Teil III: Fairness und Governance

Datenschutzzertifizierung: Ende des Dornröschenschlafs? Potentiale und Erfolgsfaktoren der Zertifizierung als Instrument für eine effektive und grundrechtsorientierte Data Governance[1]

Gerrit Hornung und Marcel Kohpeiß

Zusammenfassung

Das Vollzugsdefizit des „alten" Datenschutzrechts war ein zentrales Motiv des europäischen Gesetzgebers für seine Reform. Das Governance-System der DSGVO verfügt nunmehr über einen Instrumentenmix, bei dem gerade die Zertifizierung erhebliche Potentiale für eine Effektuierung des Datenschutzes hat. Die ersten genehmigten Programme und aktuelle Diskussionen zeigen allerdings, dass eine effektive Zertifizierung voraussetzungsvoll ist und etliche Fragen ungeklärt sind. Zwei zentrale Herausforderungen sind der Umgang mit spezialgesetzlichen Anforderungen und mit ungeklärten, für die Verarbeitungspraxis wichtigen Rechtsfragen; Letzteres lässt sich exemplarisch an der Frage der Drittlandsübermittlung verdeutlichen. (Nur) wenn diese und andere Herausforderungen adressiert werden, kann die Zertifizierung ein wichtiger Baustein einer grundrechtsorientierten Data Governance der Zukunft werden.

1. Einleitung

Das Konzept einer unabhängigen Prüfung, ob datenschutzrechtliche Vorgaben beim Angebot von Waren oder Dienstleistungen eingehalten werden, ist inzwischen mehr als 20 Jahre alt. Auf Basis dieser Überlegungen[2] und der überzeugenden Argumente für derartige unabhängige Überprüfungs-

1 Der Text ist im Rahmen des BMBF-Projekts Data Protection Certification for Educational Information Systems (DIRECTIONS) (FKZ 01PP21003C) entstanden.

2 Eine erste umfassende Konzeption eines Audits (die tlw. mit der „Zertifizierung" nach der DSGVO deckungsgleich ist) findet sich bei *Roßnagel*, Datenschutzaudit: Konzeption, Durchführung, gesetzliche Regelung, 2000; ferner *Bizer*, in: Bäumler/v. Mutius, Datenschutzgesetze der dritten Generation, 1999, S. 54 ff.; zum Überprüfungskonzept: *Königshofen*, DuD 2000, 357-360; *Drews/Kranz*, DuD 2000, 226-230.

konzepte verabschiedeten mehrere Bundesländer gesetzliche Regelungen.[3] Wichtigstes Beispiel für eine erfolgreich umgesetzte und genutzte Regelung war § 4 LDSG-SH a.F., der i.V.m. mit der Datenschutzauditverordnung-SH zu einer Vielzahl von Datenschutzaudits und Zertifizierung führte.[4]

Nicht zuletzt wegen des Erfolges dieses Selbstregulierungsinstruments sowie wegen nachfolgender, europaweiter Forschungsaktivitäten im Bereich der Datenschutzzertifizierungen und Datenschutzaudits[5] gelang es, das Thema in den Gesetzgebungsprozess der europäischen Datenschutzreform einzubringen und Zertifizierungsvorschriften in Art. 42 und Art. 43 DSGVO zu verankern. Diese dienen nunmehr als europaweit einheitliche Rechtsgrundlagen für die Zertifizierung, den Zertifizierungsprozess sowie die Akkreditierung von Zertifizierungsstellen und müssen nur an wenigen Stellen durch nationale Umsetzungsvorschriften ergänzt werden.[6]

Aus einer breiteren Perspektive fügen sich die genannten Regelungen der DSGVO in ein Geflecht von Zertifizierungen ein, das gerade im IT-Bereich in den letzten Jahren ständig dichter und zugleich heterogener geworden ist. Weitere Beispiele sind die Cybersicherheitszertifizierung gem. Art. 58 des Rechtsakts zur Cybersicherheit[7] i.V.m. § 9a BSIG, das KRITIS-Sicherheitszertifikat nach § 8a Abs. 3, Abs. 5 BSIG sowie das freiwillige IT-Sicherheitskennzeichen nach § 9c BSIG.[8]

Eine effektive Zertifizierung von Datenverarbeitungsvorgängen eröffnet erhebliche Chancen für eine Vielzahl von Akteuren (Abschnitt 2). Es ist deshalb nicht verwunderlich, dass große Hoffnungen in die neuen europäischen Regelungen gelegt werden. Demgegenüber ist das Zwischenergebnis einigermaßen ernüchternd, denn von außen betrachtet scheint die Zertifizierung seit der Verabschiedung der DSGVO im Jahre 2016 zu schlafen: Eine Zertifizierung von Datenverarbeitungsvorgängen nach der DSGVO ist bisher nicht erfolgt. Jedoch scheint es nach über fünf Jahren Licht am

3 Z.B. § 5 DSG-MV a.F., § 7b BremDSG a.F., § 4 LDSG-SH a.F.

4 Durch das ULD vergebenen Gütesiegel: https://www.datenschutzzentrum.de/guetesiegel/register/.

5 V.a. das EuroPriSe-Projekt, das sich bereits 2009 als Ansatz zu einem europäischen Datenschutzsiegel aus dem Siegel des ULD heraus entwickelte; zur historischen Entwicklung s. *Richter*, ZD 2020, 84 (85).

6 In Deutschland § 39 BDSG.

7 VO (EU) 2019/881; näher *Mirtsch*, in: Mangelsdorf u.a. (Hrsg.), Normen und Standards für die digitale Transformation, 2019, 141 (151 ff.); *Kowalski*/*Intemann*, DuD 2018, 415-419.

8 Dazu *Hornung*, NJW 2021, 1985 (1989); *Schallbruch*, CR 2021, 450 (457 f.); zum Verfahren: BSI, Verfahrensbeschreibung zur Erteilung von IT-Sicherheitskennzeichen, 2022.

Ende des Tunnels zu geben: Gegen Ende des Jahres 2022 bogen mehrere Zertifizierungsprogramme auf die Zielgerade ein, und ein erstes Programm wurde genehmigt (Abschnitt 3). Diese und andere noch folgende Programme werden sich in den nächsten Jahren teils ergänzen und teils zueinander in Konkurrenz treten. Im Rahmen dieses Wettbewerbs werden sich mit zunehmender Anwendung der einzelnen Kriterienkataloge neue Gewohnheiten und Best Practices herausbilden, aber auch neue Probleme in der Anwendung und hinsichtlich der zu erzielenden Wirkung offenbaren. Schon jetzt ist absehbar, dass eine effektive Datenschutzzertifizierung vor noch ungelösten Problemen steht, die von den bisherigen Zertifizierungsprogrammen noch nicht vollständig adressiert werden (Abschnitt 4). Der vorläufige Zwischenstand ergibt deshalb, dass die Zertifizierung erhebliche Chancen für eine effektive Data Governance eröffnet, bis auf Weiteres aber offenbleibt, ob diese Potenziale gehoben werden können (Abschnitt 5).

2. Zertifizierung als Data Governance-Instrument

Die DSGVO hat eine umfassende Konsolidierung des Datenschutzrechts auf europäischer Ebene bewirkt. Im Innovationsgehalt unterscheiden sich ihre materiellrechtlichen und ihre verfahrensrechtlichen Teile erheblich.[9] Während sich erstere nur moderat von der alten Datenschutz-Richtlinie (DSRL) abheben (wie etwa der Vergleich von Art. 5, 6 und 9 DSGVO mit Art. 6, 7 und 8 DSRL ergibt), hat die Verordnung die datenschutzrechtlichen Governance-Instrumente grundlegend neu geordnet, um dem noch unter der DSRL bestehenden Vollzugsdefizit des europäischen Datenschutzrechts zu begegnen.[10]

2.1 Governance-Instrumente der DSGVO

Bemerkenswert ist dabei, dass der europäische Gesetzgeber sowohl klassische hoheitliche Instrumente wie aufsichtsbehördliche Anordnungsbefugnisse und Bußgelder gestärkt, als auch andere Instrumente der DSRL modifiziert oder Governance-Instrumente gänzlich neu in das europäische Datenschutzrecht eingeführt hat, so u.a. im Bereich der regulierten Selbstregu-

9 *Hornung/Spiecker gen. Döhmann*, in: Simitis u.a. (Hrsg.), Datenschutzrecht, 2019, Einl. Rn. 208 ff.

10 Ebd., m.w.N.

lierung. Beispiele dafür bilden, neben der neuen Zertifizierung (Art. 42, 43 DSGVO), die Möglichkeit zur Ausarbeitung von Verhaltensregeln (Art. 40, 41 DSGVO) sowie die erstmals europaweit vorgesehene Pflicht zur Benennung eines Datenschutzbeauftragten (Art. 37, 38 DSGVO).

Mit der Stärkung bereits in der DSRL existierender und der Einführung neuer Durchsetzungsinstrumente hat der europäische Gesetzgeber demnach den Versuch unternommen, den zum großen Teil bereits in der DSRL enthaltenen materiellen Anforderungen an Datenverarbeitungsprozesse zu mehr praktischer Wirksamkeit zu verhelfen. Der Zertifizierung als zuvor nicht im europäischen Datenschutzrecht enthaltenes Governance-Instrument kommt dabei eine zentrale Rolle zu.

2.2 Funktionen der Datenschutz-Zertifizierung

Aus einer Governance-Perspektive vermag die Zertifizierung mehrere Funktionen zu erfüllen.[11] Wenn eine Zertifizierungsstelle oder eine Aufsichtsbehörde gemäß Art. 42 Abs. 1 DSGVO die Einhaltung der Verordnung bei Verarbeitungsvorgängen eines Verantwortlichen oder Auftragsverarbeiters bestätigt, so gewinnen diese – erstens – für sich selbst, aber auch im Falle eines späteren Rechtsstreits ein erhebliches Maß an Sicherheit hinsichtlich der Rechtskonformität ihres Vorgehens. Eine Zertifizierung bietet nach der Verordnung zwar keine vollständige Gewähr hierfür, da sie lediglich einen „Faktor" bzw. „Gesichtspunkt" bei der Bewertung bildet.[12] Es steht aber zu erwarten, dass in der aufsichtsbehördlichen und gerichtlichen Praxis eine zumindest weitreichende faktische Rechtssicherheit gewonnen werden kann.

Durch eine solche Orientierung der Aufsichtsbehörden an einer zuverlässigen Zertifizierung könnte – zweitens – die aufsichtsbehördliche Tätigkeit deutlich erleichtert werden. Dieser Faktor ist wichtig, da die Behörden trotz der personellen Erweiterung im Zuge der Verabschiedung der DSGVO nach wie vor nicht über die Ressourcen verfügen, um dem Daten-

11 *Scholz,* in: Simitis u.a. (Hrsg.), Datenschutzrecht, 2019, Art. 42 DSGVO Rn. 4 ff. m.w.N.

12 S. Art. 24 Abs. 3 DSGVO (allgemeine Verantwortlichkeit), Art. 25 Abs. 3 DSGVO (Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen), Art. 28 Abs. 5 DSGVO (Beauftragung eines zuverlässigen Auftragsverarbeiters), Art. 32 Abs. 3 DSGVO (Sicherheit der Verarbeitung). Darüber hinaus kann die Zertifizierung gemäß Art. 46 Abs. 2 lit. f DSGVO auch eine geeignete Garantie für die Übermittlung in Drittländer sein, s.u. Kap. 4.2.2.

schutz in den vielfältigen Einzelfallgestaltungen der Praxis zu Wirksamkeit zu verhelfen.[13]

Ein wesentliches Element schon der allerersten Konzepte einer Datenschutzzertifizierung gilt außerdem auch für die DSGVO, nämlich – drittens – die Hoffnung, mit einer freiwilligen Zertifizierung der Verantwortlichen und Auftragsverarbeiter Marktanreize zur Entwicklung und zum Einsatz rechtskonformer technischer Lösungen zu setzen.[14] Denn erfolgreiche Zertifizierungen bieten die Möglichkeit, gegenüber Kunden eine nicht nur behauptete, sondern eine nachgewiesene Einhaltung des geltenden Datenschutzrechts zu demonstrieren. Eine entsprechende Nachfrage anderer Marktteilnehmer vorausgesetzt, würde sich aus diesem Wettbewerbsvorteil ein Druck auf konkurrierende Anbieter ergeben, sich ebenfalls einer Zertifizierung zu unterziehen.

Wenn sich die Zertifizierung wichtiger Anbieter in dieser Weise allgemein verbreitet, so würde schlussendlich – viertens – die Durchsetzung des Datenschutzrechts in Europa allgemein verbessert und damit das Grundrecht auf Datenschutz der betroffenen Personen gestärkt. Dies gilt auch in internationaler Perspektive, also mit Blick auf eine globale Data Governance. Denn die Zertifizierung bietet mehrere Ansatzpunkte für eine Regulierung globaler Datenflüsse und einen „Export" europäischer Datenschutzstandards und der mit ihnen verbundenen Wertvorstellungen. Es ist nicht unwahrscheinlich, dass „weiche" Durchsetzungsinstrumente wie die Zertifizierung auf einer globalen Ebene sogar effektiver sind als der Versuch, mit klassischen Methoden von Befehl und Zwang zu operieren.[15]

---

13 *Roßnagel*, Datenschutzaufsicht nach der EU-Datenschutz-Grundverordnung, 2017, 179.

14 Zu diesen erhofften Markteffekten vgl. u.a.: *Roßnagel* in: Roßnagel (Hrsg.) Handbuch Datenschutzrecht, 2003, Kap. 3.7 Rn. 1ff.; *Bäumler*, DuD 2004, 80 ff.; s. allgemeiner die Beiträge in *Bäumler/v. Mutius* (Hrsg.), Datenschutz als Wettbewerbsvorteil, 2002.

15 Dieses Problem soll hier nicht vertieft werden. Das im Ausgangspunkt umfassendste Instrument zur globalen Verbreitung europäischer Standards ist die unmittelbare Erstreckung der DSGVO auf Anbieter in Drittländern, wie sie nach dem Marktortprinzip (Art. 3 Abs. 2 lit. a DSGVO) bzw. dem Beobachtungsprinzip (Art. 3 Abs. 2 lit. b DSGVO) erfolgt. Diese Erstreckung leidet jedoch an grundsätzlichen Durchsetzungsproblemen, da die Verantwortlichen in diesen Fällen noch nicht einmal eine Niederlassung in der Union haben. Zwar können auch Zertifizierungsstellen nur begrenzt auf Anbieter aus Drittländern Einfluss nehmen. Immerhin bleibt aber als Sanktionen der Entzug der Zertifizierung möglich, und allgemein könnten weiche Instrumente, die Gegebenheiten im Drittland gegebenenfalls stärker berücksichtigen, in anderen Weltregionen auf Dialogbereitschaft treffen und so besser zur globalen Standardsetzung beitragen als aufsichtsbehördliche Anstrengungen.

2.3 Komplexität der Abläufe

Das Instrument der Zertifizierung lässt sich auf verschiedene Arten gestalten. An einem Ende des Spektrums sind Selbstzertifizierungen zu verorten, bei denen keinerlei externe Stelle eine Prüfung vornimmt, sondern allenfalls Sanktionen für den Fall drohen, dass die Behauptung der Einhaltung bestimmter Standards nicht den Tatsachen entspricht. Am anderen Ende stehen staatliche Zertifizierungen, die gesetzlich als Voraussetzung für den Markteintritt eines Anbieters vorgeschrieben werden. Das Zertifizierungskonzept der DSGVO ist innerhalb dieses Spektrums in einem mittleren Bereich zu verorten. Die Zertifizierung ist nach Art. 42 Abs. 3 DSGVO freiwillig. Sie wird gemäß Art. 42 Abs. 5 DSGVO durch eine neutrale Stelle, d.h. eine Aufsichtsbehörde oder eine nach Art. 43 DSGVO akkreditierte Zertifizierungsstelle, vorgenommen. Die staatliche Letztverantwortung wird insbesondere bei privaten Zertifizierungsstellen durch die Akkreditierung, die aufsichtsbehördliche Kontrolle der akkreditierten Stelle (Art. 43 Abs. 7 i.V.m. Art. 58 Abs. 2 lit. h DSGVO) sowie die notwendige Genehmigung der Zertifizierungskriterien (Art. 42 Abs. 5 DSGVO) durch die zuständige Aufsichtsbehörde oder den Europäischen Datenschutzausschuss (EDSA) sichergestellt.

Nur unvollständig werden demgegenüber in der Verordnung selbst die Verfahrensabläufe geregelt, die im Vorfeld der Genehmigung der Zertifizierungskriterien absolviert werden müssen.[16] Dies gilt insbesondere für die Rolle des sog. Programmeigners, nämlich einer Person oder Organisation, die v.a. für die Entwicklung und Aufrechterhaltung des Konformitätsbewertungsprogrammes einer Zertifizierung verantwortlich ist[17] und dieses im Anschluss entweder selbst als Zertifizierungsstelle nutzt oder an andere Zertifizierungsstellen lizensiert.

16 Zum Verfahren: DSK, Anforderungen an datenschutzrechtliche Zertifizierungsprogramme, Version 1.8, v. 16.04.2021; EDSA, Document on the procedure for the adoption of the EDPB opinions regarding national criteria for certification and European Data Protection Seals, v. 14.02.2023.

17 Vgl. DIN EN ISO/IEC 17065:2021 Ziffer 3.11, sowie DIN EN ISO/IEC 17067:2013 Ziffer 6.3.

3. Aktueller Stand Deutschland und Europa

Nach einigen Jahren des Dornröschenschlafs seit Inkrafttreten der DSGVO hat die Entwicklung von Datenschutzzertifizierungen im Jahre 2022 eine erhebliche Dynamik gewonnen. Mehr als viereinhalb Jahre nach dem Geltungsbeginn der DSGVO genehmigte die luxemburgische Aufsichtsbehörde (CNPD) mit dem Kriterienkatalog „GDPR-Certified Assurance-Report based Processing Activities (GDPR-CARPA)" das europaweit erste DSGVO-Zertifizierungsprogramm.[18] Nach Akkreditierung der EY PFS Solutions S.à r.l ist die EU-weit erste akkreditierte DSGVO-Zertifizierungsstelle bereits fähig nach dem GDPR-CARPA-Programm zu zertifizieren. Bei CARPA handelt es sich um einen Kriterienkatalog, der einen allgemeinen Ansatz verfolgt. Der Anwendungsbereich der Zertifizierung, bzw. des Kriterienkataloges ist dementsprechend nicht beschränkt. Jegliche Verarbeitungsprozesse Verantwortlicher und Auftragsverarbeiter lassen sich, unabhängig von den verwendeten Technologien, anhand des Katalogs auf ihre Vereinbarkeit mit den Voraussetzungen der DSGVO überprüfen.[19]

Einen ebenso als allgemein zu klassifizierenden Ansatz verfolgt der nachfolgend im Jahr 2022 genehmigte Kriterienkatalog des European Privacy Seals (EuroPriSe), das mittlerweile durch eine privatwirtschaftliche GmbH getragen wird. Nach der Genehmigung durch die Aufsichtsbehörde Nordrhein-Westfalens im Oktober 2022 hat EuroPriSe nun auch seinen Kriterienkatalog veröffentlicht, eine genehmigte Akkreditierungsstelle gibt es (Stand August 2023) jedoch auch in Deutschland noch nicht. Die allgemein gehaltenen EuroPriSe-Kriterien können lediglich auf Verarbeitungsprozesse von Auftragsverarbeitern angewendet werden, dies allerdings unabhängig von den verwendeten Technologien.

Von diesen allgemeinen sind sektor- und technologiebezogene Zertifizierungen und deren Kriterienkataloge zu unterscheiden. Zu diesen gehören bspw. das Programm European Cloud Service Data Protection Certification (AUDITOR) sowie das Anschlussprojekt Data Protection Certification for Educational Information Systems (DIRECTIONS). AUDITOR adres-

18 Zum Verfahrensstand: CNPD, Die CNPD nimmt «GDPR-CARPA» an.; CARPA-Kriterien: CNPD, Décision N° 15/2022, 2022; CNPD, Die CNPD ist die erste Datenschutzbehörde in Europa, die einer DSGVO-Zertifizierungsstelle Akkreditierung erteilt hat.

19 Zum Inhalt *Helmke/Link/Schild*, DuD 2023, 100-107.

siert bisher ausschließlich Anbieter von Cloud-Dienstleistungen.[20] Der AUDITOR-Kriterienkatalog befindet sich aktuell in den letzten Zügen des Genehmigungsverfahrens, dem informellen Reviewverfahren, das begleitet durch die federführende Landesaufsichtsbehörde vor dem EDSA geführt wird. Erfolgt im Rahmen des Verfahrensabschlusses die finale Stellungnahme des EDSA, so wird es zeitnah durch die federführende Landesbehörde zur Genehmigung der Kriterien kommen.[21] Das Anschlussprojekt DIRECTIONS[22] verfolgt den Ansatz einer sektorspezifischen und technologieabhängigen Zertifizierung für den Bereich von schulischen Informationssystemen.

Allgemeine Ansätze einer Zertifizierung haben den Vorteil, dass sie auf jegliche Art der Datenverarbeitung anwendbar sind. Der Vorteil von sektorspezifischen, technologieabhängigen Ansätzen ist demgegenüber die rechtliche und verfahrenstechnische Konkretisierungsleistung, die durch spezielle Kriterienkataloge erbracht werden kann. So kann durch Konkretisierung der datenschutzrechtlichen Anforderungen, die im besonderen Maße die jeweiligen bereichspezifischen Risiken in Betracht ziehen (bspw. Risiken bei der Verarbeitung personenbezogener Daten von Kindern) eine genauere und verlässlichere Aussage über das erforderliche Schutzniveau der Verarbeitungsvorgänge getroffen werden. Die dargestellten Governance-Effekte der Zertifizierung verstärken sich dementsprechend. Diesen Vorteilen stehen der – ggf. deutlich – eingeschränkte Anwendungsbereich sowie der gegenüber einem allgemeinen Ansatz höhere Aufwand der Erarbeitung einer Vielzahl von Kriterienkatalogen gegenüber. Es lässt sich deshalb zum jetzigen Zeitpunkt noch nicht beurteilen, ob sich im Ergebnis eher allgemeine oder eher spezifische Ansätze durchsetzen werden.

20 Näher https://www.auditor-cert.de/; zur Zertifizierung von Cloud-Angeboten s. Krcmar/Eckert/Roßnagel/Sunyaev/Wiesche (Hrsg.) Management sicherer Cloud-Services. Entwicklung und Evaluation dynamischer Zertifikate, 2018; aus rechtlicher Perspektive *Hofmann,* Dynamische Zertifizierung, 2019.

21 Zum letzten offiziellen Stand *Müller,* ZD-Aktuell 2022, 01239; zum Verfahrensablauf s. Fn. 16.

22 https://directions-cert.de/; die Autoren verantworten zusammen mit weiteren Kollegen die rechtswissenschaftlichen Teile des Projekts.

4. Einzelfragen einer effektiven Zertifizierung

Um der Zertifizierung als Governance-Instrument zu praktischer Wirksamkeit zu verhelfen und ihre spezifischen Vorteile nutzen zu können, müssen verschiedene Bedingungen erfüllt sein. Da die Zertifizierung nach Art. 42 Abs. 3 DSGVO für Verantwortliche und Auftragsverarbeiter freiwillig ist, muss sie für diese hinreichend attraktiv sein. Aufwand und Kosten müssen mithin in einem auch betriebswirtschaftlich vernünftigen Verhältnis zu den erhofften Vorteilen stehen.[23] Aus Governance-Perspektive kann dies zu Zielkonflikten führen. Schlanke Zertifizierungsprogramme mögen für Verantwortliche und Auftragsverarbeiter zunächst vorzugswürdig erscheinen. Wenn dies jedoch zu stark zulasten der angewendeten Prüftiefe geht, so wird die Funktion der Rechtssicherheit gefährdet, zumal die Zertifizierung die Verantwortung des Verantwortlichen oder Auftragsverarbeiters für die Einhaltung der Verordnung nicht mindert (Art. 42 Abs. 4 DSGVO). Prüfungsmaßstab und Prüftiefe sind letztlich entscheidende Weichenstellungen für alle oben erläuterten Funktionen der Datenschutz-Zertifizierung.

In diesem Bereich sind etliche Fragen noch ungeklärt. Von diesen werden im Folgenden zwei herausgegriffen, nämlich die Zertifizierungen bereichsspezifischer Vorschriften sowie der Umgang mit offenen bzw. umstrittenen Rechtsfragen.

4.1 Zertifizierbarkeit von Anforderungen außerhalb der DSGVO

Die DSGVO ist keine abschließende Regelung des Datenschutzrechts. Neben ihr existieren weitere Vorgaben auf europäischer Ebene, und die

23 U.a. diesem Grund ist gemäß Art. 42 Abs. 1 S. 2 DSGVO den Bedürfnissen von Kleinstunternehmen sowie kleinen und mittleren Unternehmen (KMU) Rechnung zu tragen. Dahinter steht wohl der Gedanke, diese wirtschaftlich nicht überbelasten und im Wettbewerb mit größeren Unternehmen nicht benachteiligen zu wollen, vgl. auch Art. 30 Abs. 5, EG 13 DSGVO. In der Literatur wird Art. 42 Abs. 1 S. 2 DSGVO dementsprechend vielfach so ausgelegt, dass KMU die Zertifizierung für geringere Kosten die Zertifizierung nutzen können sollen, sa.: *Scholz*, in: Simitis u.a. (Hrsg.), Datenschutzrecht, 2019, Art. 42 DSGVO Rn. 20; *Paal/Kumkar*, in: Paal/Pauly (Hrsg.), DS-GVO BDSG, 2021, Art. 42 Rn. 8; *Duisberg*, ZD 2018, 53. Wie dies ausgestaltet und wie insbesondere Marktverzerrungen verhindert werden sollen, ist bisher ebenso unklar wie eine denkbare Berücksichtigung der Interessen von KMU in anderen Rollen (z.B. als Zertifizierungsstelle). Eindeutig ist dagegen, dass für KMU keine Absenkung des DSGVO-Schutzniveaus vorgenommen werden darf, s. *Hofmann*, Dynamische Zertifizierung, 2019, S. 318 m.w.N.

Verordnung selbst lässt mit ihren zahlreichen Öffnungsklauseln mitgliedstaatliche Spezialregelungen zu. Je nach mitgliedstaatlichem Regelungsansatz wird eine umfassende datenschutzrechtliche Bewertung der Verarbeitungsvorgänge eines Verantwortlichen oder Auftragsverarbeiters dementsprechend die Anwendung nicht nur der Verordnung, sondern auch derartiger spezialgesetzlicher Regelungen erfordern. Es ist jedoch unklar, ob diese auch im Rahmen der Zertifizierung zu berücksichtigen sind.

Grundsätzliche Überlegungen

Für die Unzulässigkeit der Zertifizierung von Kriterien, die sich nicht den Vorschriften der DSGVO selbst entnehmen lassen, lässt sich zunächst der Wortlaut des Art. 42 Abs. 1 S. 1 DSGVO anführen. Danach dienen Zertifizierungsverfahren dazu, nachzuweisen, dass „diese Verordnung" eingehalten wird. Eine Berücksichtigung jedenfalls mitgliedstaatlicher Spezialgesetze könnte außerdem zu einer Fragmentierung der Zertifizierungsverfahren führen, die einer europaweiten einheitlichen Anwendung und einem produktiven Wettbewerb der Verfahren im Binnenmarkt abträglich sein könnte.

Demgegenüber spricht für eine über den Wortlaut der DSGVO hinausgehende Berücksichtigung von spezialgesetzlichen Datenschutzregelungen, dass die erläuterten Zwecke und Funktionen der Zertifizierung bei einer Beschränkung auf die Verordnung als Prüfungsmaßstab gefährdet werden würden. Denn die durch das Zertifikat bestätigte Rechtskonformität würde sich in diesem Fall regelmäßig nur auf einen Teil der für einen Verantwortlichen oder Auftragsverarbeiter geltenden materiell- und verfahrensrechtlichen Anforderungen erstrecken. Eine Entlastung der Aufsichtsbehörden und eine verbesserte Durchsetzung des Datenschutzrechts (das zweite und vierte der oben erläuterten Ziele) könnte auf diesem Wege zwar noch partiell erreicht werden. Der Zugewinn an Rechtssicherheit dürfte dagegen jedoch mehr als nur teilweise leiden. Denn mit den speziellen datenschutzrechtlichen Regelungen, würde regelmäßig der Teil der rechtlichen Vorgaben ausgeklammert, dessen Einhaltung im jeweiligen Marktsegment von besonderer Bedeutung ist. Dies kann den Eintritt der genannten Markteffekte erheblich bedrohen.[24]

24 Wenn Anbieter beispielsweise im Markt schulischer Informationssysteme mit einem Zertifikat auftreten, das lediglich die Einhaltung der DSGVO-Vorschriften bestätigt, die Einhaltung der der Schulgesetze der Länder jedoch ausklammert, könnten Schul-

Differenzierung nach Typen von Spezialgesetzen

Um sich einer Lösung des Problems zu nähern, bietet es sich an, zwischen verschiedenen speziellen Vorschriften zu unterscheiden. Dies sind

1. bereichsspezifische, unmittelbar geltende europäische Datenschutznormen (Verordnungen),
2. nationale Normen in Umsetzung bereichsspezifischer europäischer Richtlinien sowie
3. nationale Normen, die in Ausfüllung von Öffnungsklauseln der DSGVO erlassen werden.

Das wohl wichtigste Beispiel für eine bereichspezifische Verordnung wäre eine künftige e-Privacy-VO, so deren Gesetzgebungsgeschichte irgendwann enden sollte.[25] Aber auch in anderen Verarbeitungssektoren zeichnet sich eine Tendenz des europäischen Gesetzgebers ab, bereichsspezifische Datenschutznormen zu verabschieden. Dies gilt beispielsweise für mehrere Regelungen der geplanten KI-Verordnung.[26] Die Entwürfe zu diesen Rechtsakten enthalten weder eine Erweiterung des Anwendungsbereichs von Art. 42 Abs. 1 DSGVO noch andere Regelungen zur Datenschutzzertifizierung.[27] Soweit ersichtlich, gilt dasselbe für alle bereits existierenden bereichsspezifischen EU-Verordnungen mit datenschutzrechtlichen Regelungen.[28] Daraus ließe sich der Schluss ziehen, dass die spezialgesetzlichen

---

träger und Schulen bei entsprechenden Beschaffungsentscheidungen nicht anhand des Zertifikats darauf vertrauen, dass die Informationssysteme rechtskonform einsetzbar sind.

25 Entwurf: COM(2017) 10 Final. Das Parlament hat am 26.10.2017 (Report: A8-0324/2017), der Rat am 10.02.2021 (Council, 6078/21) eine Position verabschiedet. Ein Ende des Trilogs ist nicht in Sicht.

26 Der Entwurf (COM(2021) 206 final) enthält etwa eine Verarbeitungsbefugnis zur Vermeidung von Verzerrungen der KI-Systeme (Art. 10 Abs. 5 KI-VO-E) und eine Erlaubnis zur Zweckänderung für die Verarbeitung in KI-Reallaboren (Art. 54 Abs. 1 KI-VO-E); näher *Hornung*, in: Rostalski (Hrsg.), Künstliche Intelligenz. Wie gelingt eine vertrauenswürdige Verwendung in Deutschland und Europa?, 2022, 91 ff.

27 Dies gilt bspw. für die Entwürfe zur e-Privacy-VO. Art. 1 Abs. 3 e-Privacy-VO-E (COM/2017/010 final) und Art. 1 Abs. 3 e-Privacy-ÄndV-Parlament (A8-0324/2017) ordnen an, dass die e-Privacy-VO die DSGVO präzisieren und ergänzen soll. Dies lässt Rückschlüsse auf eine gewünschte Harmonisierung der Rechtsakte zu, klärt aber nicht, ob die „ergänzenden" Normen der geplanten Verordnung trotz des Wortlauts von Art. 42 Abs. 1 DSGVO zertifizierbar sein sollen.

28 Eine Ausnahme bildet die VO (EU) 2018/1725, die die Datenverarbeitung durch Organe, Einrichtungen und sonstige Stellen der Union regelt. Sie ist allerdings keine echte Spezialregelung, sondern das Äquivalent zur DSGVO in diesem Bereich, sodass

Anforderungen nicht Maßstab einer Datenschutzzertifizierung sein sollen. Allerdings gibt es für eine derartige Regelungsabsicht des Gesetzgebers ebenfalls keinerlei Anhaltspunkte. Angesichts fehlender Hinweise in den Gesetzgebungsmaterialien spricht alles dafür, dass dem europäischen Gesetzgeber das Problem überhaupt nicht bewusst war. Ohne derartige Anhaltspunkte sollte mit Blick auf die Gefahr einer erheblichen Gefährdung der Regelungsziele der DSGVO-Zertifizierung nicht angenommen werden, dass europaweite bereichsspezifische Regelungen nicht zertifizierbar sind. Dies würde wichtige Segmente der europäischen Datenwirtschaft von der Zertifizierung ausschließen. Dieses Ergebnis allein auf den Wortlaut von Art. 42 Abs. 1 DSGVO zu stützen, ist übermäßig formalistisch und deshalb nicht überzeugend.

Bis zu einer künftigen e-Privacy-Verordnung ist das instruktivste Beispiel für die zweite Gruppe nationales Datenschutzrecht, das in Umsetzung der aktuellen e-Privacy-Richtlinie erlassen wurde. In Deutschland betrifft dies die Vorgaben des Telekommunikation-Telemedien-Datenschutz-Gesetzes (TTDSG). Verarbeitungsvorgänge im Anwendungsbereich der Richtlinie und dieses Gesetzes fallen grundsätzlich in den Anwendungsbereich der DSGVO,[29] die speziellen nationalen Anforderungen gehen jedoch nach Art. 95 DSGVO vor. Auch bei diesen Regelungen gibt es keinen Anhaltspunkt dafür, dass der europäische Gesetzgeber ihre Zertifizierbarkeit im Rahmen der Verabschiedung der DSGVO ausschließen wollte. Mit Blick auf den europaweit zumindest grundsätzlich einheitlichen Norminhalt dürfte eine Zersplitterung von Zertifizierungsprogrammen beherrschbar sein. Für eine Einbeziehung in die Zertifizierung spricht auch, dass komplexe Gesamtsysteme Teilkomponenten enthalten können, die unter das TTDSG fallen (etwa Videokonferenzfunktionen oder Messenger).[30] Die Anbieter derartiger Systeme von einer weitreichenden Rechtssicherheit

die Übernahme der Rechtsfolgen der Zertifizierung (Art. 26 Abs. 3, Art. 27 Abs. 3, Art. 29 Abs. 5 und Abs. 6, Art. 33 Abs. 4, Art. 48 Abs. 2 lit. d, EG 49, EG 51 S. 2, EG 65 S. 2 VO (EU) 2018/1725) gesetzgeberisch nahe lag.

29 Bereichsspezifische europäische Regelungen, die nicht aufgrund Spezialität der DSGVO vorgehen, sondern jenseits ihres Anwendungsbereichs liegen, werden hier ausgeklammert – v.a. die Datenverarbeitung zur Straftatbekämpfung (Regelung in der JI-Richtlinie und nationalen Umsetzungen) sowie die VO (EU) 2018/1725 (s. Fn. 28). Die JI-Richtlinie wirft im Bereich der Zertifizierung spezielle Fragen auf, s. *Johannes*, Die Polizei 2020, 409.

30 Auf die genaue Abgrenzung zwischen TTDSG und DSGVO bei derartigen Komponenten kommt es hier nicht an; dazu *Schellhas-Mende/Wiedemann/Blum*, DuD 2022, 291; *Roßnagel*, NJW 2023, 400.

auszuschließen und auf eine Teilzertifizierung zu verweisen, dient weder deren Interessen noch den Interessen anderer Marktteilnehmer. Dementsprechend erscheint es sinnvoll, im Rahmen eines modularen Aufbaus von Kriterienkatalogen die Anforderungen beispielsweise des Telekommunikation-Telemedien-Datenschutz-Gesetzes in einem Teilmodul zu kapseln, das immer dann angewendet wird, wenn die zu zertifizierenden Verarbeitungsvorgänge insgesamt oder Teile von ihnen in den Anwendungsbereich dieses Spezialgesetzes fallen.

Das Argument der fehlenden Aussagekraft gilt schließlich auch für nationale Normen, die in Ausfüllung von Öffnungsklauseln der DSGVO erlassen werden. Der Wortlaut von Art. 42 Abs. 1 DSGVO dürfte hier sogar weniger entgegenstehen als bei bereichsspezifischen Regelungen auf europäischer Ebene, da es immerhin möglich ist, nationale Normen im Bereich der Öffnungsklauseln (insbesondere bei verpflichtenden Regelungsaufträgen) in einem weiten Sinne als Teil der Verordnung zu begreifen. Gewichtiger sind jedoch die bereits erläuterten teleologischen Argumente. Insbesondere im Bereich besonders umfassender Öffnungsklauseln (vor allem Art. 6 Abs. 2 und Abs. 3, aber auch Art. 88 DSGVO) würde man bei einem engen Verständnis große Teile der für einen zu zertifizierenden Datenverarbeitungsvorgang geltenden rechtlichen Anforderungen von der Zertifizierung ausschließen. Hinzu kommt wie im Bereich des TTDSG das Problem, dass einzelne, gegebenenfalls sehr spezielle nationale Normen das angestrebte Ziel einer rechtssicheren Zertifizierung eines Gesamtsystems torpedieren würden.

Betrachtet man also abschließend die vorgenommenen Untersuchungen der drei identifizierten Vorschriftsbereiche, so stehen dem schlichten Wortlautargument, auf welches sich die Annahme der Unmöglichkeit einer Zertifizierung von bereichspezifischen Vorschriften stützt, eine Fülle an Argumenten entgegen. Im Ergebnis ist deshalb, insbesondere wegen der genannten teleologischen Argumente, die Miteinbeziehung von bereichsspezifischen, außerhalb der DSGVO liegenden Datenschutzvorschriften in die Zertifizierung nach Art. 42 DSGVO vorzugswürdig.

Konkrete Umsetzung

Mit Blick auf das wünschenswerte Ziel einer europaweit einheitlichen Zertifizierung hebt sich die erste Gruppe von Spezialgesetzen von den anderen beiden ab. Wenn über die DSGVO hinausgehende, europaweit einheitliche Normen existieren, so können Zertifizierungsprogramme aus verschiede-

nen Mitgliedstaaten diese im Rahmen von Kriterienkatalogen berücksichtigen, die sich gegenseitig ergänzen oder miteinander in Konkurrenz treten. Sollen dagegen nationale Normen in Umsetzung von Richtlinien oder Ausfüllung von Öffnungsklauseln[31] in die Kriterienkataloge eingebunden werden, so muss eine Lösung für das Problem gefunden werden, dass die mitgliedstaatlichen Entscheidungsbefugnisse praktisch unvermeidlich zu einer erheblichen Heterogenität der speziellen Anforderungen führen werden.[32] Zumindest für Programmeigner in Mitgliedstaaten mit einer hohen Anzahl von Datenverarbeitungen, die durch spezifische nationale Normen reguliert sind, könnte ein Weg darin bestehen, auf eine europaweite Genehmigung des Kriterienkatalogs zu verzichten und sich auf ein nationales Zertifizierungsprogramm zu beschränken. Allerdings stellt dies jedenfalls in föderalen Mitgliedstaaten wie Deutschland nur eine Teillösung dar, wenn die Gliedstaaten für die entsprechende Rechtsmaterie zuständig sind.

Eine Lösung für dieses Problem hat sich bisher nicht herausgebildet. Der kleinteiligste Ansatz bestünde darin, für jede (Teil-)Rechtsordnung ein spezifisches Kriterienmodul zu erstellen. Wenn ein Anbieter die Märkte mehrerer Rechtsordnungen adressieren möchte, könnten die Kriterien kumuliert oder (bei entsprechender Inhaltsgleichheit) abstrahiert und gemeinsam geprüft werden. Allerdings würde ein solches Vorgehen den Aufwand sowohl bei der konkreten Zertifizierung als auch bei der Erarbeitung und kontinuierlichen Aktualisierung des Kriterienkatalogs erheblich vergrößern. Je mehr (Teil-)Rechtsordnungen zu berücksichtigen und je variantenreicher die einzelnen Gesetzgeber aktiv sind, desto unrealistischer wird es, dass ein Programmeigner die erforderlichen Überarbeitungen und eine Aufsichtsbehörde die nachfolgenden Genehmigungen der Änderungen in einer für die Praxis der Zertifizierung notwendigen Geschwindigkeit erledigen können.

---

31 Auch wenn diese Fälle dogmatisch zu trennen sind, verschwimmen die Unterschiede in der praktischen Wirkung hinsichtlich der Handlungsspielräume der Mitgliedstaaten. Angesichts der vielen Öffnungsklauseln ist es deshalb zwar rechtlich unzutreffend, faktisch aber korrekt, die DSGVO als „Hybrid" zwischen Verordnung und Richtlinie zu bezeichnen, vgl. *Martini* u.a., Die Datenschutz-Grundverordnung und das nationale Recht, 2016, S. 1 f; *Hornung/Spiecker gen. Döhmann*, in: Simitis u.a. (Hrsg.), Datenschutzrecht, 2019, Einl. Rn. 226.

32 Zu den Öffnungsklauseln s. insoweit allgemein *Martini* u.a., Die Datenschutz-Grundverordnung und das nationale Recht, 2016, S. 9 ff; *Hornung/Spiecker gen. Döhmann*, in: Simitis u.a. (Hrsg.), Datenschutzrecht, 2019, Einl. Rn. 226 ff. und *Weiß*, Öffnungsklauseln in der DSGVO und nationale Verwirklichung im BDSG, 2022.

Zumindest in solchen Fällen stellt sich die Frage, in welchem Umfang die Berücksichtigung konkreter spezialgesetzlicher Anforderungen entweder in den Prozess der Zertifizierung oder sogar in die zu zertifizierenden Prozesse des Verantwortlichen oder Auftragsverarbeiters verlagert werden kann. Letzteres könnte darauf hinauslaufen, im Zertifizierungsprozess nicht die Einhaltung von ohnehin rasch veränderlichen spezialgesetzlichen Regelungen zu prüfen und zu bestätigen, sondern die Existenz eines wirksamen organisatorischen Prozesses beim Verantwortlichen oder Auftragsverarbeiter, mit dessen Hilfe die jeweils für einen spezifischen Verarbeitungsvorgang geltenden spezialgesetzlichen Regelungen geprüft, operationalisiert und eingehalten werden.[33] Der DSGVO lässt sich nichts dazu entnehmen, ob ein solches Modell zulässig ist und welche Anforderungen an dieses zu stellen sein könnten; eine Stellungnahme jedenfalls der deutschen Aufsichtsbehörden und des EDSA zu dieser Frage fehlt. Zumindest in stark volatilen spezialgesetzlichen Regelungsbereichen dürfte ein solcher oder ähnlicher Weg aber alternativlos sein, wenn man nicht auf die Prüfung der entsprechenden speziellen Anforderungen verzichten möchte.

4.2 Umgang mit ungeklärten Rechtsfragen

Eine zweite grundsätzliche Herausforderung der datenschutzrechtlichen Zertifizierung ist der vielfach generische Charakter insbesondere der materiellrechtlichen Vorgaben der DSGVO.[34] Dieser führt gemeinsam mit dem immer noch jungen Alter der Verordnung dazu, dass viele konkrete Anforderungen an unterschiedliche Verarbeitungsvorgänge unklar und umstritten sind. Der erforderliche Prozess der Konkretisierung umfasst ein komplexes Geflecht von Akteuren.[35] Von diesen kann nur der EuGH Vorgaben machen, die für alle anderen Beteiligten verbindlich sind. Schon aufgrund der begrenzten Kapazität des Gerichtshofs, aber auch aufgrund seiner spezifischen, einzelfallorientierten Arbeitsweise wird es aber auch mittel- und langfristig unmöglich sein, sich ausschließlich an seiner Rechtsprechung zu orientieren. Dies führt dazu, dass die an einem Zertifizierungsprozess Beteiligten (Verantwortliche und Auftragsverarbeiter, Zerti-

33 Diesen Ansatz verfolgt der GDPR-CARPA-Kriterienkatalog aus Luxemburg: *Helmke/Link/Schild*, DuD 2023, 100, 101; zur dynamischen Zertifizierung vgl. *Hofmann*, Dynamische Zertifizierung, 2019.

34 Näher *Hornung/Spiecker gen. Döhmann*, in: Simitis u.a. (Hrsg.), Datenschutzrecht, 2019, Einl. Rn. 211.

35 Ebd. Rn. 234, 180 ff., 264 ff.

fizierungsstellen, Programmeigner, Aufsichtsbehörden, ggf. Europäischer Datenschutzausschuss) einen Weg finden müssen, um mit ungelösten und umstrittenen Rechtsfragen umzugehen.

Verdeutlichung: Drittlandsübermittlung als Problem der globalen Data Governance

Die Notwendigkeit der Konkretisierung ist ein allgemeines Governance-Problem der DSGVO, das sich – in Verbindung mit der Zertifizierung – an etlichen Beispielen verdeutlichen lässt. Im Folgenden wird zu diesem Zweck der vielfach diskutierte Bereich der Übermittlung personenbezogener Daten in Drittländer gewählt. Die Frage der Konkretisierung der in der Praxis oft unklaren Übermittlungsgrundlagen wird in diesem Zusammenhang zu einer Frage der globalen Data Governance.

Die DSGVO hat die früheren Bestimmungen der DSRL zur Übermittlung in Drittländer in vielen Details verändert und neue Schutzinstrumente eingeführt. Dabei wurden insbesondere die Kriterien für derartige Übermittlungen konkretisiert und etliche Anforderungen aus der Rechtsprechung des EuGH zu Art. 25 f. DSRL in den Normtext übernommen. Der Grundansatz ist indes unverändert:[36] Die Harmonisierung der datenschutzrechtlichen Vorschriften im Binnenmarkt führt zum grundsätzlichen Wegfall von Beschränkungen der Datenflüsse zwischen den Mitgliedstaaten; dieser Wegfall kann aber nur gerechtfertigt werden, wenn bei Übermittlungen aus dem Binnenmarkt[37] in andere Jurisdiktionen harmonisierte Anforderungen gelten, die ein Absenken des Schutzes ausschließen oder zumindest auf ein erträgliches Maß beschränken. Dass damit durchaus erhebliche Einschränkungen globaler Datenflüsse einhergehen können, kann für Datenverarbeiter Probleme verursachen, die – wegen bestehender Verarbeitungsprozesse und globaler Abhängigkeiten – schwierig für sie zu lösen sind. Diesen Umstand nimmt der europäische Gesetzgeber jedoch in gewissem Umfang hin.

36 *Schantz,* in: Simitis u.a. (Hrsg.), Datenschutzrecht, 2019, Art. 44 DSGVO Rn. 4 ff. zu den Herausforderungen nach dem Brexit: *Hofmann/Stach*, ZD 2021, 1 ff.; *Wittershagen*, The Transfer of Personal Data from the European Union to the United Kingdom post-Brexit, 2023.

37 Dies schließt EWR-Staaten ein, die aufgrund des Beschlusses des EWR-Ausschusses Nr. 154/2018 v. 6.7.2018 (Abl. L 183, 19.7.2018, S. 23–26) nicht als Drittländer iSd. Art. 44 DSGVO gelten.

Die für Datenexporteure und -importeure einfachste Variante ist die Übermittlung in Drittländer, für die die Europäische Kommission einen Angemessenheitsbeschluss nach Art. 45 DSGVO getroffen hat.[38] Allerdings hat der EuGH in den zwei wegweisenden Entscheidungen Safe Harbor[39] und Privacy Shield[40] hohe Anforderungen an die Bejahung eines angemessenen Datenschutzniveaus gestellt und die jeweiligen Kommissionsbeschlüsse für ungültig erklärt.[41] Mit der Executive Order 14086 von US-Präsident Biden[42] und dem darauf gestützten erneuten Angemessenheitsbeschluss der Kommission[43] ist das Problem zwar für die USA – jedenfalls bis zu einer zu erwartenden weiteren gerichtlichen Prüfung auch dieses Beschlusses – gelöst . Die Diskussionen in Wissenschaft und Praxis seit der Privacy-Shield-Entscheidung und die erheblichen Probleme, die der Wegfall des Angemessenheitsbeschlusses für Datenverarbeiter verursacht hat, die Geschäftsmodelle mit transatlantischen Datenübermittlungen auf ihn gestützt haben,[44] sind aber weiterhin relevant. Dies betrifft zum einen das Szenario einer Ungültigkeitserklärung des Privacy Frameworks durch den EuGH,[45] zum anderen aber auch Datenübermittlungen in Drittstaaten, für die kein Angemessenheitsbeschluss vorliegt.

38 Dies gilt aktuell für Korea, Andorra, Argentinien, Kanada, Färöer, Guernsey, Israel, Isle of Man, Japan, Jersey, Neuseeland, Schweiz, Uruguay und das Vereinigte Königreich.

39 EuGH, Urt. v. 6.10.2015 – C-362/14 (Schrems/Digital Rights Ireland – Schrems I), NJW 2015, 3151.

40 EuGH, Urt. v. 16.7.2020 – C-311/18 (Facebook Ireland/Schrems – Schrems II), NJW 2020, 2613.

41 Der EuGH bemängelte die extensiven Zugriffsrechte der US-Geheimdienste nach der Übertragung (vgl. insb. Sec. 702 FISA) sowie die mangelhaften Rechtschutzmöglichkeiten gegen Zugriffe. Beide Beschlüsse wurden deshalb wegen Unvereinbarkeit mit Art. 7, 8 und 47 GRCh für ungültig erklärt, vgl. EuGH NJW 2015, 3151 Rn. 94 ff.; EuGH, NJW 2020 2613 Rn.198 f. Näher *Vladeck*, DSK-Gutachten zum aktuellen Stand des US-Überwachungsrechts und der Überwachungsbefugnisse.

42 POTUS, Executive Order 14086.

43 EU-KOM, Commission Implementing Decision of 10.7.2023 pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council on the adequate level of protection of personal data under the EU-US Data Privacy Framework.

44 *Dehmel/Ossman-Magiera/Weiss*, MMR 2023, 17 ff.

45 Das EU-Parlament hat eine Beschlussvorlage des LIBE-Ausschusses angenommen, in dem es seine Zweifel am Angemessenheitsbeschluss aufführt und die EU-KOM zu Änderungen aufruft: Resolution 2023/2501(RSP); EDSA fordert EU-KOM zur genauen Prüfung der EO auf: Opinion 5/2023; die EO als unzureichend betrachtend: LfDI BW, interne Einschätzung v. 22.10.2022; differenzierend: HmbBfDI, Datenschutz in den USA v. 29.11.2022.

In beiden Szenarien werden weiterhin die Anforderungen zum Tragen kommen, die der EuGH und in der Folge auch der EDSA für Datenübermittlungen mit Hilfe von geeigneten Garantien im Sinne des Art. 46 DSGVO formuliert haben. Für Standarddatenschutzklauseln (SCCs, Art. 46 Abs. 2 lit. c DSGVO) hat der EuGH die grundsätzliche Vereinbarkeit mit Art. 7, 8 und 47 der GRCh bestätigt. Voraussetzung ist jedoch, dass im Rahmen der SCCs durch individuelle Verpflichtungen der Datenimporteure und Datenexporteure ein Schutzniveau sichergestellt wird, das dem europäischen Grundrechtsschutz gleichwertig ist. Dies müssen die Datenexporteure vor einer Übermittlung überprüfen, während die Datenimporteure, zumindest im Rahmen der SCCs, den Exporteur benachrichtigen müssen, falls sie nicht (mehr) in der Lage sind, ein gleichwertiges Schutzniveau zu garantieren. Fehlt es von Anfang an oder nachträglich an einer Gleichwertigkeit, sind die Datenexporteure verpflichtet, die Übermittlung auszusetzen, wenn sie nicht durch anderweitige Maßnahmen ein gleichwertiges Schutzniveau (wieder)herstellen können. Dementsprechend gewährleisten die SCCs, in rechtmäßiger und konsequenter Anwendung, ein gleichwertiges und damit den Anforderungen des Art. 44 Abs. 1 DSGVO entsprechendes Schutzniveau.[46]

Die Überprüfungsverpflichtung der Datenexporteure wird in der Praxis durch sogenannte Transfer-Impact-Assessments (TIAs) umgesetzt.[47] Der EDSA hat diese Verpflichtung folgerichtig auch auf andere Übermittlungsinstrumente des Art. 46 DSGVO erweitert. [48] Ergibt die Beurteilung im Zuge eines TIA (oder einer gleichwertigen Überprüfung), dass kein gleichwertiges Schutzniveau besteht, benennt der EDSA als anderweitige Maßnahmen eine Vielzahl an vertraglichen, technischen oder organisatorischen Instrumenten, von denen die Anonymisierung, bzw. eine dieser gleichstehende Verschlüsselung, regelmäßig unverzichtbar sein wird.[49]

Für die Zertifizierung bedeutet dies, dass für alle Drittländer, in die ein Verantwortlicher oder Auftragsverarbeiter Daten übermitteln möchte,

46 Zur Rechtmäßigkeit der SCCs und den Anforderungen an die Datenexporteure: EuGH, NJW 2020, 2613, Rn. 134 ff.

47 *Baumgartner/Hansch/Roth*, ZD 2021, 608, 609.

48 EDSA, Empfehlungen 01/2020, Rn. 15 ff., vgl. zudem die Anforderung zur Überprüfung der tatsächlichen Möglichkeit der Gewährleistung eines gleichwertigen Schutzniveaus iRd. Empfehlungen zu den folgenden Übermittlungsinstrumenten: BCRs: EDSA, Recommendations 1/2022, Rn. 39; CoCs: EDSA, Leitlinien 4/2021, Rn. 36. Zertifizierungen: EDSA, Guidelines 07/2022, Rn. 45.

49 EDSA, Empfehlungen 01/2020, Rn. 79 ff., insb. Rn. 85 ff.

die datenschutzrechtliche Rechtslage, die Möglichkeiten und Grenzen der gewählten Übermittlungsinstrumente sowie gegebenenfalls zusätzlich erforderliche (vor allem technische) Maßnahmen zur Gewährleistung eines angemessenen Schutzniveaus eine Rolle spielen müssen.

Zwei Varianten der Zertifizierung: Datenexporteur oder Datenimporteur

Die Zertifizierung kann nach der DSGVO im Rahmen der Drittlandsübermittlung in zwei Konstellationen eine Rolle spielen. Zum einen besteht die Möglichkeit, die Art. 44 ff. DSGVO in die Zertifizierung von Verarbeitungsvorgängen eines Datenexporteurs in der Union einzubeziehen. Soll eine Übermittlung in ein Drittland erfolgen, für das kein Angemessenheitsbeschluss vorliegt, so muss im Rahmen der Zertifizierung das Vorliegen einer geeigneten Garantie nach Art. 46 Abs. 2 DSGVO geprüft werden.

Zum anderen hat der europäische Gesetzgeber im Zuge der Regelung der Datenschutzzertifizierung in der DSGVO diese auch selbst als geeignete Garantie aufgenommen (Art. 42 Abs. 2 und Art. 46 Abs. 2 lit. f DSGVO). Diese adressiert Fälle, in denen sich der Datenimporteur im Drittland einer Zertifizierung nach Art. 42 DSGVO unterzieht, um durch die Einhaltung der jeweiligen Zertifizierungskriterien die Gewährleistung eines gleichwertigen Schutzniveaus sicherzustellen.[50] Der Gesetzgeber hat zugleich die Governance-Herausforderung realisiert, dass die Einhaltung der Vorgaben eines Kriterienkatalogs in Drittländern schwerer kontrollierbar ist und außerdem im Falle von Verstößen entsprechende Sanktionen deutlich schlechter durchsetzbar sein werden.

Der Gesetzgeber versucht, dieses Durchsetzungsproblem durch die Vorgabe in Art. 42 Abs. 2 und Art. 46 Abs. 2 lit. f DSGVO zu adressieren, dass die Verantwortlichen oder Auftragsverarbeiter mittels vertraglicher oder sonstiger rechtlich bindender Instrumente die verbindliche und durchsetzbare Verpflichtung eingehen müssen, die geeigneten Garantien anzuwenden; dies bezieht sich insbesondere auf die Rechte der betroffenen Personen. Eine solche Verpflichtung ändert zwar nichts daran, dass die rechtlichen Befugnisse und praktischen Möglichkeiten der Aufsichtsbehörden als staatliche Letztverantwortliche im System der regulierten Selbstregulierung der Zertifizierung in diesem Bereich erheblich schwächer ausgeprägt sind als innerhalb des Binnenmarktes. Dies ist allerdings ein Problem aller Garantien von Art. 46 Abs. 2 DSGVO, die auf Drittländer angewendet werden,

50 EDSA, Guidelines 07/2022.

welche weder allgemein noch im konkreten Verarbeitungssektor ein angemessenes Schutzniveau aufweisen.

Der EDSA hat sich mit dieser neuen Variante bereits befasst. Er betont, dass die allgemeinen Leitlinien für die Zertifizierung auch für ihre Nutzung als Übermittlungsinstrument gelten.[51] Wie bei den anderen geeigneten Garantien sind außerdem auch im Rahmen der Art. 42 Abs. 2 und Art. 46 Abs. 2 lit. f DSGVO die zusätzlichen Maßnahmen zur Gewährleistung eines gleichwertigen Schutzniveaus zu beachten.[52]

Die Empfehlungen des EDSA zielen darauf ab, die in der Folge der Schrems II-Entscheidung konkretisierten Anforderungen (s.o. 4.2.1) auch im Rahmen von Datenübermittlungen anzuwenden, die auf genehmigte Zertifizierungsmechanismen gestützt werden sollen. Der EDSA verlangt deshalb u.a. die Durchführung eines TIA sowohl auf Seiten des Datenimporteurs im Drittland, wenn dieser sich zertifizieren lassen will,[53] als auch auf Seiten des Datenexporteurs in der Union, wenn er sich auf dieses Instrument stützen möchte; Letzterer kann allerdings die Bestätigung der Zertifizierungsstelle, dass der Importeur das TIA ordnungsgemäß durchgeführt hat, als „important element" für seine eigene Bewertung verwenden.[54] Wenn der konkrete Zertifizierungsmechanismus keinen effektiven Schutz gewährleisten kann, so sind (wie bei Standarddatenschutzklauseln und anderen Übermittlungsinstrumenten) ergänzende Maßnahmen zu ergreifen.

Folgen für Zertifizierungsverfahren und Kriterienkatalog

Im Ergebnis bietet die Datenschutzzertifizierung damit ein umfassendes Instrument zur Übermittlung in Drittländer ohne angemessenes Datenschutzniveau, wenn sich:

1. der Datenexporteur einer Zertifizierung unterzieht, in der er die Einhaltung des Kapitel V (einschließlich der Vornahme eines TIA bzw. einer Gleichwertigkeitsüberprüfung) nachweist, oder

51 Ebd. Rn. 37. Dies bezieht sich auf EDSA, Leitlinien 1/2018.

52 EDSA, Empfehlungen 01/2020.

53 Dies hat der Datenimporteur als allgemeine Anforderung an die Nutzung einer geeigneten Garantie ohnehin vorzunehmen: EDSA, Empfehlungen 01/2020, Rn. 28, vgl. zudem EDSA, Guidelines 07/2022, Rn. 45.

54 S. EDSA, Guidelines 07/2022, Rn. 21. In der ersten Fassung der Guidelines sollte der Exporteuer nicht auf die Bewertung der Zertifizierungsstelle, sondern auf die des Importeurs vertrauen dürfen. Außerdem ist die Qualifizierung „important" hinzugetreten; dies dürfte die Bewertungspraxis des Exporteurs erleichtern.

2. der Datenimporteur einer Zertifizierung unterzieht und damit die Einhaltung der Art. 42 Abs. 2 und 46 Abs. 2 lit. f DSGVO nachweist, sowie beide Parteien eine Gleichwertigkeitsüberprüfung vornehmen.

Der EDSA handelt konsequent, wenn er seine Konkretisierung der materiellrechtlichen Vorgaben aus Art. 46 Abs. 2 DSGVO für alle Übermittlungsinstrumente anwendet. Aus der Perspektive des Programmeigners ist damit allerdings noch nicht geklärt, auf welcher Stufe des Prozesses diese Konkretisierung „eingebaut" oder (falls die Konkretisierungsleistung des Ausschusses als ganz oder teilweise nicht überzeugend bewertet wird) modifiziert werden kann oder muss. Zu dieser Frage haben sich die Aufsichtsbehörden bisher nicht geäußert.

Eine Möglichkeit dürfte darin bestehen, im Kriterienkatalog mehr oder weniger den Inhalt der Art. 44 ff. DSGVO auf abstrakter Ebene zu wiederholen und die Prüfung der Anforderungen an das konkrete Übermittlungsinstrument auf die Zertifizierungsstellen zu übertragen. Es bliebe sodann in Zertifizierungsstellen überlassen, im Einzelfall Art. 46 Abs. 2 DSGVO anzuwenden und bei der insoweit erforderlichen konkretisierenden Auslegung den Empfehlungen des EDSA ganz, teilweise oder gar nicht zu folgen. Eine Abweichung dürfte allerdings den Einsatz aufsichtsbehördlicher Maßnahmen gegen die akkreditierte Zertifizierungsstelle nach sich ziehen (Art. 43 Abs. 7 DSGVO), die zum Widerruf der Zertifizierung führen können (Art. 42 Abs. 7 DSGVO). Gegen derartige Maßnahmen könnten sich sodann die Zertifizierungsstelle und der Verantwortliche bzw. der Auftragsverarbeiter gerichtlich zur Wehr setzen. Diese Möglichkeit der gerichtlichen Kontrolle der Maßstäbe, die der EDSA für den Einsatz der Zertifizierung zur Drittlandsübermittlung formuliert hat, ist vor allem deshalb bedeutsam, da die Leitlinien, Empfehlungen und Beschlüsse des Ausschusses grundsätzlich nicht direkt angegriffen werden können.[55]

Die zweite Möglichkeit liegt darin, dass ein Programmeigner in einem Kriterienkatalog demgegenüber eine selbstständige Konkretisierung der Art. 44 ff. DSGVO vornimmt. Für diese Variante stellen sich wiederum neue, bislang nicht diskutierte Fragen.

55 So jedenfalls EuG, T-709/21 v. 7.12.2022 (WhatsApp v. EDSA) Rn. 50 ff., a.A. *Hermann/Miller*, ZeuS 2021, 617-662. Die Rechtswegmöglichkeiten werden hier aus systematischer Perspektive aufgezeigt. Es soll nicht bewertet werden, ob die EDSA-Vorgaben rechtskonform sind.

Naheliegend dürfte es sein, im ersten Schritt die Anforderungen des EuGH und des EDSA für den Kriterienkatalog zu übernehmen. Für Übermittlungen in die USA folgt daraus allerdings das Problem, dass der neue Angemessenheitsbeschluss der Kommission nach Ansicht vieler Kritiker die Vorgaben des Gerichtshofs gerade nicht einhält.[56] Es würde jedoch zu weit gehen und die in der DSGVO normierte Rolle der Zertifizierungsstelle überschreiten, wenn man von ihr verlangen würde, im Rahmen der Zertifizierung einen existierenden Angemessenheitsbeschluss am Maßstab der gerichtlichen Entscheidungen auf seine Gültigkeit hin zu überprüfen und im Falle eines negativen Ergebnisses von dem Verantwortlichen oder Auftragsverarbeiter zu fordern, eine andere Rechtsgrundlage für die Übermittlung zu wählen. Eine Ausnahme dürfte allenfalls für evidente Fälle denkbar sein.

In einem zweiten Schritt könnten für die Nutzung von Art. 46 Abs. 2 DSGVO die Vorgaben des EDSA zu TIAs und ergänzenden vertraglichen, technischen oder organisatorischen Maßnahmen in einen Kriterienkatalog aufgenommen werden. Vergleichbar ihrer Berücksichtigung (erst) in der konkreten Zertifizierung stellt sich auch hier die Frage von Abweichungen. Nimmt ein Programmeigner Modifizierungen vor, so steht zu erwarten, dass ein entsprechender Kriterienkatalog von der zuständigen Aufsichtsbehörde oder vom EDSA nicht genehmigt wird. Eine entsprechende Ablehnung könnte sodann gerichtlich angegriffen werden. Im Rahmen eines solchen Prozesses (der bisher noch nicht vorgekommen ist) würden damit auch die Konkretisierungsleistungen des Ausschusses für Art. 46 DSGVO geprüft.

Eine letzte, restriktive Möglichkeit des Umgangs mit Drittlandsübermittlungen im Rahmen eines Kriterienkatalogs bestünde in ihrem Ausschluss. Da die nach Art. 42 Abs. 1 DSGVO zu bestätigende Einhaltung der Verordnung auch gegeben ist, wenn in einem Kriterienkatalog engere oder zusätzliche Anforderungen formuliert werden, ist es zulässig, im Rahmen von Zertifizierungsprogrammen freiwillig über das Niveau der DSGVO hinausgehende Anforderungen zu erfüllen.[57] Es wäre deshalb möglich, Verantwortlichen und Auftragsverarbeitern im Rahmen einer Zertifizierung

56 Die Gründe können nicht vertieft werden, insoweit Fn. 45 sowie *Roßnagel*, ZD 2022, 305 ff.

57 Für die Zulässigkeit der Integration strengerer Anforderungen: *Hornung*, in: Auernhammer, DSGVO/BDSG, 7. Aufl. 2020, Art. 42 DSGVO Rn. 48; *Scholz*, in: Simitis u.a. (Hrsg.), Datenschutzrecht, 2019, Art. 42 DSGVO Rn. 26; a.A. *Will*, in: Ehmann/Selmayr, DSGVO, 2. Auflage 2018, Art. 42 Rn. 33.

zu bestätigen, dass sie auf eine Datenübermittlung in alle Länder außerhalb der EU oder beispielsweise in Länder mit (gegebenenfalls: trotz Angemessenheitsbeschlusses) zweifelhaftem Datenschutzniveau verzichten. Ob für eine solche Zertifizierung eine Nachfrage besteht oder die Verantwortlichen und Auftragsverarbeiter auf andere Zertifizierungsverfahren ausweichen, ist eine offene Frage. Es erscheint aber zumindest nicht ausgeschlossen, dass Dienstleister sich in dieser Weise zertifizieren lassen, um gegenüber potentiellen Auftraggebern demonstrieren zu können, dass die derzeitige unsichere Rechtslage und das Damoklesschwert einer Entscheidung des EuGH zum Data Privacy Framework sie nicht tangiert.

5. Fazit und Ausblick

Die Genehmigung der ersten Kriterienkataloge für DSGVO-Zertifizierungen verspricht spannende Zeiten: Sowohl interessierte Verantwortliche und Auftragsverarbeiter als auch betroffene Personen und Aufsichtsbehörden werden mit großem Interesse auf die beginnende Praxis der Zertifizierung blicken. Dies betrifft vor allem die Prüftiefe bei der Anwendung der Kriterien, aber auch den Umgang mit noch offenen Fragen des Zertifizierungsprozesses.

Die Untersuchung hat gezeigt, dass eine wirksame Zertifizierung zumindest im Grundsatz die Zertifizierbarkeit bereichsspezifischer Anforderungen an die Datenverarbeitung voraussetzt. Bisher haben sich aber noch keine Maßstäbe dafür herausgebildet, auf welcher Ebene und durch welche Akteure die Anwendung bereichsspezifischer Normen erfolgen soll.

Der unbestimmte Charakter vieler Normen der DSGVO ist eines ihrer allgemeinen Governance-Probleme. Dieses muss im Rahmen der Zertifizierung in spezifischer Weise adressiert werden. Programmeigner und Zertifizierungsstellen stehen dabei vor der Herausforderung, die Konkretisierungen der Rechtsprechung und des EDSA zu übernehmen und zu rationalisieren, oder aber sie (um den Preis von Rechtsstreitigkeiten) zu hinterfragen. Das Beispiel der Datenübermittlungen in Drittländer zeigt, dass dies für die Praxis der Datenschutzzertifizierung keine kleine Herausforderung sein wird. Angesichts des neuen Angemessenheitsbeschlusses der Kommission steht zu erwarten, dass die Zertifizierung im transatlantischen Verhältnis jedenfalls bis zu einer gerichtlichen Kontrolle durch das Data Privacy Framework überlagert werden wird. Dies mindert ihre grundsätzliche Rolle insbesondere für andere Weltregionen jedoch nicht.

Trotz dieser und weiterer Herausforderungen zeigt sich im Gesamtbild, dass die Datenschutzzertifizierung erhebliche Potenziale hat, um in Zukunft als Instrument einer effektiven und grundrechtsorientierten Data Governance zu dienen. Die Zertifizierung kann nicht alle offenen Fragen der DSGVO adressieren oder gar alle Durchsetzungsdefizite des Datenschutzrechts beheben. Sie könnte aber einen wesentlichen Baustein des Instrumentenkastens der Zukunft bilden. Dies gilt sowohl innerhalb der EU als auch – gerade wegen der Möglichkeit einer Zertifizierung von Verantwortlichen und Auftragsverarbeitern außerhalb der Union – mit Blick auf globale Datenflüsse und die Herausbildung weltweiter Regeln.

Literatur

Baumgartner, Ulrich; Hansch, Guido; Roth, Heiko (2021): Die neuen Standardvertragsklauseln der EU-Kommission für Datenübermittlungen in Drittstaaten. *Zeitschrift für Datenschutz (ZD)*, S. 608-613.

Bäumler, Helmut (2004): Ein Gütesiegel auf den Datenschutz. Made in Schleswig-Holstein. *Datenschutz und Datensicherheit (DuD)*, S. 80-84.

Bäumler, Helmut; Mutius, Albert von (1999): *Datenschutzgesetze der dritten Generation*. Köln: Luchterhand.

–– (2002): *Datenschutz als Wettbewerbsvorteil*. Wiesbaden: Vieweg.

Bundesamt für Sicherheit in der Informationstechnik (BSI); Verfahrensbeschreibung zur Erteilung von IT-Sicherheitskennzeichen. URL: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/IT-Sicherheitskennzeichen/Verfahrensbeschreibung.pdf?__blob=publicationFile&v=3 (besucht am 01.08.2023).

Comission Nationale pour la Protection des Données (CNPD) (08.06.2022): Die CNPD nimmt das Zertifizierungsverfahren «GDPR-CARPA» an. URL: https://cnpd.public.lu/de/actualites/national/2022/06/adpoption-gdpr-carpa.html (besucht am 01.08.2023).

Comission Nationale pour la Protection des Données (CNPD) (13.05.2022): Décision N° 15/2022 du 13 mai 2022 de la Commission nationale pour la protection des données portant exécution de l'article 15 de la loi du 1er août 2018 portant organisation de la Commission nationale pour la protection des données et du régime général sur la protection des données. URL: https://cnpd.public.lu/dam-assets/fr/professionnels/certification/decision-n-15-2022-du-13-mai-2022-criteres-de-certification.pdf (besucht am 01.08.2023).

Comission Nationale pour la Protection des Données (CNPD) (14.10.2022): Die CNPD ist die erste Datenschutzbehörde in Europa, die einer DSGVO Zertifizierungsstelle eine Akkreditierung erteilt hat. URL: https://cnpd.public.lu/de/actualites/national/2022/10/premier-agrement-certification.html (besucht am 01.08.2023)

Datenschutzkonferenz (DSK) (2021): Anforderungen an datenschutzrechtliche Zertifizierungsprogramme, Version 1.8, v. 16.04.2021. URL: https://www.datenschutzkonferenz-online.de/media/ah/DSK_Anwendungshinweis_Zertifizierungskriterien.pdf (besucht am 01.08.2023).

Dehmel, Susanne; Osmann-Magiera, Ludmilla Lea; Weiß, Rebekka (2023): Drittstaatentransfers nach Schrems II. *Zeitschrift für IT-Recht und Recht der Digitalisierung (MMR)*, S. 17-22.

Drews, Hans-Ludwig; Kranz, Hans Jürgen (2000): Datenschutzaudit – Anmerkungen zum Rechtsgutachten von Alexander Roßnagel vom Mai 1999. *Datenschutz und Datensicherheit (DuD)*, S. 226-230.

Duisberg, Alexander (2018): Zertifizierung und der Mittelstand – Quo Vadis?. *Zeitschrift für Datenschutz (ZD)*, S. 53-54.

Ehmann, Eugen; Selmayr, Martin (Hrsg.) (2018): *DSGVO-Kommentar*, 2. Auflage. München: C.H. Beck.

Europäischer Datenschutzsauschuss (EDSA) (04.06.2019): Leitlinien 1/2018 für die Zertifizierung und Ermittlung von Zertifizierungskriterien nach den Artikeln 42 und 43 der Verordnung (EU) 2016/679.

–– (18.06.2021): Empfehlungen 01/2020 zu Maßnahmen zur Ergänzung von Übermittlungstools zur Gewährleistung des unionsrechtlichen Schutzniveaus für personenbezogene Daten.

–– (22.02.2022): Leitlinien 4/2021 über Verhaltensregeln als Instrument für Übermittlungen.

–– (20.06.2023): Recommendations 1/2022 on the application for approval and on the elements and principles to be found in Controller Binding Corporate Rules (Art. 47 GDPR).

–– (14.02.2023): Guidelines 07/2022 on certification as a tool for transfers. Version 2.0.

–– (14.02.2023) Document on the procedure for the adoption of the EDPB opinions regarding national criteria for certification and European Protection Seals.

–– (28.02.2023) Opinion 5/2023 on the EU- Commission Draft Implementing Decision on the adequate protection of personal data under the EU-US Data Privacy Framework.

EU-Kommission (10.01.2017): Proposal for a Regulation of the European Parliament and the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications), COM(2017) 10 Final. URL: https://eur-lex.europa.eu/legal-content/DE/ALL/?uri=CELEX%3A52017PC0010 (besucht am 01.08.2023)

EU-Parlament (20.07.2017): Report on the proposal for a regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications), A8-0324/2017. URL: https://www.europarl.europa.eu/doceo/document/A-8-2017-0324_EN.html (besucht am 01.08.2023)

–– (11.05.2023): Adequacy of the protection afforded by the EU-U.S. Data Privacy Framework European Parliament resolution of 11 May 2023 on the adequacy of the protection afforded by the EU-US Data Privacy Framework (2023/2501(RSP)). URL: https://www.europarl.europa.eu/doceo/document/TA-9-2023-0204_EN.pdf (besucht am 01.08.2023).

–– (10.07.2023): Commission Implementing Decision of 10.7.2023 pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council on the adequate level of protection of personal data under the EU-US Data Privacy Framework C(2023) 4745 final. URL: https://commission.europa.eu/system/files/2023-07/Adequacy%20decision%20EU-US%20Data%20Privacy%20Framework_en.pdf (besucht am 01.08.2023)

Eßer, Martin; Kramer, Philipp; v. Lewinski, Kai (Hrsg.) (2020): *Auernhammer – DSGVO/BDSG Kommentar*, 7. Auflage. Köln: Carl Heymanns.

EWR-Ausschuss (06.07.2018): Beschluss des gemeinsamen EWR-Ausschusses zur Änderung des Anhangs XI (Elektronische Kommunikation, audiovisuelle Dienste und Informationsgesellschaft) und des Protokolls 37 (mit der Liste gemäß Artikel 101) des EWR-Abkommens [2018/1022], OJ L 183, 19.7.2018, p. 23–26.

Hamburgischer Beauftragter für Datenschutz und die Informationsfreiheit (LfDI HH) (29.11.2022): Datenschutz in den USA – aktuelle Lage. URL: https://datenschutz-hamburg.de/pages/executiveorder/ (besucht am 01.08.2023).

Hermann, Christoph; Miller, A. Simon (2021): Direktklagemöglichkeiten gegen Beschlüsse des EDSA. *Zeitschrift für Europarechtliche Studien (ZeuS)*, S. 617-662.

Hofmann, Johanna (2019): *Dynamische Zertifizierung – Datenschutzrechtliche Zertifizierung nach der DSGVO am Beispiel des Cloud Computing?* Baden-Baden: Nomos.

Hofmann, Johanna; Stach, Benjamin (2021): Soft Brexit – die Ruhe vor dem Sturm? Was müssen Unternehmen ab 2021 beachten? *Zeitschrift für Datenschutz (ZD)*, S. 3 – 8.

Hornung, Gerrit (2021): Das IT-Sicherheitsgesetz 2.0: Kompetenzaufwuchs des BSI und neue Pflichten für Unternehmen. *Neue Juristische Wochenschrift (NJW)*, S. 1985-1991.

–– (2022): Trainingsdaten und die Rechte von betroffenen Personen – in der DSGVO und darüber hinaus? In: Rostalski, Frauke (Hrsg.): *Künstliche Intelligenz. Wie gelingt eine vertrauenswürdige Verwendung in Deutschland und Europa?* Tübingen: Mohr Siebeck, S. 91-120.

Johannes, Paul Christoph (2020): Zertifizierung von Datenverarbeitungsvorgängen bei der Polizei. *Die Polizei*, S. 409-415.

Kowalski, Bernd; Intemann, Matthias (2018): Perspektiven der IT-Sicherheits-Zertifizierung für Europas Märkte. *Datenschutz und Datensicherheit (DuD)*, S. 415-419.

Königshofen, Thomas (2000): Chancen und Risiken eines gesetzlich geregelt Datenschutzaudits. Der Versuch einer Versachlichung der Diskussion. *Datenschutz und Datensicherheit (DuD)*, S. 357-360.

Krcmar, Helmut; Eckert, Claudia; Roßnagel, Alexander; Sunyaev, Ali; Wiesche, Manuel (2018): *Management sicherer Cloud-Services – Entwicklung und Evaluation dynamischer Zertifikate*. Wiesbaden: Springer Fachmedien.

Der Landesbeauftragte für Datenschutz und Informationsfreiheit Baden-Württemberg (LfDI BW) (22.10.2022): Interne Einschätzung des LfDI Baden-Württemberg zur Frage, ob die Executive Order des US-Präsidenten der erhoffte Befreiungsschlag in Sachen internationaler Datentransfers darstellt. URL: https://fragdenstaat.de/anfrage/einschaetzung-zum-eu-u-s-data-privacy-framework/746772/anhang/executiveorder-lfdi-bawu.pdf (besucht am 01.08.2023).

Martini, Mario; Kühling, Jürgen; Heberlein, Johanna; Kühl, Benjamin; Nink, David; Quirin, Weinzierl; Wenzel, Michael (2016): *Die Datenschutz-Grundverordnung und das nationale Recht*. Münster: Monsenstein und Vannerdat.

Mirtsch, Mona (2019): Kapitel 9: Konformitätsbewertung im Bereich Cybersicherheit. In: Mangelsdorf, Axel and Weiler, Petra (Hrsg.): *Normen und Standards für die digitale Transformation: Werkzeuge, Praxisbeispiele und Entscheidungshilfen für innovative Unternehmen, Normungsorganisationen und politische Entscheidungsträger*. Berlin, Boston: De Gruyter Oldenbourg, S. 141-164.

Müller, Johannes (2022): AUDITOR: Zwischenstand im Forschungsprojekt „European Cloud Service Data Protection Certification". *Zeitschrift für Datenschutz-Aktuell (ZD-Aktuell)*, 2022, 01239.

Paal, Boris P.; Pauly, Daniel A. (Hrsg.) (2021), *DS-GVO BDSG – Kompakt Kommentar*, 3. Auflage, München: C.H. Beck.

President of the United States (7.10.2022): Executive Order On Enhancing Safeguards For United States Signals Intelligence Activities. URL: https://www.whitehouse.gov/briefing-room/presidential-actions/2022/10/07/executive-order-on-enhancing-safeguards-for-united-states-signals-intelligence-activities/ (besucht am 01.08.2023).

Rat der EU (10.02.2021): Proposal for a Regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications) – Mandate for negotiations with EP, 6087/21.

Richter, Frederik (2020): Zertifizierung unter der DS-GVO – Chance eines erleichterten internationalen Datenverkehrs darf nicht verpasst werden. *Zeitschrift für Datenschutz (ZD)*, S. 84-87.

Roßnagel, Alexander (2000): *Datenschutzaudit: Konzeption, Durchführung, gesetzliche Regelung*. Wiesbaden: Springer.

–– (2003): *Handbuch Datenschutzrecht*. München: C.H. Beck.

–– (2017): *Datenschutzaufsicht nach der EU-Datenschutz-Grundverordnung*. Wiesbaden: Springer.

–– (2022): Was folgt auf das Privacy Shield? Ein Privacy Framework oder Schrems III? *Zeitschrift für Datenschutz (ZD)*, S. 305-306.

–– (2023): Videokonferenzen als Telekommunikationsdienste. *Neue Juristische Wochenschrift (NJW)*, S. 400-405.

Schallbruch, Martin (2021): Das IT-Sicherheitsgesetz 2.0 – neue Regeln für Unternehmen und IT-Produkte. *Computer und Recht (CR)*, S. 450-458.

Schellhas-Mende, Friederike; Wiedemann, Nils; Blum, Nicolas (2022): Videokonferenzsysteme als Telekommunikationsdienst. *Datenschutz und Datensicherheit (DuD)*, S. 291-295.

Simitis, Spiros; Hornung, Gerrit; Spiecker gen. Döhmann, Indra (Hrsg.) (2019): *Kommentar Datenschutzrecht (DSGVO mit BDSG)*. Baden-Baden: Nomos.

Unabhängiges Landeszentrum für Datenschutz, Register der verliehenen Datenschutzsiegel, URL: https://www.datenschutzzentrum.de/guetesiegel/register/ / (besucht am 01.08.2023).

Vladeck, Stephen I. (15.11.2021): Datenschutzkonferenz (DSK) Gutachten zum aktuellen Stand des US-Überwachungsrechts und der Überwachungsbefugnisse. URL: https://www.datenschutzkonferenz-online.de/media/weitere_dokumente/Vladek_Rechtsgutachten_DSK_de.pdf (besucht am 01.08.2023).

Weiß, Martin (2022): *Öffnungsklauseln in der DSGVO und nationale Verwirklichung im BDSG*. Baden-Baden: Nomos.

Wittershagen, Leonie (2023): *The Transfer of Personal Data from the European Union to the United Kingdom post-Brexit*. Berlin, Boston: De Gruyter.