Richtlinie zum Umgang mit sog. „Datenpannen“

Nach Art. 33 DSGVO sind Verletzungen des Schutzes personenbezogener Daten unverzüglich und möglichst binnen 72 Stunden an die zuständige Aufsichtsbehörde zu melden.
Art. 4 Nr. 12 DSGVO definiert dabei die „Verletzung des Schutzes personenbezogener Daten“ 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 wurde.
Wenn eine solche Verletzung voraussichtlich ein hohes Risiko für die persönlichen Rechte und Freiheiten der betroffenen Person zu Folge hat, so ist gemäß Art. 34 DSGVO neben der Aufsichtsbehörde auch die von einer Verletzung des Schutzes personenbezogener Daten betroffene Person unverzüglich zu benachrichtigen.
Im Rahmen der Bewertung einer “Datenschutzverletzung” gibt die Erheblichkeitsschwelle, die in Erwägungsgrund 85 genannt wird ein Indiz, ob eine Meldung an die Aufsichtsbehörde zu erfolgen hat.
Sollte die Bewertung ergeben, dass keine Meldung an die Aufsichtsbehörde erfolgt, wird die Datenschutzverletzung mit entsprechender Begründung, weshalb keine Meldung erfolgte, intern dokumentiert.

I. Was sind Datenpannen

Nach Art. 4 Nr.12 DSGVO ist eine Datenpanne (Verletzung des Schutzes personenbezogener Daten) **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.

Beispiele für Sachverhalte, die als Datenpanne gelten können:

- die Löschung personenbezogener Daten durch eine nicht autorisierte Person,
- Wiederherstellung eines Backups ist nicht möglich,
- Abhandenkommen eines Schlüssels zur Entschlüsselung von personenbezogenen Daten,

- Datendiebstahl etwa durch Hacking oder physisches Eindringen,
- Verlust eines mobilen betrieblichen Datenträgers (Mobiltelefon, Laptop, etc.).

Datenschutzrechtlich ist in Artt. 33 und 34 DSGVO bestimmt, wie im Falle einer Datenpanne zu verfahren ist. Das Unternehmen als datenschutzrechtlich Verantwortlicher unterliegt ggf. einer Meldepflicht des Vorfalls gegenüber der Aufsichtsbehörde und der betroffenen Person.

II. Verhalten im Falle der Kenntnisnahme einer Datenpanne

Der Umgang mit einer Datenpanne unterscheidet sich je nach Rolle des Verarbeitenden. Unterschieden wird zwischen der Rolle als Auftragsverarbeiter (dazu a) und der Rolle als Verantwortlicher (dazu b).

1. Position „Auftragsverarbeiter“

a) Erste Schritte

Sobald Sie als Auftragsverarbeiter Kenntnis von einer Datenpanne erlangen, sind Sie gem. Art. 33 Abs. 2 DSGVO dazu verpflichtet, **Ihren Auftragsgeber** von dem Vorfall **in Kenntnis** zu setzen.

Hierzu sollten Sie **neben der internen Aufklärung** der Datenpanne, Ihren Datenschutzbeauftragten **Dr. Volker Wodianka** vom Vorfall in Kenntnis setzen und mit ihm die **Meldung an** den **Auftraggeber vorbereiten**.

Da Ihr Auftragsgeber in den meisten Fällen dazu verpflichtet ist, die Datenpanne innerhalb von 72 Stunden an die zuständige Aufsichtsbehörde zu melden, sollten Sie als Auftragsverarbeiter **nach Absprache** mit Ihrem Datenschutzbeauftragten die Datenpanne **unverzüglich** an diesen **melden**. So hat Ihr Auftragsgeber genug Zeit das Ausmaß der Datenpanne zu dokumentieren. Unverzüglich heißt in diesem Kontext, **sobald** Sie die **unter II. aufgeführten Informationen gesammelt** haben.

b) Meldung an den Auftragsgeber

Die von Ihnen als Auftragsverarbeiter zu erbringende Meldung muss in Anlehnung an Art. 33 Abs. 3 DSGVO mindestens die folgenden, notwendigen Informationen enthalten:

- eine **Beschreibung der Art der Verletzung**, woraus ersichtlich wird, welche Kategorien von Daten betroffen sind, wie viele Personen ungefähr betroffen sind und wie viele Datensätze ungefähr von der Datenpanne betroffen sind,
- ggfs. eine Beschreibung der **möglichen Folgen der Datenpanne**,
- eine **Beschreibung der Maßnahmen**, die ergriffen worden sind, um die möglichen Auswirkungen der Datenpanne abzumildern.

Die **weitere Risikobewertung** der Datenpanne **obliegt Ihrem Auftraggeber**, da er Verantwortlicher der Datenverarbeitung ist. Zudem nimmt auch ausschließlich Ihr Auftragsgeber eine Meldung gegenüber der Aufsichtsbehörde vor, falls dies erforderlich ist.

2. Position „Verantwortlicher“

a) Erste Schritte

Sobald Sie Kenntnis von einer Datenpanne erhalten, sind Sie dazu verpflichtet den Fachbereichsleiter sowie dem betrieblichen Datenschutzbeauftragten **Dr. Volker Wodianka** von dem Vorfall **in Kenntnis** zu setzen. Ein **darüberhinausgehendes Handeln** Ihrerseits ist **nicht erforderlich**. Sie sind insbesondere nicht dazu berechtigt, die Datenpanne der von der Verletzung der Sicherheit betroffenen Person oder der Aufsichtsbehörde zu melden. Diese Entscheidung obliegt der Unternehmensleitung.
Die nachfolgenden Bewertungsmaßstäbe sind nicht geeignet zu entscheiden, ob Sie intern eine Datenpanne melden, da es sich bei der Frage des Umgangs mit der Datenpanne in Bezug auf bestehende Meldepflichten um eine komplexe Prüfung handelt. Bitte teilen Sie daher die o.g. Sachverhalte in jedem Fall mit.

b) Bewertung der Datenpanne

Der **Fachbereichsleiter analysiert** sodann in Zusammenarbeit **mit** dem betrieblichen **Datenschutzbeauftragten** die **Datenpanne** nach ihrem Ursprung, etwaiger Beschränkungsmöglichkeiten und Unterbindungsmaßnahmen.

Darüber hinaus ist zu überprüfen, inwieweit die Verletzung des Datenschutzes voraussichtlich zu einem **Risiko für die Rechte und Freiheit** der durch die Datenpanne betroffenen Person führt.
Kriterien für die Bewertung des bestehenden Risikos und insofern wichtige Bestandteil der internen Meldung an den Fachbereichsleiter sind:

- Art der Datenschutzverletzung
- Art, Sensibilität und Umfang der betroffenen Daten
- Identifizierbarkeit betroffener Personen
- Anzahl und besondere Eigenschaften der betroffenen Personen
- Schwere der Folgen für die betroffene Person
- ergriffene Maßnahmen, die Risiko eindämmen bzw. beschränken
- Eintrittswahrscheinlichkeit des Risikos

Zur **Bestimmung des Risikos** ist die Schwere der möglichen Folgen für die Rechte und Freiheit der betroffenen Person in Verbindung mit der Eintrittswahrscheinlichkeit dieser Folgen zu prüfen. Das Risiko steigt zum einen mit zunehmender Schwere und zum

anderen mit steigender Eintrittswahrscheinlichkeit der Folgen der Datenschutzverletzung.

Ein hohes 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.

3. Meldung der Datenpanne

Nur so weit die **Risikoabwägung** ergibt, dass keinerlei Risiken im obigen Sinne bestehen, bedarf es keiner Meldung der Datenpanne an die Aufsichtsbehörde. Sofern auch nur ein **geringfügiges Risiko** festgestellt werden kann, ist die Datenpanne der mit den Informationen nach Art.33 DSGVO **zu melden**.

Für den Fall, dass die Datenpanne **ein hohes Risiko** für die Rechte und Freiheit der betroffenen Person zur Folge hat, bedarf es neben der Meldung an die Aufsichtsbehörde **zusätzlich** einer **Meldung der Verletzung gegenüber der betroffenen Person**. Der Inhalt einer solchen Meldung ist 34 DSGVO zu entnehmen. Die Meldung gegenüber der betroffenen Person ist nicht fristgebunden.

4. Gesetzliche Frist- und Dokumentationsvorgaben

Für die Bewertung der Datenpanne stehen dem Verantwortlichen **maximal 72 Stunden** ab Kenntnisnahme von der Datenpanne zur Verfügung.
Der gesamte Vorgang ist **detailliert zu dokumentieren**, auch wenn gar keine Meldung an die Aufsichtsbehörde erfolgt. Insoweit unterliegt der Verantwortliche der Datenverarbeitung der gesetzlichen Rechenschaftspflicht aus Art.33 Abs.5, 5 Abs.2 DSGVO, die Gegenstand einer Überprüfung durch die Aufsichtsbehörde sein kann.