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.

II Zertifizierung - Art.42 DS-GVO

Sinn und Zweck von Zertifizierungen

Im Datenschutzalltag trifft man häufig auf eine grundlegende Fragestellung: „*Woher weiß man eigentlich, ob datenschutzrechtliche Vorgaben von einem Unternehmen eingehalten werden?*“. Eine auf den ersten Blick einfache und pragmatische Lösung wäre, sich dies durch entsprechende Zertifikate nachweisen zu lassen.

Bisherige Erfahrung des BayLDA

Das BayLDA hat in seinen aufsichtlichen Kontrollen nach § 38 BDSG zwar festgestellt, dass Unternehmen oft verschiedenste Zertifikate vorweisen konnten – jedoch genügten diese bislang *in keinem einzigen Fall*, um die Fragen aus dem Prüfumfang des BayLDA ausreichend zu beantworten. Meist handelte es sich um Zertifizierungsverfahren, die nur am Rande mit Datenschutz zu tun hatten - statt diesen in den Fokus zu rücken. Zudem war größtenteils nicht transparent, was im Zertifizierungsverfahren tatsächlich geprüft wurde.

Zertifizierung nach der DS-GVO

Die Begriffe Zertifizierung und Zertifizierungsverfahren werden in der DS-GVO besonders erwähnt. An zentraler Stelle findet man im Kapitel IV „*Verantwortlicher und Auftragsverarbeiter*“ den Abschnitt 5 zum Thema „*Verhaltensregeln und Zertifizierung*“. Dort befindet sich schließlich der entscheidende Kernartikel zum Thema Zertifizierung: „*Art. 42 Zertifizierung*“. Dieser Artikel regelt in acht Absätzen, welche neuen Anforderungen und Möglichkeiten für Datenschutz-Zertifizierungen bestehen.

Förderung von Zertifizierungen

Einleitend weist Art. 42 Abs. 1 darauf hin, dass auch die Aufsichtsbehörden die Einführung von datenschutzspezifischen Zertifizierungsverfahren fördern sollen. Damit könnten Verantwortliche oder Auftragsverarbeiter künftig Nachweise erbringen, dass ihre Datenverarbeitungsvorgänge mit den Vorschriften der DS-GVO im Einklang stehen.

Einhaltung der DS-GVO – auch mit Zertifikat

Art. 42 Abs. 4 hebt hervor, dass eine erfolgreiche Zertifizierung ein Unternehmen (egal ob Verantwortlicher oder Auftragsverarbeiter) nicht davon befreit, die Vorgaben der DS-GVO weiterhin einzuhalten – was eigentlich selbstverständlich sein sollte.

Ebenso verdeutlicht Art. 42 Abs. 4 DS-GVO aber auch, dass die Aufgaben und Befugnisse der zuständigen Aufsichtsbehörden durch ein Zertifikat unberührt bleiben. Nach Einschätzung des BayLDA kann ein solches Zertifikat jedoch bei aufsichtlichen Kontrollen von Vorteil sein.

Zertifizierungsstellen

Interessant wird sicherlich zu beobachten sein, wer künftig Zertifikate vergeben kann – und dies auch tatsächlich in der Praxis umsetzt. Nach Art. 42 Abs. 5 können sowohl (akkreditierte) Zertifizierungsstellen als auch die zuständigen Aufsichtsbehörden eine Datenschutz-Zertifizierung nach DS-GVO erteilen.

Voraussetzung für eine Zertifizierung

Damit eine Zertifizierung durchgeführt werden kann, muss der Verantwortliche dem Auditor (egal ob Zertifizierungsstelle oder Aufsichtsbehörde) alle für die Durchführung des Zertifizierungsverfahrens erforderlichen Informationen zur Verfügung stellen (Art. 42 Abs. 6 DS-GVO). Somit wird es künftig umso wichtiger, die eigenen Verarbeitungsvorgänge zu kennen und transparent zu dokumentieren.

Unternehmen, die bereits jetzt über ein strukturiertes Verfahrensverzeichnis und eine gut aufgestellte Datenschutz-Organisation verfügen, haben zumindest heute wesentliche Voraussetzungen dafür erfüllt.

Rahmenbedingungen

Art. 42 Abs. 7 weist darauf hin, dass eine Zertifizierung zeitlich begrenzt zu erteilen ist. So besteht eine Höchstdauer von drei Jahren, die aber bei Erfüllung der einschlägigen Voraussetzungen unter denselben Bedingungen verlängert werden kann. Gleichzeitig kann die zuständige Aufsichtsbehörde die Zertifizierung widerrufen, wenn die Voraussetzungen für die Zertifizierung nicht oder nicht mehr erfüllt werden.

Ausblick zu Datenschutz-Zertifizierungen

Zertifizierungen nach der DS-GVO haben sehr großes Potenzial, künftig bei Verarbeitungsvorgängen (u. a. bei Auftragsdatenverarbeitung) Klarheit darüber zu verschaffen, ob die gesetzlichen Datenschutz-Anforderungen eingehalten werden. So können insbesondere Cloud-Dienste entscheidend profitieren, da Kunden und vor allem auch betroffene Personen selbst sich leichter ein Bild von einem bestimmten Produkt hinsichtlich dessen Datenschutzniveaus machen können.

Voraussetzung hierfür ist jedoch, dass neue, praxistaugliche Zertifizierungsverfahren entwickelt werden. Bei bestehenden Zertifizierungsverfahren muss zwangsläufig eine Überarbeitung hinsichtlich der neuen Vorgaben stattfinden.

Das BayLDA befürwortet deshalb die Entwicklung abgestimmter, länderübergreifend geltender Kriterien, damit auch im Vollzug der Aufsichtsbehörden eine einheitliche Bewertung im Sinne der DS-GVO ermöglicht wird. Ein Wildwuchs zahlreicher unterschiedlicher Zertifizierungsverfahren sollte im Interesse aller Beteiligten vermieden werden.