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.

VII Sanktionen nach der DS-GVO

Umfassende Bußgeldandrohungen
Die Datenschutz-Grundverordnung stellt in Art. 83 Abs. 4 bis 6 eine deutlich breitere Palette an Verstößen unter Bußgeldandrohung als das derzeit noch geltende Bundesdatenschutzgesetz. Die *weitaus meisten* Vorschriften der DS-GVO, in denen Pflichten für Verantwortliche oder Auftragsverarbeiter geregelt sind, sehen bei Verstoß die Möglichkeit einer *Geldbuße* vor. Nach dem Willen des europäischen Gesetzgebers (so Erwägungsgrund 148) sollen Verstöße gegen bußgeldbewehrte Pflichten der DS-GVO grundsätzlich eine Sanktion zur Folge haben. Ausnahmen soll es *nur bei geringfügigen Verstößen* sowie in Fällen geben, in denen eine Geldbuße gegen eine natürliche Person unverhältnismäßig belastend wäre.

Geldbuße droht auch bei technisch-organisatorischen Verstößen
Nach der DS-GVO stellt nun auch der Verstoß gegen die Pflicht zur Ergreifung geeigneter und angemessener technischer und organisatorischer Maßnahmen zum Schutz personenbezogener Daten eine Ordnungswidrigkeit dar. Dies ist eine *wichtige Neuerung* gegenüber dem heute noch geltenden Recht.

Besonders bemerkenswert ferner:
Auch Verstöße Verantwortlicher gegen die Pflichten zu datenschutzfreundlicher Technikgestaltung und zu datenschutzfreundlichen Voreinstellungen können zu Geldbußen führen.

Dies unterstreicht insgesamt die *große Bedeutung*, die der Gesetzgeber den technisch-organisatorischen Maßnahmen und den Grundsätzen „privacy by design“ und „privacy by default“ für einen effektiven Datenschutz zumisst.

Mögliche Adressaten von Geldbußen
Geldbußen können gegen

- Verantwortliche oder
- Auftragsverarbeiter

verhängt werden.

Daneben können aber auch

- Zertifizierungsstellen sowie
- Stellen, die zur Überwachung sog. genehmigter Verhaltensregeln (CoC) akkreditiert sind,

bei Verstößen gegen ihre Verpflichtungen mit Geldbuße belegt werden.

Hierbei ist davon auszugehen, dass Unternehmen für Verstöße, die durch ihre Mitarbeiter begangen werden, grundsätzlich einstehen müssen und somit geahndet werden können. Inwieweit auch Geldbußen gegen Mitarbeiter als solche verhängt werden können, regelt die DS-GVO selbst nicht. In diesem Punkt ist das nationale Umsetzungsgesetz abzuwarten.

Erhöhter Bußgeldrahmen

Die Ahndung mit Geldbuße muss – in den Worten des Gesetzes – *wirksam*, *verhältnismäßig* und *abschreckend* sein. Für Geldbußen gegen Unternehmen steht bei einem Teil der Verstöße ein Bußgeldrahmen von bis zu 10 Mio. € oder bis zu 2% des weltweit erzielten Jahresumsatzes zur Verfügung, je nachdem, welcher Betrag höher ist. Für einen Teil der Verstöße beträgt der Bußgeldrahmen sogar *bis zu 20 Mio. € oder bis zu 4% des weltweiten Jahresumsatzes*.

Sofern das geahndete Unternehmen zu einer Unternehmensgruppe bzw. einem Konzern gehört, ist hierbei nicht allein der Jahresumsatz des eigentlichen geahndeten Rechtsträgers (also des Verantwortlichen bzw. Auftragsverarbeiters) maßgeblich, sondern der Jahresumsatz der gesamten Unternehmensgruppe bzw. des gesamten Konzerns. Dies geht ausdrücklich aus der Gesetzesbegründung hervor, die auf den „wirtschaftlichen Unternehmensbegriff" des Vertrags über die Arbeitsweise der Europäischen Union verweist (Erwägungsgrund 150).

Kriterien für die Höhe von Geldbußen

Der Gesetzgeber zählt eine Reihe von Kriterien auf, die bei der Festlegung der Höhe von Geldbußen zu berücksichtigen sind. So wirken sich z. B. einschlägige *frühere Verstöße* erschwerend aus. Ebenfalls zu berücksichtigen ist, inwieweit der Verantwortliche bzw. Auftragsverarbeiter mit der Aufsichtsbehörde zusammengearbeitet hat. Erteilt etwa ein Unternehmen der Aufsichtsbehörde im Rahmen einer aufsichtlichen Untersuchung unzutreffende oder unvollständige Auskünfte, dürfte dies als erschwerender Umstand zu werten sein; dies ist in der Rechtsprechung des Europäischen Gerichtshofs im Bereich des Wettbewerbsrechts anerkannt.

Für die Bemessung von Geldbußen kann künftig der Europäische Datenschutzausschuss – das Gremium der Aufsichtsbehörden der EU-Mitgliedstaaten – Leitlinien entwickeln. Schon deshalb muss davon ausgegangen werden, dass es mittelfristig zu einer *gleichmäßigen Anwendung der Sanktionsmöglichkeiten in Europa* kommen wird. Dies ist auch der erklärte Wille des Gesetzgebers.

Ausblick zu drohenden Bußgeldern

Aus den Sanktionsvorschriften der DS-GVO spricht der deutliche Wille des Gesetzgebers, Datenschutzverstöße konsequent und bei Bedarf auch empfindlich zu ahnden. Dies ist ein deutliches Signal, dass sich eine Inkaufnahme von Datenschutzverstößen nicht lohnt.

Unternehmen müssen den Datenschutz daher zwangsläufig noch mehr als bisher in den Fokus ihrer eigenen Aufmerksamkeit nehmen.