus dem die Pflicht zur Information von Betroffenen über den Umfang der Datenverarbeitung und die Zwecke, für die die Daten verarbeitet werden, resultiert. Hierzu gehört auch die Information darüber, ob die Daten des Betroffenen ausreichend gegen den Zugriff Unbefugter geschützt werden. Diese Information dient für Betroffene als Basis, um entscheiden zu können, ob sie einer (weiteren) Datenverarbeitung durch das Unternehmen zustimmen oder dieser widersprechen wollen.

Da ein Datenschutzvorfall, neben Konsequenzen wie Bußgeldern oder Schadensersatzansprüchen, angesichts der unter der DSGVO geltenden Informationspflichten auch mit einem Imageverlust des Unternehmens verbunden sein kann, gilt es, entsprechenden Vorfällen soweit möglich vorzubeugen und, sollte es in der Praxis tatsächlich einmal zu einem Datenschutzvorfall kommen, zügig zu handeln, um negative Folgen nach Möglichkeit abzumildern.

Pflichten unter der DSGVO

Zunächst ist festzuhalten, dass die DSGVO den weithin gebräuchlichen Begriff des „Datenschutzvorfalls" an sich nicht kennt, sondern die Pflichten des Verantwortlichen vielmehr an die „Verletzung des Schutzes personenbezogener Daten" anknüpft. Für die rechtliche Bewertung kommt es folglich darauf an, in welchen Fällen eine solche Verletzung vorliegt. Art. 4 Nr. 12 DSGVO definiert den Begriff der „Verletzung des Schutzes personenbezogener Daten" als jede 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. Vor dem Hintergrund, dass personenbezogene Daten von dem Verantwortlichen grundsätzlich nur im rechtlich zulässigen Umfang verarbeitet werden dürfen und vor unbefugtem Zugriff zu schützen sind, geht es bei einer Verletzung des Schutzes personenbezogener Daten im Kern folglich darum, dass in irgendeiner Form gegen diese Grundsätze der ordnungsgemäßen Datenverarbeitung verstoßen wird; etwa in Form eines Datenverlusts, einer nicht ordnungsgemäßen Nutzung oder einer unbefugten Offenlegung.

In der Praxis kann in Bezug auf Datenschutzvorfälle in der Regel zwischen einmaligen Vorkommnissen – etwa der Fehlversendung einer E-Mail an einen falschen Verteiler – und der systematischen Nichteinhaltung datenschutzrechtlicher Vorgaben – etwa dem Nichtergreifen von Absicherungsmaßnahmen – differenziert werden. Zu berücksichtigen ist außerdem, dass nicht nur ein unberechtigter Zugriff von außerhalb des Unternehmens oder ein sonstiges schädigendes Verhalten eines Dritten (z. B. Datenabfluss oder Datenlöschung) die Meldepflicht auslösen kann. Das versehentliche Fehlverhalten eines Mitarbeiters sowie die versehentliche Löschung und der versehentliche Verlust von personenbezogenen Daten innerhalb des Unternehmens können ebenfalls eine Meldung des Vorfalls erforderlich machen. Letzteren Fällen kann etwa durch aktuelle und vollständige Sicherungen des Datenbestandes entgegengewirkt werden.

Sicherheit der Verarbeitung, Art. 32 DSGVO

Um Datenschutzvorfälle zu vermeiden, hat jedes Unternehmen nach Art. 32 Abs. 1 DSGVO zunächst angemessene technische und organisatorische Maßnahmen zur Absicherung der Datenverarbeitungsprozesse im Unternehmen zu ergreifen. Die Auswahl der konkreten Maßnahmen hat dabei unter anderem unter Berücksichtigung der Art, des Umfangs, der Umstände und der Zwecke der konkreten Datenverarbeitungen sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos für die Betroffenen zu erfolgen. Hinsichtlich der Beurteilung der Angemessenheit nimmt Art. 32 Abs. 2 DSGVO außerdem explizit Bezug auf die mit der Datenverarbeitung einhergehenden Risiken – konkret die Vernichtung, den Verlust, die Veränderung oder die unbefugte Offenlegung bzw. den unbefugten Zugang zu personenbezogenen Daten, unabhängig davon, ob diese unbeabsichtigt oder unrechtmäßig erfolgen –, bei deren Eintreten die DSGVO entsprechend der obigen Definition von einer Verletzung des Schutzes personenbezogener Daten ausgeht. Die Maßnahmen i.S.v. Art. 32 DSGVO dienen folglich gerade dazu, Datenschutzvorfällen unter Berücksichtigung der konkreten Umstände der Verarbeitungssituation entgegenzuwirken.

Um dem Risiko eines Datenschutzvorfalls und den damit einhergehenden Verpflichtungen und Konsequenzen soweit möglich aus dem Weg zu gehen bzw. dieses zu minimieren, sollten Unternehmen sich deshalb mit ihren Datenverarbeitungen auseinandersetzen und bereits im Vorfeld die erforderlichen technischen und organisatorischen Maßnahmen zur Absicherung der einzelnen Prozesse ergreifen. Neben physisch umsetzbaren Maßnahmen (z. B. Alarmanlagen sowie die Sicherung von Türen und Fenstern) und Maßnahmen, die mittels Soft- oder Hardware realisiert werden können (z. B. Passwörter, Virenschutz, Verschlüsselung sowie Archivierungs- und Backup-Konzepte), gehören hierzu insbesondere auch Handlungsanweisungen sowie Verfahrens- und Vorgehensweisen, die von den Mitarbeitern des Unternehmens zu beachten sind (z. B. Regelungen zur Verschwiegenheit sowie Umgang mit ausgedruckten Informationen). Zu Nachweiszwecken empfiehlt es sich, die getroffenen Maßnahmen in einer Übersicht zu dokumentieren. Werden Dienstleister bei der Datenverarbeitung eingesetzt, sollte von diesen in gleicher Weise eine Dokumentation der dort getroffenen technischen und organisatorischen Maßnahmen angefordert werden, wobei zusätzlich die dokumentierten Maßnahmen auf ihre Angemessenheit zu prüfen sind.

Meldepflicht, Art. 33 DSGVO

Kommt es trotz Absicherungsmaßnahmen in der Praxis zu einer Verletzung des Schutzes personenbezogener Daten, löst dieser Umstand nach Art. 33 Abs. 1 DSGVO grundsätzlich eine Meldepflicht gegenüber der Aufsichtsbehörde aus. Auf eine Meldung kann nur dann verzichtet werden, wenn der Vorfall voraussichtlich nicht zu einem Risiko für die Rechte und Freiheiten natürlicher Personen führt; insoweit muss das Unternehmen abwägen, welche negativen Folgen sich aus der Verletzung für die Betroffenen ergeben können. An einem Risiko kann es etwa dann fehlen, wenn ein Laptop, auf dem ausschließlich verschlüsselte Daten abgelegt sind, abhandenkommt und alle Daten umgehend per Fernwartung von dem Gerät entfernt werden können. Kann ein Risiko für die Betroffenen hingegen nicht ausgeschlossen werden, hat unverzüglich eine Meldung gegenüber der zuständigen Aufsichtsbehörde zu erfolgen. Für die Rechtzeitigkeit der Meldung gibt es ein Zeitfenster von 72 Stunden nach Kenntniserlangung, jede weitere Verzögerung muss gegenüber der Aufsichtsbehörde begründet werden. Mit der Meldung fragt die Aufsichtsbehörde zahlreiche Daten und Angaben ab:

> Eine Beschreibung der Art der Verletzung des Schutzes personenbezogener Daten, soweit möglich mit Angabe der Kategorien und der ungefähren Zahl der betroffenen Personen sowie eine Angabe der betroffenen Datenkategorien und der ungefähren Anzahl der betroffenen Datensätze,
>
> der Namen und die Kontaktdaten des Datenschutzbeauftragten oder einer sonstigen Anlaufstelle,
>
> eine Beschreibung der wahrscheinlichen Folgen des Vorfalls,
>
> eine Beschreibung der ergriffenen oder vorgeschlagenen Maßnahmen zur Behebung des Vorfalls sowie gegebenenfalls Maßnahmen zur Abmilderung der möglichen nachteiligen Auswirkungen.

Hat ein Unternehmen Datenverarbeitungsprozesse an einen Dienstleister, konkret einen Auftragsverarbeiter, ausgelagert, hat dieser das für die Datenverarbeitung verantwortliche Unternehmen über einen (möglichen) Datenschutzvorfall umgehend zu informieren, damit dieses seiner Meldepflicht nachkommen kann. Die Meldepflicht verbleibt insoweit bei der verantwortlichen Stelle, also dem Auftraggeber.

Eine besondere Form sieht Art. 33 DSGVO für die Meldung nicht vor. Die Aufsichtsbehörden haben allerdings die Möglichkeit zur digitalen Meldung von Datenschutzvorfällen über Online-Portale eingeführt und erwarten auch deren Nutzung. Für eine Meldung sollten daher die jeweiligen Online-Formulare der Aufsichtsbehörden genutzt werden. Die dort abgefragten Daten können zugleich als Orientierung für die interne Dokumentation genutzt werden.

Benachrichtigungspflicht, Art. 34 DSGVO

Hat der Datenschutzvorfall ein hohes Risiko für die Rechte und Freiheiten der Betroffenen zur Folge, muss der Verantwortliche die Betroffenen – über seine Meldepflicht hinaus – nach Art. 34 Abs. 1 DSGVO unverzüglich über den Vorfall informieren. Die Benachrichtigungspflicht kann gem. Art. 34 Abs. 3 lit. a) DSGVO entfallen, wenn der Verantwortliche geeignete technische und organisatorische Sicherheitsvorkehrungen getroffen hat, durch die die Daten unzugänglich werden (z. B. Verschlüsselung). Gleiches gilt nach Art. 34 Abs. 3 lit. b) und c) DSGVO, wenn durch nachträgliche Maßnahmen ein hohes Risiko für die Betroffenen nicht mehr besteht oder die Meldung an die Betroffenen mit einem unverhältnismäßigen Aufwand verbunden wäre. In letzterem Fall entfällt allerdings nicht die grundsätzliche Benachrichtigungspflicht. Es hat nur keine unmittelbare Benachrichtigung der einzelnen Personen, sondern vielmehr eine öffentliche Bekanntmachung des Vorfalls zum Beispiel in der Tageszeitung zu erfolgen.

Von einem hohen Risiko für die Betroffenen, an das die Regelung des Art. 34 DSGVO anknüpft, kann in der Regel etwa dann ausgegangen werden, wenn besonders sensible Daten und/oder eine große Anzahl an Daten oder Personen von dem Vorfall betroffen sind. Ob ein hohes Risiko vorliegt, richtet sich allerdings grundsätzlich nach den jeweiligen Umständen des Einzelfalls.

Der Verantwortliche hat die Betroffenen nach Art. 34 Abs. 2 DSGVO in klarer und einfacher Sprache über den Vorfall zu informieren. Hinsichtlich des Umfangs der Informationspflicht wird auf die an die Aufsichtsbehörde zu meldenden Informationen verwiesen. Eine besondere Form für die Benachrichtigung sieht die DSGVO mit Ausnahme des Sonderfalls der öffentlichen Bekanntmachung hingegen nicht vor. Abzuraten ist allerdings von Gestaltungen, bei denen die konkreten Hintergründe bewusst verschleiert werden. In der Vergangenheit haben zahlreiche Unternehmen etwa ohne nähere Erläuterung darum gebeten, „aus Sicherheitsgründen“ neue Passwörter zu nutzen, wenn es zuvor einen erfolgreichen Datendiebstahl einschließlich der Zugangsdaten gab.

Die Benachrichtigungspflicht gem. Art. 34 DSGVO ist bei Annahme eines hohen Risikos zusätzlich zu der Meldepflicht gegenüber der Aufsichtsbehörde gem. Art. 33 DSGVO zu erfüllen. Die Aufsichtsbehörden fragen in diesen Fällen auch regelmäßig ab, ob und wie die Benachrichtigung der Betroffenen erfolgt ist. Natürlich ist es einer verantwortlichen Stelle auch unbenommen, bei einem geringeren Risiko die Betroffenen zu informieren; eine Pflicht besteht insoweit allerdings nicht.

Dokumentationspflicht

Unabhängig von etwaigen Melde- oder Benachrichtigungspflichten haben Verantwortliche nach Art. 33 Abs. 5 DSGVO jede Verletzung des Schutzes personenbezogener Daten zumindest intern umfassend zu dokumentieren. Die Dokumentation muss dabei alle im Zusammenhang mit dem Vorfall stehenden Fakten, die Auswirkungen sowie die ergriffenen Abhilfemaßnahmen enthalten. Gem. Art. 33 Abs. 5 S. 2 DSGVO ist die Dokumentation der Aufsichtsbehörde auf Verlangen zudem vorzulegen, damit diese die Einhaltung der Meldepflichten sowie die Erwägungen des Unternehmens überprüfen kann. Unabhängig von dieser Verpflich-

tung kann die interne Dokumentation vom Unternehmen auch dazu genutzt werden zu überprüfen, ob seine Datenverarbeitungsprozesse besondere Schwachstellen aufweisen oder Angriffspunkte bieten, um auf dieser Basis bessere Absicherungsmaßnahmen zu implementieren.

Soweit die jeweils zuständige Aufsichtsbehörde im Rahmen ihres Meldeportals die Möglichkeit bietet, auch Vorfälle unterhalb der Erheblichkeitsschwelle mittels des Online-Formulars zu erfassen, bietet sich diese Form der Dokumentation an, da so alle relevanten Informationen zentral gesammelt werden können. Bei Angabe eines geringen Risikos wird das ausgefüllte Meldeformular in der Regel nicht an die Aufsichtsbehörde übermittelt, kann aber exportiert und abgelegt werden.

Konzept zum Vorgehen bei Datenschutzvorfällen

Aufgrund der knappen Frist von maximal 72 Stunden, innerhalb derer die Meldung gegenüber der Aufsichtsbehörde sowie die Benachrichtigung der Betroffenen erfolgen muss, ist es erforderlich, einen Prozess im Unternehmen zu etablieren, der das konkrete Vorgehen regelt, sofern es trotz der getroffenen Absicherungsmaßnahmen zu einem Datenschutzvorfall kommen sollte. Die Aufsichtsbehörden vertreten insoweit teilweise sogar die Auffassung, dass eine ordnungsgemäße Meldung nur dann sichergestellt werden kann, wenn das Unternehmen für entsprechende Fälle klare Abläufe vorgesehen hat. Diese sind unter Berücksichtigung der Rechenschaftspflicht von Unternehmen gem. Art. 5 Abs. 2 DSGVO auch nachzuweisen.

Aus den genannten Gründen bietet sich die Erstellung eines Konzepts zum Vorgehen bei Datenschutzvorfällen an, innerhalb dessen geregelt wird, welche Maßnahmen und Vorgänge im Unternehmen einzuleiten sind, wenn Anhaltspunkte für einen möglichen Datenschutzvorfall vorliegen. Das Konzept sollte zum einen Informationen darüber enthalten, bei Vorliegen welcher Voraussetzungen eine Meldung gegenüber der Aufsichtsbehörde und eine Benachrichtigung der Betroffenen zu erfolgen hat. Zum anderen sollte etwa mittels einer Checkliste festgehalten werden, welche Informationen von den jeweils zuständigen Mitarbeitern dokumentiert werden müssen, damit das Unternehmen den ordnungsgemäßen Umgang mit dem jeweiligen Vorfall auch abseits von Melde- und Benachrichtigungspflichten nachweisen kann. Darüber hinaus empfiehlt sich die Erstellung eines Notfall-Reaktionsplans, der im Unternehmen bei Verdachtsfällen verwendet werden kann. Der Plan dient den Mitarbeitern als Hilfestellung, um die vorgesehenen Abläufe unmittelbar nach Kenntniserlangung anstoßen zu können und sollte deshalb konkrete Handlungsanweisungen, die die tatsächlichen Gegebenheiten im Unternehmen berücksichtigen, enthalten. Entsprechende Anweisungen können sich etwa darauf beziehen, in welchen Fällen der zuständige Vorgesetzte oder der Datenschutzbeauftragte zu informieren ist und welche Informationen an ihn weiterzuleiten sind. Darüber hinaus sollte geregelt werden, welche Stellen zur Kommunikation mit der Aufsichtsbehörde oder den Betroffenen befugt sind und wer über die Einleitung und Durchführung von Gegenmaßnahmen entscheidet und für diese zuständig ist.

Verstoß gegen die Pflichten aus Art. 32 – 34 DSGVO

Kommen Unternehmen ihren datenschutzrechtlichen Verpflichtungen nicht nach, können die Aufsichtsbehörden nach Art. 83 DSGVO Bußgelder in Höhe von bis zu 10 Mio. Euro oder bis zu 2 % des gesamten weltweit erzielten Jahresumsatzes verhängen. Dies gilt gem. Art. 83 Abs. 4 lit. a) DSGVO auch dann, wenn Verantwortliche ihren Pflichten nach den Art. 32 – 34 DSGVO nicht nachkommen, sie also keine ausreichenden Absicherungsmaßnahmen in Form von technischen und organisatorischen Maßnahmen ergreifen oder ihren Melde- und Benachrichtigungspflichten gegenüber der Aufsichtsbehörde und den Betroffenen nicht umfänglich innerhalb der vorgesehenen Fristen nachkommen. Darüber hinaus drohen im Falle von Datenschutzverstößen und Datenverlusten materielle und immaterielle Schadensersatzansprüche der betroffenen Personen nach Art. 82 DSGVO.

Vielfach bestehen Bedenken, dass die Aufsichtsbehörde erst durch die Meldung eines Datenvorfalls auf ein Problem aufmerksam gemacht wird, das dann gegebenenfalls zu Sanktionen der Aufsichtsbehörde führen kann. Es ist aber davon abzuraten, nur solche Datenschutzvorfälle der Aufsichtsbehörde zu melden, wenn mit einer Kenntnis der Behörden – etwa aufgrund einer Beschwerde eines Betroffenen – ohnehin zu rechnen ist. Auf nationaler Ebene sieht § 43 BDSG immerhin vor, dass Daten aus der Meldung bzw. Benachrichtigung in einem gerichtlichen Verfahren nicht gegen die verantwortliche Stelle verwertet werden dürfen. Zwar beinhaltet dies keine Garantie, dass die Aufsichtsbehörde nicht weiter tätig wird, dennoch soll auf diese Weise der Anreiz für eine Meldung erhöht werden.

Fazit

In Anbetracht der drohenden Konsequenzen – namentlich Bußgelder und Image-Verlust – stellen Datenschutzvorfälle ein erhebliches Risiko für Unternehmen dar. Aus diesem Grund sollten Unternehmen ihre Datenverarbeitungsprozesse frühzeitig durch geeignete und angemessene technische und organisatorische Maßnahmen absichern. Um die ordnungsgemäße Auseinandersetzung mit der Thematik nachweisen zu können, empfiehlt sich insoweit die Erstellung einer entsprechenden Übersicht, mittels derer die zuständigen Mitarbeiter gleichzeitig einen guten Überblick über das Sicherheitsniveau im Unternehmen erhalten und auf dieser Basis Verbesserungsprozesse anstoßen können. Insbesondere unter Berücksichtigung der seitens der Aufsichtsbehörden statuierten Anforderungen ist darüber hinaus ein Konzept zu erstellen, das vertiefte Informationen dazu enthält, wie bei einem (möglichen) Datenschutzvorfall konkret vorzugehen ist, welche gesetzlichen Pflichten einzuhalten und welche Maßnahmen zu ergreifen sind. Mit Hilfe eines entsprechenden Konzeptes wird das Unternehmen in die Lage versetzt, erforderlichenfalls schnell und fehlerfrei zu reagieren und auf diese Weise mögliche Konsequenzen abzumildern.

Christina Prowald/Dr. Sebastian Meyer

Kontakt:

BRANDI Rechtsanwälte
Partnerschaft mbB
Adenauerplatz 1
33602 Bielefeld

Christina Prowald
Wissenschaftliche Mitarbeiterin

T +49 521 96535 - 890
F +49 521 96535 - 113
M christina.prowald@brandi.net

Kontakt:

BRANDI Rechtsanwälte
Partnerschaft mbB
Adenauerplatz 1
33602 Bielefeld

Dr. Sebastian Meyer, LL.M.
Rechtsanwalt und Notar mit Amtssitz in Bielefeld
Fachanwalt für Informationstechnologierecht (IT-Recht)
Datenschutzauditor (TÜV)

T +49 521 96535 - 812
F +49 521 96535 - 113
M sebastian.meyer@brandi.net