Alisha Gühr, Irene Karper, Sönke Maseberg

Der lange Weg zur Akkreditierung nach Art. 42 DSGVO

Praxiserfahrungen und Situationsbericht

Mit Inkrafttreten der EU-Datenschutz-Grundverordnung (DSGVO) liegen seit 2018 Vorgaben für ein gesetzliches Datenschutz-Zertifikat vor. Bevor aber die ersten Zertifikate nach Art. 42 DSGVO erteilt werden können, müssen auf Seiten aller Beteiligten diverse Hürden genommen werden.

1 Einleitung

Dieser Beitrag berichtet von unseren Aktivitäten für die Zulassung als akkreditierte Zertifizierungsstellen, welche Datenschutz-Zertifikate gem. Art. 42 DSGVO erteilen soll. In einem ersten Schritt muss dazu ein sogenanntes Konformitätsbewertungsprogramm samt Kriterien erstellt und von mehreren Behörden abgenommen werden; dieses bildet die Basis für die darauffolgende Zulassung von Zertifizierungsstellen. Danach können Datenschutz-Zertifikate erteilt werden. Zur besseren Einordnung des Themas beginnen wir mit einem kurzen historischen Abriss.

Alisha Gühr

Auditorin datenschutz cert GmbH

E-Mail: aguehr@datenschutz-cert.de

Dr. Irene Karper

Zertifizierungsstelle datenschutz cert GmbH

E-Mail: ikarper@datenschutz-cert.de

Dr. Sönke Maseberg

Geschäftsführer datenschutz cert GmbH

E-Mail: smaseberg@datenschutz-cert.de

2 Vor der DSGVO

Überlegungen zu einem Datenschutz-Zertifikat gab es ja viele: Auf gesetzlicher Ebene etwa im früheren Bundesdatenschutzgesetz (BDSG a.F.), wo 2009 in § 9a ein Datenschutz-Audit versprochen wurde, mangels Ausführungsbestimmungen aber niemals kam. Das Datenschutz-Gütesiegel des Unabhängigen Landeszentrums für Datenschutz Schleswig-Holstein[1] ist sicherlich als Vorreiter und Benchmark anzusehen, aber auch dieses Siegel hat unter dem Einfluss der DSGVO den Dienst vorerst eingestellt. Es bleiben aktuell nur proprietäre Gütesiegel, wie etwa das international anerkannte und beachtenswerte European Privacy Seal der EuroPriSe GmbH[2]. Und es gab natürlich noch viele andere proprietäre Siegel, insb. zur Auftragsdatenverarbeitung gem. § 11 des früheren BDSG. Diese Siegel und Zertifikate unterlagen jedoch keiner Qualitätskontrolle von außen. Die Vertrauenswürdigkeit der Zertifikate war nicht in allen Fällen gesichert, die Kompetenz der Zertifizierungsstellen nicht geprüft. Lediglich die Stiftung Datenschutz hatte und hat es sich zur Aufgabe gemacht, hier einen Marktüberblick zu schaffen[3]. Dieser „Wildwuchs" an Zertifikaten sollte mit der DSGVO eigentlich ein Ende haben, denn in Art. 42 und 43 DSGVO werden endlich verbindliche und unmittelbar in den EU-Mitgliedstaaten geltende Regelungen für Datenschutz-Zertifizierungen getroffen.

2.1 Intention der DSGVO

Die DSGVO [1] definiert u.a. verschiedene Anforderungen an Verantwortliche und Auftragsverarbeiter. Zudem ist ein Paradigmenwechsel eingeführt worden, wonach Verantwortliche –

1 Details online verfügbar unter: www.datenschutzzentrum.de/guetesiegel/ (letzter Abruf: 07/2020)

2 Details online verfügbar unter: www.european-privacy-seal.eu (letzter Abruf: 07/2020)

3 Online verfügbar unter: https://stiftungdatenschutz.org/themen/datenschutzzertifizierung/zertifikate-uebersicht/ (letzter Abruf: 07/2020)

und in der Folge dann auch Auftragsverarbeiter – eine Rechenschaftspflicht trifft, die Umsetzung der Anforderungen nachzuweisen, vgl. dazu etwa Art. 5 (2): *„Der Verantwortliche ist für die Einhaltung des Absatzes 1 verantwortlich und muss dessen Einhaltung nachweisen können („Rechenschaftspflicht").*"

Zu der Frage, wie die Erfüllung dieser Pflichten nachgewiesen werden kann, wird in Art. 24 (3) DSGVO auch sogleich eine Möglichkeit angesprochen: *„Die Einhaltung […] eines genehmigten Zertifizierungsverfahrens gemäß Artikel 42 kann als Gesichtspunkt herangezogen werden, um die Erfüllung der Pflichten des Verantwortlichen nachzuweisen.*"[4] Analog kann die Umsetzung von Privacy-by-Design und Privacy-by-Default gem. Art. 25 (3) DSGVO über ein *„genehmigtes Zertifizierungsverfahren gemäß Artikel 42 […] als Faktor herangezogen werden*". Dieser „Faktor" als Nachweis der Erfüllung von Pflichten wird in weiteren Artikeln analog erwähnt:

- für Auftragsverarbeiter in Art. 28 (5) DSGVO und
- für technisch-organisatorische Maßnahmen in Art. 32 (3) DSGVO.

Aber was sind nun „genehmigte Zertifizierungsverfahren" gem. Art. 42 DSGVO? Dieser beschreibt die grundsätzliche Intention des Gesetzgebers, „datenschutzspezifische Zertifizierungsverfahren" zu fördern, wobei die Begriffe Gütesiegel, Zertifikate, Siegel, Logos, etc. synonym zu verstehen sind. Und der Vollständigkeit halber soll auch hier noch der Erwägungsgrund 100 zitiert werden: *„Um die Transparenz zu erhöhen und die Einhaltung dieser Verordnung zu verbessern, sollte angeregt werden, dass Zertifizierungsverfahren sowie Datenschutzsiegel und -prüfzeichen eingeführt werden, die den betroffenen Personen einen raschen Überblick über das Datenschutzniveau einschlägiger Produkte und Dienstleistungen ermöglichen.*"

Wie genau diese „datenschutzspezifische Zertifizierungsverfahren" aussehen sollen, hat der Gesetzgeber in Art. 43 DSGVO vorgegeben. Neben staatlichen Stellen ist ein privatwirtschaftliches Modell vorgesehen: eine Akkreditierung durch die nationale Akkreditierungsstelle gem. ISO/IEC 17065 im gemeinsamen Verfahren mit der zuständigen Datenschutz-Aufsichtsbehörde. Dazu aber später mehr.

Wichtig ist hier, dass dem Gesetzgeber gem. Art. 42 DSGVO ein einheitliches „Europäisches Datenschutzsiegel" vorschwebt. Dazu müssen die Kriterien nicht nur von den zuständigen (regionalen) Datenschutz-Aufsichtsbehörden abgenommen werden, sondern auch dem Europäischen Datenschutz-Ausschuss EDSA (European Data Protection Board – EDPB). Die vom EDSA europaweit zugelassenen Zertifizierungsverfahren sollen zentral gelistet werden.[5]

3 Motivation

Bevor wir aber auf die konkreten Anforderungen der DSGVO zu einem Datenschutz-Zertifikat eingehen, kurz zur Motivation für Verantwortliche und Auftragsverarbeiter. Wieso sollten diese ein Interesse daran haben, einen Verarbeitungsvorgang gem. DSGVO zertifizieren zu lassen? Aus unserer Sicht sind dafür insbesondere sieben Gründe ausschlaggebend:

- Kundenanforderung: Kunden sind zunehmend in Sachen Datenschutz sensibilisiert – nicht erst seit der DSGVO. Ein Datenschutz-Zertifikat kann einen Vorteil bei der Gewinnung von Kunden darstellen.
- Besserer Datenschutz: Die Erfahrung zeigt: Wenn unabhängige Prüfer auf einen Sachverhalt gucken und diesen prüfen, wird dieser besser.
- Vorlage bei Aufsichtsbehörden: Aufsichtsbehörden verlangen immer häufiger den Nachweis für die Erfüllung von Anforderungen. Ein akkreditiertes Zertifikat kann helfen. Und wenn die Behörde trotzdem selber prüfen will, beruhigt manchmal, dass schon vorher eine andere zugelassene Stelle geprüft hat.
- Reduktion der Haftung: Die DSGVO sieht Strafen und Bußgelder vor. Von daher sind Datenschutz-Verstöße relevant für das interne Risikomanagement. Ein akkreditiertes Zertifikat kann zu einer Reduzierung von verhängten Bußgeldern beitragen.
- Datenschutz-Themen intern besser durchsetzen: Manch ein betrieblicher Datenschutzbeauftragter wird uns zustimmen: Bei einigen Kunden ist die Umsetzung von Datenschutz-Anforderungen schwierig bis unmöglich. Wenn aber ein benötigtes Zertifikat davon abhängt, kann manch Anforderung schneller umgesetzt werden.
- Marktzutrittsvoraussetzung: Datenschutz-Zertifikate können als Qualitätsnachweis von Kunden gefordert werden, etwa in Ausschreibungen. Damit stellen sie Marktzutrittsvoraussetzungen dar. Oder zumindest einen Vorteil gegenüber Mitbewerbern.
- Vereinfachung der Audits ihrer Kunden: Auch hier kann ein Datenschutz-Zertifikat einen Vorteil darstellen, insbesondere bei Auftragsverarbeitern, wenn Kunden diese nicht selber prüfen müssen, sondern auf ein Zertifikat verweisen können.

Nach unserer Erfahrung überwiegen diese Vorteile auch unter Berücksichtigung von Kosten, Aufwänden und Zeitabläufen zur Erlangung eines Zertifikates, denn der Verarbeitungsvorgang muss sowieso konform zur DSGVO ausgestaltet sein. Etwaige (Mehr-)Aufwände beziehen sich also eigentlich nur auf die Darstellung und Dokumentation gemäß des jeweiligen Zertifizierungsschemas zzgl. der Aufwände für Auditierung und Zertifizierung selbst. Damit „rechnet" sich das Zertifikat allemal.

4 Der Fahrplan zum Zertifikat

Nun wollen wir die Entwicklung eines „genehmigten Zertifizierungsverfahrens" beschreiben. Dazu müssen wir zunächst in die „Akkreditierungswelt" eintauchen, um die Normen, die gleich folgen, einordnen zu können. Und vielleicht vorab auch nochmal das Wort „Akkreditierung" erklären.

Es gibt ein weltweites System von Akkreditierungsstellen, die über die International Accreditation Forum (IAF) miteinander verbunden sind. Wie Akkreditierungsstellen arbeiten, ist in einer ISO-Norm – der ISO/IEC 17000 – geregelt. Die Akkreditierungsstellen begutachten sich hinsichtlich ihrer Arbeitsweise gegenseitig in sogenannten Shadowing-Verfahren. Auf europäischer Ebene existiert in jedem EU-Land genau eine Akkreditierungsstelle, vgl. EU-Verordnung 765/2008. In Deutschland ist dies die Deutsche Akkreditierungsstelle (DAkkS), die von Bund, Ländern und Verbänden als beliehene Stelle getragen wird. Damit ist die DAkkS in Deutschland der einzige „Anwender" der ISO/IEC 17000.

4 Art. 24 (3) DSGVO erwähnt als weiteren Gesichtspunkt sogenannte „genehmigte Verhaltensregeln; diese sind nicht Gegenstand dieses Beitrags.

5 Online verfügbar unter: edpb.europa.eu/our-work-tools/accountability-tools/certification-mechanisms-seals-and-marks_de (letzter Abruf: 07/2020)

Akkreditierungsstellen wiederum akkreditieren andere Stellen zu verschiedenen Akkreditierungsbereichen und Standards, die dann wiederum Prüfungen, Audits oder Inspektionen durchführen und Zertifikate erteilen. Auch dafür gibt es ISO-Normen, etwa:

- ISO/IEC 17021-1 für Stellen, die Managementsysteme zertifizieren
- ISO/IEC 17020 für Inspektionsstellen
- ISO/IEC 17025 für Prüfstellen
- ISO/IEC 17065 für Stellen, die Produkte und Dienstleistungen zertifizieren
- ISO/IEC 17024 für Stellen, die Personen zertifizieren

Ferner gibt es Konkretisierungen, wie etwa die ISO/IEC 27001, für Stellen, die Informationssicherheits-Managementsysteme gemäß ISO/IEC 27001 zertifizieren. Damit wird nun erstmals auch ein Standard angesprochen, der einem größeren Kreis bekannt sein dürfte. Eine andere, sehr bekannte Norm ist ISO 9001 für Qualitäts-Managementsysteme. Alle Stellen, die QM-Systeme zertifizieren, sind damit nach ISO/IEC 17021-1 akkreditiert.

Wozu dieser Überblick über diese ganzen Normen? Nun, in der DSGVO ist die Akkreditierungsnorm schlicht vorgegeben: In Art. 43 DSGVO ist ISO/IEC 17065 fest verankert. Damit sind übrigens auch alle Überlegungen, einen Datenschutzbeauftragten oder ein Datenschutz-Managementsystem gemäß DSGVO zu zertifizieren, vergebens – auch wenn die ISO/IEC 27701 beispielsweise als Ergänzung zur ISO/IEC 27001 einen sehr interessanten Ansatz darstellt. Personen oder Managementsysteme sind schlichtweg – zumindest im Sinne des Art. 42 DSGVO – nicht zertifizierbar. Natürlich können Personen als Datenschutzbeauftragte und Datenschutz-Managementsysteme zertifiziert werden – und womöglich gibt es auch Institutionen, die diese Nachweise entsprechend akzeptieren – aber der in der DSGVO versprochene „Gesichtspunkt zum Nachweis der Umsetzung" liegt hier nicht vor. Zudem darf ein Hinweis auf die DSGVO bei Personen oder Managementsystem-Zertifikaten nicht enthalten sein. DSGVO-Zertifikate gibt es nur gemäß Art. 42 und 43, und damit nur über eine Akkreditierung auf Basis der ISO/IEC 17065 [2]. Fassen wir zusammen: Eine Akkreditierung für DSGVO-Zertifikate erfolgt ausschließlich auf Basis der ISO/IEC 17065.

Anders als bei ISO 9001 oder ISO/IEC 27001, wo die zugehörigen Akkreditierungsnormen exakt vorgeben, wie eine Zertifizierung mit Auditierung zu erfolgen hat, ist dies bei ISO/IEC 17065 per se nicht gegeben. Damit muss zunächst in einem sogenannten Konformitätsbewertungsprogramm (KBP) festgeschrieben werden, wie eine Zertifizierungsstelle überhaupt feststellt, ob Kriterien eingehalten werden. Und neben diesen Zertifizierungsprozessen muss noch festgeschrieben werden, welche Kriterien überhaupt gelten. Denn anders als bei ISO 9001 oder ISO/IEC 27001 sind bei der DSGVO die Vorgaben nicht klar vorgegeben. Natürlich definiert die DSGVO die rechtlichen Vorgaben, aber hieraus sind prüfbare Kriterien zu entwickeln, um eine einheitliche Zertifizierung zu ermöglichen. Damit ist der Arbeitsauftrag klar:

- Es sind prüfbare Kriterien zu entwickeln und
- es ist ein Konformitätsbewertungsprogramm (KBP) zu erstellen, in dem die konkreten Zertifizierungsprozesse beschrieben sind.

Für das Erstellen eines KBP gibt es verschiedene Hilfestellungen – einmal auf ISO-Ebene durch die ISO/IEC 17067-Norm [3], ergänzt durch verschiedene DAkkS-Regelwerke. Darüber hinaus hat der Gesetzgeber den Aufsichtsbehörden ein Mitspracherecht eingeräumt. Aus diesem Grund gibt es weitere Vorgabedokumente – sowohl von deutscher als auch europäischer Seite:

- „Anforderungen zur Akkreditierung gemäß Art. 43 Abs. 3 DSGVO i.V.m. DIN EN ISO/IEC 17065" der Datenschutzkonferenz (DSK) [5]
- "Guidelines 1/2018 on certification and identifying certification criteria in accordance with Articles 42 and 43 of the Regulation" des EDSA [6]
- „Guidelines 4/2018 on the accreditation of certification bodies under Article 43 of the General Data Protection Regulation (2016/679)" des EDSA [7]

Damit ist der Arbeitsauftrag jetzt noch klarer:

- Es ist ein Konformitätsbewertungsprogramm mit Kriterien zu entwickeln, die den folgenden Vorgaben genügt: ISO/IEC 17065, ISO/IEC 17067, DAkkS-Regel, DSK-Papier und EDPB-Guidelines.

Bevor eine Stelle also nach diesem Programm akkreditiert werden und sodann Zertifikate erteilen kann, muss das Programm als solches abgenommen werden, auch hierfür ist der Begriff „Akkreditierung" korrekt.

4.1 Zulassung = Akkreditierung + Befugsniserteilung

Nun kommen wir das erste Mal auf das Zusammenspiel von DAkkS und Datenschutzaufsichtsbehörden zu sprechen, denn der Gesetzgeber hat in der DSGVO die Zulassung aufgeteilt: Einerseits die Akkreditierung durch die nationale Akkreditierungsstelle – in Deutschland durch die DAkkS – und andererseits die Befugniserteilung durch die zuständige Datenschutz-Aufsichtsbehörde. „Zuständig" meint hier die Datenschutz-Aufsichtsbehörde des Bundeslandes, in dem die Zertifizierungsstelle ihren Hauptsitz hat.

Dass noch kein Programm (Stand: Juni 2020) abgenommen und noch keine Zertifizierungsstelle akkreditiert ist, hat unter anderem auch damit zu tun, dass die DAkkS und die Datenschutz-Aufsichtsbehörden des Bundes und aller Bundesländer zunächst ihre Zusammenarbeit abstimmen mussten, damit etwa eine Abnahme der Kriterien in Bremen auch in Hamburg anerkannt werden kann.

Und es gibt noch eine weitere Besonderheit: Das große Ziel der DSGVO ist die europäische Harmonisierung des Datenschutzes, auch unter Nutzung von einheitlichen Datenschutz-Zertifikaten. Deshalb sollen auch Datenschutz-Zertifikate, die etwa in Portugal erteilt wurden, in Deutschland akzeptiert werden. Aus diesem Grund ist auch der EDSA bei der Abnahme der Kriterien einzubeziehen. Und zwar grundsätzlich sowohl für rein nationale Kriterien als auch solche, die beim EDSA angemeldet werden, damit diese zum „Europäischen Datenschutz-Gütesiegel" geadelt werden können.

Damit ist der Fahrplan jetzt klar: Nach Erstellung des Programms mit den Kriterien erfolgt die Abnahme durch DAkkS und zuständiger Datenschutz-Aufsichtsbehörde, nach Abstimmung untereinander und mit dem EDSA. Danach liegen akkreditierte Programme mit Kriterien vor. Und auf dieser Basis können dann Zertifizierungsstellen zugelassen werden. Die Zulassung der Stelle umfasst selber eine Akkreditierung durch die DAkkS und eine Befugniserteilung der zuständigen Aufsichtsbehörde.

5 Unser Ansatz

Wie zuvor schon kurz erwähnt, haben wir den Prozess gestartet, ein Konformitätsbewertungsproramm (KBP) mit Kriterien erstellt und eingereicht. Derzeit befinden wir uns noch im Prüfungsprozess durch DAkkS und unserer LfDI. Aktuell (Stand: Juni 2020) liegt noch keine Abnahme vor. Von daher können wir im Nachfolgenden zwar einen Einblick in unseren Ansatz[6] gewähren, aber keine Garantie dafür übernehmen, dass dieser Ansatz auch in der Praxis funktionieren wird. Damit sind alle nachfolgenden Ausführungen unter Vorbehalt zu betrachten.

5.1 Das Konformitätsbewertungsprogramm

Wie funktioniert denn nun unser Konformitätsbewertungsprogramm? Zunächst einmal hilft ein Blick in die Normen ISO/IEC 17065 [2] und ISO/IEC 17067 [3], denn hier ist beschrieben, wie ein solches Programm gestaltet sein muss. Etliche der Überschriften finden sich in fast allen Akkreditierungsnormen wieder, so dass diese Anforderungen Zertifizierungsstellen durchaus geläufig sein dürften:

- Vertragswerk
- Unabhängigkeit
- Haftung
- Organisation mit Ressourcen
- Zertifizierungsprozess
- Managementsystem

Zentrale Herausforderung bei der Erstellung des Programms war es, Regeln zu schaffen, die ein einheitliches Zertifizieren ermöglicht. Wir möchten daher hier auf drei wichtige und in den folgenden Abschnitten näher beschriebene Aspekte näher eingehen.

Generischer Ansatz
Die DSGVO ist generisch. Sie gilt für alles und jeden. Von daher war unser Anspruch, auch das Programm so generisch aufzustellen, dass das Programm für alles und jeden genutzt werden kann. Zwar gibt es spezifische Datenschutz-Anforderungen für bestimmte Bereiche, wie etwa im Bereich Gesundheit oder Soziales. Jedoch legt es der oben genannte Aufwand für eine Entwicklung eines solchen Programmes schon nahe, dass nicht für jede Branche ein eigenes Programm entwickelt werden kann. Vielmehr sind die Auditorinnen und Auditoren in einem Zertifizierungsaudit angehalten, sich mit den branchenspezifischen Anforderungen, Orientierungshilfen, der Rechtsprechung und Gesetzgebungen vertraut zu machen und diese einzubeziehen. Erfahrungen aus dem KRITIS-Bereich zu branchenspezifischen Sicherheitsstandards (B3S) zeigen, dass dieses Model gut funktionieren kann.

Scope
Zertifiziert werden kann ein Datenverarbeitungsvorgang beim Verantwortlichen und/oder Auftragsverarbeiter. Dies bedeutet, dass der Untersuchungsgegenstand klar beschrieben werden muss. Wir haben uns dafür entschieden, dafür folgende Elemente zu nutzen:

- Datenverarbeitungsvorgang im Sinne einer rechtlichen Charakterisierung des konkreten Datenverarbeitungsvorgangs
- Datenschutz-Managementsystem mit den internen Prozessen zur Steuerung der Datenschutz-Konformität
- Prozesse zur Realisierung des Datenverarbeitungsvorgangs mit den eigentlichen Prozessen, die für den konkreten Datenverarbeitungsvorgang benötigt werden
- physische Infrastruktur mit Standorten und Räumen
- IT-Infrastruktur mit Servern, Clients, Netzkomponenten, Datenbanken, Speichersystemen und Schnittstellen
- Applikationen, über die der Datenverarbeitungsvorgang realisiert wird
- Dienstleister, die für die Realisierung des Datenverarbeitungsvorgangs eingesetzt werden

Diese Elemente charakterisieren damit den Datenverarbeitungsvorgang, der zertifiziert werden kann, und werden uns gleich noch wieder begegnen, wenn es um die Kriterien geht.

Evaluierungsmethoden
Zuvor aber noch die Frage, durch welche Evaluierungsmethoden überprüft werden soll, ob die Kriterien angemessen umgesetzt werden. Denn diese sind üblicherweise auf Methoden zurückzuführen, die in der Akkreditierungswelt bekannt sind. Sicherlich können sie auch frei definiert werden, dann aber mit erhöhtem Beschreibungs- und Abstimmungsbedarf. Und wichtig: Da letztlich eine Akkreditierung auf Basis von ISO/IEC 17065 ausgesprochen wird, kann nicht nur ein Audit – wie es beispielsweise in Managementsystemen bekannt ist – herangezogen werden.

Wie gesagt, diese Überlegungen in unserem Programm sind noch nicht abgenommen und damit als vorläufig zu betrachten.

5.5 Die Kriterien

Grundlage der von uns gewählten Kriterien ist natürlich der gesetzliche Rahmen, den die DSGVO bietet. Die DSGVO ist damit der Maßstab. Das Programm und die Kriterien sollen dann – wenn sie einmal abgenommen sind – auch möglichst lange Bestand haben. Deshalb sollen Best-Practice-Ansätze, Einzelfallentscheidungen oder Festlegungen der Aufsichtsbehörden auf nachrangige Dokumente verlagert werden; zudem werden Auditorinnen und Auditoren eingesetzt, die den aktuellen Stand der Rechtsprechung, branchenspezifische Standards und Vorgaben der Aufsichtsbehörden kennen.

Die Vorgaben der DSGVO sind alleine aber nicht prüfbar, da sie viel zu abstrakt sind. Deshalb wurden ausgehend von der DSGVO prüfbare Kriterien entwickelt. Im Ergebnis gibt es jetzt 50 solcher Kriterien. Diese sind alle gleich aufgebaut:

- eindeutiger Identifier und Name
- Anforderung: die normative Anforderung
- Verweis DSGVO: Hinweis zur (gesetzlichen) Anforderung
- Umsetzungshinweis: hier finden sich Beispiele oder Erläuterungen
- Nachweise: hier finden sich Beispiele für Nachweise, die der Kunde zur Verfügung stellt, um die Umsetzung nachzuweisen
- Details zur Methodik mit Angabe der Zielobjektkategorie und Evaluierungsmethode

Die 50 einzelnen Kriterien sind in elf Gruppen thematisch aufgeteilt:

- P.1 Zulässigkeit der Datenverarbeitung
- P.2 Grundsätze

6 Mit Stand Juli 2020 haben auch andere Stellen ein KBP eingereicht, wie etwa die EuroPriSe GmbH (siehe https://www.european-privacy-seal.eu/EPS-en/News/n/9565/europrise-celebrates-10th-anniversary-and-looks-forward-to-the-gdpr-) oder das Forschungskonsortium „AUDITOR" (vgl. https://www.auditor-cert.de/publikationen/).

- P.3 Pflichten des Verantwortlichen
- P.4 Auftragsverarbeitung
- P.5 Technisch-organisatorische Maßnahmen
- P.6 Datenschutz-Management
- P.7 Datenverarbeitung außerhalb der EU
- P.8 Betroffenenrechte
- P.9 Beschwerde-Management
- P.10 Applikations-Management
- P.11 Förderung des Datenschutzes

Die Evaluierungsmethoden wirken mit den „Elementen", die den Geltungsbereich charakterisieren, wie folgt zusammen: über die Beschreibung des Kriterienkatalogs ist festgelegt,

- welches Kriterium
- auf welches „Element" „wirkt" und
- durch welche Evaluierungsmethoden geprüft und bewertet werden kann.

Auch für die Kriterien gilt: Diese Überlegungen sind noch nicht abgenommen und damit als vorläufig zu betrachten.

Der sonstige Zertifizierungsprozess orientiert sich an typischen Zertifizierungsprozessen:

- ein Zertifikat ist drei Jahre gültig
- es gibt jährliche Überwachungsaudits
- der Zertifizierung geht eine Evaluierung voraus
- es gibt rechtliche und technische Auditoren sowie Zertifizierer

Der Antragsteller muss zu Beginn verschiedene Referenzdokumente zur Verfügung stellen, die einerseits den Untersuchungsgegenstand exakt beschreiben – dazu werden die o.g. „Elemente" aufgenommen – und andererseits muss er die Umsetzung der Anforderungen dokumentieren. Die Methodik unseres Ansatzes gewährleistet durch eine Art „Statement of Applicability" (SoA), dass Anforderungen – je nach Anwendungsszenario – angewählt werden können. Darüber wird der generische Ansatz unsere Zertifizierungsprozesses realisiert. Antragsteller müssen somit auch mitwirken an der oftmals schwierigen Abgrenzung des Zertifizierungsgegenstandes.

Zudem gibt es von den Aufsichtsbehörden eine vorgefertigte Zertifikatsvorlage, danach muss das Zertifikat auf Seite 2 eine Art Kurzgutachten mit weiteren Details aufweisen. Jede Zertifizierungsstelle muss außerdem ein Verzeichnis zertifizierter Verarbeitungsvorgänge bereitstellen. Was uns dann noch beschäftigen wird: Die Zertifizierungsstellen werden irgendwann DSGVO-Zertifikate erteilen können, aber auch hier wird die zuständige Datenschutz-Aufsichtsbehörde ein Wörtchen mitreden können – wie das genau ausgestaltet werden kann und wird, wird noch zu klären sein.

Bezüglich der Kosten und Zeitabläufe ergibt sich aktuell folgendes Bild: Die Kosten liegen nach aktueller Planung etwas unterhalb eines ISO/IEC 27001-Zertifizierungsverfahrens und Auditierung und Zertifizierung lassen sich nach aktueller Einschätzung innerhalb weniger Wochen durchführen – wenn denn alle Anforderungen erfüllt sind.

6 Wünsche

Ausgehend von den an uns während der Entwicklung herangetragenen Anmerkungen diverser Stakeholder und erster Pilotkunden lassen sich die folgenden Wünsche bzw. Verbesserungsvorschläge festhalten:

- Der ganze Prozess muss jetzt endlich starten. Die DSGVO ist nunmehr über zwei Jahre in Betrieb. Und noch immer gibt es keine DSGVO-Zertifikate.
- Dazu müssen die Abstimmungen zwischen DAkkS, den LfDIs und dem EDSA abgeschlossen werden. Alle beteiligten Behörden müssen so ausgestattet sein, dass sie ihren Aufgaben nachkommen können.
- Wenn dann endlich Zertifizierungsprogramme da und Stellen akkreditiert sind, müssen diese Programme bekannt gemacht werden. Auch das ist noch eine große Hürde, denn die Kunden müssen die jeweiligen Schemata erst kennenlernen und ihre Verarbeitungsvorgänge, die sie zertifizieren lassen möchten, dementsprechend beschreiben. Das betrifft dann auch Berater und ggf. die (Fort-)Entwicklung entsprechender Datenschutz-Tools.
- Und letztlich ist auch wichtig, dass dann – wenn genehmigte Zertifizierungsverfahren vorliegen, mit dem „Wildwuchs" Schluss gemacht wird und nicht-akkreditierte „DSGVO-Zertifikate" vom Markt genommen werden.

7 Fazit

Mit der Datenschutz-Grundverordnung (DSGVO) liegt endlich ein gesetzlicher Rahmen für ein Datenschutz-Zertifikat vor, ausgestatte mit dem hehren Ziel, ein europaweit einheitliches Datenschutz-Gütesiegel zu schaffen. Dies ist ein Ansatz, auf den viele Beteiligte seit Jahren warten.

Die Vorgaben, um ein solches „genehmigtes Zertifizierungsverfahren" zu schaffen, sind anspruchsvoll. Alle Beteiligten sind jetzt aufgefordert, die letzten Aktivitäten umzusetzen, um endlich ein belastbares Datenschutz-Zertifikat zu schaffen.

Literatur

[1] Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung).

[2] DIN EN ISO/IEC 17065, „Konformitätsbewertung – Anforderungen an Stellen, die Produkte, Prozesse und Dienstleistungen zertifizieren (ISO/IEC 17065:2012)", Januar 2013.

[3] DIN EN ISO/IEC 17067, „Konformitätsbewertung – Grundlagen der Produktzertifizierung und Leitlinien für Produktzertifizierungsprogramme (ISO/IEC 17067:2013)", Dezember 2013.

[4] Deutsche Akkreditierungsstelle (DAkkS), „Regel zur Prüfung der Feststellung der Akkreditierungsfähigkeit neuer privater Konformitätsbewertungsprogramme", Regel 71 SD 0 016, Revision 1.3, 27.11.2018.

[5] Datenschutzkonferenz, „Anforderungen zur Akkreditierung gemäß Art. 43 Abs. 3 DSGVO i.V.m. DIN EN ISO/IEC 17065", Version 1.2, 21.01.2020

[6] European Data Protection Board (EDPB), "Guidelines 1/2018 on certification and identifying certification criteria in accordance with Articles 42 and 43 of the Regulation", Version 3.0, 04.06.2019.

[7] European Data Protection Board (EDPB), „Guidelines 4/2018 on the accreditation of certification bodies under Article 43 of the General Data Protection Regulation (2016/679)", Version 3.0, 04.06.2019.