Was tun bei Daten-schutz-Pannen?

MELDEPFLICHT *Wenn mit personenbezogenen Daten schlampig umgegangen wird, muss die Aufsichtsbehörde informiert werden. Vor allem Dienststellen müssen darauf achten.*

VON **BRUNO SCHIERBAUM**

Behörden und sonstige öffentliche Stellen als Verantwortliche im Sinne der Datenschutz-Grundverordnung (DS-GVO)[1] müssen diese bis zum 25.5.2018 umsetzen[2] und somit auch einige Veränderungen im Umgang mit so genannten »Datenschutz-Pannen« beachten. Das ist neu für öffentliche Stellen. In den Art. 33 und 34 DS-GVO ist zwingend vorgeschrieben, wie der Verantwortliche bei einer Verletzung des Schutzes personenbezogener Daten vorzugehen hat. Bereits in § 42 a BDSG ist eine entsprechende Regelung enthalten, die unter dem umgangssprachlichen Begriff »Datenschutz-Panne«[3] diskutiert wurde. Art. 33 DS-GVO enthält einige Neuerungen, von denen zwei an dieser Stelle herausgestellt werden sollen.

Erstens: Im Gegensatz zu § 42a BDSG umfasst Art. 33 DS-GVO unterschiedslos alle Verantwortlichen und somit auch Behörden und sonstige öffentliche Stellen. Für die Nichtberücksichtigung öffentlicher Stellen[4] im aktuellen geltenden BDSG gibt es keine nachvollziehbaren Gründe[5].

Zweitens: Zudem beschränken sich »Datenschutz-Pannen« künftig nicht nur auf besonders sensible Daten[6], sondern auf alle personenbezogenen Daten, also auch auf alle Beschäftigten-Daten.

Mit Hilfe der Regelungen des Art. 33 und 34 DS-GVO soll insbesondere Transparenz über erfolgte Datenschutzverletzungen geschaffen werden. Den Datenschutz-Aufsichtsbehörden und dem Betroffenen werden rechtliche Möglichkeiten eingeräumt, um die durch die Datenschutzverletzung entstehenden Folgeschäden möglichst zu vermeiden bzw. zu minimieren.[7]

Meldung gegenüber der Aufsichtsbehörde

Grundsätzlich besteht eine Meldepflicht bei Datenschutzverletzungen (Datenschutz-Pannen). In der DS-GVO ist unter anderem geregelt, welche Vorfälle der Aufsichtsbehörde bzw. dem Betroffenen gemeldet werden müssen. Die Verordnung regelt zudem die Fristen für eine Meldung, ihren Inhalt und die Dokumentationspflichten des Verantwortlichen.

▸ Verantwortlicher für die Meldung

Für die Einhaltung der Art. 33 und 34 DS-GVO und der damit verbundenen Meldepflicht gegenüber der Aufsichtsbehörde und einer Benachrichtigung des Betroffenen ist der Verantwortliche zuständig. Der Begriff des Verantwortlichen ist in Art. 4 Nr. 7 DS-GVO definiert (siehe Randspalte). Als mögliche Adressaten der DS-GVO sind natürliche oder juristische Personen, Behörden, Einrichtungen und sonstige Stellen genannt. Auf die Organisationsform kommt es nicht an. Sowohl natürliche und juristische Personen als auch vergleichbare Personenmehrheiten können

DARUM GEHT ES

1. Wenn der Schutz personenbezogener Daten verletzt wird, kann das für die Betroffenen einen Schaden verursachen.

2. Besteht ein solches Risiko, muss die Datenschutz-Panne unverzüglich der Aufsichtsbehörde gemeldet werden.

3. Der Personalrat muss darauf achten, dass mit Datenschutz-Pannen ordnungsgemäß umgegangen wird.

1 Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27.4.2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung) – Abl. Nr. L 119 S. 1.
2 Nach Art. 99 Abs. 2 DS-GVO gilt die Verordnung ab dem 25.5.2018.
3 Vgl. Däubler/Klebe/Wedde/Weichert, Bundesdatenschutzgesetz, § 42a Rn. 1a.
4 In einigen Landesdatenschutzgesetzen sind dem 42a BDSG vergleichbare Regelungen enthalten, so zum Beispiel § 27a LDSG SH, § 23 LDSG MV.
5 Vgl. Däubler/Klebe/Wedde/Weichert, a.a.O., § 42a Rn. 3.
6 Nach § 42a BDSG sind »Datenschutz-Pannen« nur dann gegeben, wenn bestimmte personenbezogene Daten unrechtmäßig übermittelt werden oder auf sonstige Weise unrechtmäßig zur Kenntnis gelangt sind. Es handelt sich um besondere Arten personenbezogener Daten (§ 3 Abs. 9 BDSG), personenbezogene Daten, die einem Berufsgeheimnis unterliegen, personenbezogene Daten, die sich auf strafbare Handlungen oder Ordnungswidrigkeiten beziehen oder personenbezogene Daten zu Bank- und Kreditkartenkonten.
7 Vgl. Gola (Hrsg.), DS-GVO, Art. 33 Rn. 2.

Bei Datenschutz-Pannen ist die Aufsichtsbehörde immer dann zu informieren, wenn als Folge ein Risiko für die betroffenen Beschäftigten besteht.

»Verantwortliche« im Sinne der DS-GVO sein, unabhängig davon, ob sie öffentlich-rechtlich oder privatrechtlich organisiert sind.[8]

▸ Meldepflicht des Auftragsverarbeiters

Den Auftragsverarbeiter selbst – nach Art. 4 Nr. 8 DS-GVO derjenige, der die personenbezogenen Daten im Auftrag des Verantwortlichen verarbeitet – trifft keine Meldepflicht gegenüber der Aufsichtsbehörde. Nach Art. 33 Abs. 2 DS-GVO ist er aber verpflichtet, den Verantwortlichen, für den er im Rahmen von Datenverarbeitung im Auftrag als Auftragnehmer tätig ist, zu informieren, wenn ihm eine Verletzung des Schutzes personenbezogener Daten bekannt wird.

▸ Meldung an die Aufsichtsbehörde

Die DS-GVO nutzt in Bezug auf die Datenschutzaufsicht den Begriff »Aufsichtsbehörde«[9], lässt aber den Mitgliedstaaten die Möglichkeit der Organisation der Datenschutz-Aufsicht. Denn nach Art. 51 Abs. 1 DS-GVO kann jeder Mitgliedstaat vorsehen, dass eine oder mehrere unabhängige Behörden für die Überwachung der Anwendung der DS-GVO zuständig sind. Das BDSG n.F. hat die Zuständigkeiten der Datenschutzaufsicht in § 9 bzw. § 40 BDSG n.F. geregelt. So wird der Bundesbeauftragte für den Datenschutz weiterhin für die öffentlichen Stellen des Bundes und die Landesdatenschutzbeauftragten für die öffentlichen Stellen der Länder bzw. wie aktuell als Aufsichtsbehörden[10] für die nicht-öffentlichen Stellen zuständig sein. Gegenüber den entsprechenden Behörden sind dann im Falle einer Datenschutz-Panne die jeweiligen öffentlichen bzw. nicht-öffentlichen Einrichtungen meldepflichtig.

▸ Verletzung 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 oder ob vorsätzlich oder fahrlässig gehandelt wurde.[11]

▸ Personenbezogene Daten

Es muss sich um personenbezogene Daten handeln. Dabei spielt die Sensibilität der Daten[12] – im Gegensatz zur aktuellen Fassung des § 42a BDSG – keine Rolle. Der Begriff »personenbezogene Daten« ist in Art. 4 Abs. 1 DS-GVO definiert (siehe folgenden Infokasten). Er unterscheidet sich nicht grundlegend von dem Begriff »personenbezogene Daten« im aktuellen BDSG und in den LDSG. Von einer Datenschutz-Panne können unter anderem Daten der Beschäftigten, der Bewerber, der Kunden, der Bürger, der Patienten oder Klienten betroffen sein.

DEFINITION

Verantwortlicher nach Art. 4 Nr. 7 DS-GVO
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 ...

ÜBERBLICK

Personenbezogene Daten
Personenbezogene Daten sind nach Art. 4 Nr. 1 DS-GVO alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person (im Folgenden »betroffene Person«) beziehen; als identifizierbar wird eine natürliche Person angesehen, die direkt oder indirekt, insbesondere mittels Zuordnung zu einer Kennung (wie einem Namen, zu einer Kennnummer, zu Standortdaten, zu einer Online-Kennung oder zu einem oder mehreren besonderen Merkmalen) identifiziert werden kann, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind.

8 Vgl. Kühling/Buchner (Hrsg.), DS-GVO, Art. 4 Rn. 9.
9 So zum Beispiel in Art. 33 DS-GVO, in dem es um den Umgang mit »Datenschutz-Pannen« geht oder in den Art. 51 ff. DS-GVO, in denen Zuständigkeit, Aufgaben und Befugnisse der Aufsichtsbehörde geregelt sind.
10 Im Folgenden wird der Begriff »Aufsichtsbehörde« aus der DS-GVO für die verschiedenen Datenschutzaufsichtsbehörden in Deutschland verwendet, denn es wird weiterhin einen Bundesbeauftragten für den Datenschutz und Landesbeauftragte für den Datenschutz geben, die für öffentliche Stellen der Länder und nicht öffentliche Stellen zuständig sind.
11 Vgl. Sydow (Hrsg.), Europäische Datenschutzgrundverordnung, Art. 33 Rn. 7.
12 Hierzu Kersting, in diesem Heft ab Seite 34.

Verletzung des Datenschutzes

In Art. 4 Nr. 12 DS-GVO 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… oder zur unbefugten Offenlegung von oder zum unbefugten Zugang zu personenbezogenen Daten führt, die übermittelt, gespeichert oder auf sonstige Weise verarbeitet wurden. Dabei ist es nicht von Bedeutung, ob diese Maßnahmen unbeabsichtigt oder unrechtmäßig erfolgen.

(Kein) Risiko für 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 DS-GVO).

Der Begriff »voraussichtlich« macht deutlich, dass ein Schaden für die Rechte und Freiheiten der betroffenen Person durch die »Datenschutz-Panne« noch nicht eingetreten sein muss. Es muss aktuell mit dem Datenschutzverstoß noch kein Risiko bestehen. Der Verantwortliche wird eine Prognose über die Folgen der »Datenschutz-Panne« anstellen müssen. Diese Prognoseentscheidung unterliegt grundsätzlich der vollen gerichtlichen Kontrolle.[13]

Eine Meldung ist nur dann erforderlich, wenn als Folge der Datenschutz-Panne »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.[14] Der Erwägungsgrund 85 nennt Beispiele für Schäden, die in diesem Zusammenhang relevant sein können und eine Meldepflicht auslösen sollten (siehe Randspalte).

Frist zur Meldung

Nach Art. 33 Abs. 1 DS-GVO muss die Meldung an die Aufsichtsbehörde unverzüglich und möglichst innerhalb von 72 Stunden nach Bekanntwerden der Datenschutz-Panne 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.[15] »Unverzüglich« meint, dass der Verantwortliche zu einer Meldung ohne schuldhaftes Zögern (§ 121 BGB) verpflichtet ist.[16] 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.[17] Im Einzelfall kann – vor dem Hintergrund einer unverzüglich zu erfolgenden Meldung – eine Meldung erst nach 72 Stunden zu spät sein. Erfolgt eine Meldung an die Aufsichtsbehörde nicht binnen 72 Stunden, so ist eine Begründung für die Verzögerung beizufügen (Art. 33 Abs. 1 Satz 2 DS-GVO).

Form der Meldung

Die DS-GVO schreibt eine besondere Form der Meldung nicht vor. Die Meldung kann in allen erdenklichen Arten erfolgen, also telefonisch, per Fax, per Mail oder per Briefpost[18]. In dringenden Fällen wird vor dem Hintergrund, dass die Meldung unverzüglich zu erfolgen hat, eine telefonische Kontaktaufnahme[19] mit der Aufsichtsbehörde geboten sein. Eine ausführliche Meldung kann dann zum Beispiel per Brief, per Mail oder per Fax nachgeschoben werden.[20] Der Meldepflichtige trägt die Verantwortung für einen Nachweis des Zugangs der Meldung an die Aufsichtsbehörde.[21]

Inhalt der Meldung

Die DS-GVO macht in Art. 33 Abs. 3 genaue Vorgaben über den Mindestinhalt der Meldung der Datenschutzverletzung gegenüber der Aufsichtsbehörde. Die Meldung muss zumindest Folgendes 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 und

BEISPIELE

Mögliche Schäden
Die Verletzung des Schutzes personenbezogener Daten kann einen physischen, materiellen oder immateriellen Schaden nach sich ziehen, wie etwa

- den Kontrollverlust über personenbezogene Daten,
- 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.

13 Vgl. Paal/Pauly (Hrsg.), Datenschutz-Grundverordnung, Art. 33 Rn. 26.
14 Vgl. ErwGr. 85; vgl. auch Sydow (Hrsg.), a.a.O., Art. 33 Rn. 9.
15 Vgl. Paal/Pauly (Hrsg.), a.a.O., Art. 33 Rn. 18.
16 Vgl. Sydow (Hrsg.), a.a.O., Art. 33 Rn. 13.
17 So ErwGr. 87.
18 Vgl. Gola (Hrsg.), a.a.O. Art. 33 Rn. 36.
19 Vgl. Gola (Hrsg.), a.a.O., Art. 33 Rn. 36.
20 Vgl. Marschall, Datenschutz-Praxis 8/17, 3.
21 Vgl. Gola (Hrsg.), a.a.O., Art. 33 Rn. 36.

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 Autragsverarbeiter 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. 1 g DS-GVO eingeräumt.

- 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.

Pflichten zur Dokumentation

Der Verantwortliche muss die Verletzungen des Schutzes personenbezogener Daten einschließlich aller im Zusammenhang mit der Datenschutzverletzung stehenden Fakten dokumentieren. Die Dokumentation muss auch die Auswirkungen und die ergriffenen Abhilfemaßnahmen umfassen. Sie geht damit über die reine Zusammenfassung des Vorfalls hinaus.[22] Die Dokumentation hat den Zweck, dass die Aufsichtsbehörde überprüfen kann, ob die Meldepflicht eingehalten worden ist. Dies beinhaltet aber nicht die Verpflichtung, die Dokumentation der Datenschutzverletzung der Aufsichtsbehörde zukommen zulassen. Die Dokumentation muss lediglich vorgehalten werden, um der Aufsichtsbehörde eine Kontrolle zu ermöglichen.[23] Dazu kann die Aufsichtsbehörde nach Art. 58 Abs. 1 a) DS-GVO den Verantwortlichen anweisen, die entsprechenden Informationen zur Verfügung zu stellen.

Benachrichtigung der betroffenen Person

Die Datenschutzverletzung ist aber nicht nur der Aufsichtsbehörde, sondern auch der betroffenen Person mitzuteilen. Diese Benachrichtigung muss unverzüglich erfolgen, wenn die Datenschutzverletzung voraussichtlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen zur Folge hat (Art. 34 Abs. 1 DS-GVO). Die Benachrichtigungen sollen in enger Absprache mit der Aufsichtsbehörde geschehen.[24] Zu den Begriffen »unverzüglich« und »voraussichtlich« gilt das oben Gesagte entsprechend.

Zentral für die Benachrichtigung des Betroffenen ist das voraussichtlich »hohe Risiko« für die Rechte und Freiheiten natürlicher Personen. Die DS-GVO definiert nicht, wann ein hohes Risiko voraussichtlich gegeben ist. Die Einschätzung eines »hohen Risikos« liegt beim Verantwortlichen. Er wird in diesem Fall auch eine Risikoprognose aufstellen müssen.

▸ Frist, Inhalt, Form der Benachrichtigung

Wie die Meldung an die Aufsichtsbehörde hat die Benachrichtigung des Betroffenen »unverzüglich«, also ohne schuldhaftes Zögern 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 bspw. Strafverfolgungsbehörden erteilten Weisungen zu erfolgen«. Da die Benachrichtigung mit der Aufsichtsbehörde abgesprochen werden soll, erfolgt die Benachrichtigung des Betroffenen zeitlich nach erfolgter Meldung bei der Aufsichtsbehörde[25]. Zudem ist die betroffene Person sofort zu benachrichtigen, sofern dies notwendig ist, um das Risiko eines unmittelbaren Schadens abzuwenden.[26]

In Bezug auf den Inhalt der Benachrichtigung schreibt Art. 34 Abs. 2 DS-GVO 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 DS-GVO keine Vorgaben vor. In Art. 12 DS-GVO 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 (Art. 12 Abs. 1 DS-GVO).

▸ Ausnahmen

In drei Ausnahmefällen ist eine Benachrichtigung der betroffenen Person nicht erforderlich (Art. 34 Abs. 3 DS-GVO), nämlich:

22 Sydow (Hrsg.), a.a.O., Art. 33 Rn. 28.
23 Vgl. Paal/Pauly (Hrsg.), a.a.O., Art. 33 Rn. 58.
24 So der ErwGr. 86 Satz 3.
25 Vgl. Gola (Hrsg.), a.a.O., Art. 34 Rn. 13.
26 So ErwGr. 86.

- der Verantwortliche hat geeignete technische und organisatorische Sicherheitsvorkehrungen getroffen, und diese Vorkehrungen wurden auf die von der Verletzung der betroffenen personenbezogenen Daten angewandt, insbesondere solche, durch die die personenbezogenen Daten für alle Personen, die nicht zum Zugang zu den personenbezogenen Daten befugt sind, unzugänglich gemacht werden, etwa durch Verschlüsselung;
- der Verantwortliche hat durch nachfolgende Maßnahmen sichergestellt, dass das hohe Risiko für die Rechte und Freiheiten der betroffenen Person aller Wahrscheinlichkeit nach nicht mehr besteht;
- die Benachrichtigung wäre mit einem unverhältnismäßigen Aufwand verbunden. In diesem Fall hat stattdessen eine öffentliche Bekanntmachung oder eine ähnliche Maßnahme zu erfolgen, durch die die betroffenen Personen vergleichbar wirksam informiert werden.

▸ Befugnisse der Aufsichtsbehörde

§ 34 Abs. 4 DS-GVO sieht die Möglichkeit vor, dass die Aufsichtsbehörde bei positiver Prognose eines Risikos für die Betroffenen den Verantwortlichen zur Benachrichtigung auffordern kann. Diese Möglichkeit wirkt als eine Art Korrektiv, und zwar dann, wenn der Verantwortliche die Bewertung eines Risikos einseitig zu seinen Gunsten auslegt[27] und die betroffene Person nicht benachrichtigt.

Sanktionen bei Verstößen

Für Behörden und öffentliche Stellen wird bei Datenschutzverstößen keine Geldbuße verhängt werden. Der deutsche Gesetzgeber hat insofern mit dem neuen § 43 Abs. 3 BDSG die Öffnungsklausel in der DS-GVO genutzt. Die Landesgesetzgeber werden in ihren neuen Landesdatenschutzgesetzen wahrscheinlich eine entsprechende Regelung treffen. Auch wenn kein Bußgeld verhängt wird, kann sich die Behörde aber mit ihrer Datenschutz-Panne im Tätigkeitsbericht des Bundes bzw. des Landesbeauftragten wiederfinden. Zudem können Betroffene auch gegen Behörden ihre Rechte nutzen. So kann der Betroffene Schadensersatzansprüche geltend machen, sofern er einen Schaden erleidet, zum Beispiel dadurch, dass die Benachrichtigung nach Art. 34 DS-GVO gar nicht oder nicht rechtzeitig erfolgt. Zudem kommt eine Haftung im Hinblick auf eine Datenschutzverletzung als solche in Betracht. Das kommt dann zum Tragen, wenn zwar nach Art. 34 DS-GVO eine Benachrichtigung rechtmäßig erfolgt ist, aber ein Schaden für den Betroffenen nicht bzw. nicht vollständig abgewendet werden konnte.[28]

Für nicht-öffentliche Stellen können Bußgelder verhängt werden. Für Verstöße, die den Art. 33 und 34 DS-GVO betreffen, wie zum Beispiel gegen die Verpflichtung zur Meldung von Datenschutzverletzungen gegenüber der Aufsichtsbehörde, gegen die Benachrichtigung der Betroffenen oder gegen die Verpflichtung zur Dokumentation werden gemäß Art. 83 Abs. 4 a) DS-GVO Geldbußen von bis zu 10 Millionen Euro oder im Fall eines Unternehmens von bis zu 2 Prozent seines gesamten weltweit erzielten Jahresumsatzes des vorangegangenen Geschäftsjahres verhängt, je nachdem, welcher der Beträge höher ist.

Aufgaben für den Personalrat

Personalräte sind gut beraten, sich auch mit dem Thema Datenschutz-Pannen nach Art. 33 und 34 DS-GVO zu befassen. Denn von diesen Pannen können sowohl Daten der Beschäftigten als auch Daten der Bewerber betroffen sein. Daher hat der Personalrat im Rahmen seines Überwachungsrechts nach § 68 Abs. 1 Nr. 2 BPersVG und entsprechender Vorschriften der Landespersonalvertretungsgesetze darauf zu achten, dass sich der Arbeitgeber zum Beispiel hinsichtlich der Meldepflicht gegenüber der Aufsichtsbehörde und der Benachrichtigungspflicht gegenüber dem betroffenen Beschäftigen an die Vorgaben der DS-GVO hält. Der Personalrat kann aber auch seine Mitbestimmungsrechte[29] nutzen, um den Umfang der Verarbeitung personenbezogener Daten, das Zugriffsberechtigungskonzept und die Übermittlung personenbezogener Daten an Dritte sehr genau zu regeln. Kommt es hier zu einer Datenschutz-Panne, kann der Personalrat, zusätzlich zu den Maßnahmen, die der Beschäftigte ergreifen kann, auf die Einhaltung der Dienstvereinbarung achten. ◁

Bruno Schierbaum,
BTQ Niedersachsen GmbH,
Oldenburg.

27 Vgl. Kühling/Buchner (Hrsg.), a.a.O., Art. 34 Rn. 5.

28 Vgl. Gola (Hrsg.), a.a.O., Art. 34 Rn. 17.

29 Hierzu Thannheiser, in diesem Heft ab S. 8.