Universität Regensburg

Datenschutzbeauftragte

Ass. jur. Susanne Stingl

Dienstgebäude "Altes Finanzamt"
Raum 134, 1. OG.
Landshuter Straße 4
93047 Regensburg

Telefon 0941 943-5376
Fax 0941 943-5369
E-Mail dsb@ur.de

Merkblatt der Datenschutzbeauftragten

Stand: 24.08.2023

Datenpanne und was nun?

Die Universität Regensburg als datenschutzrechtlich Verantwortliche hat nach Art. 33 DSGVO „Datenpannen" unverzüglich zu melden. Eine Datenpanne liegt immer dann vor, wenn der Schutz personenbezogener Daten verletzt wurde oder eine solche Verletzung droht. Die Pflicht zur Meldung solch einer Datenpanne entsteht mit Eintritt der Verletzung.

Nach Art. 4 Nr. 12 DSGVO ist eine *„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, die übermittelt, gespeichert oder auf sonstige Weise verarbeitet wurden".*

Die Meldepflicht besteht unabhängig davon, ob personenbezogene Daten betroffen sind oder es sich um besondere Kategorien personenbezogener Daten, also besonders sensibler Daten, handelt.

Eine Ausnahme der Meldepflicht gilt jedoch, wenn die Verletzung des Schutzes der personenbezogenen Daten voraussichtlich nicht zu einem Risiko für die Rechte und Freiheiten natürlicher Personen führt. Diese Prognoseentscheidung enthält mögliche Auswirkungen der festgestellten Schutzverletzung und berücksichtigt die Eintrittswahrscheinlichkeit und die mögliche Schadensschwere.

1. Zeitpunkt der Meldung

Die Meldung des Verantwortlichen hat unverzüglich - innerhalb von 72 Stunden - zu erfolgen. Die Frist für die Meldung beginnt zu dem Zeitpunkt zu laufen, zu dem der Verantwortliche Kenntnis erlangt und die Datenpanne entdeckt wird. Dabei ist es unerheblich, von wem eine Verletzung von personenbezogenen Daten entdeckt wurde.

Sollten Sie eine Datenpanne bzw. einen Vorfall entdecken, dann zögern Sie bitte nicht, uns und Ihrer/Ihrem Vorgesetzten die Datenpanne sofort zu melden. Füllen Sie auch bitte gleich unser Formular zur Meldung einer Datenpanne aus und kontaktieren uns umgehend. So können wir schnellstmöglich reagieren, weiteren Schaden abwenden und prüfen, ob der Vorfall der/dem Landesbeauftragten für Datenschutz zu melden ist.

2. Inhalt der Meldung

Für die Meldung sind spezifische Informationen erforderlich. Auf unserer Webseite finden Sie hier ein Formular, das die wesentlichen Informationen abfragt.

Art. 33 Abs. 3 DSGVO konkretisiert den Inhalt der an die Aufsichtsbehörde zu meldenden Informationen und stellt den Mindestumfang dar. In Einzelfällen kann es erforderlich sein, dass weitere Informationen als die in Art. 33 Abs. 3 DSGVO geforderten Punkte mitgeteilt werden müssen.

Für die Aufsichtsbehörde muss es mit den gemeldeten Informationen möglich sein, sich ein umfassendes Bild des Vorfalles machen zu können. Sie muss die Form und den Umfang der Verletzung der personenbezogenen Daten nachvollziehen können und auch erkennen können, welche Risiken sich dadurch für die Betroffenen ergeben und welche Maßnahmen zur Abwehr von weiteren Verletzungen sowie zur Schadensverhinderung oder -minimierung zu ergreifen sind oder schon ergriffen worden sind.

Im Einzelnen finden Sie hier noch einmal die Mindestanforderungen an die zu meldenden Informationen:

a. Art der Verletzung des Schutzes personenbezogener Daten (Art. 33 Abs. 3 lit. a) DSGVO)

Zunächst ist die **Art der Verletzung** des Schutzes personenbezogener Daten nach Art. 33 Abs. 3 lit. a) DSGVO mitzuteilen. Hier ist an jede Verletzungshandlung zu denken, die die Sicherheit der Daten verletzt und somit ein Verletzungserfolg eintritt.

Als Verletzungserfolge sind insbesondere die Vernichtung, den Verlust oder die Veränderung personenbezogener Daten zu nennen, aber auch die Kenntnisnahme von unberechtigten Dritten entweder durch unbefugtes Offenlegen von oder den unbefugten Zugang zu personenbezogenen Daten.

Es kann an folgende Szenarien gedacht werden:

- Ist ein Gerät oder sind Unterlagen, Postsendungen verloren gegangen?
- Wurden E-Mails mit personenbezogenen Daten unverschlüsselt versendet?
- Handelt es sich um einen Hackerangriff, eine Schadsoftware oder eine Phishing-Attacke?
- Wurden Materialen oder Geräte nicht datenschutzgerecht entsorgt?
- Wurden Zugriffsrechte missbraucht oder wurden Daten unbeabsichtigt veröffentlich?
- Zeigt ein Webportal falsche oder fremde Daten an?
- Wurden personenbezogene Daten an falsche Empfänger gesendet?)

b. Betroffene personenbezogene Daten (Art. 33 Abs. 3 lit. a) DSGVO)

Entscheidend für die Bewertung einer möglichen Meldepflicht der Datenpanne an die Aufsichtsbehörde stellen auch die **betroffenen personenbezogenen Daten** nach Art. 33 Abs. 3 lit. a) DSGVO dar.

Es ist mitzuteilen, ob es sich um personenbezogene Daten oder um besondere Kategorien nach Art. 9 DSGVO handelt.

Personenbezogene Daten können bspw. folgende sein: Name und Vorname, Geburtsdatum, Anschrift/Adresse, Identifikationsdaten wie Personalausweisdaten, Lokalisationsdaten, Daten, welche die Verfolgung von Straftaten und Ordnungswidrigkeiten betreffen, die dem Steuer-, dem Sozial-, dem Berufs- oder einem besonderen Amtsgeheimnis unterliegen, …

Besondere Kategorien personenbezogener Daten sind unter anderem: rassische und ethnische Herkunft, politische Meinung, religiöse oder weltanschauliche Überzeugungen, Gewerkschaftszugehörigkeit, Genetische Daten, Biometrische Daten, Gesundheitsdaten, Daten zum Sexualleben oder der sexuellen Orientierung.

Zudem ist die ungefähre Anzahl von betroffenen Datensätzen anzugeben und wer überhaupt von diesem Vorfall betroffen ist.

c. Folgen der Verletzung des Schutzes personenbezogener Daten (Art. 33 Abs. 3 lit. c) DSGVO)

Die Aufsichtsbehörde ist daran interessiert, welche **konkreten Folgen** die Verletzung des Schutzes personenbezogener Daten nach Art. 33 Abs. 3 lit. c) DSGVO hat. Hier sollte die Beschreibung nach der jeweiligen Einschätzung der wahrscheinlichen Folgen und die mögliche Auswirkung auf die betroffenen Personen vorgenommen werden.

Entscheidend ist hierbei, ob die Vertraulichkeit, die Integrität und die Verfügbarkeit verletzt wurden.

d. Ergriffene oder geplante Maßnahmen (Art. 33 Abs. 3 lit. d) DSGVO)

Der Aufsichtsbehörde ist zudem mitzuteilen, ob bereits **technische und/oder organisatorische Maßnahmen** umgesetzt sind und sicherstellen, dass der Vorfall beendet ist und zukünftig nicht nochmals auftreten wird.

Hält die Aufsichtsbehörde die getroffenen Maßnahmen nicht für ausreichend, so liegt es in ihrem Ermessen geeignete Maßnahmen anzuordnen, um negative Folgen für die betroffenen Personen gänzlich abzuwenden oder zumindest zu minimieren.

Soweit noch keine entsprechenden Maßnahmen umgesetzt wurden, ist der Aufsichtsbehörde auch mitzuteilen, welche technischen und/oder organisatorischen Maßnahmen geplant sind, um den Vorfall zu beenden und damit der Vorfall zukünftig nicht mehr auftraten wird.

Bei derartigen Mitteilungen ist im Rahmen des Informationsumfangs auch immer an die Gefahr der Offenbarung von Betriebs- und Geschäftsgeheimnissen sowie von möglichen Verstößen gegen etwaige gesetzliche Geheimhaltungspflichten zu denken.

3. Information der Betroffenen

Der Aufsichtsbehörde ist zudem mitzuteilen, ob eine Information der betroffenen Personen über den Datenschutzvorfall stattgefunden hat. Dies ist dahingehend zu beurteilen, ob der Vorfall ein hohes Risiko für die persönlichen Rechte und Freiheiten natürlicher Personen zur

Folge hat. Ist dies der Fall, sind die betroffenen Personen unverzüglich darüber zu informieren.

Die Benachrichtigung der Betroffenen hat in klarer und einfacher Sprache zu erfolgen. Dabei ist die Art der Verletzung des Schutzes der personenbezogenen Daten darzulegen und auch die Folgen der Verletzung und bereits ergriffene oder geplante Maßnahmen anzureißen.

4. Folgen eines Verstoßes gegen die Meldepflicht

Der Verstoß gegen die Meldepflicht kann für den Verantwortlichen eine Haftung und eine Schadensersatzplicht nach Art. 82 DSGVO begründen.

Sollten Sie weitere Fragen zu dem Vorgehen bei Datenpannen haben, dann melden Sie sich gerne unter dsb@ur.de.