datenschutz cert

dsc-Whitepaper
17.02.2022

Zur Gültigkeit eines DSGVO-Zertifikates

Mit Einführung der Europäischen Datenschutzgrundverordnung (DSGVO) im April 2018 wurde erstmals ein europaweit einheitlicher gesetzlicher Rahmen für eine Datenschutz-Zertifizierung gesetzt. Nun mehren sich die Zeichen, dass diese DSGVO-Zertifizierungen gem. Art. 42 DSGVO bald an den Start gehen könnten. Deshalb stellt sich zunehmend die Frage, wo ein solches DSGVO-Zertifikat gültig ist. Kann eine im Mitgliedsland A nach Art. 43 DSGVO akkreditierte Zertifizierungsstelle DSGVO-Zertifikate im Land B ausstellen? Ist ein im Land A ausgestelltes DSGVO-Zertifikat auch im Land C gültig?

Der vorliegende Beitrag soll diese Frage klären – nicht nur für nationale Kriterien, sondern auch für das berühmte Europäische Datenschutzsiegel („European Data Protection Seal“).

1. Vorbemerkungen

Vorab aber drei Vorbemerkungen:

1. Warum dauert das so lange?
2. Was bedeutet „Gültigkeit“ eigentlich?
3. Wer ist die „zuständige Datenschutzaufsichtsbehörde“?

1.1. Zum Zulassungsprozess

Warum dauert das so lange? Wer sich mit Zertifizierungen auskennt – etwa ISO 9001 oder ISO/IEC 27001 –, der weiß, dass sowohl die Kriterien, wonach geprüft wird, als auch, wie geprüft und zertifiziert wird, durch entsprechende Akkreditierungsnormen[1] weltweit vorgegeben ist. Bei der DSGVO ist das anders: Der Gesetzgeber hat mit der DSGVO den Akkreditierungsrahmen ISO/IEC 17065 für Produkte und Dienstleistungen vorgegeben. Dadurch muss zunächst durch einen sogenannten Programmeigner[2] entwickelt und abgenommen werden:

- das Schema/System, wie geprüft und zertifiziert wird;
- die Kriterien, deren Einhaltung geprüft und mit dem Zertifikat bestätigt wird.

Erst auf dieser Grundlage – Schema und Kriterien – können sich Zertifizierungsstellen akkreditieren lassen.

Hinweis in eigener Sache: Die datenschutz cert GmbH hat 2019 diesen Prozess gestartet und ihr selbst entwickeltes Schema (Konformitätsbewertungsprogramm) mit den Kriterien (Kriterienkatalog) für die „IT-gestützte Verarbeitung personenbezogener

[1] Die Akkreditierungsnorm für Managementsysteme ISO/IEC 17021-1 normiert, wie eine Zertifizierung erfolgt; diese Anforderungen sind mit der ISO/IEC 27006 auf Informationssicherheitsmanagementsysteme (ISMS) gem. ISO/IEC 27001 konkretisiert worden.

[2] Ein Programmeigner kann in diesem Fall z. B. eine Zertifizierungsstelle sein.

Daten“ bei den zuständigen Behörden eingereicht. Die Abnahme[3] durch die Deutsche Akkreditierungsstelle (DAkkS) und die zuständige Datenschutzaufsichtsbehörde – in diesem Fall die Landesbeauftragte für Datenschutz und Informationsfreiheit der Freien Hansestadt Bremen (LfDI Bremen) – ist (vorläufig) abgeschlossen.

1.2. Zur Gültigkeit

Was bedeutet „Gültigkeit“ eigentlich? Es gibt keine gesetzliche Pflicht zur Zertifizierung eines Verarbeitungsvorgangs gem. Art. 42 DSGVO. Ein Zertifikat ist gem. Art. 42 Abs. 3 DSGVO stets freiwillig:

> „Die Zertifizierung muss freiwillig [...] sein.“

Die DSGVO besagt, dass ein Art. 42 DSGVO-Zertifikat als „Faktor“ herangezogen werden kann. Dieser Faktor wird an mehreren Stellen der DSGVO erwähnt:

Für die Einhaltung von Privacy-by-Design und -by-Default gem. Art. 25 Abs. 3 DSGVO:

> „Ein genehmigtes Zertifizierungsverfahren gemäß Artikel 42 kann als Faktor herangezogen werden, um die Erfüllung der in den Absätzen 1 und 2 des vorliegenden Artikels genannten Anforderungen nachzuweisen.“

Für die Einhaltung der DSGVO bei Auftragsverarbeitern gem. Art. 28 Abs. 5 DSGVO:

> „Die Einhaltung [...] eines genehmigten Zertifizierungsverfahrens gemäß Artikel 42 durch einen Auftragsverarbeiter kann als Faktor herangezogen werden, um hinreichende Garantien im Sinne der Absätze 1 und 4 des vorliegenden Artikels nachzuweisen.“

Zur Umsetzung technisch-organisatorischer Maßnahmen gem. Art. 32 Abs. 3 DSGVO:

> „Die Einhaltung [...] eines genehmigten Zertifizierungsverfahrens gemäß Artikel 42 kann als Faktor herangezogen werden, um die Erfüllung der in Absatz 1 des vorliegenden Artikels genannten Anforderungen nachzuweisen.“

Hier kommt ein wichtiger Charakter der DSGVO zum Tragen, wonach der Verantwortliche bzw. Auftragsverarbeiter die Umsetzung und Einhaltung der DSGVO nachweisen muss. Und für diesen Nachweis kann ein DSGVO-Zertifikat als „Faktor“ herangezogen werden.

Warum sollte ein Verantwortlicher oder Auftragsverarbeiter dies tun? Nun, als Vorteile werden häufig genannt:

- Unterstützung der Rechenschaftspflicht gem. Art. 5 Abs. 2 DSGVO: Ein DSGVO-Zertifikat kann als Nachweis für die Erfüllung von Pflichten herangezogen werden, so dass etwa bei der Einbeziehung von Auftragsverarbeitern keine eigenständige Prüfung mehr vorgenommen werden muss.

[3] Lesen Sie auch den Blogbeitrag vom 03.02.2022 zur vorläufigen Annahme unseres „information privacy standard“ unter https://www.datenschutz-notizen.de/dsgvo-zertifizierungsprogramm-vorlaeufig-abgenommen-3033656/

- Besserer Datenschutz: Durch die Prüfung unabhängiger Gutachter steigt das Datenschutzniveau insgesamt. Ebenso verstärkt sich intern die Motivation, Datenschutzthemen umzusetzen, wenn davon eine Zertifizierung abhängt.
- Vorlage bei Aufsichtsbehörden: Das Zertifikat dient zum Nachweis der Erfüllung von Anforderungen z. B. bei einer Prüfung seitens der Behörden.
- Reduktion von Rückstellungen bzgl. Geldbußen: Ein DSGVO-Zertifikat wird im Rahmen der Verhängung von Geldbußen und Festsetzung der Höhe mit einbezogen und kann als ein mildernder Umstand berücksichtigt werden, vgl. Art. 83 Abs. 2 j DSGVO.
- Marktzutrittsvoraussetzung: In bestimmten Bereichen sind Datenschutz-Zertifikate als Qualitätsnachweis erforderlich, z. B. für das Anbieten von Videosprechstunden gemäß § 5 der Anlage 31b zum BMV-Ärzte.
- Haftungsreduzierung: Bei Datenschutz-Vorfällen kann das Zertifikat zu einer Haftungserleichterung führen.
- Besseres Image: Kunden legen vermehrt den Fokus auf Datenschutz – durch ein DSGVO-Zertifikat ergibt sich bei der Gewinnung von Kunden ein Wettbewerbsvorteil gegenüber nicht zertifizierten Unternehmen.
- Und damit nicht zuletzt Wettbewerbsvorteile durch guten Datenschutz.

Wenn schon keine gesetzliche Pflicht zur Vorlage eines DSGVO-Zertifikates besteht, kann es aber doch in einem sehr relevanten Bereich eine Art von Pflicht darstellen: nämlich im Kontext der **Drittstaaten-Übermittlung**; hier kann ein Art. 42 DSGVO-Zertifikat einen zulässigen Mechanismus darstellen, dazu später mehr.

Es kommt also darauf an, wer ein Art. 42 DSGVO-Zertifikat akzeptiert und welchen (Entscheidungs-)Faktor er diesem Zertifikat beimisst.

Beispiel: Ein Unternehmen in Land A möchte einen Auftragsverarbeiter gem. Art. 28 DSGVO einsetzen. Ein DSGVO-Zertifikat soll als Entscheidungskriterium bei der Auswahl eines Dienstleisters dienen. Wenn also ein Auftragsverarbeiter ein DSGVO-Zertifikat aus Land B hat, dann kann das Unternehmen diesen Sachstand mit einem Faktor belegen und entsprechend berücksichtigen. Wenn ein Mitbewerber dieses Auftragsverarbeiters sogar ein DSGVO-Zertifikat aus Land A vorweist, ist dieser Faktor womöglich größer.

Worauf es hier im Detail ankommt – und warum die Ländergrenzen so entscheidend sind –, dazu gleich mehr nach der letzten Vorbemerkung.

1.3. Zur Zuständigkeit der Aufsichtsbehörden

Wer ist die „zuständige Datenschutzaufsichtsbehörde“? Der Begriff der „zuständigen Aufsichtsbehörde“ taucht in der DSGVO an vielen Stellen auf – aber Obacht: in verschiedenen Bedeutungen. Manchmal ist die für eine Zertifizierungsstelle zuständige Aufsichtsbehörde gemeint, manchmal aber die für einen Verantwortlichen oder Auftragsverarbeiter zuständige Aufsichtsbehörde, der über einen DSGVO-zertifizierten Verarbeitungsvorgang verfügt.

Zunächst taucht der Begriff der „zuständigen Aufsichtsbehörden“ im Kontext der Zertifizierung i. S. d. DSGVO bei der Abnahme der Kriterien auf, vgl. Art. 43 Abs. 3 DSGVO:

„Die Akkreditierung von Zertifizierungsstellen nach den Absätzen 1 und 2 erfolgt anhand der Anforderungen, die von der gemäß Artikel 55 oder 56 zuständigen Aufsichtsbehörde [...] genehmigt wurden."

Zuständige Aufsichtsbehörde ist hier die für den Programmeigner zuständige Aufsichtsbehörde.

Dann taucht der Begriff der „zuständigen Aufsichtsbehörden" im Kontext der Zulassung von Zertifizierungsstellen auf, vgl. Art. 43 Abs. 1 lit. b DSGVO:

„Die Mitgliedstaaten stellen sicher, dass diese Zertifizierungsstellen von [...] folgenden Stellen akkreditiert werden: [...]

b) der nationalen Akkreditierungsstelle, die gemäß der Verordnung (EG) Nr. 765/2008 des Europäischen Parlaments und des Rates im Einklang mit EN-ISO/IEC 17065/2012 und mit den zusätzlichen von der gemäß Artikel 55 oder 56 zuständigen Aufsichtsbehörde festgelegten Anforderungen benannt wurde."

Hier ist die zuständige Aufsichtsbehörde also die für eine Zertifizierungsstelle zuständige Aufsichtsbehörde.

Und sodann wird der Begriff der „zuständigen Aufsichtsbehörden" im Kontext der Zertifizierung von Verarbeitungsvorgängen von Verantwortlichen und Auftragsverarbeitern genannt, vgl. Art. 43 Abs. 1 DSGVO:

„Unbeschadet der Aufgaben und Befugnisse der zuständigen Aufsichtsbehörde gemäß den Artikeln 57 und 58 erteilen oder verlängern Zertifizierungsstellen [...] nach Unterrichtung der Aufsichtsbehörde — damit diese erforderlichenfalls von ihren Befugnissen gemäß Artikel 58 Absatz 2 Buchstabe h Gebrauch machen kann — die Zertifizierung."

Dies ist wichtig: Hier ist die Aufsichtsbehörde zuständig, die im Geltungsbereich des Verantwortlichen oder Auftragsverarbeiters liegt, deren Verarbeitungsvorgang geprüft und zertifiziert wurde. Denn gem. Art. 58 Abs. 2 lit. h DSGVO gilt:

„Jede Aufsichtsbehörde verfügt über sämtliche folgenden Abhilfebefugnisse, die es ihr gestatten, [...]

h) eine Zertifizierung zu widerrufen oder die Zertifizierungsstelle anzuweisen, eine gemäß den Artikel 42 und 43 erteilte Zertifizierung zu widerrufen, oder die Zertifizierungsstelle anzuweisen, keine Zertifizierung zu erteilen, wenn die Voraussetzungen für die Zertifizierung nicht oder nicht mehr erfüllt werden [...]."

Weitere Fundstellen zu den Aufgaben und Befugnissen der Aufsichtsbehörde in ihrem Hoheitsgebiet finden sich u.a. in Art. 57 Abs. 1 lit. n DSGVO:

„Unbeschadet anderer in dieser Verordnung dargelegter Aufgaben muss jede Aufsichtsbehörde in ihrem Hoheitsgebiet [...]

n) die Einführung von Datenschutzzertifizierungsmechanismen und von Datenschutzsiegeln und -prüfzeichen nach Artikel 42 Absatz 1 anregen und Zertifizierungskriterien nach Artikel 42 Absatz 5 billigen [...]“

Oder in Art. 57 Abs. 1 lit. o DSGVO:

„Unbeschadet anderer in dieser Verordnung dargelegter Aufgaben muss jede Aufsichtsbehörde in ihrem Hoheitsgebiet [...]

o) gegebenenfalls die nach Artikel 42 Absatz 7 erteilten Zertifizierungen regelmäßig überprüfen [...]“

Sowie in Art. 58 Abs. 1 lit. c DSGVO:

„Jede Aufsichtsbehörde verfügt über sämtliche folgenden Untersuchungsbefugnisse, die es ihr gestatten, [...]

c) eine Überprüfung der nach Artikel 42 Absatz 7 erteilten Zertifizierungen durchzuführen [...]“

Damit ist klar: In Art. 42 Abs. 1 DSGVO geht es also um die grundsätzlichen Befugnisse einer Aufsichtsbehörde, ein konkretes Zertifikat betreffend, dies kann meiner Meinung nach nicht auf die für die Zertifizierungsstelle zuständige Aufsichtsbehörde reduziert werden. Dazu Art. 55 Abs. 1 DSGVO:

„Jede Aufsichtsbehörde ist für die Erfüllung der Aufgaben und die Ausübung der Befugnisse, die ihr mit dieser Verordnung übertragen wurden, im Hoheitsgebiet ihres eigenen Mitgliedstaats zuständig.“

Merke: Eine Aufsichtsbehörde ist stets für ihr jeweiliges Territorium zuständig.

Diese Überlegungen präzisieren damit auch eine Vorgabe der deutschen Datenschutzkonferenz (DSK)[4]:

„Die Zertifizierungsstelle unterrichtet die zuständige Datenschutzaufsichtsbehörde über die Zertifizierung schriftlich mindestens eine Woche vor Erteilung der Zertifizierung. Diese Unterrichtung muss den Namen des Kunden, die Beschreibung des Zertifizierungsgegenstands und das öffentliche Kurzgutachten enthalten.“

Fazit: Damit ist hier als zuständige Aufsichtsbehörde diejenige gemeint, die für den Verantwortlichen oder Auftragsverarbeiter zuständig ist, der ein DSGVO-Zertifikat anstrebt.

Dazu noch ein interessanter Ansatz zu Abs. 7.1.2 aus dem DSK-Papier[4]:

4 Datenschutzkonferenz, „Anforderungen zur Akkreditierung gemäß Art. 43 Abs. 3 DS-GVO i. V. m. DIN EN ISO/IEC 17065“, Version 1.4, 08.10.2020.

„Die zuständige Aufsichtsbehörde ist zu benachrichtigen, bevor eine Zertifizierungsstelle in einem neuen Mitgliedstaat von einem Satellitenbüro aus ein zugelassenes Europäisches Datenschutzgütesiegel in Betrieb nimmt."

Wer ist hier die „zuständige Aufsichtsbehörde"? Dazu müsste zunächst das Wort „Satellitenbüro" näher erläutert werden. Eine Definition fehlt jedoch im DSK-Papier. Es scheint aber, dass hier ein Büro gemeint ist, in dem keine für die Zertifizierung relevanten Aktivitäten stattfinden, also insbesondere keine Zertifizierungsentscheidungen. Das Satellitenbüro ist also keine „critical location" und somit nicht Bestandteil der Akkreditierung. Damit ist hier auch die zuständige Aufsichtsbehörde in dem neuen Mitgliedstaat gemeint. Eventuell ist es aber auch sinnvoll, die für die Zertifizierungsstelle zuständige Aufsichtsbehörde zu benachrichtigen.

Übrigens ist diese Diskussion womöglich nur innerhalb Deutschlands mit dem föderalen Ansatz und den Zuständigkeiten der Landesbeauftragten für den Datenschutz interessant, und weniger in EU-Ländern, die nur eine zentrale Aufsichtsbehörde haben.

Andererseits ergeben diese Überlegungen vielleicht wiederum Sinn, wenn man perspektivisch über das Europäische Datenschutzsiegel nachdenkt – dazu später mehr.

2. Szenarien

Bevor nun verschiedene Szenarien beleuchtet werden, welche Zertifizierungsstelle aus welchem Land nach welchen Kriterien einen Verarbeitungsvorgang zertifiziert, kurz zur Erinnerung:

„Die Akkreditierung von Zertifizierungsstellen nach den Absätzen 1 und 2 erfolgt anhand der Anforderungen, die von der gemäß Artikel 55 oder 56 zuständigen Aufsichtsbehörde [...] genehmigt wurden."

Das bedeutet, dass Schema und Kriterien für das jeweilige Land zugelassen werden.

Hintergrund sind vor allem die Öffnungsklauseln, die in der DSGVO für nationale Besonderheiten vorgesehen sind, und in den Zertifizierungskriterien entsprechend berücksichtigt werden müssen.

Beispiel A: Ein Programmeigner in Land A erstellt Schema und Kriterien, die Abnahme erfolgt durch die zuständige Aufsichtsbehörde in Land A. Anschließend lässt sich eine Zertifizierungsstelle in Land A nach diesem Schema mit Kriterien akkreditieren und kann danach Verarbeitungsvorgänge von Verantwortlichen und Auftragsverarbeitern in Land A zertifizieren; hier liegt sodann eine volle Akzeptanz und Gültigkeit vor. Die Wirkung als „Faktor" für eine Entscheidung wäre somit maximal.

Beispiel B: Die Zertifizierungsstelle in Land A zertifiziert einen Verarbeitungsvorgang in Land B. Da die Kriterien für Land B nicht abgenommen sind, muss hier angenommen werden, dass die Wirkung als „Faktor" geringer ausfällt.

Der Programmeigner könnte aber natürlich das Schema und die Kriterien auch in Land B abnehmen lassen und sich eine Zertifizierungsstelle danach in Land B akkreditieren lassen. Dann gäbe es auch die volle Gültigkeit in Land B.

3. Europäisches Datenschutzsiegel

Damit aber nicht alle Programmeigner ihr Schema mit Kriterien in allen EU-Staaten abnehmen lassen müssen, sieht die DSGVO das Europäische Datenschutzsiegel („European Data Protection Seal"; nicht zu verwechseln mit dem privatwirtschaftlichen EuroPriSe-Siegel) vor, vgl. Art. 42 Abs. 5 DSGVO:

> „Werden die Kriterien vom Ausschuss genehmigt, kann dies zu einer gemeinsamen Zertifizierung, dem Europäischen Datenschutzsiegel, führen."

Die Idee des Europäischen Datenschutzsiegel ist es, dass Schema und Kriterien vom Europäischen Datenschutz-Ausschuss (EDSA)[5] unter Einbeziehung aller Aufsichtsbehörden der EU geprüft und abgenommen werden und auf einer Webseite[6] gelistet werden. Derzeit (Stand 17.02.2022) gibt es noch keine Einträge auf dieser Webseite.

Der Zulassungsprozess für diese Genehmigung ist definiert[7]; dieser Prozess sieht eine umfangreiche Stellungnahme der Aufsichtsbehörden der EU-Staaten vor, wobei die für den Programmeigner zuständige Aufsichtsbehörde eine wichtige und zentrale Rolle einnimmt.

Wenn dann ein Schema mit Kriterien vom EDSA abgenommen sein sollte, gilt folgendes:

Eine Zertifizierungsstelle lässt sich in Land A durch die zuständigen Aufsichtsbehörden akkreditieren. Ein wichtiger Aspekt dieser Akkreditierung wird in jedem Fall die Kenntnis der entsprechenden nationalen Gesetze und Auslegung etwaiger Öffnungsklauseln sein.

Dann müsste gelten: Eine Zertifizierungsstelle aus Land A zertifiziert Verarbeitungsvorgänge von Verantwortlichen und Auftragsverarbeitern in Land B mit dem Europäischen Datenschutzsiegel. Dieses Zertifikat genießt auch in Land B die volle Gültigkeit und Akzeptanz (Wirkung als „Faktor" wäre maximal).

4. Drittstaaten

Regelmäßig stellt die Übermittlung personenbezogener Daten in Drittländer Unternehmen vor Probleme. In diesen Fällen müssen geeignete Garantien vorgelegt werden. Diese können gem. Art. 46 Abs. 2 lit. f DSGVO in einem genehmigten Zertifizierungsmechanismus liegen.

> (2) Die in Absatz 1 genannten geeigneten Garantien können, ohne dass hierzu eine besondere Genehmigung einer Aufsichtsbehörde erforderlich wäre, bestehen in [...]
>
> f) einem genehmigten Zertifizierungsmechanismus gemäß Artikel 42 zusammen mit rechtsverbindlichen und durchsetzbaren Verpflichtungen des Verantwortlichen oder

---

[5] engl. European Data Protection Board (EDPB)

[6] Die Webseite ist erreichbar unter https://edpb.europa.eu/our-work-tools/accountability-tools/certification-mechanisms-seals-and-marks_de

[7] EDPB, „EDSA-Dokument über das zu einer gemeinsamen Zertifizierung („Europäisches Datenschutzsiegel") führende Verfahren zur Genehmigung von Zertifizierungskriterien durch den EDSA", 28. Januar 2020

des Auftragsverarbeiters in dem Drittland zur Anwendung der geeigneten Garantien, einschließlich in Bezug auf die Rechte der betroffenen Personen [...]“

Damit wäre also folgendes Szenario denkbar: Ein Unternehmen in Land C, das kein Mitgliedsstaat der EU ist, lässt einen Verarbeitungsvorgang von einer Zertifizierungsstelle in Land A (Mitglied der EU) zertifizieren, deren nationale Kriterien nur für Land A zugelassen ist. Die volle Gültigkeit ist hier nur aus dem Land A heraus zu erwarten. Falls hier Kriterien des Europäischen Datenschutzsiegels angewendet werden, wäre es innerhalb der EU vollständig gültig. Die zuständige Aufsichtsbehörde wäre in diesem Fall übrigens der Ausschuss, vgl. dazu Art. 70 Abs. 1 lit. o DSGVO:

(1) Der Ausschuss stellt die einheitliche Anwendung dieser Verordnung sicher. Hierzu nimmt der Ausschuss von sich aus oder gegebenenfalls auf Ersuchen der Kommission insbesondere folgende Tätigkeiten wahr: [...]

o) [...] Führung eines öffentlichen Registers [...] der in Drittländern niedergelassenen zertifizierten Verantwortlichen oder Auftragsverarbeiter gemäß Artikel 42 Absatz 7 [...]“

5. Satellitenbüro

Zum Abschluss noch eine akkreditierungstechnische Besonderheit unter dem Stichwort „Satellitenbüro“:

Eine Zertifizierungsstelle, akkreditiert in Land A, hat ein Büro in Land B. In dem Büro in Land B werden keine zertifizierungskritischen Aktivitäten durchgeführt – das Büro ist also „non-critical“. Die Zertifikate entstammen nach wie vor der Zertifizierungsstelle aus Land A.

Wenn aber im Büro in Land B auch zertifizierungsrelevante Aktivitäten („critical“) ausgeführt werden sollen, müsste sich die Zertifizierungsstelle in Land B auch akkreditieren lassen und die Befugnis erteilt bekommen, vgl. Art. 43 Abs. 1 lit. b DSGVO:

„Die Mitgliedstaaten stellen sicher, dass diese Zertifizierungsstellen von [...] folgenden Stellen akkreditiert werden: [...]

b) der nationalen Akkreditierungsstelle, die gemäß der Verordnung (EG) Nr. 765/2008 des Europäischen Parlaments und des Rates im Einklang mit EN-ISO/IEC 17065/2012 und mit den zusätzlichen von der gemäß Artikel 55 oder 56 zuständigen Aufsichtsbehörde festgelegten Anforderungen benannt wurde.“

Eine erneute Akkreditierung müsste gleichwohl über die EU-Richtlinie 765/2008 zur Akkreditierungslandschaft[8] nicht erforderlich sein, da sich sonst EU-Richtlinie und -Verordnung entgegenstehen würden.

[8] VERORDNUNG (EG) Nr. 765/2008 DES EUROPÄISCHEN PARLAMENTS UND DES RATES vom 9. Juli 2008 über die Vorschriften für die Akkreditierung und Marktüberwachung im Zusammenhang mit der Vermarktung von Produkten und zur Aufhebung der Verordnung (EWG) Nr. 339/93 des Rates

6. Fazit

DSGVO-Zertifikate werden kommen. Und sie werden perspektivisch so selbstverständlich sein wie ISO/IEC 27001-Zertifikate bei Rechenzentren. Sie werden eine wichtige Grundlage für Datenübermittlung in Drittstaaten darstellen und sie werden – neben einer Haftungsreduktion – maßgeblich ein Qualitätskriterium für Auftragsverarbeiter darstellen.

DSGVO-Zertifikate werden aber kein rein nationales Thema sein. Sie werden europaweite Gültigkeit, Akzeptanz und Relevanz haben. Von daher ist die Frage, nach welchem Schema welche Zertifizierungsstelle aus welchem Land einen Verarbeitungsvorgang eines Verantwortlichen oder Auftragsverarbeiters aus welchem Land zertifiziert, essentiell.

Die gesetzlichen Vorgaben und Interpretationen der Behörden liegen vor, erscheinen aber nicht nur anspruchsvoll, sondern in Teilen auch widersprüchlich und manchmal missverständlich formuliert.

Was denken Sie? Haben Sie andere Interpretationen? Schreiben Sie mir!