EU-Datenschutz-Grundverordnung (DSGVO): Meldung von Datenschutzverletzungen (Data Breach Notification)

Welche Pflichten sind bei Datenschutzverletzungen zu beachten?

Stand: 29.05.2018

Hinweis:
Die Bestimmungen der DSGVO und des österreichischen Datenschutzgesetzes (DSG) in der Fassung des Datenschutz-Anpassungsgesetzes 2018 und des Datenschutz-Deregulierungs-Gesetzes 2018 gelten seit 25.5.2018. Alle Datenverarbeitungen müssen dieser Rechtslage entsprechen. (Siehe dazu „Überblick")

Die DSGVO definiert eine „Verletzung des Schutzes personenbezogener Daten" (data breach) 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 wurden.

Als **„data breach"** kann daher z.B. ein Vorfall verstanden werden, durch den Unbefugten der Zugriff auf Daten möglich wird (z.B. Verlust eines Datenträgers, Hackerangriff ...). Dadurch kann den betroffenen Personen ein physischer, materieller oder immaterieller Schaden entstehen, wie etwa Verlust der Kontrolle über ihre personenbezogenen Daten, Identitätsdiebstahl oder –betrug, finanzielle Verluste, Rufschädigung, Verlust der Vertraulichkeit von dem Berufsgeheimnis unterliegenden Daten oder andere erhebliche wirtschaftliche oder gesellschaftliche Nachteile.

Daher sieht die DSGVO für den Fall einer solchen Verletzung des Schutzes personenbezogener Daten folgende Melde- und Benachrichtigungspflichten vor:

1. Meldung an die zuständige **Aufsichtsbehörde,** wenn die Verletzung des Schutzes personenbezogener Daten voraussichtlich zu einem **Risiko** für die Rechte und Freiheiten natürlicher Personen führt sowie
2. Benachrichtigung der **betroffenen Person**, wenn die Verletzung des Schutzes personenbezogener Daten voraussichtlich ein **hohes Risi**ko für die persönlichen Rechte und Freiheiten natürlicher Personen zur Folge hat.

Wird dem Auftragsverarbeiter eine Verletzung des Schutzes personenbezogener Daten bekannt, so muss er diese unverzüglich dem Verantwortlichen melden.

Meldung an die Aufsichtsbehörde

Die Meldung einer Datenschutzverletzung an die Aufsichtsbehörde muss unverzüglich und möglichst binnen 72 Stunden nachdem dem Verantwortlichen diese Verletzung bekannt wurde, erfolgen. Erfolgt die Meldung erst nach Ablauf von 72 Stunden, so ist diese Verzögerung zu begründen.

Die Meldung hat zumindest folgende Informationen zu enthalten:

- eine Beschreibung der Art der Verletzung des Schutzes personenbezogener Daten (wenn möglich mit Angabe der Kategorien und der ungefähren Zahl der betroffenen Personen, der betroffenen Kategorien und der ungefähren Zahl der personenbezogenen Datensätze),
- den Namen und die Kontaktdaten des Datenschutzbeauftragten oder einer sonstigen Anlaufstelle für weitere Informationen,
- eine Beschreibung der wahrscheinlichen Folgen der Verletzung des Schutzes personenbezogener Daten,
- eine Beschreibung der vom Verantwortlichen ergriffenen oder vorgeschlagenen Maßnahmen zur Behebung der Datenschutzverletzung und gegebenenfalls Maßnahmen zur Abmilderung ihrer möglichen nachteiligen Auswirkungen.

Der Verantwortliche muss alle Verletzungen des Schutzes personenbezogener Daten einschließlich aller damit im Zusammenhang stehenden Fakten (Auswirkungen, ergriffene Abhilfemaßnahmen) dokumentieren. Diese Dokumentation dient der Aufsichtsbehörde zur Überprüfung der korrekten Einhaltung der Meldepflicht.

Hinweis:
Ein Muster findet sich unter EU-Datenschutz-Grundverordnung (DSGVO): Data Breach Notification - Muster Meldung an die Aufsichtsbehörde.

Benachrichtigung der betroffenen Person

Die betroffene Person ist im Falle eines voraussichtlich hohen Risikos unverzüglich von der Datenschutzverletzung zu benachrichtigen. Diese Benachrichtigung muss zumindest Folgendes beinhalten:

- eine Beschreibung der Art der Verletzung des Schutzes personenbezogener Daten in klarer und einfacher Sprache,
- den Namen und die Kontaktdaten des Datenschutzbeauftragten oder einer sonstigen Anlaufstelle für weitere Informationen,
- eine Beschreibung der wahrscheinlichen Folgen der Datenschutzverletzung,
- eine Beschreibung der vom Verantwortlichen ergriffenen oder vorgeschlagenen Maßnahmen zur Behebung der Verletzung des Schutzes personenbezogener Daten und gegebenenfalls Maßnahmen zur Abmilderung ihrer möglichen nachteiligen Auswirkungen.

Eine Benachrichtigung der betroffenen Person ist nicht erforderlich, wenn

- auf die von der Verletzung betroffenen personenbezogenen Daten geeignete technische und organisatorische Sicherheitsvorkehrungen angewandt wurden (insbesondere wenn dadurch unbefugte Personen keinen Zugang zu diesen Daten haben, etwa durch Verschlüsselung),
- der Verantwortliche durch nachträgliche Maßnahmen sichergestellt hat, dass das hohe Risiko für die Rechte und Freiheiten der betroffenen Person aller Wahrscheinlichkeit nach nicht mehr besteht, oder
- die Benachrichtigung mit einem unverhältnismäßigen Aufwand verbunden wäre. In diesem Fall muss jedoch eine öffentliche Bekanntmachung erfolgen, oder eine ähnliche Maßnahme ergriffen werden, damit die betroffenen Personen vergleichbar wirksam informiert werden.

Hinweis:
Ein Muster findet sich unter EU-Datenschutz-Grundverordnung (DSGVO): Data Breach Notification - Muster Benachrichtigung der betroffenen Person.

Geldstrafen

Bei Verstößen gegen diese Melde- und Benachrichtigungspflicht drohen Geldbußen von bis zu EUR 10 Mio oder im Fall eines Unternehmens von bis zu 2 % des gesamten weltweit erzielten Jahresumsatzes des vorangegangenen Geschäftsjahres.

Relevante Artikel der DSGVO: Art 4 Z 12, Art 33, Art 34

Relevante Erwägungsgründe: 85 - 88

Quelle:https://www.wko.at/service/wirtschaftsrecht-gewerberecht/EU-Datenschutz-Grundverordnung:-Meldung-von-Datenschutzve.html