Umgang mit Datenpannen

Die DS-GVO regelt in den Artikeln 33 und 34 den Umgang bei Datenpannen. Dabei sieht die DS-GVO eine abgestufte Meldepflicht vor:

1. Eine Meldung an die Aufsichtsbehörde hat immer zu erfolgen, es sei denn, dass die Datenpanne „voraussichtlich nicht zu einem Risiko“ für den Betroffenen führt.

2. Eine Benachrichtigung der betroffenen Person muss dagegen nur dann erfolgen, wenn ein *hohes* Risiko für deren Rechte und Freiheiten besteht.
Auch ist eine Information des Betroffenen nicht (mehr) erforderlich, wenn geeignete technische und organisatorische Maßnahmen vorhanden sind, die den Unbefugten Zugang auf die personenbezogenen Daten praktisch nicht ermöglichen – als explizites Beispiel ist die Verschlüsselung genannt.
Ebenso kann auf eine Benachrichtigung des Betroffenen verzichtet werden, wenn wirksame Maßnahmen zur Schadensbegrenzung ergriffen wurden und diese das hohe Risiko, das zum Zeitpunkt der Datenpanne bestand, eliminiert haben. Wie dieses Szenario in der Praxis ablaufen kann, muss insbesondere von Seiten der Aufsichtsbehörden noch geklärt werden.

Jeden Vorfall der Aufsichtsbehörde melden?

Wer die deutsche mit der englischen Fassung der DS-GVO vergleicht, stellt schnell fest, dass es sich nicht um einen Übersetzungsfehler handelt, sondern in der Tat vom Grundsatz her jede Verletzung des Schutzes personenbezogener Daten der zuständigen Aufsichtsbehörde gemeldet werden muss, es sei denn, dass sie „voraussichtlich nicht zu einem Risiko“ des Betroffenen führt
bzw. „unlikely to result in a risk“. Dies könnte sich jedoch im Alltag eines Unternehmens als große Herausforderung herausstellen, da bei den meisten Vorfällen nicht auszuschließen ist, dass ein solches Risiko besteht. Von daher ist zu erwarten, dass sich die Aufsichtsbehörden hierzu näher abstimmen, damit verständlich wird, nach welchen Kriterien eine Risikobewertung stattfindet und wann konkret eine Meldung erforderlich wird.

Umfang und Zeitpunkt der Meldung

Die Meldung der Datenpanne muss innerhalb von 72 Stunden bei der zuständigen Aufsichtsbehörde stattfinden. Ein Überschreiten der Frist ist nur in begründeten Fällen möglich. Meldungen nach Art. 33 DS-GVO umfassen u. a. die Art der Datenpanne, die Kategorien von betroffenen Daten, die Anzahl der Betroffenen und der Datensätze, eine Einschätzung der Folgen für den Betroffenen sowie die Maßnahmen zur Ursachenbeseitigung bzw. zur Schadensminimierung beim Betroffenen.