EU-Datenschutz-Grundverordnung (DS-GVO)

Das BayLDA auf dem Weg zur Umsetzung der Verordnung

Wichtiger Hinweis zu diesem Dokument:
Die DS-GVO wird nach der Übergangsphase von zwei Jahren am 25. Mai 2018 wirksam. Die Aufsichtsbehörden sind aktuell bemüht, durch intensive Abstimmungsrunden eine einheitliche Sichtweise der neu geregelten Grundlagen und Anforderungen an den Datenschutz auf europäischer Ebene zu erzielen. Das BayLDA beteiligt sich deshalb an verschiedenen Arbeitskreisen, die sich dieser Herausforderung auch in Deutschland stellen. In der Zwischenzeit möchte das BayLDA Interessierten einen Einblick gewähren, welche Themenkomplexe der DS-GVO derzeit auch in der bayerischen Aufsichtsbehörde intensiv diskutiert werden. Das BayLDA veröffentlicht deshalb in regelmäßigen Abständen (geplant: zweimal im Monat) ein kurzes Papier zu einem ausgewählten Schwerpunkt. Das BayLDA weist ausdrücklich darauf hin, dass es sich hierbei um keine verbindlichen Auffassungen handelt, sondern um gegenwärtige Interpretationen und Meinungen zur DS-GVO. Kommentare zum dargestellten gegenwärtigen Verständnis nimmt das BayLDA gerne entgegen.

VIII Umgang mit Datenpannen – Art. 33 und 34 DS-GVO

Es kann (fast) jeden treffen

Gehackt, bestohlen oder verloren. Die Möglichkeiten, dass personenbezogene Daten in unbefugte Hände gelangen, sind vielseitig: Sei es bspw. eine Webanwendung, die eine bislang unbekannte SQL-Injection-Lücke aufweist, ein neuer Bug im Webserver, der einen Vollzugriff auf Systemebene ermöglicht, ein verloren gegangener USB-Stick oder ein Einbruch in den schlecht gesicherten Serverraum, der mit einem Verlust der Backup-Platten einhergeht.

Stand heute: Hohe Hürden für eine Meldung

Bereits heute sind manche dieser unbefugten Datenzugriffe, umgangssprachlich *Datenpannen* genannt, meldepflichtig. Nach § 42a BDSG müssen dafür allerdings *zwei* Voraussetzungen erfüllt sein:

1. Die personenbezogenen Daten müssen als sehr sensibel gelten, was z. B. bei Bank- und Gesundheitsdaten der Fall ist.
2. Zusätzlich muss davon auszugehen sein, dass im konkreten Vorfall ein hohes Risiko für den Betroffenen gegeben ist, d. h. *schwerwiegende Beeinträchtigungen* drohen.

Diese Voraussetzungen führen heute dazu, dass nur vereinzelt Meldungen an die zuständige Aufsichtsbehörde gemacht werden. Die jährliche Gesamtzahl solcher Meldungen bewegt sich daher meist nur in einem zweistelligen Bereich. Eine sehr große Dunkelziffer bezüglich nicht erkannter und nicht gemeldeter (Hacking-) Vorfälle kann durchaus vermutet werden. Sofern jedoch eine meldepflichtige Datenpanne vorliegt, ist auch der Betroffene zu informieren.

Stand morgen: Deutlich abgesenkte Hürden

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.

Die Meldung ist kein Wunschkonzert

Die Verpflichtung zur Meldung von Datenpannen ist durchaus ernst zu nehmen - das zeigt schon alleine der mögliche Bußgeldrahmen von bis zu 10 Mio. Euro bzw. 2% des Umsatzes.

Ausblick zur Meldung von Datenpannen

Wenn sensible Daten im Unternehmen abhandenkommen, drohen meist schwer zu kalkulierende Auswirkungen - vom Vertrauensverlust bei Kunden, Image-Schäden gegenüber Geschäftspartnern bis hin zu großen finanziellen Einbußen, die sich auf das Jahresergebnis niederschlagen können. Schon heute zeigt sich, dass eine aktive und umfassende Zusammenarbeit mit der Aufsichtsbehörde nicht nur hilft, die Schäden hierbei besser einzugrenzen, sondern auch geeignet ist, um die Betroffenen fachgerecht zu informieren.

Spannende Fragen werden nun sicherlich sein, ob die Verantwortlichen den neuen umfassenderen Anforderungen zur Meldung von Datenpannen nachkommen und inwieweit auch die Aufsichtsbehörden mit dem wahrscheinlichen Anstieg von Meldungen organisatorisch zurechtkommen. Das BayLDA bereitet derzeit einen Online-Service für verantwortliche Stellen zur effizienten Datenpannen-Meldung vor.