Vorsicht bei Datenschutzpannen

MELDEPFLICHTEN *Bei Datenschutzverletzungen sind die Aufsichtsbehörde und die Betroffenen zu benachrichtigen. Sonst kann es Ärger geben. Über das Vorgehen bei Pannen sollten sich auch Betriebs- und Personalräte informieren: Es könnten auch Beschäftigtendaten unter die Räder geraten.*

VON **BRUNO SCHIERBAUM**

Im Falle einer Verletzung des Schutzes personenbezogener Daten muss der Verantwortliche diesen Vorfall unverzüglich der Aufsichtsbehörde melden. Das schreibt Art. 33 Abs. 1 der Datenschutzgrundverordnung (DSGVO) vor. Bereits in § 42a des alten Bundesdatenschutzgesetzes (BDSG-alt) ist eine solche Regelung enthalten, die unter dem umgangssprachlichen Begriff Datenschutzpanne diskutiert wurde.[1] Die DSGVO enthält einige Neuerungen, von denen zwei besonders wichtig sind:

- Im Gegensatz zu § 42a BDSG-alt umfasst Art. 33 DSGVO unterschiedslos alle Verantwortlichen und somit auch öffentliche Stellen.
- Datenschutzpannen beschränken sich nicht mehr nur auf besonders sensible Daten, sondern auf alle personenbezogenen Daten – also auch auf alle Beschäftigtendaten.

Die Art. 33 und Art. 34 der DSGVO sollen insbesondere Transparenz über Datenschutzpannen schaffen. Den Aufsichtsbehörden und den Betroffenen werden rechtliche Möglichkeiten eingeräumt, um mögliche Folgeschäden durch die Datenschutzverletzung zu vermeiden oder zumindest zu minimieren.[2]

Meldung an die Aufsichtsbehörde

Grundsätzlich besteht eine Meldepflicht bei Datenschutzverletzungen. In der DSGVO ist

1 Siehe Däubler/Klebe/Wedde/Weichert, BDSG, § 42a Rn. 1a

2 Vgl. Gola (Hrsg.), DSGVO, Art. 33 Rn. 2

unter anderem geregelt, bei welchen Vorfällen eine Meldung gegenüber der Aufsichtsbehörde oder eine Benachrichtigung gegenüber dem Betroffenen erfolgen muss, die Fristen für eine Meldung, deren Inhalt und die Dokumentationspflichten des Verantwortlichen.

▸ Verantwortlicher für die Meldung

Für die Einhaltung der Vorgaben der DSGVO, einer erforderlichen Meldepflicht gegenüber der Aufsichtsbehörde und einer Benachrichtigung des Betroffenen ist der Verantwortliche zuständig. Der Begriff des Verantwortlichen ist in Art. 4 Nr. 7 DSGVO definiert. Als mögliche Adressaten der DSGVO sind natürliche oder juristische Personen, Behörden, Einrichtungen und sonstige Stellen genannt. Es wird deutlich, dass es auf die Organisationsform nicht ankommt, sondern dass sowohl natürliche und juristische Personen als auch vergleichbare Personenmehrheiten »Verantwortliche« im Sinne der DSGVO sein können, unabhängig davon, ob sie öffentlich-rechtlich oder privatrechtlich organisiert sind.[3]

▸ Meldepflicht des Auftragsverarbeiters

Den Auftragsverarbeiter selbst trifft keine Meldepflicht gegenüber der Aufsichtsbehörde. Er ist aber nach Art. 33 Abs. 2 DSGVO verpflichtet, den Verantwortlichen, für den er als Auftragnehmer tätig ist, zu informieren, wenn ihm eine Verletzung des Schutzes personenbezogener Daten bekannt wird.

▸ Verletzung des Schutzes personenbezogener Daten

Voraussetzung für eine Meldepflicht gegenüber der zuständigen Aufsichtsbehörde ist die Verletzung des Schutzes personenbezogener Daten. Dabei ist es unerheblich, ob den Verantwortlichen ein Verschulden trifft und ob es sich um vorsätzliches oder fahrlässiges Tun handelt.[4]

Art. 4 Abs. 1 DSGVO definiert den Begriff der personenbezogenen Daten. Er unterscheidet sich nicht grundlegend von dem aus dem alten BDSG und den Landesdatenschutzgesetzen bekannten. Von einer Datenschutzpanne können Daten von Beschäftigten, Bewerbern, Kunden, Bürgern, Patienten oder Klienten betroffen sein.

In Art. 4 Nr. 12 DSGVO ist definiert, was konkret unter »Verletzung des Schutzes personenbezogener Daten« zu verstehen ist. Es geht um eine Verletzung der Sicherheit, die zur Vernichtung, zum Verlust, zur Veränderung, zur unbefugten Offenlegung oder zum unbefugten Zugang zu personenbezogenen Daten führt, die übermittelt, gespeichert oder auf sonstige Weise verarbeitet werden. Dabei ist es nicht von Bedeutung, ob diese Maßnahmen unbeabsichtigt oder unrechtmäßig erfolgen.

DEFINITION

Art. 4 Nr. 7 DSGVO – Verantwortlicher
Der Begriff Verantwortlicher bezeichnet die natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet [...]

▸ Risiko für die Rechte und Freiheiten

Eine Meldepflicht trifft den Verantwortlichen nicht in jedem Fall. Die Meldung an die Aufsichtsbehörde muss nicht erfolgen, wenn die Verletzung des Schutzes personenbezogener Daten »voraussichtlich nicht zu einem Risiko für die Rechte und Freiheiten natürlicher Personen führt«, Art. 33 Abs. 1 DSGVO.

Der Begriff »voraussichtlich« macht deutlich, dass ein Schaden für die Rechte und Freiheiten der betroffenen Person durch die Datenschutzpanne noch nicht eingetreten sein muss. Es muss aktuell mit dem Datenschutzverstoß noch kein Risiko bestehen. Der Verantwortliche wird eine Prognose über die Folgen der Panne anstellen müssen. Die Prognoseentscheidung unterliegt grundsätzlich der vollen gerichtlichen Kontrolle.[5]

Eine Meldung muss nur dann erfolgen, wenn mit der Datenschutzpanne »ein Risiko für die Rechte und Freiheiten natürlicher Personen« besteht. Ein solches Risiko ist immer dann anzunehmen, wenn ein physischer, materieller oder immaterieller Schaden für den Betroffenen zu erwarten ist.[6] Der Erwägungsgrund 85 nennt Beispiele für Schäden, die in diesem Zusammenhang relevant sein können und eine Meldepflicht auslösen.

DARUM GEHT ES

1. Die Verletzung des Schutzes personenbezogener Daten kann Schäden bei Betroffenen verursachen.

2. Besteht ein solches Risiko, muss unverzüglich eine Meldung an die Datenschutzbehörde erfolgen.

3. Die Belegschaftsvertretung hat im Rahmen ihres Überwachungsrechts darauf zu achten, dass sich der Arbeitgeber bei Pannen richtig verhält.

3 Kühling/Buchner (Hrsg.), DSGVO, Art. 4 Rn. 9
4 Vgl. Sydow (Hrsg.), EU-DSGVO, Art. 33 Rn. 7
5 Vgl. Paal/Pauly (Hrsg.), DSGVO, Art. 33 Rn. 26
6 Erwägungsgrund 85; vgl. auch Sydow (Hrsg.), aaO., Art. 33 Rn. 9

EU-DATENSCHUTZ-GRUNDVERORDNUNG

Art. 33 – Meldung an die Aufsichtsbehörde
(1) 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.

ÜBERBLICK

Art. 4 Nr. 1 DSGVO – Personenbezogene Daten

Personenbezogene Daten bezeichnet alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person (im Folgenden »betroffene Person«) beziehen; als identifizierbar wir deine natürliche Person angesehen, die direkt oder indirekt, insbesondere mittel Zuordnung zur Kennung wie einem Namen, zu einer Kennnummer, zu Standortdaten, zu einer Online-Kennung oder zu einem oder mehreren besonderen Merkmalen, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind, identifiziert werden kann [...]

Frist, Form und Inhalt der Meldung

Die Meldung an die Aufsichtsbehörde hat nach Art. 33 Abs. 1 DSGVO unverzüglich und möglichst innerhalb von 72 Stunden nach Bekanntwerden der Datenschutzpanne zu erfolgen. Die Mitteilungspflicht des Verantwortlichen entsteht genau zu dem Zeitpunkt, zu dem ihm die Verletzung bekannt wird. Er muss hinreichende Kenntnis erlangt haben, so dass er eine sinnvolle Meldung gegenüber der Aufsichtsbehörde abgeben kann.[7]
»Unverzüglich« meint, dass der Verantwortliche zu einer Meldung ohne schuldhaftes Zögern (§ 121 Bürgerliches Gesetzbuch) verpflichtet ist.[8] Bei der Feststellung, ob die Meldung unverzüglich erfolgt ist, sollten die Art und Schwere der Verletzung des Schutzes personenbezogener Daten und deren Folgen und Auswirkungen für die betroffene Person berücksichtigt werden.[9] Das heißt, dass im Einzelfall – vor dem Hintergrund einer unverzüglich zu erfolgenden Meldung – eine Meldung nach 72 Stunden zu spät sein kann.

Erfolgt eine Meldung an die Aufsichtsbehörde nicht binnen 72 Stunden, so ist eine Begründung für die Verzögerung beizufügen. Die DSGVO schreibt eine besondere Form der Meldung nicht vor. In dringenden Fällen wird vor dem Hintergrund, dass die Meldung unverzüglich zu erfolgen hat, eine telefonische Kontaktaufnahme mit der Aufsichtsbehörde geboten sein.[10]

Eine ausführliche Meldung kann dann zum Beispiel per Brief, E-Mail oder Fax erfolgen.[11] Der Meldepflichtige trägt die Verantwortung für einen Nachweis des Zugangs der Meldung an die Aufsichtsbehörde.[12]

Die DSGVO macht genaue Vorgaben über den Mindestinhalt der Pannenmeldung gegenüber der Aufsichtsbehörde. Sie muss nach Art. 33 Abs. 2 zumindest enthalten:

- 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,
- den Namen und die Kontaktdaten des Datenschutzbeauftragten oder einer sonstigen Anlaufstelle für weitere Informationen,
- eine Beschreibung der wahrscheinlichen Folgen der Verletzung des Schutzes personenbezogener Daten,
- eine Beschreibung der von dem Verantwortlichen ergriffenen oder vorgeschlagenen Maßnahmen zur Behebung der Datenschutzverletzung und gegebenenfalls Maßnahmen zur Abmilderung ihrer möglichen nachteiligen Auswirkungen.

Benachrichtigung der betroffenen Person

Über die Meldung der Datenschutzverletzung bei der Aufsichtsbehörde hinaus, ist die betroffene Person zu benachrichtigen. Dies hat unverzüglich zu erfolgen, wenn die Datenschutzpanne voraussichtlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen zur Folge hat, Art. 34 Abs. 1 DSGVO. Die Benachrichtigungen sollen in enger Absprache mit der Aufsichtsbehörde erfolgen.[13]

Zentral für die Benachrichtigung des Betroffenen ist das voraussichtlich »hohe Risiko« für die Rechte und Freiheiten natürlicher Personen. Die DSGVO definiert nicht, wann ein hohes Risiko voraussichtlich gegeben ist. Die Einschätzung eines »hohes Risikos« liegt

7 Siehe Paal/Pauly (Hrsg.), aaO., Art. 33 Rn. 18
8 Vgl. Sydow (Hg.), aaO., Art. 33 Rn. 13
9 So Erwägungsgrund 87
10 Vgl. Gola (Hrsg.), DSGVO, Art. 33 Rn. 36
11 Marschall, So gehen sie mit Datenpannen richtig um, Datenschutz-Praxis 8/17, 3
12 Vgl. Gola (Hrsg.), aaO., Art. 33 Rn. 36
13 So der Erwägungsgrund 86 Satz 3

DSGVO – ERWÄGUNGSGRUND 85

Beispiele für Verletzungen des Schutzes personenbezogener Daten

- der Kontrollverlust über personenbezogene Daten oder
- die Einschränkung der Rechte der natürlichen Person,
- Diskriminierung,
- Identitätsdiebstahl oder -betrug,
- finanzielle Verluste,
- unbefugte Aufhebung der Pseudonymisierung,
- Rufschädigung,
- Verlust der Vertraulichkeit von dem Berufsgeheimnis unterliegenden Daten oder
- andere erhebliche wirtschaftliche oder gesellschaftliche Nachteile.

beim Verantwortlichen. Er wird in diesem Fall auch eine Risikoprognose aufstellen müssen. In diesem Zusammenhang ist von Bedeutung, dass der Verantwortliche das Risiko der Fehleinschätzung und die Verhängung eines Bußgelds trägt.[14]

▸ Frist, Inhalt und Form der Benachrichtigung

Wie die Meldung an die Aufsichtsbehörde hat die Benachrichtigung des Betroffenen »unverzüglich« zu erfolgen. Die Erwägungsgründe enthalten einige Anhaltspunkte hinsichtlich des Zeitpunkts der Benachrichtigung. So hat nach Erwägungsgrund 86 eine Benachrichtigung der betroffenen Person »stets so rasch wie nach allgemeinem Ermessen möglich, in enger Absprache mit der Aufsichtsbehörde und nach Maßgabe der von dieser oder anderen zuständigen Behörden wie beispielsweise Strafverfolgungsbehörden erteilten Weisungen zu erfolgen«.

Da zudem die Benachrichtigung mit der Aufsichtsbehörde abgesprochen werden soll, erfolgt die Benachrichtigung des Betroffenen zeitlich nach erfolgter Meldung bei der Aufsichtsbehörde.[15] Zudem wird deutlich gemacht, dass die betroffene Person sofort zu benachrichtigen ist, sofern dies notwendig ist, um das Risiko eines unmittelbaren Schadens abzuwenden.[16]

In Bezug auf den Inhalt der Benachrichtigung schreibt Art. 34 Abs. 2 DSGVO vor, dass diese in einer klaren und einfachen Sprache die Art der Verletzung des Schutzes personenbezogener Daten und zumindest folgende weitere Informationen enthält:

- den Namen und die Kontaktdaten des Datenschutzbeauftragten oder einer sonstigen Anlaufstelle für weitere Informationen,
- eine Beschreibung der wahrscheinlichen Folgen der Verletzung des Schutzes personenbezogener Daten,
- eine Beschreibung der von dem Verantwortlichen ergriffenen oder vorgeschlagenen Maßnahmen zur Behebung der Verletzung des Schutzes personenbezogener Daten und gegebenenfalls Maßnahmen zur Abmilderung ihrer möglichen nachteiligen Auswirkungen.

Hinsichtlich der Form sieht Art. 34 DSGVO keine Vorgaben vor. In Art. 12 DSGVO sind grundlegende Punkte für die Rechte der Betroffenen – wozu auch das Recht auf Benachrichtigung gehört – geregelt. Danach können die Informationen schriftlich oder in anderer Form, gegebenenfalls auch elektronisch erfolgen.

▸ Pflicht zur Benachrichtigung

Art. 34 Abs. 3 DSGVO enthält drei Ausnahmen, bei deren Vorliegen eine Benachrichtigung nicht erforderlich ist:

- der Verantwortliche geeignete technische und organisatorische Sicherheitsvorkehrungen getroffen hat und diese Vorkehrungen auf die von der Verletzung der betroffenen personenbezogenen Daten angewandt wurden, insbesondere solche, durch die die personenbezogenen Daten für alle Personen, die nicht zum Zugang zu den personenbezogenen Daten befugt sind, unzugänglich ge-

14 Gola (Hrsg.), aaO., Art. 34 Rn. 5
15 Gola (Hrsg.), aaO., Art. 34 Rn. 13
16 So Erwägungsgrund 86

EU-DATENSCHUTZ-GRUNDVERORDNUNG

Art. 34 – Benachrichtigung der betroffenen Person
(1) 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.

macht werden, etwa durch Verschlüsselung;
- der Verantwortliche durch nachfolgende Maßnahmen sichergestellt hat, dass das hohe Risiko für die Rechte und Freiheiten der betroffenen Person aller Wahrscheinlichkeit nach nicht mehr besteht;
- dies mit einem unverhältnismäßigen Aufwand verbunden wäre. In diesem Fall hat stattdessen eine öffentliche Bekanntmachung oder eine ähnliche Maßnahme zu erfolgen, durch die die betroffenen Personen vergleichbar wirksam informiert werden.

Die Aufsichtsbehörde kann bei positiver Prognose eines Risikos für die Betroffenen vom Verantwortlichen eine Benachrichtigung verlangen, Art. 34 Abs. 4 DSGVO. Diese Möglichkeit wirkt als eine Art Korrektiv und zwar dann, wenn der Verantwortliche die Bewertung eines Risikos einseitig zu seinen Gunsten auslegt[17] und die betroffene Person nicht benachrichtigt.

Pflicht zur Dokumentation

Der Verantwortliche hat die Verletzungen des Schutzes personenbezogener Daten einschließlich aller im Zusammenhang mit der Datenschutzverletzung stehenden Fakten zu dokumentieren. Die Dokumentation muss Auswirkungen und Abhilfemaßnahmen umfassen. Sie geht damit über die reine Zusammenfassung des Vorfalls hinaus[18] und ermöglicht der Aufsichtsbehörde so, die Einhaltung der Meldepflicht zu prüfen. Dies beinhaltet aber nicht die Verpflichtung, die Dokumentation der Datenschutzverletzung der Aufsichtsbehörde zukommen zulassen. Sie ist lediglich vorzuhalten.[19] Dazu kann die Aufsichtsbehörde nach Art. 58 Abs. 1a DSGVO den Verantwortlichen anweisen, die entsprechenden Informationen zur Verfügung zu stellen.

Sanktionen bei Verstößen

Für Verstöße, die den Art. 33 und 34 DSGVO betreffen, wie zum Beispiel gegen die Pflicht zur Meldung von Datenschutzverletzungen gegenüber der Aufsichtsbehörde, gegen die Benachrichtigung der Betroffenen oder gegen die Dokumentationspflicht werden gemäß Art. 83 Abs. 4a DSGVO Geldbußen von bis zu zehn Millionen Euro oder im Fall eines Unternehmens von bis zu zwei Prozent seiner gesamten weltweit erzielten Jahresumsatzes des vorangegangenen Geschäftsjahres verhängt, je nachdem, welcher der Beträge höher ist. Gegen Behörden und öffentliche Stellen wird keine Geldbuße verhängt. Der deutsche Gesetzgeber hat hier die Öffnungsklausel in der DSGVO genutzt und dies in § 43 Abs. 3 BDSG-neu festgelegt.[20]

Der Betroffene kann Schadensersatzansprüche geltend machen, sofern er einen Schaden erleidet, etwa dadurch, dass die Benachrichtigung nach Art. 34 DSGVO gar nicht oder nicht rechtzeitig erfolgt. Zudem kommt eine Haftung im Hinblick auf eine Datenschutzverletzung als solche in Betracht. Dieses kommt dann zum Tragen, wenn zwar nach Art. 34 DSGVO eine Benachrichtigung rechtmäßig erfolgt ist, ein Schaden für den Betroffenen nicht oder nicht vollständig abgewendet werden konnte.[21]

Aufgaben für Betriebs- und Personalräte

Betriebs- und Personalräte sind gut beraten, sich auch mit dem Thema Datenschutzpannen nach den Art. 33 und 34 DSGVO zu befassen. Denn von diesen Pannen können sowohl Beschäftigten- als auch Bewerberdaten betroffen sein. Insoweit haben sie im Rahmen ihres Überwachungsrechts hinsichtlich bestehender Gesetze und Verordnungen darauf zu achten, dass sich der Arbeitgeber zum Beispiel hinsichtlich der Meldepflicht gegenüber der Aufsichtsbehörde und der Benachrichtigungspflicht gegenüber dem Betroffenen an die Vorgaben der Datenschutzgrundverordnung hält.

Denkbar ist aber auch, dass über die Nutzung der Mitbestimmungsrechte im Rahmen einer Betriebs- oder Dienstvereinbarung sehr genau der Umfang der Verarbeitung personenbezogener Daten, das Zugriffsberechtigungskonzept und das Übermitteln personenbezogener Daten an Dritte geregelt ist. Kommt es hier zu einer Datenschutzpanne können Arbeitnehmervertretungen – zusätzlich zu den Maßnahmen, die der Beschäftigte ergreifen kann – auf gerichtlichem Weg auf die Einhaltung der Betriebs- oder Dienstvereinbarung hinwirken. ◁

Bruno Schierbaum,
BTQ Niedersachsen GmbH,
schierbaum@btq.de
www.btq.de

EUROPÄISCHER DATENSCHUTZ-AUSSCHUSS

Für die Feststellung von »Verletzungen des Schutzes personenbezogener Daten«, für die Feststellung der »Unverzüglichkeit« und »zu den Umständen, unter denen der Verantwortliche oder der Auftragsverarbeiter die Verletzung des Schutzes personenbezogener Daten zu melden hat«, ist zu erwarten, dass der Europäische Datenschutzausschuss Leitlinien, Empfehlungen oder Verfahren erarbeitet und veröffentlicht, in denen diese Begriffe und Vorgaben präzisiert werden. Diese Befugnis wird dem Europäischen Datenschutzausschuss in Art. 70 Abs. 1g DSGVO eingeräumt.

17 Vgl. Kühling/Buchner (Hrsg.), aaO., Art. 34 Rn. 5
18 Sydow (Hrsg.), aaO., Art. 33 Rn. 28
19 Vgl. Paal/Pauly (Hrsg.), aaO., Art. 33 Rn. 58
20 Es ist davon auszugehen, dass die Landesgesetzgeber in ihren neuen Landesdatenschutzgesetzen ebenfalls von der Möglichkeit, keine Geldbußen gegen öffentliche Stellen der Länder zu verhängen, Gebrauch machen werden.
21 Vgl. Gola (Hrsg.), aaO., Art. 34 Rn. 17