EU-Datenschutz-Grundverordnung – Nr. 11

Melde- und Benachrichtigungspflichten bei Datenschutzverletzungen

Nach der Europäischen Datenschutzgrundverordnung (DS-GVO) unterliegen Unternehmen im Falle einer Verletzung des Schutzes personenbezogener Daten folgenden Pflichten: der Meldepflicht gegenüber der Aufsichtsbehörde gemäß Art. 33 und der Benachrichtungspflicht des Betroffenen gemäß Art. 34. Diese Pflichten sind im Vergleich zu der bisher geltenden Regelung des § 42a Bundesdatenschutzgesetz (BDSG) umfangreicher.

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 entscheidet. Innerhalb eines Unternehmensverbundes können auch mehrere als gemeinsam Verantwortliche kooperieren, sog. Joint Controllers.

Liegt eine Auftragsverarbeitung vor, ist der Auftragsverarbeiter verpflichtet, den Verantwortlichen unverzüglich 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 DSGVO stellt jede 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, eine meldepflichtige Verletzung dar.

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 solchen 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,
- die rassische oder ethnische Herkunft, politische Meinung, religiöse oder weltanschauliche Überzeugungen, Gewerkschaftszugehörigkeit, genetische Daten, Gesundheitsdaten, Angaben zum Sexualleben oder strafrechtliche Verurteilungen betreffen,
- die Arbeitsleistung, wirtschaftliche Lage, Gesundheit, persönliche Vorlieben, Zuverlässigkeit, Verhalten, Aufenthaltsort oder den Ortswechsel betreffen, analysieren oder prognostizieren zwecks Profilings,
- personenbezogene Daten schutzbedürftiger Personen, insbesondere Kinder, betreffen oder
- 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 ungefährer Zahl der Betroffenen und der Datensätze enthalten. Außerdem ist Name und Kontakt des Datenschutzbeauftragten zu benennen. Abschließend hat eine Beschreibung der wahrscheinlichen Folgen der Datenschutzverletzung, sowie der von dem Verantwortlichen ergriffenen und vorgeschlagenen Maßnahmen zur Behebung zu erfolgen.

- ➢ Es muss im Unternehmen geregelt sein/werden, wie die interne Meldung und an wen (Verantwortlicher/betrieblicher Datenschutzbeauftragter/IT-Sicherheitsbeauftragter) zu erfolgen hat.
- ➢ Ist eine Meldung notwendig, sind aber noch keine Einzelheiten der Verletzung bekannt, sollte innerhalb der 72 Stunden eine kurze Meldung an die Aufsichtsbehörde erfolgen mit dem Hinweis, dass weitere Einzelheiten folgen werden.
- ➢ Die Aufsichten beabsichtigen, für eine Meldung von Datenverletzungen ein Internet-basiertes Formular zur Verfügung zu stellen.

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 Sprach abgefasst werden. Darüber hinaus sind Name und Kontakt des Datenschutzbeauftragten zu nennen.

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

Die DS-GVO sieht vor, dass bei einem Verstoß gegen die Pflichten aus Artikel 33 und 34 Bußgeldern von bis zu zwei Prozent des weltweit erzielten Jahresumsatzes des vorangegangen Geschäftsjahres verhängt werden können.

Hiervon trifft § 43 Abs. 4 BDSG-neu eine abweichende Regelung: Danach kann eine Meldung nach Art. 33 DS-GVO oder eine Benachrichtigung nach 34 DS-GVO in einem Ordnungswidrigkeitenverfahren gegen den Meldepflichtigen oder Benachrichtigenden nur mit dessen Zustimmung verwendet werden. Ob diese Abweichung im nationalen Recht zukünftig Bestand haben wird, bleibt abzuwarten. Über die Vereinbarkeit der Ausnahme mit Europarecht besteht aktuell Uneinigkeit. Letztendlich werden wohl die Gerichte hierüber entscheiden. Es empfiehlt sich daher aus Unternehmersicht, sich an den Anforderungen der DS-GVO zu orientieren und die weitere Entwicklung aufmerksam zu beobachten.

Weitere Dokumente:

Hinweise des Bayerischen Landesamts für Datenschutzaufsicht: https://www.lda.bayern.de/media/baylda_ds-gvo_8_data_breach_notification.pdf

Stand: September 2017

Mitgliedsunternehmen der IHK Bonn/Rhein-Sieg erteilt weitere Information:

Detlev Langer, Tel: 0228/2284 134, Fax: 0228/2284-222, Mail: langer@bonn.ihk.de
Tamara Engel, Tel: 0228/2284 208, Fax: 0228/2284-222, Mail: engel@bonn.ihk.de
Bonner Talweg 17, 53113 Bonn, www.ihk-bonn.de

Verantwortlich: Deutsche Industrie- und Handelskammertag DIHK, Breite Str. 29, 10178 Berlin, www.dihk.de