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.

I Sicherheit der Verarbeitung - Art. 32 DS-GVO

Sicherheit im Datenschutzfokus

Begrifflichkeiten wie Datensicherheit, IT-Sicherheit und technischer Datenschutz werden im heutigen Datenschutzalltag zwar häufig verwendet, aber leider immer wieder miteinander vermischt oder auch verwechselt. Es besteht deshalb ein nicht unwesentlicher Interpretationsspielraum, welche technischen Sicherheitsmaßnahmen auch aus Datenschutzgesichtspunkten erforderlich sind.

Der derzeitig relevante § 9 BDSG zu den technischen und organisatorischen Maßnahmen hält sich – trotz Anlage – eher bedeckt, wenn es darum geht, geeignete Maßnahmen nach festen Kriterien zu bestimmen. Da der § 9 BDSG in der bisherigen Form nicht mehr bestehen wird, stellt sich die Frage, welche Regelungen die DS-GVO nun zur Informationssicherheit trifft und wie diese zu verstehen sind.

Besondere Bedeutung hat Art. 32 DS-GVO, der den Titel „Sicherheit der Verarbeitung“ trägt. In diesem Artikel wird vergleichsweise ausführlich beschrieben, nach welchen Kriterien technische und organisatorische Maßnahmen zu wählen sind, um ein angemessenes Schutzniveau zu gewährleisten.

Wer die DS-GVO weiter liest, wird rasch feststellen, dass auch an vielen anderen Stellen der Verordnung entsprechende Fachbegriffe zur Sicherheit aus Art. 32 erwähnt werden. Nachfolgend werden deshalb grundlegende Begriffe, die nach Einschätzung des BayLDA eine bedeutsame Rolle spielen, näher dargestellt und eingeordnet.

Schutzziele im Sicherheitsumfeld

Die klassischen Schutzziele der IT-Sicherheit wie *Vertraulichkeit*, *Integrität* und *Verfügbarkeit* findet man in der DS-GVO an zentraler Stelle in Art. 32 Abs. 1. Während diese für viele verantwortliche Stellen altbekannt sind und in der jetzigen Verarbeitungspraxis schon Berücksichtigung finden, ist in der DS-GVO auch

ein neuer Begriff vorhanden: Die *Belastbarkeit* (engl. „resilience“). Für Verantwortliche gilt es demnach künftig auch die Belastbarkeit der Systeme und Dienste, die in Zusammenhang mit der Verarbeitung stehen, zu gewährleisten. Nähere Angaben, welche Maßnahmen zur Belastbarkeit positiv beitragen, nennt die DS-GVO nicht.

Schutzbedarf personenbezogener Daten

Um beurteilen zu können, was ein angemessenes Schutzniveau nach Art 32. Abs. 1 ist, muss im Vorfeld für den Verantwortlichen klar sein, welchen Schutzbedarf die relevanten personenbezogenen Daten besitzen. Hierbei existieren in der Praxis bereits heute verschiedene Ansätze, die in der Regel auf das Schadenspotential abzielen. Vereinfacht wird man in Kategorien des Schutzbedarfs *normal*, *hoch* und *sehr hoch* sprechen und handeln können. Die Schutzbedarfsfeststellung ist als ein erster Schritt essentiell, wenn es später darum geht, *geeignete* technische und organisatorische Maßnahmen auszuwählen.

Risikobewertung

Der Begriff des Risikos wird mehrfach in der DS-GVO verwendet. Die Maßnahmen, die zum Schutz von personenbezogenen Daten getroffen werden sollen, müssen künftig unter Berücksichtigung des Risikos ausgewählt werden. Hierbei besteht nun die Herausforderung, objektive Kriterien für Eintrittswahrscheinlichkeit und Schwere eines Risikos für die Rechte und Freiheiten natürlicher Personen festzulegen. Während heute bereits einige Unternehmen verschiedene Risikobewertungsansätze etabliert haben, gilt es künftig, nicht mehr alleinig die Unternehmenswerte, sondern im Sinne des Datenschutzes den Betroffene in den Fokus der Risikobewertung zu setzen.

Technische und organisatorische Maßnahmen

Die DS-GVO spricht in Art. 32 von *geeigneten* technischen und organisatorischen Maßnahmen, die der Verantwortliche unter Berücksichtigung u. a. des *Stands der Technik* und der *Implementierungskosten* zu treffen hat. Folglich wird einerseits stets zu prüfen bleiben, was beim jeweiligen Verfahren als Stand der Technik angesehen wird. Anderseits wird auch die Verhältnismäßigkeit einer Maßnahme hinsichtlich des Aufwands zu diskutieren sein.

Nachweise der Konformität

Inwieweit ein Verantwortlicher sich an die Verarbeitungsgrundsätze der DS-GVO hält und die Sicherheit der Verarbeitung gewährleistet, wird auch im Rahmen einer Nachweiserbringung relevant werden (siehe *Rechenschaftspflicht* nach Art. 5 Abs. 2 DS-GVO). So werden genehmigte Verhaltensregeln ebenso wie Zertifizierungen an Bedeutung gewinnen.

Ausblick zur Sicherheit

Technische Aspekte der Datenverarbeitung, die bislang eher unter „IT-Sicherheit“ anzusiedeln waren, bekommen durch die DS-GVO eine höhere Bedeutung für Datenschutzverantwortliche als es bislang durch das BDSG abgebildet wurde. In den nächsten Jahren müssen hierfür jedoch auf europäischer Ebene objektive Kriterien und Methoden festgelegt werden, um künftig geeignete Maßnahmen auszuwählen.