Kurzpapier Nr. 9

Zertifizierung nach Artikel 42 DS-GVO

Dieses Kurzpapier der unabhängigen Datenschutzbehörden des Bundes und der Länder (Datenschutzkonferenz – DSK) dient als erste Orientierung insbesondere für den nicht-öffentlichen Bereich, wie nach Auffassung der DSK die Datenschutz-Grundverordnung (DS-GVO) im praktischen Vollzug angewendet werden sollte. Diese Auffassung steht unter dem Vorbehalt einer zukünftigen - möglicherweise abweichenden - Auslegung des Europäischen Datenschutzausschusses.

Sinn und Zweck von Zertifizierungen

Im Datenschutzalltag trifft man häufig auf eine grundlegende Fragestellung: *„Woher weiß man, ob datenschutzrechtliche Vorgaben von einem Unternehmen oder einer Behörde eingehalten werden?“*. Eine auf den ersten Blick einfache und pragmatische Lösung wäre, sich dies durch entsprechende Zertifizierungen nachweisen zu lassen. Mit den Artikeln 42 und 43 der DS-GVO legt der Gesetzgeber einen rechtlichen Grundstein für europäisch einheitliche Akkreditierungs- und Zertifizierungsverfahren, die dazu dienen, die Einhaltung der DS-GVO bei Verarbeitungsvorgängen nachzuweisen.

Bisherige Erfahrungen der Aufsichtsbehörden

Die Aufsichtsbehörden haben in ihren Kontrollen zwar festgestellt, dass Organisationen oft verschiedenste Zertifikate vorweisen konnten – jedoch war häufig unklar, inwieweit die gesetzlichen Anforderungen an den Datenschutz ausreichend berücksichtigt wurden. Manche bestehende Zertifizierungsverfahren, wie beispielsweise das Informationssicherheitsmanagement nach ISO 27001, decken nur einen Teilbereich des Datenschutzes ab und haben mitunter auch die betroffenen Personen mit ihren Rechten und Freiheiten nicht im Mittelpunkt der Betrachtung.

Förderung von Zertifizierungen

Einleitend weist Artikel 42 Absatz 1 DS-GVO darauf hin, dass unter anderem auch die Aufsichtsbehörden auf Unionsebene die Einführung von datenschutzspezifischen Zertifizierungsverfahren, Datenschutzsiegeln und -prüfzeichen fördern sollen. Diese dienen dazu, nachzuweisen, dass die DS-GVO bei Verarbeitungsvorgängen von Verantwortlichen oder Auftragsverarbeitern eingehalten wird. Bis es jedoch so weit ist, dass die Verordnung umgesetzt und angewandt werden kann, müssen die Mitgliedstaaten in einer engen Zusammenarbeit die in der DS-GVO geforderten Mechanismen und Kriterien entwickeln. Dies ist zeitlich, räumlich und kapazitiv eine große Herausforderung für alle Beteiligten.

Vorteile einer Zertifizierung

Die DS-GVO nennt explizit einige Anwendungsbereiche, bei denen eine Zertifizierung für den Nachweis der Einhaltung der Grundverordnung als Faktor mit herangezogen werden kann:

- Erfüllung der Pflichten des Verantwortlichen (Artikel 24 Absatz 3)
- Erfüllung der Anforderungen an Technikgestaltung und datenschutz-freundliche Voreinstellungen des Artikel 25 Absatz 1 und 2 (vergleiche Absatz 3)
- Garantien des Auftragsverarbeiters nach Artikel 28 (vergleiche Absatz 5 und 6)
- Sicherheit der Verarbeitung (Artikel 32 Absatz 3)
- Datenübermittlung an ein Drittland (Artikel 46 Absatz 2 Buchstabe f)
- Datenschutz-Folgeabschätzung (Erwägungsgrund 90)

Daneben kann ein Zertifikat auch für Marketingzwecke genutzt werden, um sowohl Geschäftskunden, Verbrauchern als auch Bürgern gegenüber die Beachtung des Datenschutzrechts darzustellen.

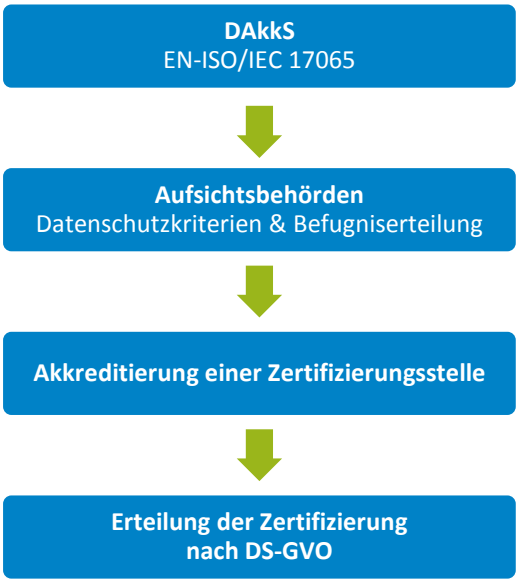
Einhaltung der DS-GVO – auch mit Zertifikat

Artikel 42 Absatz 4 hebt hervor, dass eine erfolgreiche Zertifizierung eine Organisation (unabhängig davon, ob Verantwortlicher oder Auftragsverarbeiter) nicht von der Verantwortung für die Einhaltung der DS-GVO befreit. Ebenso verdeutlicht Artikel 42 Absatz 4, dass die Aufgaben und Befugnisse der zuständigen Aufsichtsbehörden von einer Zertifizierung unberührt bleiben. Ein nach DS-GVO genehmigtes Zertifizierungsverfahren kann jedoch bei aufsichtlichen Kontrollen von Vorteil sein und die Prüfung erleichtern.

Zertifizierungsstellen

Nach Artikel 42 Absatz 5 DS-GVO können sowohl akkreditierte Zertifizierungsstellen als auch die zuständigen Aufsichtsbehörden eine Datenschutz-Zertifizierung nach DS-GVO erteilen. Die Akkreditierung nimmt in Deutschland die Deutsche Akkreditierungsstelle GmbH (DAkkS) zusammen mit den Aufsichtsbehörden gemäß § 39 Akkreditierung DSAnpUG („BDSG-neu“) vor. Die Kriterien für die Akkreditierung werden von den Aufsichtsbehörden entwickelt und beruhen unter anderem auf einschlägigen ISO-Normen (siehe Abbildung). Eine einvernehmliche Entscheidung der beiden Parteien in einem eigens dafür eingerichteten Ausschuss ist Voraussetzung für die Akkreditierung einer Zertifizierungsstelle. Erst danach und nach der Erteilung der Befugnis durch die zuständige Aufsichtsbehörde, kann die Zertifizierungsstelle tätig werden. Sie darf im Anschluss, nach entsprechender Prüfung der Einhaltung der DS-GVO, Zertifizierungen erteilen.

Gesamtverfahren im Überblick



Voraussetzung für eine Zertifizierung

Damit eine Zertifizierung durchgeführt werden kann, muss die zu zertifizierenden Stelle alle für die Durchführung des Zertifizierungsverfahrens erforderlichen Informationen zur Verfügung stellen und Zugang zu den betroffenen Verarbeitungstätigkeiten gewähren (Artikel 42 Absatz 6 DS-GVO). Somit wird es künftig umso wichtiger, die eigenen Verarbeitungsvorgänge zu kennen und transparent zu dokumentieren. Unternehmen, die bereits jetzt Informationssicherheit leben, über ein Datenschutz-Managementsystem verfügen und sich mit der Umsetzung der DS-GVO befassen, erfüllen bereits wesentliche Voraussetzungen.

Rahmenbedingungen

Artikel 42 Absatz 7 DS-GVO weist darauf hin, dass eine Zertifizierung zeitlich begrenzt zu erteilen ist. So besteht eine Höchstdauer von drei Jahren, die bei Erfüllung der einschlägigen Voraussetzungen verlängert werden kann. Die zuständige Zertifizierungsstelle und die Aufsichtsbehörde können die Zertifizierung widerrufen, wenn die Voraussetzungen für die Zertifizierung nicht oder nicht mehr erfüllt werden.

Ausblick zu Datenschutz-Zertifizierungen

Zertifizierungen nach der DS-GVO bieten das Potenzial, künftig bei Verarbeitungsvorgängen (unter anderem bei Auftragsverarbeitung) Klarheit darüber zu verschaffen, ob die gesetzlichen Datenschutzanforderungen eingehalten werden. So können etwa Cloud-Dienste entscheidend profitieren, da deren Kunden und vor allem auch betroffene Personen sich selbst leichter ein Bild von einem bestimmten Produkt hinsichtlich der Einhaltung der DS-GVO machen können. Voraussetzung hierfür sind jedoch auf die DS-GVO ausgerichtete, praxistaugliche Zertifizierungsverfahren. Bei bestehenden Zertifizierungsverfahren muss zwangsläufig eine Überarbeitung hinsichtlich der neuen Vorgaben stattfinden.

Die Aufsichtsbehörden des Bundes und der Länder arbeiten derzeit intensiv an der 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 Zertifizierungs-verfahren sollte gerade mit Blick auf ein einheitliches europäisches Datenschutzniveau im Interesse aller Beteiligten vermieden werden.