

Kurzpapier Nr. 9

Zertifizierung nach Art. 42 DS-GVO

Dieses Kurzpapier der unabhängigen Datenschutzbehörden des Bundes und der Länder (Datenschutzkonferenz/DSK) dient als erste Orientierung insbesondere für den nichtöffentlichen 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 einen Faktor darstellen, um 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.

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 (Art. 24 Abs. 3)
- Erfüllung der Anforderungen an Technikgestaltung und datenschutzfreundliche Voreinstellungen des Art. 25 Abs. 1 und 2 (vgl. Abs. 3)
- Garantien des Auftragsverarbeiters nach Art. 28 (vgl. Abs. 5 und 6)
- Sicherheit der Verarbeitung (Art. 32 Abs. 3)
- Datenübermittlung an ein Drittland (Art. 46 Abs. 2 Buchst. f)
- Datenschutz-Folgenabschätzung (ErwGr. 90)

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

Einhaltung der DS-GVO – auch mit Zertifikat

Art. 42 Abs. 4 DS-GVO 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 Art. 42 Abs. 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.

Zertifizierungskriterien

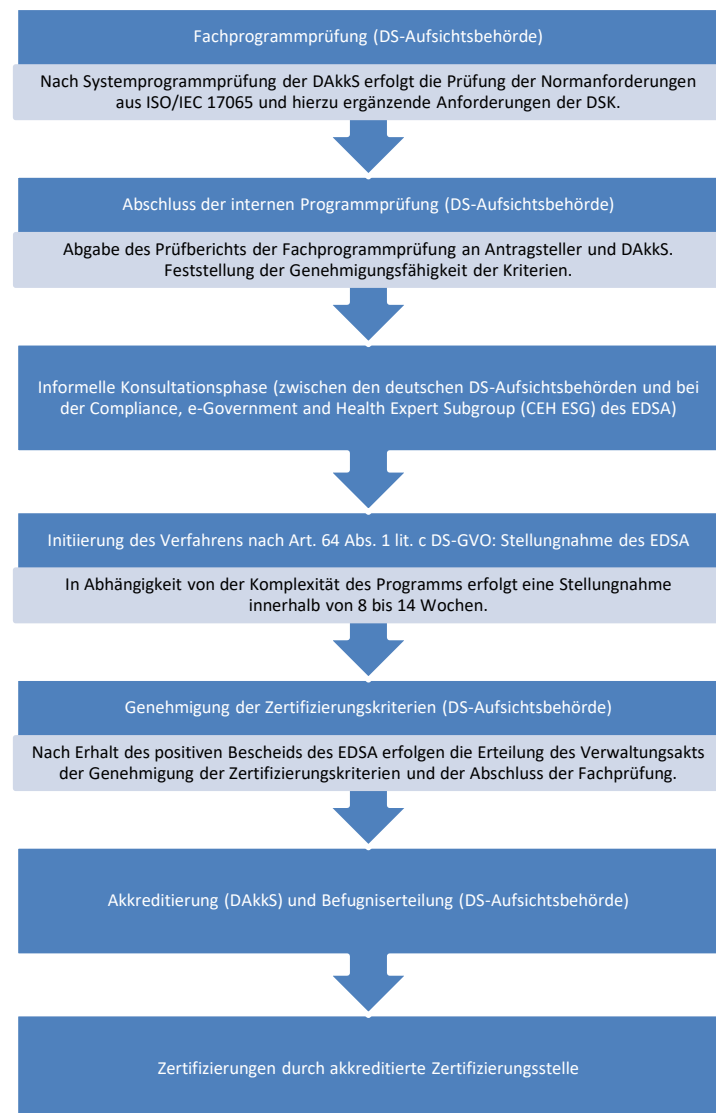
Bevor Zertifizierungsstellen akkreditiert werden können, benötigen diese einen genehmigten Kriterienkatalog, auf dessen Basis die Zertifizierungen erfolgen können. Bei nationalen Zertifizierungsverfahren erfolgt die Genehmigung durch die zuständige Aufsichtsbehörde. Die Aufsichtsbehörden des Bundes und der Länder haben länderübergreifend geltende Prüfkriterien entwickelt, damit auch bei der Genehmigung von Kriterienkatalogen deutschlandweit eine einheitliche Bewertung im Sinne der DS-GVO ermöglicht wird.

Bei europäischen Zertifizierungsverfahren, die sich an mehrere Mitgliedstaaten der EU richten, nimmt der Europäische Datenschutzausschuss die Genehmigung vor.

Zertifizierungsstellen

Nach Art. 42 Abs. 5 DS-GVO können sowohl akkreditierte Zertifizierungsstellen als auch die zuständigen Aufsichtsbehörden eine Datenschutzzertifizierung nach DS-GVO erteilen. Die Akkreditierung nimmt in Deutschland die Deutsche Akkreditierungsstelle GmbH (DAkkS) zusammen mit den Aufsichtsbehörden gemäß § 39 BDSG vor. Die deutschen Kriterien für die Akkreditierung wurden von den Aufsichtsbehörden entwickelt und beruhen u. a. auf einschlägigen ISO-Normen (siehe Abbildung). Eine einvernehmliche Entscheidung der zuständigen Aufsichtsbehörde und der DAkkS 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 zertifizierende Stelle alle für die Durchführung des Zertifizierungsverfahrens erforderlichen Informationen zur Verfügung stellen und Zugang zu den betroffenen Verarbeitungstätigkeiten gewähren (Art. 42 Abs. 6 DS-GVO). Somit wird es künftig umso wichtiger, die eigenen Verarbeitungsvorgänge zu kennen und transparent zu dokumentieren. Unternehmen, die Informationssicherheit leben, über ein Datenschutzmanagementsystem verfügen und die DS-GVO umsetzen, erfüllen bereits wesentliche Voraussetzungen.

Rahmenbedingungen

Art. 42 Abs. 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, bei Verarbeitungsvorgängen (u. a. bei Auftragsverarbeitung) Klarheit darüber zu verschaffen, ob die gesetzlichen Datenschutzanforderungen eingehalten werden. So können etwa Dienstleistungen, die auf bestimmten Produkten von Anbietern basieren (z. B. Cloud-Dienste) entscheidend profitieren, da deren Kunden und vor allem auch betroffene Personen sich selbst leichter ein Bild von einer bestimmten Dienstleistung und dem ggf. damit verbundenen Produkt hinsichtlich der Einhaltung der DS-GVO machen können. Voraussetzung hierfür sind jedoch auf die DS-GVO ausgerichtete, praxistaugliche Zertifizierungsverfahren. Deshalb haben die deutschen Aufsichtsbehörden einheitliche Anforderungen an Zertifizierungskriterien aufgestellt. Diese bilden die Basis der Bewertung von Zertifizierungsprogrammen durch die Aufsichtsbehörden. Programmeigner sowie die zu akkreditierenden Zertifizierungsstellen können sich schon bei der Erstellung ihrer Dokumente hieran orientieren.

Verweise

DSK: Anforderungen zur Akkreditierung gemäß Art. 43 Abs. 3 DS-GVO i. V. m. DIN EN ISO/IEC 17065 (08.10.2020), https://www.datenschutzkonferenz-online.de/media/ah/20201008_din17065_Ergaenzungen_deutsch_nach_opinion.pdf

DSK: Anforderungen an datenschutzrechtliche Zertifizierungsprogramme (Version 2.0), https://www.datenschutzkonferenz-online.de/media/ah/DSK_Zertifizierungskriterien_V2.0_Stand_21062022.pdf

DAkKS: Projekt Datenschutz – im Überblick, <https://www.dakks.de/index.php/de/projekt-datenschutz-2.html>

Anmerkung zur Nutzung dieses Kurzpapiers:

Dieses Kurzpapier darf – ohne Rückfrage bei einer Aufsichtsbehörde – kommerziell und nicht kommerziell genutzt, insbesondere vervielfältigt, ausgedruckt, präsentiert, verändert, bearbeitet sowie an Dritte übermittelt oder auch mit eigenen Daten und Daten Anderer zusammengeführt und zu selbständigen neuen Datensätzen verbunden werden, wenn der folgende Quellenvermerk angebracht wird: Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder (Datenschutzkonferenz). Datenlizenz Deutschland – Namensnennung – Version 2.0 (www.govdata.de/dl-de/by-2-0).