



Melde- und Benachrichtigungspflichten bei Datenschutzverletzungen

Nach der Europäischen Datenschutzgrundverordnung (DS-GVO) unterliegen Unternehmen im Falle einer Verletzung des Schutzes personenbezogener Daten folgenden Pflichten:

- Meldepflicht gegenüber der Aufsichtsbehörde (Artikel 33)
- Benachrichtigungspflicht des Betroffenen (Artikel 34).

I. Meldepflicht gegenüber Aufsichtsbehörde

1. Für wen gilt die Meldepflicht?

Adressat der Regelung ist jeder Verantwortliche im Sinne der DS-GVO. Dies ist jede natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die – allein oder gemeinsam – über die Zwecke und Mittel der Verarbeitung personenbezogener Daten entscheidet. Innerhalb eines Unternehmensverbundes können auch mehrere als gemeinsam Verantwortliche kooperieren, so genannte Joint Controllers.

Liegt eine Auftragsverarbeitung vor, ist der Auftragsverarbeiter verpflichtet, den Verantwortlichen unverzüglich über die Verletzung personenbezogener Daten zu informieren. Dieser nimmt dann die Meldung an die Aufsichtsbehörde vor.

2. Wann besteht die Meldepflicht?

Grundsätzlich ist ein Unternehmen verpflichtet, jede Verletzung des Schutzes personenbezogener Daten an die zuständige Aufsichtsbehörde zu melden. Nach Artikel 4 Nr. 12 DS-GVO stellt jede Verletzung der Sicherheit, die 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, eine meldepflichtige Verletzung dar. Es kommt dabei nicht darauf an, ob dies unbeabsichtigt oder unrechtmäßig erfolgte.

Die Meldung ist unverzüglich und möglichst binnen 72 Stunden vorzunehmen. Kann die 72-Stunden-Frist nicht eingehalten werden, ist der Meldung eine Begründung für die Verzögerung beizufügen. Eine Meldung kann ausnahmsweise unterbleiben, wenn die Datenschutzverletzung nicht zu einem Risiko für die Rechte und Freiheiten der betroffenen Personen führt.

Ein Risiko – und damit eine Meldepflicht – besteht nach Erwägungsgrund 75 der DS-GVO immer bei Verarbeitungen, die

- zu physischem, materiellen oder immateriellen Schaden,
- Diskriminierung, Identitätsdiebstahl/-betrug, finanziellem Verlust, Rufschädigung, Vertraulichkeitsverlust von dem Berufsgeheimnis unterliegenden personenbezogenen Daten, unbefugter Aufhebung der Pseudonymisierung, erheblichen wirtschaftlichen oder gesellschaftlichen Nachteilen führen können
- betroffene Personen um Rechte und Freiheiten bringt oder diese an der Kontrolle personenbezogener Daten hindert
- rassische oder ethnische Herkunft, politische Meinung, religiöse oder weltanschauliche Überzeugungen, Gewerkschaftszugehörigkeit, genetische Daten, Gesundheitsdaten, Angaben zum

Sexualleben, strafrechtliche Verurteilungen betreffen

- Arbeitsleistung, wirtschaftliche Lage, Gesundheit, persönliche Vorlieben, Zuverlässigkeit, Verhalten, Aufenthaltsort, Ortswechsel betreffen, analysieren oder prognostizieren zwecks Profilings
- personenbezogene Daten schutzbedürftiger Personen, insbesondere Kinder, betreffen
- große Mengen personenbezogener Daten und eine große Anzahl von betroffenen Personen betreffen.

3. Inhalt der Meldung

Die Meldung an die Aufsichtsbehörde muss mindestens die Beschreibung der Art der Verletzung, die Angabe von Kategorien und ungefährender Zahl der Betroffenen und der Datensätze enthalten. Außerdem ist Name und Kontakt des Datenschutzbeauftragten zu nennen. Abschließend hat eine Beschreibung der wahrscheinlichen Folgen der Datenschutzverletzung sowie der von dem Verantwortlichen ergriffenen und vorgeschlagenen Maßnahmen zur Behebung zu erfolgen.

II. Benachrichtigungspflicht gegenüber dem Betroffenen

1. Wann ist zu benachrichtigen?

Hat die Datenschutzverletzung voraussichtlich ein hohes Risiko für die persönlichen Rechte und Freiheiten der betroffenen Person zur Folge, hat der Verantwortliche den Verstoß nicht wie dargestellt nur der zuständigen Aufsichtsbehörde zu melden, sondern muss darüber hinaus die betroffene Person ohne unangemessene Verzögerung benachrichtigen.

2. Ausnahme von der Benachrichtigungspflicht

Eine Benachrichtigung muss nicht erfolgen, wenn

- Risiken für die betroffene Person durch geeignete technische und organisatorische Sicherheitsvorkehrungen ausgeschlossen wurden oder
- der Verantwortliche durch nachfolgende Maßnahmen sichergestellt hat, dass das hohe Risiko für Rechte und Freiheiten der betroffenen Person nicht mehr besteht oder
- dies mit einem unverhältnismäßigen Aufwand verbunden wäre. In diesem Fall hat eine öffentliche Bekanntmachung o. ä. zu erfolgen.

3. Inhalt der Benachrichtigung

Die Benachrichtigung muss Angaben über die Art der Verletzung, die wahrscheinlichen Folgen sowie die zur Behebung ergriffenen oder vorgeschlagenen Maßnahmen enthalten. Diese Angaben müssen in klarer und einfacher Sprache abgefasst werden. Darüber hinaus sind Name und Kontakt des Datenschutzbeauftragten zu nennen.

III. Was passiert bei Verstoß gegen die Melde-/ oder Benachrichtigungspflicht?

Bei Verstoß gegen die Pflichten aus Artikel 33 und 34 können Bußgelder von bis zu zwei Prozent des weltweit erzielten Jahresumsatzes des vorangegangenen Geschäftsjahrs verhängt werden.

Rechtshinweis

Die Veröffentlichung von Merkblättern ist ein Service der IHK Trier für ihre Mitgliedsunternehmen. Dabei handelt es sich um eine zusammenfassende Darstellung der rechtlichen Grundlagen, die nur erste Hinweise enthält und keinen Anspruch auf Vollständigkeit erhebt. Eine anwaltliche Beratung im Einzelfall kann dadurch nicht ersetzt werden. Obwohl dieses Merkblatt mit größtmöglicher Sorgfalt erstellt wurde, kann eine Haftung für die inhaltliche Richtigkeit nicht übernommen werden.