Die Landesbeauftragte für den Datenschutz Niedersachsen

Meldung von Datenschutzverstößen

Fragen und Antworten zur DS-GVO

Was ist ein Datenschutzverstoß?

In der Datenschutz-Grundverordnung werden alle Fälle von Datenschutzverstößen unter dem Begriff der „Verletzung des Schutzes personenbezogener Daten“ zusammengefasst. Eine solche Verletzung - auch Datenpanne genannt - liegt vor, wenn es zu einem Fall kommt, der

a) zur Vernichtung, zum Verlust oder zur Veränderung (egal ob unbeabsichtigt oder unrechtmäßig) oder

b) zur unbefugten Offenlegung von beziehungsweise zum unbefugten Zugang zu personenbezogenen Daten führt, die übermittelt, gespeichert oder auf sonstige Weise verarbeitet wurden.

Was muss ich tun, wenn ich eine Datenpanne in meinem Verantwortungsbereich bemerke?

Liegt eine Verletzung des Schutzes personenbezogener Daten vor, muss die verantwortliche Stelle gemäß Art. 33 der DS-GVO unverzüglich und **möglichst binnen 72 Stunden nach Bekanntwerden** der Verletzung eine Meldung an die Aufsichtsbehörden abgeben. Sollte diese Frist von 72 Stunden nicht eingehalten werden, muss die Verzögerung später zusammen mit der Meldung begründet werden.

Eine Meldepflicht besteht nur dann nicht, wenn die Verletzung des Schutzes personenbezogener Daten voraussichtlich nicht bzw. nur zu einem geringen Risiko für die Rechte und Freiheiten natürlicher Personen führt.

Warum ist es so wichtig, Datenschutzverstöße zu melden?

Die Verletzung des Schutzes personenbezogener Daten kann zu einem **physischen, materiellen oder immateriellen Schaden** für natürliche Personen führen, wenn nicht rechtzeitig und angemessen reagiert wird. Zu diesen möglichen Schäden zählt die DS-GVO etwa die Diskriminierung von Personen, Identitätsdiebstahl oder -betrug, finanzielle Verluste, Rufschädigung, und weitere erhebliche wirtschaftliche oder gesellschaftliche Nachteile für die Betroffenen.

Dementsprechend kann es als Ordnungswidrigkeit geahndet werden, wenn Sie trotz Pflicht eine Panne nicht melden oder eine der betroffenen Personen nicht benachrichtigen.

Wie kann ich einen Datenschutzverstoß melden?

Die Landesbeauftragte für den Datenschutz Niedersachsen hat für die Meldung von Datenschutzverstößen ein eigenes Online-Formular entwickelt. Sie finden es hier.

Ich habe aus Versehen personenbezogene Daten gelöscht. Muss ich das auch melden?

In der Regel müssen Sie das. Denn nach DS-GVO ist es nicht nur meldepflichtig, wenn Dritte unberechtigt Kenntnis von Daten erlangen, sondern auch wenn diese versehentlich gelöscht oder vernichtet werden.

Wann führt die Verletzung des Schutzes personenbezogener Daten voraussichtlich nicht zu einem Risiko im Sinne des Art. 33 Abs. 1 DS-GVO, sodass die Meldepflicht entfällt?

Die DS-GVO verfolgt den **risikobasierten Ansatz**. Verschiedene Pflichten treffen Verantwortliche nur, oder nur in bestimmter Form, wenn z.B. ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen vorliegt.

Dass eine Verarbeitung **kein** Risiko birgt, ist nicht denkbar. Art. 33 DS-GVO ist daher so zu lesen, dass die Meldepflicht entfällt, wenn nur ein **geringes** Risiko für die Rechte und Freiheiten natürlicher Personen besteht. Bei der Ermittlung des Risikos spielt neben der Art der betroffenen Daten auch der Umfang eine Rolle (wie viele Daten von wie vielen Personen sind betroffen).

Beispiele für geringes Risiko:

- Unbefugte haben Zugang zu personenbezogenen Daten erhalten oder sich verschafft, die aber verschlüsselt sind: Eine Verletzung der Vertraulichkeit von (nach dem Stand der Technik) verschlüsselten Daten, die mit einer bisher nicht „geknackten“ Methode verschlüsselt wurden, birgt ein sehr geringes Risiko für die Rechte und Freiheiten der betroffenen Personen. Die Daten sind nämlich für Dritte faktisch nicht lesbar. Hier ist jedoch zu bedenken, ob es auch zu einer Verletzung der Verfügbarkeit gekommen ist: Wenn die Daten etwa gestohlen wurden und daher nun für den Verantwortlichen verloren sind, kann auch bei verschlüsselten Daten ein zu meldender Datenschutzverstoß vorliegen. Hier kommt es dann auf die Art der verlorenen Daten an: die verlorene Geburtstagliste der Abteilung dürfte nur ein geringes Risiko darstellen (keine Meldepflicht), der Verlust sämtlicher Kundenkontaktdaten jedoch wenigstens ein mittleres (Meldepflicht).

- Verlust eines verschlüsselten USB-Sticks oder Smartphones: Siehe bereits vorheriges Beispiel. Sollte allerdings lediglich ein einfacher Zugriffschutz aktiviert sein, der in der Vergangenheit bereits überwunden wurde, liegt eher ein mittleres Risiko vor.

- Fehlversandter Brief kam ungeöffnet zurück: Wenn verschlossene Briefe – egal ob mit der Hauspost oder einem Postdienstleister versandt – ungeöffnet zurückkommen, weil sie den falschen Empfänger erreicht haben und dieser sie hat zurückgehen lassen, besteht in der Regel ein nur geringes Risiko für die betroffene Person.

- Brief mit falscher Anlage: Wenn aus der Anlage lediglich Namen und Daten zu z.B. gebuchten Hotelzimmern (einschließlich Zeiträumen) hervorgehen, ist das Risiko eher gering. Anders zu beurteilen ist der Fall, wenn der Brief bzw. die Anlage die vollständigen Anschriften oder gar Bankverbindungen der betroffenen Personen enthält – dann ist nicht von einem nur geringen Risiko auszugehen und die Meldepflicht besteht.

Wann liegt ein „hohes Risiko“ im Sinne des Art. 34 Abs. 1 DS-GVO vor, d.h., wann sind die betroffenen Personen zu benachrichtigen?

Nicht jeder voraussichtlich eintretende Schaden führt dazu, dass die betroffenen Personen benachrichtigt werden müssen. Eine Benachrichtigung ist erforderlich, wenn mit **erheblichen Konsequenzen bzw. schwerwiegenden Beeinträchtigungen** zu rechnen ist. Es kann sinnvoll sein, sich die Frage zu stellen: **„Könnten die betroffenen Personen etwas tun, das ihr eigenes Schadensrisiko verringert?“** (Z.B. Änderung des Passwortes bei gehackten Online-Accounts, Sperrung der Kreditkarte bei gestohlenen Kreditkartendaten)

Wenn die Antwort auf diese Frage „Ja.“ lautet, sollten Sie in aller Regel benachrichtigen.

Die Abgrenzung, wann ein „hohes“ Risiko vorliegt, statt nur eines „mittleren“ ist wichtig, um zu erkennen, ob die Benachrichtigungspflicht nach Art. 34 Abs. 1 DS-GVO greift.

Beispiele:

- Gelangen Bankverbindungen an unbefugte Dritte, kann ein hohes Risiko vorliegen, sodass auch die Betroffenen zu benachrichtigen wären. Das hohe Risiko entfällt insbesondere, wenn die Unterlagen nach glaubhafter Angabe aller Empfänger vernichtet wurden bzw. dem Absender unbeschädigt und ohne dass eine Kopie angefertigt wurde zurückgegeben wurden. Eine Benachrichtigung der Betroffenen ist dann nicht mehr erforderlich. Sofern alle diese Feststellungen binnen der Meldefrist getroffen werden konnten, muss Sie also lediglich eine Meldung an die Aufsichtsbehörde unter Darlegung dieser Umstände abgeben.

- Der Verantwortliche konnte sofort denjenigen, der sich unrechtmäßig Zugang zu personenbezogenen Daten verschafft hat, identifizieren und davon abhalten, die Daten irgendwie weiterzuverwenden. Sollte es sich jedoch um sehr sensible Daten gehandelt haben, insbesondere von wenigen Individuen, sodass sie der Täter sich gemerkt haben könnte – z.B. über Erkrankungen der betroffenen Personen – ist dennoch von einem schweren Bruch der Vertraulichkeit und damit einer Benachrichtigungspflicht auszugehen.

Ich habe bemerkt, dass bei einem anderen Verantwortlichen eine Verletzung des Schutzes personenbezogener Daten in seinem Verantwortungsbereich vorliegt. Muss ich eine Meldung nach Art. 33 Abs. 1 DS-GVO an die Aufsichtsbehörde machen?

Die Pflicht der Meldung nach Art. 33 Abs. 1 DS-GVO trifft **nur datenschutzrechtlich „Verantwortliche“** im Sinne des Art. 4 Nr. 7 DS-GVO. Nach Auffassung der Landesbeauftragten für den Datenschutz Niedersachsen wird ein Unternehmen oder eine Behörde nicht zum „Verantwortlichen“, wenn es oder sie z.B. Empfänger eines irrtümlich versendeten Faxes, einer E-Mail oder Briefes ist. Solche „Irrläufer“ sollten Sie unmittelbar vernichten. Briefe sollten Sie ungeöffnet an den Zusteller zurückgeben. Sie sollten zudem jede weitere

Kenntnisnahme des Inhalts vermeiden, sobald festgestellt wurde, dass es sich um einen „Irrläufer“ handelt. Beschäftigte sollten entsprechend unterwiesen werden.

Muss ich einen anderen Verantwortlichen darüber informieren, dass in seinem Verantwortungsbereich eine Verletzung des Schutzes personenbezogener Daten nach Art. 33 DS-GVO vorgekommen ist?

Die DS-GVO schreibt niemandem vor, einen anderen Verantwortlichen über dessen Verletzung des Schutzes personenbezogener Daten zu informieren. Dies gilt unabhängig davon, auf welche Weise Sie von dieser Datenschutzverletzung erfahren haben.

Allerdings ist besonders in Fällen fehlgegangener Faxe, am falschen Drucker ausgedruckter Dokumente oder auch irrtümlich in Briefumschläge gelangter Dokumente (zu dem eigentlich richtig zugestellten Dokument hinzu) ein Hinweis an den jeweiligen Verantwortlichen für diesen sicher hilfreich. Er kann dann die Meldepflicht nach Art. 33 DSGVO selbst prüfen und ggf. weitere Schritte einleiten.

Eine Sonderregelung besteht für **Auftragsverarbeiter** gegenüber dem Verantwortlichen, für den sie tätig sind. Nach Art. 33 Abs. 2 DS-GVO müssen sie Datenschutzverstöße dem Verantwortlichen melden. Grund ist vor allem, dass es sich dabei um Verstöße im Verantwortungsbereich des Verantwortlichen handelt, die dieser wiederum ggf. der Aufsichtsbehörde melden muss.

Die Landesbeauftragte für den Datenschutz Niedersachsen
Prinzenstraße 5
30159 Hannover
Telefon 0511 120-4500
Fax 0511 120-4599
E-Mail an Ansprechpartner schreiben