Anforderungen an datenschutzrechtliche Zertifizierungsprogramme

Datenschutzrechtliche Prüfkriterien, Prüfsystematik und Prüfmethoden zur Anpassung und Anwendung der technischen Norm DIN EN ISO/IEC 17067 (Programmtyp 6)

Version 2.0 (21.06.2022)

Inhalt

1 Ziel und Einordnung

1.1 Ziel

Zur Vorbereitung einer Akkreditierung muss die Zertifizierungsstelle oder der Programmeigner ein Zertifizierungsprogramm erstellen und durch die DAkkS[1] gem. DIN EN ISO/IEC 17011 auf Eignung prüfen lassen (vgl. DAkkS-Regel 71 SD 0016). Wesentlicher Teil dieses Zertifizierungsprogramms sind die Zertifizierungskriterien zur Umsetzung der datenschutzrechtlichen Anforderungen. Diese werden gem. Art. 57 Abs. 1 lit. n DSGVO i. V. m. Art. 42 Abs. 5 DSGVO[2] entweder von der zuständigen Datenschutzaufsichtsbehörde genehmigt oder (i. d. R. über die zuständige Aufsichtsbehörde) dem Europäischen Datenschutzausschuss zur Genehmigung bzw. Billigung gem. Art. 63, 64 Abs. 1 lit. c übermittelt.

Das vorliegende Dokument beschreibt die Mindestanforderungen an die Zertifizierungskriterien, die ergänzend zu den Vorgaben der DIN EN ISO/IEC 17067 von allen Zertifizierungsprogrammen erfüllt sein müssen. Aufgrund der Spezifika eines Zertifizierungsprogramms können sich weitere Anforderungen ergeben.

Ein Zertifizierungsprogramm muss somit zwingend die folgenden Anforderungen an eine Zertifizierung enthalten:

(1) Die Anforderungen aus der DIN EN ISO/IEC 17067 (Programmtyp 6);

(2) die für alle Zertifizierungsprogramme bestehenden Mindestanforderungen aus dem vorliegenden Dokument;

(3) soweit erforderlich, Spezialanforderungen: Diese können sich z. B. daraus ergeben, dass ein Zertifizierungsprogramm auf einen spezifischen Bereich ausgerichtet ist, spezifische Verarbeitungsvorgänge adressiert oder potenzielle Zertifizierungsgegenstände in den Anwendungsbereich von spezialrechtlichen Regelungen fallen.

---

1 Die Deutsche Akkreditierungsstelle GmbH (DAkkS) hat ihre rechtliche Grundlage im Akkreditierungsstellengesetz (AkkStelleG) gem. EU-VO 765/2008.

2 Sofern es sich um Artikel aus der DSGVO handelt, wird im weiteren Verlauf auf den Zusatz „DSGVO“ verzichtet.

Weitere Anforderungen können durch die Akkreditierungsstellen insbesondere unter Berücksichtigung der Leitlinien des Europäischen Datenschutzausschusses (EDSA)[3], der Beschlüsse der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder, der Rechtsprechung oder der Akkreditierungspraxis aufgestellt werden.

Das vorliegende Dokument hat aus den vorgenannten Gründen keinen Anspruch auf Vollständigkeit. Es soll den deutschen Aufsichtsbehörden bei der Bewertung von Zertifizierungsprogrammen als einheitliche Bewertungsgrundlage dienen und Programmeignern sowie Zertifizierungsstellen bei der Erstellung ihrer Dokumente als Orientierung helfen.

1.2 Einordnung in die Regelungssystematik

Ausgangspunkt für die Ausgestaltung von Zertifizierungsprogrammen ist die DIN EN ISO/IEC 17067[4].

Diese Norm enthält keine fachspezifischen Aspekte, sodass zur Formulierung von Anforderungen an datenschutzrechtliche Kriterien gem. Art. 42 Abs. 5 Anpassungen und Ergänzungen der DIN EN ISO/IEC 17067 durch die unabhängigen Aufsichtsbehörden erfolgen.

Die Anwendung der DIN EN ISO/IEC 17067 beinhaltet die Definition und Abgrenzung verschiedener Programmtypen. Aufgrund der datenschutzrechtlichen Prüferfahrung und -praxis in den zuständigen Aufsichtsbehörden müssen Zertifizierungsprogramme für Datenschutzsiegel und -prüfzeichen gem. Art. 42 am Programmtyp 6 ausgerichtet werden.

---

3 Siehe insbesondere „Leitlinien 1/2018 für die Zertifizierung und Ermittlung von Zertifizierungskriterien nach den Artikeln 42 und 43 der Verordnung (EU) 2016/679“ https://edpb.europa.eu/our-work-tools/our-documents/leitlinien/guidelines-12018-certification-and-identifying-certification_de.

4 DIN EN ISO/IEC 17067 ist in der Anwendung der technischen Normen die Folgenorm von DIN EN ISO/IEC 17065, die zur Anwendung in Art. 43 Abs. 1 lit. b gesetzlich festgelegt ist.

1.3 Prüfverfahren

Das Zertifizierungsprogramm muss einen Prüfprozess vorsehen, der eine praktische Überprüfung, eine technische Bewertung und rechtliche Beurteilung der andauernden Einhaltung der Anforderungen des jeweiligen Zertifizierungsprogramms ermöglicht (Aktualität). Ergeben sich aus der jeweiligen Überprüfung, Bewertung und Beurteilung Änderungsbedarfe, sind entsprechend geeignete Maßnahmen zu ergreifen. Dieser Prüfprozess muss zum Zeitpunkt der Zertifizierung implementiert sein und für den gesamten Geltungszeitraum aufrechterhalten und gewährleistet werden.

In einem Zertifizierungsprogramm ist neben den unter 1.1 genannten Zertifizierungsanforderungen darzulegen, mit welchem Prüfverfahren eine akkreditierte Zertifizierungsstelle die Zertifizierungsgegenstände prüft.

Das datenschutzrechtliche Prüfverfahren muss geeignet sein, die ordnungsgemäße Umsetzung datenschutzrechtlicher Anforderungen und die Wirksamkeit technisch-organisatorischer Maßnahmen für den Zertifizierungsgegenstand gegenüber den festgelegten genehmigten Kriterien gem. Art. 42 Abs. 5 festzustellen und zu belegen. DSGVO-Konformität wird erreicht, wenn ein solcher Nachweis für den Zertifizierungsgegenstand erbracht wird.

Jedes Zertifizierungsprogramm muss den Anspruch haben, dass eine ordnungsgemäß erteilte Zertifizierung zu keiner Beanstandung in einer datenschutzrechtlichen Prüfung des Zertifizierungsgegenstands durch eine unabhängige Aufsichtsbehörde führt. Somit muss ein Zertifizierungsprogramm geeignet sein, die DSGVO-Konformität des Zertifizierungsgegenstands vollumfänglich zu prüfen und nachzuweisen. Die Aufsichtsbehörde kann jederzeit ihre aufsichtsrechtlichen Befugnisse ausüben und z. B. bei einer Prüfung zu dem Ergebnis kommen, dass eine Datenverarbeitung rechtswidrig ist.

1.4 Basisdokumente

Dieses Dokument zur Ausgestaltung von Kriterien gem. Art. 42 Abs. 5 mit dazugehöriger Prüfsystematik und den dazugehörigen Prüfmethoden i. V. m. DIN EN ISO/IEC 17067 (Programmtyp 6) baut auf

- den Vorgaben aus Art. 43,
- den genannten sowie themenspezifischen Leitlinien des EDSA,
- den Normen ISO/IEC 17065 und ISO/IEC 17067 und
- dem Ergänzungspapier der DSK[5] gem. Art. 43 Abs. 3 i. V. m. DIN EN ISO/IEC 17065 für Zertifizierungsstellen, die im Rahmen der Akkreditierung durch die DAkkS im Einvernehmen mit den zuständigen unabhängigen Aufsichtsbehörden geprüft werden, auf.

5 „Anforderungen an eine Akkreditierung gem. Art. 43 i. V. m. DIN EN ISO/IEC 17065“ unter https://www.datenschutzkonferenz-online.de/media/ah/20201008_din17065_Ergaenzungen_deutsch_nach_opinion.pdf.

2 Zertifizierungskriterien und Anforderungen an einen Zertifizierungsgegenstand

2.1 Grundsätzliche Anforderungen

2.1.1 Beschreibung des Zertifizierungsgegenstands

Im Zertifizierungsprogramm ist festzulegen, für welche Verarbeitungstätigkeiten es angewendet werden soll. Dies definiert den Anwendungsbereich des Zertifizierungsprogramms. Der Anwendungsbereich soll nur Verarbeitungen im sachlichen und räumlichen Anwendungsbereich der DSGVO enthalten.[6]

Die Mindestanforderungen an die Zertifizierungsprogramme nach 2.1.3 sowie 2.2 ff. sind zu berücksichtigen. Diese müssen sowohl von der akkreditierten Zertifizierungsstelle als auch von der zuständigen Datenschutzaufsichtsbehörde überprüft werden. Wenn es sich um ein generisches Zertifizierungsprogramm handelt, sind die datenschutzrechtlichen Anforderungen vor der Durchführung einer Zertifizierung zu konkretisieren und durch die Zertifizierungsstelle auf Vollständigkeit zu prüfen. Das Zertifizierungsprogramm muss vorsehen, dass sich die Zertifizierung einer Verarbeitungstätigkeit eines Verantwortlichen auf alle diesbezüglichen Verarbeitungsschritte erstreckt, die durch den Verantwortlichen selbst – auch in gemeinsamer Verantwortung mit einem anderen Verantwortlichen – und durch alle einbezogenen Auftragsverarbeiter einschließlich sämtlicher Unterauftragsverarbeiter vollzogen werden.

2.1.2 Angaben des Antragstellers zum Zertifizierungsgegenstand

Zertifizierungsprogramme sollen Vorgaben dazu enthalten, welche Angaben über die zu zertifizierende Verarbeitung, also den Zertifizierungsgegenstand, der Antragsteller der Zertifizierungsstelle vor Aufnahmen des Prüfverfahrens vorzulegen hat. Folgende

---

6 Hinweis: Der Verantwortliche/Auftragsverarbeiter muss nicht unter den räumlichen Anwendungsbereich der DSGVO fallen, vgl. Art. 42 Abs. 2. Nicht betrachtet wird vorliegend z. B. der Anwendungsbereich der Richtlinie (EU) 2016/680 des Europäischen Parlamentes und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung sowie zum freien Datenverkehr und zur Aufhebung des Rahmenbeschlusses 2008/977/JI des Rates („JI-Richtlinie"), da die Konformität mit der JI-Richtlinie nicht Gegenstand einer Zertifizierung nach Art. 42 sein kann.

Angaben sind, soweit auf die jeweilige Verarbeitung anwendbar, mindestens zu verlangen:

1. Welche Verarbeitungsvorgänge sind mit dem Zertifizierungsgegenstand abgedeckt;
2. Welche Zwecke werden mit diesen Verarbeitungsvorgängen abgedeckt und weshalb sind diese Verarbeitungsvorgänge zur Erreichung des Zwecks erforderlich;
3. Wer sind die Empfänger bzw. Kategorien von Empfängern;
4. Welche Daten werden im Zusammenhang mit dem Zertifizierungsgegenstand verarbeitet und
   a. welche Daten sind davon besondere Kategorien personenbezogener Daten gem. Art. 9;
   b. welche Daten beziehen sich auf strafrechtliche Verurteilungen und Straftaten nach Art. 10;
   c. welche Daten beziehen sich auf Kinder im Sinn der DSGVO.
5. Wer ist Auftragsverarbeiter gem. Art. 4 Nr. 8 bzgl. welcher Verarbeitungsvorgänge des Zertifizierungsgegenstands;
6. Ist im Hinblick auf bestimmte Verarbeitungsvorgänge des Zertifizierungsgegenstands eine gemeinsame Verantwortlichkeit gem. Art. 26 gegeben
7. Eine auch in Hinblick auf die Verantwortlichkeit qualifizierte Darstellung des gesamten nach Phasen geordneten Verarbeitungsprozesses sowie des jeweiligen Akteurs- und Rollenmodells (Akteure, Rollen, Beziehungen) für jede Verarbeitungsphase[7];

7 Dies kann entweder durch eine grafische Darstellung (z.B. anhand standardisierter Darstellungsformen wie Business Process Modeling (BPM) oder Unified Modelling Language (UML)) oder in textlicher Form erfolgen.

8. Ist im Hinblick auf die Verarbeitungsvorgänge des Zertifizierungsgegenstands eine Übermittlung personenbezogener Daten

   a. Außerhalb der Europäischen Union bzw. des Europäischen Wirtschaftsraums oder

   b. An internationale Organisationen erfolgt.

   Die Datenübermittlung kann auch im Rahmen von Verwaltung, Wartung, Pflege oder Support vorliegen, um die Funktionstüchtigkeit des Zertifizierungsgegenstands im Geltungszeitraum der Zertifizierung vorzuhalten. Zu prüfen sind auch Weiterübermittlungen durch Auftragsverarbeiter.

9. Was sind Haupt- und Teilkomponenten und wie werden diese aufgegliedert (siehe auch Realisierung von Verarbeitungsvorgängen mittels Systemen und Diensten), beispielsweise durch folgende Punkte:

   a. Aufstellung aller Beteiligten – Gruppenbildung ermöglicht Zusammenfassungen (z. B. Kunden, Nutzer und Administratoren[8] etc.);

   b. Darstellung, auf welche Weise die Datenflüsse unter Nennung der Datenarten zwischen den Komponenten und Beteiligten erfasst werden;

   c. Berücksichtigung und ggf. Erläuterung gesetzlicher Grundlagen zur Verarbeitung personenbezogener Daten in den (Teil-) Komponenten und in Bezug auf die Übermittlung bei Datenflüssen und Datenarten.

Der Zusammenhang zwischen den berücksichtigten gesetzlichen Grundlagen, technischen Normen und dem Zertifizierungsgegenstand in Abhängigkeit des konkreten Einsatzes ist im Zertifizierungsprogramm nachvollziehbar darzustellen.

Als sinnvoll hat sich in der Praxis ferner eine Gegenüberstellung erwiesen, die aufzeigt, an welcher Stelle im Zertifizierungsprogramm die Anforderungen nach DIN ISO

8 Obwohl aus Gründen der Lesbarkeit im Text nur die männliche Form gewählt wurde, beziehen sich die Ausführungen auf Angehörige aller Geschlechter.

17065, 17067 sowie den einschlägigen DSK-Ergänzungspapieren erfüllt werden (kann z.B. in Form einer Matrix erfolgen).

2.1.3 Einhaltung der einschlägigen Datenschutzvorgaben

Art. 42 Abs. 1 sieht vor, dass Zertifizierungsverfahren dem Nachweis dienen sollen, dass die DSGVO bei Verarbeitungsvorgängen von Verantwortlichen und Auftragsverarbeitern eingehalten wird. Um dieses Ziel zu erreichen, müssen die jeweiligen Zertifizierungskriterien die Gewähr dafür bieten, dass die Einhaltung aller einschlägigen Vorgaben der DSGVO sichergestellt ist.

Die Leitlinien 1/2018 des EDSA zur Zertifizierung und zur Ermittlung von Zertifizierungskriterien[9] liefern in diesem Kontext eine Orientierung. Diese benennen Aspekte, die im Zertifizierungsprogramm zu berücksichtigten sind. Da es sich bei dem vorliegenden Papier um ein Dokument, das kontinuierlich weiterentwickelt wird, handelt, werden die in den folgenden Abschnitten aufgeführten Artikel der DSGVO mit unterschiedlicher Detailschärfe betrachtet. Dies ist nicht als Wertung zu verstehen und dient lediglich der Veranschaulichung.

Soweit in den folgenden Abschnitten dieses Kapitels eine Darstellung in Form von Tabellen erfolgt, sind die dort gemachten Ausführungen nicht abschließend. So sind neben den aufgeführten Prüfmethoden weitere Begutachtungstechniken möglich. Die Prüfmethoden sollten sich an den in den Normen festgelegten Evaluationsmethoden orientieren, z. B. Audit gem. ISO 17021, Testing gem. ISO 17025 oder Inspektion gem. ISO/IEC 17020.

In dieser Fassung des Dokuments werden die in Kapitel 2.12 geregelten Rechte der betroffenen Personen (Art. 12 bis 23) zunächst lediglich allgemein dargestellt, ohne die spezifischen Mindestanforderungen auszuformulieren. Letzteres behalten sich die Verfasser dieses Dokuments für eine nachfolgende Auflage vor.

---

9 https://edpb.europa.eu/our-work-tools/our-documents/leitlinien/guidelines-12018-certification-and-identifying-certification_de

2.2 Artikel 5: Grundsätze für die Verarbeitung personenbezogener Daten

Gesetzliche Tatbestandsmerkmale	*In den Zertifizierungskriterien zu behandelnde Prüfthemen und deren Umsetzung durch die Kunden[10] der Zertifizierungsstelle[11]*	*Wie prüft die Zertifizierungsstelle die Umsetzung?*
Art. 5 Abs. 1 lit. a Rechtmäßigkeit, Treu und Glauben, Transparenz	Rechtmäßigkeit, vgl. Kap. 2.3 (Art. 6). Verarbeitung nach Treu und Glauben. Nachvollziehbarkeit der Verarbeitung, Transparenz für betroffene Personen: Art. 12 ff. - Kriterien zur Beurteilung, ob personenbezogene Daten in für die betroffenen Personen nachvollziehbarer Weise verarbeitet werden;	Vgl. Kap. 2.3 (Art. 6). Vgl. insb. Kap. 2.3 (Art. 6). Dokumentenprüfung: Dokumentation der Datenflüsse; Verzeichnis der Verarbeitungstätigkeiten; Informationen nach Art. 13, 14; Dokumentation des Prozesses zur Gewährleistung und Aufrechterhaltung der Transparenz für betroffene Personen. Inspektion aller relevanten Geschäftsprozesse und Systeme, Analyse aller Datenflüsse auf Plausibilität.

10 Bezeichnet nicht nur die Kunden der Zertifizierungsstelle, sondern auch ggf. Vertragspartner der Kunden (z. B. deren Auftragsverarbeiter).
11 Zwei Ebenen der Betrachtung: In dieser Spalte werden zu den wichtigsten gesetzlichen Vorgaben die Prüfthemen aufgeführt, die in den Zertifizierungskriterien zu behandeln sind. Daneben erfolgt eine Darstellung der zur Umsetzung durch die Kunden erforderlichen Maßnahmen.

	- insb. auch Informationen über die Risiken, Vorschriften, Garantien und Rechte sowie darüber, wie diese Rechte geltend gemacht werden können (Erwägungsgrund 39). Es ist eine Dokumentation des Prozesses zur Auswahl und Umsetzung technischer und organisatorischer Maßnahmen erforderlich, die die Transparenz der Verarbeitung gewährleisten (Gewährleistungsziel Transparenz berücksichtigen).	Das Zertifizierungsprogramm muss mindestens vorgeben, dass der Zertifizierungsdienstleister die technischen und organisatorischen Maßnahmen dahingehend prüft, dass die Anforderungen zur Gewährleistung der Transparenz eingehalten werden (Dokumentenprüfung, methodische Analyse).
Art. 5 Abs. 1 lit. b Zweckbindung	Zweckbindung, vgl. insb. Kap. 2.3 (Art. 6). Es ist eine Dokumentation des Prozesses zur Auswahl und Umsetzung technischer und organisatorischer Maßnahmen erforderlich, die die Zweckbindung der Verarbeitung gewährleisten. (Gewährleistungsziel Nichtverkettung berücksichtigen).	Vgl. insb. Kap. 2.3 (Art. 6). Das Zertifizierungsprogramm muss mindestens vorgeben, dass der Zertifizierungsdienstleister die technischen und organisatorischen Maßnahmen dahingehend prüft, dass die Anforderungen zur Gewährleistung der Zweckbindung eingehalten werden (Dokumentenprüfung, methodische Analyse).

Art. 5 Abs. 1 lit. c Datenminimierung	Die Zertifizierungskriterien müssen sich auf den zu führenden Nachweis erstrecken, dass die Verarbeitungstätigkeit in einer datensparsamen Weise durchgeführt wird.	Das Zertifizierungsprogramm muss mindestens vorgeben:
	Die Kriterien müssen die Bewertung dieses Nachweises in Bezug auf die Erfüllung folgender gesetzlicher Vorgaben vorsehen:	Dokumentenprüfung, juristische Analyse der Unterlagen und Dokumentation gem. Spalte 2.
	Die Erfüllung der Bedingungen gem. Art. 5 Abs. 1 lit. c:	Das Zertifizierungsprogramm muss mindestens vorgeben, dass der Zertifizierungsdienstleister die folgenden Komponenten der Verarbeitungstätigkeit per Vor-Ort-Begehungen prüft:
	a) Kriterien, um die Angemessenheit, die Erheblichkeit und die Notwendigkeit der Verarbeitung der personenbezogenen Daten zu beurteilen,	konkrete Datenbestände und Abgleich mit den Kriterien gem. Spalte 2 a); dies kann sich auf eine Stichprobe beschränken.
	b) eine Dokumentation des Prozesses, um zu gewährleisten, dass die Verarbeitung der personenbezogenen Daten jederzeit dem Zweck angemessen und	Das Zertifizierungsprogramm muss vorgeben, dass der Zertifizierungsdienstleister die technischen und organisatorischen Maßnahmen dahingehend prüft, dass die

	erheblich sowie auf das notwendige Maß beschränkt ist (Gewährleistungsziel Datenminimierung berücksichtigen).	Anforderungen zur Gewährleistung der Datenminimierung eingehalten werden (Dokumentenprüfung, methodische Analyse zu Spalte 2 b).
Art. 5 Abs. 1 lit. d Richtigkeit	Die Zertifizierungskriterien müssen sich auf den durch den Verantwortlichen zu führenden Nachweis erstrecken, dass die Verarbeitungstätigkeit dem Grundsatz der Richtigkeit entspricht. Die Kriterien müssen die Bewertung dieses Nachweises in Bezug auf die Erfüllung folgender gesetzlicher Vorgaben vorsehen: Die Erfüllung der Bedingungen gem. Art. 5 Abs. 1 lit. d: a) Kriterien zur Bestimmung der sachlichen Richtigkeit personenbezogener Daten, b) eine Dokumentation des Prozesses zur Bestimmung der sachlichen Richtigkeit personenbezogener Daten, c) eine Dokumentation des Prozesses zur Auswahl	Das Zertifizierungsprogramm muss mindestens vorgeben: Dokumentenprüfung, juristische Analyse der Unterlagen und Dokumentation gem. Spalte 2. Das Zertifizierungsprogramm muss mindestens vorgeben, dass der Zertifizierungsdienstleister die technischen und organisatorischen Maßnahmen dahingehend

	und Umsetzung geeigneter technischer und organisatorischer Maßnahmen, die gewährleisten, dass unrichtige Daten unverzüglich gelöscht oder berichtigt werden (Gewährleistungsziel Integrität und i. V. m. Art. 16 Intervenierbarkeit berücksichtigen).	prüft, dass die Anforderungen zur Gewährleistung der Integrität eingehalten werden (Dokumentenprüfung, methodische Analyse).
Art. 5 Abs. 1 lit. e Speicherbegrenzung	Die Zertifizierungskriterien müssen sich auf den durch den Verantwortlichen zu führenden Nachweis erstrecken, dass er die Verarbeitungstätigkeit nach dem Grundsatz der Speicherbegrenzung durchführt. Die Kriterien müssen die Bewertung dieses Nachweises in Bezug auf die Erfüllung der Bedingungen gem. Art. 5 Abs. 1 lit. e vorsehen: a) Kriterien zur Bestimmung der Identifizierbarkeit einer Person, b) Kriterien zur Bestimmung der für den Zweck der Verarbeitung erforderlichen Dauer der Identifizierbarkeit einer Person,	Das Zertifizierungsprogramm muss mindestens vorgeben: Dokumentenprüfung, juristische Analyse der Unterlagen und Dokumentation gem. Spalte 2.

	c) Kriterien zur Bestimmung der geeigneten Form einer Speicherung personenbezogener Daten, die die Identifizierung einer betroffenen Person nur so lange ermöglicht, wie es für die Zwecke, für die sie verarbeitet werden, erforderlich ist, d) eine Dokumentation des Prozesses zur Auswahl und Umsetzung technischer und organisatorischer Maßnahmen, die gewährleisten, dass personenbezogene Daten in einer Form gespeichert werden, die die Identifizierung einer betroffenen Person nur so lange ermöglicht, wie es für die Zwecke, für die sie verarbeitet werden, erforderlich ist (Gewährleistungsziel Datenminimierung berücksichtigen).	d) Das Zertifizierungsprogramm muss mindestens vorgeben, dass der Zertifizierungsdienstleister die technischen und organisatorischen Maßnahmen dahingehend prüft, dass die Anforderungen zur Gewährleistung der Datenminimierung eingehalten werden (Dokumentenprüfung, methodische Analyse).
Art. 5 Abs. 1 lit. f Integrität und Vertraulichkeit	Datenverarbeitung nach dem Grundsatz der Integrität. Datenverarbeitung nach dem Grundsatz der Vertraulichkeit. Insb. Anforderungen der Art. 24, 25 (vgl. Kap. 2.4), 32 (vgl. Kap. 2.7).	Insb. Anforderungen der Art. 24, 25 (vgl. Kap. 2.4), 32 (vgl. Kap. 2.7).

	Es ist eine Dokumentation des Prozesses zur Auswahl und Umsetzung technischer und organisatorischer Maßnahmen erforderlich, die die Integrität und Vertraulichkeit der Verarbeitung gewährleisten (Gewährleistungsziele Integrität und Vertraulichkeit berücksichtigen).	Das Zertifizierungsprogramm muss mindestens vorgeben, dass der Zertifizierungsdienstleister die technischen und organisatorischen Maßnahmen dahingehend prüft, dass die Anforderungen zur Gewährleistung der Integrität und Vertraulichkeit eingehalten werden (Dokumentenprüfung, methodische Analyse).
Art. 5 Abs. 2 Rechenschaftspflicht	Nachweis der Einhaltung des Art. 5 Abs. 1 (vgl. oben).	

2.3 Artikel 6: Rechtmäßigkeit der Verarbeitung

Eine Verarbeitung personenbezogener Daten ist nur dann zulässig, wenn hierfür eine Rechtsgrundlage besteht. Art. 6 ist die zentrale Vorschrift der DSGVO zur Zulässigkeit der Verarbeitung personenbezogener Daten.

Gesetzliche Tatbestandsmerkmale	*In den Zertifizierungskriterien zu behandelnde Prüfthemen und deren Umsetzung durch die Kunden der Zertifizierungsstelle*	*Wie prüft die Zertifizierungsstelle die Umsetzung?*
Art. 6 Abs. 1 (grundsätzlich) Die Verarbeitung ist nur unter	a) Darstellung, Prüfung und Dokumentation einer Rechtsgrundlage für die jeweilige Verarbeitung aller	Dokumentenprüfung, rechtliche Analyse des Vorhandenseins einer Rechtsgrundlage insbesondere anhand

den in Abs. 1 genannten Voraussetzungen rechtmäßig.	personenbezogenen Daten für jeden einzelnen abgrenzbaren Verarbeitungsvorgang; Verarbeitungsvorgänge, die auf derselben Rechtsgrundlage beruhen, können bei der Darstellung, Prüfung und Dokumentation zusammengefasst werden. b) Soweit Kunden Verantwortlicher i.S.d. Art. 4 Nr. 7 sind: - Dokumentation von Anweisungen an die Beschäftigten zur vorgelagerten Prüfung des Vorhandenseins einer Rechtsgrundlage, auch bevor eine Änderung/Erweiterung des Zertifizierungsgegenstands erfolgt; die Anweisungen sollen auch das „wie“ der Prüfung, z. B. in Form von Leitfäden, beschreiben und Hinweise zu den Prüfungsabläufen beim Verantwortlichen enthalten. - Dokumentation von Strukturen und Zuständigkeiten für die Prüfung einer ausreichenden Rechtsgrundlage (z. B. bei Bedarf Einbindung des Rechts- oder des Datenschutzbereichs oder	der folgenden Unterlagen: der Datenschutzerklärung, der Informationen gem. Art. 13, 14, des Verzeichnisses der Verarbeitungstätigkeiten gem. Art. 30, der internen Vermerke, aus den sich die Prüfung und das Vorliegen einer Rechtsgrundlage ergibt. Dokumentenprüfung, rechtliche Analyse der Dokumentation gemäß Spalte 2, z. B. anhand von internen Richtlinien, Dienstanweisungen oder Betriebsvereinbarungen des Verantwortlichen.

	anderer zuständiger Stellen). c) Vorhandensein und Dokumentation von Abläufen und Maßnahmen, die nach Wegfall der Rechtmäßigkeit der Verarbeitung zu einer Löschung der Daten führen. Insbesondere sind auch die Anforderungen aus Art. 5 Abs. 1 lit. e zu beachten.	Dokumentenprüfung und mindestens stichprobenartige Inspektion der Abläufe und Maßnahmen gemäß Spalte 2. Ferner Prüfung gemäß Vorgaben zu Art. 5 Abs. 1 lit. e.
Art. 6 Abs. 1 lit. a Die betroffene Person hat ihre Einwilligung zu der Verarbeitung der sie betreffenden personenbezogenen Daten für einen oder mehrere bestimmte Zwecke gegeben.	a) Prüfung und Dokumentation des Vorliegens einer wirksamen Einwilligung für - jeden Verarbeitungsvorgang, - jeden Satz personenbezogener Daten, - einen oder mehrere genau bezeichnete Zwecke. b) Dabei ist insbesondere zu prüfen, ob sämtliche einschlägige Anforderungen an eine Einwilligung, insbesondere solche aus Art. 7, 8 erfüllt sind, u. a.: - Ist gewährleistet, dass für alle Verarbeitungsvorgänge und -zwecke umfassende und ausreichend deutliche Erklärungen der Betroffenen	Dokumentenprüfung, rechtliche Analyse der Einwilligung (insb. auf Vollständigkeit, Freiwilligkeit, Aktualität, Übereinstimmung mit Zweck und Verständlichkeit) anhand der Dokumentation gemäß Spalte 2 a). Inspektion der eingerichteten Abläufe und Maßnahmen zur Einholung der Einwilligung. Bei bereits stattfindenden Verarbeitungsvorgängen Stichproben der bestehenden Einwilligungen.

	(und/oder ihrer Vertreter) vor Beginn der Verarbeitung eingeholt und dokumentiert werden?	
	- Ist der Betroffene einwilligungsfähig und sind ggf. Einwilligungen (auch) der vertretungsberechtigten Personen eingeholt worden?	Dokumentenprüfung, rechtliche Analyse sowie Inspektion der (1) Abläufe zur Feststellung der Einwilligungsfähigkeit, insb. der Altersverifikation, und (2) der weiteren Abläufe im Falle der Feststellung der Einwilligungsunfähigkeit.
	- Wurde die Einwilligung freiwillig erklärt (insbesondere unter Beachtung von Über-/Unterordnungsverhältnissen und des Kopplungsverbots für die Verarbeitung)?	
	- Ist die Einwilligung jederzeit widerrufbar und führt sie zur Beendigung der Verarbeitung (oder bestehen z. B. alternative Rechtsgrundlagen für die Verarbeitung)?	Dokumentenprüfung, rechtliche Analyse der Ausgestaltung des Widerrufsprozesses sowie Inspektion. Hierzu zählen auch die Prüfung und die Inspektion der Abläufe, die dazu führen, dass die Daten nach Eingang eines Widerrufs gelöscht werden.
	- Wurde die betroffene Person und ggf. die vertretungsberechtigte(n) Person(en) vor der Erklärung der Einwilligung ausreichend und unter	

	Wahrung des Transparenzgrundsatzes aufgeklärt?	
Art. 6 Abs. 1 lit. b Die Verarbeitung ist für die Erfüllung eines Vertrags, dessen Vertragspartei die betroffene Person ist, oder zur Durchführung vorvertraglicher Maßnahmen erforderlich, die auf Anfrage der betroffenen Person erfolgt.	Benennung, Prüfung und Dokumentation des Vorliegens der folgenden Voraussetzungen:	
	a) Vorliegen eines Vertrags mit der betroffenen Person oder eines vorvertraglichen Verhältnisses auf Anfrage der betroffenen Person. Insbesondere sind diese (Vertrags-) Verhältnisse abzugrenzen von den Fällen einer unverbindlichen Kenntnisnahme von veröffentlichten Angeboten (z. B. Besuch einer Internetseite), nachvertraglichen Verhältnissen und offensichtlich unwirksamen Verträgen.	Dokumentenprüfung, rechtliche Analyse anhand von Dokumentation (insbesondere Vertragsmuster, Beschreibungen oder Vermerken zu vorvertraglichen Verhältnissen) des Bestehens eines Vertrags oder eines vorvertraglichen Verhältnisses mit der betroffenen Person.
	b) alle verarbeiteten Daten sind zur Vertragserfüllung oder zur Durchführung der vorvertraglichen Maßnahmen erforderlich.	Rechtliche und fachliche Analyse der Erforderlichkeit gem. Spalte 2 b) und c). Ferner Prüfung gemäß Vorgaben zu Art. 5 Abs. 1 lit. c.
	c) alle Verarbeitungsvorgänge sind zur Vertragserfüllung oder zur Durchführung der vorvertraglichen	Siehe b).

	Maßnahmen erforderlich. d) Dokumentation von Strukturen und Abläufen, die zu einem Vertragsschluss oder einem vorvertraglichen Verhältnis führen. zu b) bis d) sind insbesondere auch die Anforderungen aus Art. 5 Abs. 1 lit. c zu erfüllen.	Dokumentenprüfung der Strukturen und Abläufe gemäß Spalte 2 d) und Inspektion der Abläufe, die zu einem Vertragsschluss oder zu einem vorvertraglichen Verhältnis führen. Bei bereits stattfindenden Verarbeitungsvorgängen mindestens stichprobenartige Dokumentenprüfung von abgeschlossenen Verträgen oder eingegangenen vorvertraglichen Verhältnissen.
Art. 6 Abs. 1 lit. c Die Verarbeitung ist zur Erfüllung einer rechtlichen Verpflichtung erforderlich, der der Verantwortliche unterliegt.	Benennung, Prüfung und Dokumentation des Vorliegens der folgenden Voraussetzungen: a) Vorliegen einer rechtlichen Verpflichtung des Verantwortlichen, einschließlich einer Darstellung der Bedingungen des Eintritts dieser Verpflichtung, ihres Umfangs und der Umstände, die zu einem Wegfall der Verpflichtung führen können, ggf. bei feh-	Dokumentenprüfung, Analyse des Vorliegens einer rechtlichen Verpflichtung des Verantwortlichen anhand der Dokumentation gemäß Spalte 2 a).

	lender Eindeutigkeit des Wortlauts inklusive einschlägiger Auslegungsdokumentation wie z. B. Kommentarliteratur, Rechtsgutachten, Rechtsprechung.	
	b) Alle verarbeiteten Daten sind zur Erfüllung der o. g. rechtlichen Verpflichtung erforderlich.	Rechtliche und fachliche Analyse der Erforderlichkeit der Datenverarbeitung zur Erfüllung dieser Verpflichtung gem. Spalte 2 b) und c).
	c) Alle Verarbeitungsvorgänge sind zur Erfüllung der o. g. rechtlichen Verpflichtung erforderlich. zu b) bis c) sind insbesondere auch die Anforderungen aus Art. 5 Abs. 1 lit. c zu erfüllen.	Siehe b). Ferner Prüfung gemäß Vorgaben zu Art. 5 Abs. 1 lit. c.
	d) Dabei sind die in Abs. 2 und 3 in Bezug genommenen Regelungen bzw. eventuell bestehende Sonderregelungen zu beachten.	Dokumentenprüfung, rechtliche Analyse zur Beachtung der Regelungen gem. Spalte 2 d).
Art. 6 Abs. 1 lit. d	Benennung, Prüfung und Dokumentation der folgenden Voraussetzungen:	

Die Verarbeitung ist erforderlich, um lebenswichtige Interessen der betroffenen Person oder einer anderen natürlichen Person zu schützen.	a) Vorliegen lebenswichtiger Interessen der betroffenen Person oder einer anderen natürlichen Person. Erwartet wird insbesondere eine eingehende Dokumentation, wessen und welche lebenswichtigen Interessen betroffen sind. b) Alle verarbeiteten Daten sind für den Schutz der lebenswichtigen Interessen erforderlich. c) Alle Verarbeitungsvorgänge sind für den Schutz der lebenswichtigen Interessen erforderlich. Zu b) bis c) sind insbesondere auch die Anforderungen aus Art. 5 Abs. 1 lit. c zu erfüllen.	Dokumentenprüfung, rechtliche Analyse des Vorliegens lebenswichtiger Interessen einer natürlichen Person anhand der Dokumentation gemäß Spalte 2. Rechtliche und fachliche Analyse der Erforderlichkeit der Datenverarbeitung zum Schutz der o. g. lebenswichtigen Interessen gem. Spalte 2 b) und c). Ferner Prüfung gemäß Vorgaben zu Art. 5 Abs. 1 lit. c. Siehe b).
Art. 6 Abs. 1 lit. e Die Verarbeitung ist für die Wahrnehmung einer Aufgabe	Benennung, Prüfung und Dokumentation des Vorliegens folgender Voraussetzungen:	

erforderlich, die im öffentlichen Interesse liegt oder in Ausübung öffentlicher Gewalt erfolgt, die dem Verantwortlichen übertragen wurde.	a) Dem Verantwortlichen wurde die Wahrnehmung einer im öffentlichen Interesse liegenden oder in Ausübung öffentlicher Gewalt erfolgenden Aufgabe übertragen. Erwartet wird auch eine Darstellung der Bedingungen dieser Aufgabenerfüllung, ihres Umfangs und der Umstände, die zu einem Wegfall dieser Voraussetzungen führen können.	Dokumentenprüfung, rechtliche Analyse des Vorliegens einer an den Verantwortlichen übertragenen Aufgabe im Sinne des Art. 6 Abs. 1 lit. e anhand der Dokumentation gemäß Spalte 2.
	b) Alle verarbeiteten Daten sind für die Wahrnehmung der o. g. Aufgabe erforderlich.	Rechtliche und fachliche Analyse der Erforderlichkeit der Datenverarbeitung zur Wahrnehmung dieser Aufgabe gem. Spalte 2 b) und c). Ferner Prüfung gemäß Vorgaben zu Art. 5 Abs. 1 lit. c.
	c) Alle Verarbeitungsvorgänge sind für die Wahrnehmung der o. g. Aufgabe erforderlich. Zu b) bis c) sind insbesondere auch die Anforderungen aus Art. 5 Abs. 1 lit. c zu erfüllen.	Siehe b).
	d) Dabei sind insbesondere die Vorgaben des Art. 6	Dokumentenprüfung, rechtliche Analyse zur Beachtung der Regelungen gem. Spalte 2 d).

	Abs. 2 und 3 sowie eventuell bestehender Sonderregelungen, z. B. in Abhängigkeit des Anwendungskontexts, zu beachten.	
Art. 6 Abs. 1 lit. f Die Verarbeitung ist zur Wahrung der berechtigten Interessen des Verantwortlichen oder eines Dritten erforderlich, sofern nicht die Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person, die den Schutz personenbezogener Daten erfordern, überwiegen, insbesondere dann, wenn es sich bei der betroffenen Person um ein Kind handelt.	a) Darstellung, Prüfung und Dokumentation, inwiefern - die Verarbeitung im berechtigten Interesse des Verantwortlichen oder eines Dritten liegt, - es sich nicht um von Behörden in Erfüllung ihrer Aufgaben vorgenommene Verarbeitungen handelt, - die Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person nicht überwiegen, insbesondere dann, wenn es sich dabei um ein Kind handelt. b) Dokumentation des Prozesses zur Interessenabwägung, der konkrete Kriterien für die Abwägung und entsprechende Ergebnisse vorsieht. Der Prozess muss insbesondere die Darstellung vorsehen, welche und wessen konkrete Interessen gegen welche und wessen konkrete Interessen oder Rechte jeweils	Dokumentenprüfung, rechtliche Analyse des Vorliegens der Voraussetzungen des Art. 6 Abs. 1 lit. f. anhand der Dokumentation gemäß Spalte 2. Zu prüfen ist insbesondere, ob die Abwägung jeweils korrekt vorgenommen wurde. Dabei sollen auch stichprobenartig Datensätze untersucht werden, ob hierbei Kinder betroffen sind oder sein können und dies in der Abwägung entsprechend berücksichtigt wurde. Prüfung und Inspektion des Prozesses der Interessenabwägung.

	hinsichtlich welcher personenbezogenen Daten und welcher Verarbeitungsvorgänge abgewogen werden.	Mindestens Stichprobenartige Validierung der Datenflüsse zwischen Systemen und Diensten (zur Erbringung einer (spezifizierten) Dienstleistung.
Art. 6 Abs. 4 Bei nachträglicher Veränderung des Verarbeitungszwecks bestehen besondere Anforderungen gem. Art. 6 Abs. 4, wenn für den neuen Zweck keine gesetzliche Grundlage besteht oder die Betroffenen nicht auch bzgl. dieses Zwecks eine (wirksame) Einwilligung abgegeben haben.	a) Dokumentation der Zweckänderung (von welchem Zweck zu welchem?). b) Dokumentation der Begründung der Zweckänderung sowie Dokumentation der rechtlichen Prüfung der Zulässigkeit der Zweckänderung. c) Vorliegen dokumentierter Maßnahmen, damit bevorstehende Zweckänderungen erkannt werden und der geänderte Zweck rechtzeitig geprüft und ggf. weitere Vorkehrungen getroffen werden können (wie z. B. die Einholung weiterer Einwilligungen der Betroffenen).	Dokumentenprüfung: Prüfung des Vorliegens einer Zweckänderung anhand der Dokumentation gem. Spalte 2; Dokumentenprüfung, rechtliche Analyse der Zulässigkeit der Zweckänderung anhand der Dokumentation gemäß Spalte 2; Dokumentenprüfung: Prüfung der Maßnahmen zur Erkennung von Zweckänderungen und zum Vorhandensein der sich daran anschließenden notwendigen Vorkehrungen anhand der Dokumentation gemäß Spalte 2 sowie mindestens stichprobenartige Inspektion dieser Maßnahmen und Vorkehrungen.

2.4 Artikel 25: Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen

Gesetzliche Tatbestandsmerkmale	*In den Zertifizierungskriterien zu behandelnde Prüfthemen und deren Umsetzung durch die Kunden der Zertifizierungsstelle*	*Wie prüft die Zertifizierungsstelle die Umsetzung?*
Art. 25 Abs. 1 Datenschutz durch Technikgestaltung	Es muss eine datenschutzrechtliche Risikobetrachtung (siehe auch „datenschutzrechtliche Risikobetrachtung“) der Verarbeitungsvorgänge vollzogen und dokumentiert werden. Es muss der Stand der Technik beobachtet und für die eingesetzten Mittel für die Verarbeitung berücksichtigt werden. Die Mittel der Verarbeitung müssen diesem Stand angemessen folgen. (Weitere Abwägungsbelange sind Implementierungskosten, Art des Umfangs, Umstände und Zwecke der Verarbeitung, Eintrittswahrscheinlichkeiten und Schwere der mit der Verarbeitung	Dokumentenprüfung der Risikobetrachtung. Befragung von Mitarbeitern, welche Maßnahmen zur Beobachtung des Stands der Technik ergriffen werden und ob Vorschläge zur Aktualisierung der Mittel angemessen berücksichtigt werden (siehe insoweit ergänzend Vorgaben zum „Zeitpunkt der Verarbeitung“). Dokumentenprüfung von Tätigkeitsbeschreibungen oder Arbeitsanweisungen

	verbundenen Risiken für die Rechte und Freiheiten natürlicher Personen.) Es muss eine Beschreibung aller technischen und organisatorischen Maßnahmen zur Wahrung der Datenschutzgrundsätze und Aufnahme notwendiger Garantien, - um den Anforderungen der DSGVO zu genügen und - um die Rechte der betroffenen Personen zu schützen, bestehen.	Dokumentenprüfung der getroffenen Maßnahmenübersicht und Validierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Minderung des datenschutzrechtlichen Risikos.
Art. 25 Abs. 1 Zum Zeitpunkt der Festlegung der Mittel für die Verarbeitung werden geeignete technische und organisatorische Maßnahmen getroffen, die dafür ausgelegt sind, die Datenschutzgrundsätze wirksam umzusetzen und die	Es müssen Prozesse bestehen, welche die Berücksichtigung der Datenschutzgrundsätze zum Zeitpunkt der Festlegung der Mittel gewährleisten.	Dokumentenprüfung der Prozessdokumentation. Dokumentenprüfung von exemplarischen Ausschreibungen und Abnahmekriterien für Mittel der Verarbeitung. Befragung von Mitarbeitenden über Entscheidungsprozesse in der Designphase der Systeme.

notwendigen Garantien in die Verarbeitung aufzunehmen, um den Anforderungen dieser Verordnung zu genügen und die Rechte der betroffenen Personen zu schützen.	Die Festlegung auf bzw. die Entscheidung für geeignete technische und/oder organisatorische Maßnahmen muss dokumentiert und begründet werden (vgl. Art. 5 Abs. 1 lit. f i. V. m. Art. 5 Abs. 2).	Dokumentenprüfung der Entscheidungsdokumentation hinsichtlich der angemessenen Abwägung i. S. d. Art. 25 Abs. 1.
Art. 25 Abs. 1 Zum Zeitpunkt der Verarbeitung werden geeignete technische und organisatorische Maßnahmen getroffen, die dafür ausgelegt sind, die Datenschutzgrundsätze wirksam umzusetzen und die notwendigen Garantien in die Verarbeitung aufzunehmen, um den Anforderungen dieser Verordnung zu genügen und die Rechte der betroffenen Personen zu schützen.	Es müssen alle Verarbeitungstätigkeiten erfasst und auf Grundlage der Risikobetrachtung geeignete technische und organisatorische Maßnahmen zur Minderung des festgestellten Risikos umgesetzt werden (vgl. Art. 32 Abs. 1). Die Festlegung auf bzw. die Entscheidung für geeignete technische und/oder organisatorische Maßnahmen muss dokumentiert und begründet werden (vgl. Art. 5 Abs. 1 lit. f i. V. m. Art. 5 Abs. 2).	Prüfung hinsichtlich der vollständigen Erfassung aller Verarbeitungstätigkeiten anhand des Verzeichnisses der Verarbeitungstätigkeiten gem. Art. 30 bzw. von Datenflussdiagrammen, Systemübersichten, Prozessbeschreibungen, o. Ä. Validierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Minderung des datenschutzrechtlichen Risikos. Dokumentenprüfung der Entscheidungsdokumentation hinsichtlich der angemessenen Abwägung i. S. d. Art. 25 Abs. 1.

Art. 25 Abs. 2 Datenschutzfreundliche Voreinstellungen	Es müssen alle Einstellungen der Mittel der Verarbeitung geprüft werden, ob diese die Verarbeitung auf das notwendige Maß beschränken und standardmäßig auf diese beschränkte Einstellung gesetzt werden.	Prüfung der Einstellungen einer Standardkonfiguration der Mittel der Verarbeitung, bei der alle nicht erforderlichen Verarbeitungsvorgänge deaktiviert sein müssen. Prüfung der Erforderlichkeit von nicht beschränkenden Voreinstellungen anhand der Verarbeitungszwecke.
	Es muss die notwendige Menge der erhobenen Daten, der Umfang der Verarbeitung, ihre Speicherfrist und ihre Zugänglichkeit dokumentiert und begründet werden (vgl. Art. 5 Abs. 1 lit. c, e i. V. m. Art. 5 Abs. 2).	Prüfung der dokumentierten Beschränkungen, ob die aufgeführten Gründe einer weitergehenden Datenminimierung entgegenstehen.
	Es muss gewährleistet sein, dass personenbezogene Daten nicht durch die Voreinstellung einer unbestimmten Zahl von natürlichen Personen zugänglich gemacht werden.	Ermittlung der Verarbeitungsvorgänge, welche personenbezogene Daten an eine unbestimmte Zahl von natürlichen Personen zugänglich machen und anschließende Dokumentenprüfung der festgelegten Voreinstellungen.

2.5 Artikel 26:

2.5.1 Einführende Hinweise

Ausgangspunkt der Prüfung einer (gemeinsamen) Verantwortung ist der unter 2.1.1 beschriebene Zertifizierungsgegenstand. Soweit in Bezug auf die dort beschriebene Verarbeitungstätigkeit nach den unten stehenden Kriterien eine gemeinsame Verantwortung anzunehmen ist, ist der Zertifizierungsantrag (ISO 17065, 7.2) von allen gemeinsam Verantwortlichen zu stellen. Alle gemeinsam Verantwortlichen müssen eine rechtlich durchsetzbare Vereinbarung mit der Konformitätsbewertungsstelle haben.

2.5.2 Tabellarische Übersicht: Anforderungen, Formen der Umsetzung und Prüfung

Gesetzliche Tatbestandsmerkmale	*In den Zertifizierungskriterien zu behandelnde Prüfthemen und deren Umsetzung durch die Kunden der Zertifizierungsstelle*	*Wie prüft die Zertifizierungsstelle die Umsetzung?*
Art. 26 Abs. 1 S. 1 Gemeinsame Festlegung der Zwecke und Mittel zur Verarbeitung.	Im Hinblick auf Verantwortlichkeit siehe Anforderung oben in Ziff. 2.1.2 Punkt 6. Kriterien für eine zweistufige Prüfung auf Grundlage der EDSA Leitlinien 07/2020[12]:	Rechtliche Analyse: Ggf. Anwendbarkeit rechtlicher Vorschriften bzgl. Aufgaben der Verantwortlichen.

12 Leitlinien 7/2020 zu den Begriffen „Verantwortlicher“ und „Auftragsverarbeiter, Version 2.0.

	Schritt 1: Eigenschaft der Beteiligten als Verantwortliche im Sinne des Art. 4 Nr. 7 DSGVO in Bezug auf alle oder einzelne Verarbeitungsschritte. Dabei sind in Bezug auf den konkreten Zertifizierungsgegenstand folgende Kriterien zu prüfen:	Dokumentenprüfung: Prozessdokumentation im Hinblick auf die Entscheidungsprozesse hinsichtlich der Zwecke und der (wesentlichen) Mittel.
	a) rechtliche[13] oder faktische (Mit-) Bestimmung des Zwecks, („ob“ der Datenverarbeitung)[14] und	Vertragsprüfung und Prüfung sonstiger Unterlagen der Beteiligten (z. B. Datenschutzerklärung), Prüfung des Verzeichnisses der Verarbeitungstätigkeiten.
	b) rechtliche oder faktische (Mit-) Bestimmung der Mittel, („wie“ der Datenverarbeitung) Abgrenzung zwischen wesentlichen und unwesentlichen Mitteln (vgl. EDSA Leitlinien 07/2020, Rn. 39f.) für den Zertifizierungsgegenstand, insbesondere Entscheidungsbefugnis über „welche Daten“ und „wie	Audit: Insbesondere stichprobenhafte technische Prüfung, inwiefern jedenfalls die wesentlichen Feststellungen der Dokumentenprüfung der tatsächlichen Verarbeitung entsprechen.

13 Dabei kann sich die rechtliche (Mit-)Bestimmung entweder aus einer Zuweisung der Verantwortlichkeit nach Maßgabe des Art. 4 Nr. 7 Hs. 2 DSGVO ergeben oder implizit aus der gesetzlichen Zuweisung einer Aufgabe an einen Verantwortlichen nach Maßgabe der EDSA Leitlinien 07/2020, Rn. 24.

14 Zu berücksichtigen sind dabei auch Nutzungsdaten/Metadaten.

	lange“. **Schritt 2: Gemeinsame Bestimmung der Mittel und Zwecke** in Bezug auf alle oder einzelne Verarbeitungsschritte. (Abgrenzung zur Figur zweier oder mehrerer unabhängiger Verantwortlicher). Gemeinsame Bestimmung liegt dabei auch im Falle sich ergänzender Entscheidungen („converging decisions“) nach Maßgabe der EDSA Leitlinien 07/2020, Rn. 54f. vor. Die gemeinsame Bestimmung bezieht sich auf a) Zwecke und b) (wesentliche) Mittel der Verarbeitung[15].	
Art. 26 Abs. 1 Satz 2 und 3 und Abs. 2 Satz 1 und 2	Dokumentierte Prüfung, ob und inwieweit die jeweiligen Aufgaben der Verantwortlichen in Rechtsvorschriften festgelegt sind.	Prüfung der Dokumentation anhand der einschlägigen Rechtslage und Praxis.

15 Für weitere Informationen siehe EDSA Leitlinien 07/2020 Rn. 53.

		Soweit die jeweiligen Aufgaben der Verantwortlichen nicht in Rechtsvorschriften festgelegt sind, transparente vertragliche Festlegung der Inhalte aus Art. 26 Abs. 1 S. 2. Maßgeblich sind insbesondere folgende Punkte: - Vollständige Abdeckung der Pflichten gem. Art. 26 Abs. 1 Satz 2, - Maßnahmen zur Einhaltung der Datenschutzprinzipien und Gewährung der Betroffenenrechte, Festlegung der hierbei bestehenden Pflichten der beteiligten Seiten, - Klarheit, Verständlichkeit, Transparenz der Vereinbarung und insbesondere der Abgrenzungen. - Wird von der Möglichkeit der Angabe einer Anlaufstelle gem. Art. 26 Abs. 1 S. 3 Gebrauch gemacht, muss eine spezifische Prozessbeschreibung bezüglich der Funktionen der Anlaufstelle vorliegen, Übereinstimmung der Vereinbarung mit den tatsächlichen Funktionen und Beziehungen gegenüber betroffenen Personen (Art. 26 Abs. 2 S. 1).	Prüfung der zwischen den gemeinsamen Verantwortlichen zu treffenden Vereinbarung sowie Prüfung des Verzeichnisses der Verarbeitungstätigkeiten, Prüfung von Prozessbeschreibungen, der Umsetzung und der Wirksamkeit der Prozesse (insbesondere zur Wahrnehmung von Betroffenenrechten) und Audit im Hinblick auf die Prozesse, z.B. durch Simulation von Eingaben Betroffener. Prüfung der Prozessbeschreibungen nach Art. 26 Abs. 1 Satz 2 und ggf. Satz 3 (Anlaufstelle), der Umsetzung und der Wirksamkeit der Prozesse (z. B. durch Simulation interner und externer Vorfälle). Audit: Prüfung der Regelungen zur Vornahme von technischen und organisatorischen Maßnahmen im Hinblick auf die zwischen ihnen bestehenden Abhän-

		gigkeiten, Schnittstellen und von den Beteiligten eingenommenen Rollen einschließlich vereinbarter Pflichten zur (ggf. gegenseitigen) Unterstützung. Prüfung der Regelungen zur stellenübergreifenden Risikoanalyse[16], Schwellwertprüfung nach Art. 35 Abs. 1 und, soweit relevant, Erfüllung der Pflichten nach Art. 35 und 36. Prüfung der Regelungen zur Aufnahme weiterer Vertragspartner und zur Inanspruchnahme von Auftragsverarbeitern, soweit einschlägig.
	Zur Verfügung stellen[17] der wesentlichen Vereinbarungsinhalte[18] gem. Art. 26 Abs. 2 S. 2 an die betroffene Person.	Prüfung der Informationen an die Betroffenen (insb. auf Klarheit, Verständlichkeit, Transparenz der Abgrenzungen, Zugänglichkeit der Information).

16 TOMs implizieren stets eine Risikoanalyse (Art. 24, „Schwere der Risiken"). Diese sollte in Fällen des Art. 26 gemeinsam durchgeführt werden, da bei getrennter Analyse die Gefahr besteht, dass bestimmte Risiken von keinem Beteiligten gesehen werden, bzw. jeder glaubt, der andere sei für die Risiken in dem Bereich zuständig.

17 Vgl. EDSA Leitlinien 07/2020, Rn. 181.

18 Vgl. EDSA Leitlinien 07/2020, Rn. 180.

Art. 26 Abs. 3	Prüfkriterien zu: - Existenz von Rollen und Prozessen bei jedem Verantwortlichen, die die Erfüllung der Betroffenenrechte ermöglichen; - Vereinbarungen und Prozesse für den Fall, dass der jeweilige Verantwortliche nicht in der Lage ist, das Recht allein umzusetzen; - Prozesse für den Fall, dass der jeweils andere Verantwortliche das Recht nicht umsetzt, obwohl er dazu in der Lage gewesen wäre; - Prozesse für den Fall, dass der Betroffene seine Rechte aus Art. 26 Abs. 3 bei mehreren Verantwortlichen wahrnimmt und der Hinweis auf dieses Recht für die Betroffenen.	Vertragsprüfung, Prüfung von Prozessbeschreibungen, Prozessaudit (z. B. durch Simulation von Eingaben Betroffener), Prüfung der Information an die Betroffenen.

2.6 Artikel 28: Auftragsverarbeiter

2.6.1 Einführende Hinweise

Bei den Prüfkriterien zu diesem Punkt sind zwei Perspektiven zu unterscheiden:

1. Es soll der Dienst der Auftragsverarbeitung zertifiziert werden.
2. Es soll der Einsatz eines Auftragsverarbeiters durch die verantwortliche Stelle Teil der Zertifizierung sein.

Art. 28 ist die zentrale Vorschrift für Auftragsverarbeiter in der DSGVO. Der Verantwortliche darf sich gem. Art. 28 Abs. 1 nur solcher Auftragsverarbeiter bedienen, die hinreichende Garantien dafür bieten, dass sie geeignete technische und organisatorische Maßnahmen für einen ausreichenden Datenschutz anwenden. Zum Beleg solcher Garantien können als Faktoren auch genehmigte Verhaltensregeln des Auftragsverarbeiters nach Art. 40 oder Zertifizierungen nach Art. 42 herangezogen werden.

2.6.2 Tabellarische Übersicht: Anforderungen, Formen der Umsetzung und Prüfung

Gesetzliche Tatbestandsmerkmale	*In den Zertifizierungskriterien zu behandelnde Prüfthemen und deren Umsetzung durch die Kunden der Zertifizierungsstelle*	*Wie prüft die Zertifizierungsstelle die Umsetzung?*
Auftragsverarbeitung muss im konkreten Einsatz vorliegen und rechtlich zulässig sein.	Alternative 1 (Zertifizierung eines Auftragsverarbeiters):	Siehe Prüfmethoden zu Art. 26 Abs. 1 S. 1.

	Es ist zu prüfen und zu dokumentieren, ob eine Auftragsverarbeitung oder eine gemeinsame Verantwortung i. S. d. Art. 26 vorliegt. Hierbei sind die zu Art. 26 Abs. 1 S. 1 Schritt 1 aufgestellten Kriterien maßgeblich.	
	Alternative 2 (Einsatz eines Auftragsverarbeiters durch einen zu zertifizierenden Verantwortlichen): Der Verantwortliche muss alle relevanten Informationen seitens des Auftragsverarbeiters zu dessen Dienstleistung haben, um einschätzen zu können, ob die Auftragsverarbeitung in seinem Bereich zulässig ist. Es ist zu prüfen und zu dokumentieren, ob eine Auftragsverarbeitung oder eine gemeinsame Verantwortung i. S. d. Art. 26 vorliegt. Hierbei sind die zu Art. 26 Abs. 1 S. 1 Schritt 1 aufgestellten Kriterien maßgeblich. Je nach Einsatzbereich sind die Besonderheiten der Zulässigkeit bzw. ggf. bestehende Einschränkungen zu	Siehe Prüfmethoden zu Art. 26 Abs. 1 S. 1. Im Übrigen Prüfung des Angebotstextes des Auftragsverarbeiters bzw. der Beschreibung seiner Dienstleistung und der übrigen Unterlagen.

	beachten (z. B. bzgl. Verarbeitung von Personalakten im Auftrag oder auch im Gesundheitsbereich).	
Art. 28 Abs. 1 Hinreichende Garantien für geeignete technische und organisatorische Maßnahmen.	Vorliegen genehmigter Verhaltensregeln (Art. 40) oder Zertifizierung (Art. 42) oder sonstige Garantien (Audits, Zertifizierungen, Dokumentation, Kontrollmöglichkeiten durch Auftraggeber etc.).	In der Regel alle folgenden Prüfmethoden: - Prüfung von Genehmigungen/Zertifizierungen, - Vor-Ort-Prüfung der technischen und organisatorischen Maßnahmen und - Dokumentenprüfung.
Art. 28 Abs. 3 Vorliegen eines Auftragsverarbeitungsvertrags (schriftlich/elektronisches Format).	Ausreichende Regelung zu insbesondere den Mindestinhalten gem. Art. 28 Abs. 3: - Gegenstand und Dauer der Verarbeitung (Art. 28 Abs. 3 S. 1); - Art und Zweck der Verarbeitung (Art. 28 Abs. 3 S. 1); - Art der personenbezogenen Daten (Art. 28 Abs. 3 S. 1); - Kategorien von betroffenen Personen (Art. 28 Abs. 3 S. 1);	- Rechtliche Analyse des Vertrags auf Vollständigkeit und rechtliche Zulässigkeit. - Eingehende rechtliche Prüfung der konkreten vertraglichen Umsetzung und des Vorhandenseins ausreichender technischer und organisatorischer Maßnahmen (vgl. dazu Ausführungen zu Art. 32).

	- Dokumentierte Weisungslage für den Auftragsnehmer (Art. 28 Abs. 3 lit. a); - Gewährleistung der Vertraulichkeit oder Verschwiegenheit (Art. 28 Abs. 3 lit. b); - Ergreifen adäquater technischer und organisatorischer Maßnahmen des Auftragsverarbeiters (Art. 28 Abs. 3 lit. c); - Regelung zur Inanspruchnahme von Subunternehmern (Art. 28 Abs. 3 lit. d); - Unterstützung des Auftragsnehmers bei dessen Pflicht zur Beantwortung von Anträgen auf Wahrnehmung von Betroffenenrechten. Sind hierfür beim Auftragnehmer geeignete technische und organisatorische Maßnahmen zugesichert (Art. 28 Abs. 3 lit. e)? - Vorgaben zur Unterstützung des Verantwortlichen bei der Einhaltung der Vorgaben aus Art. 32 bis 36 (Art. 28 Abs. 3 lit. f); - Vorgaben zur Löschung/Rückgabe nach Abschluss der vereinbarten Leistung (Art. 28 Abs. 3 lit. g);	

	- Zurverfügungstellung aller erforderlichen Informationen durch Auftragnehmer an den Verantwortlichen zum Nachweis der Pflichten (Art. 28 Abs. 3 lit. h, Art. 5 Abs. 2); - Ermöglichung von Überprüfungen (einschließlich Inspektionen) (Art. 28 Abs. 3 lit. h) oder Vorliegen eines Prozesses bei dem Verantwortlichen, mit dem dieser die Einhaltung der Vorgaben beim Auftragnehmer fortlaufend kontrollieren kann; - Vereinbarung einer Informationspflicht des Auftragsverarbeiters, wenn er der Auffassung ist, eine Weisung sei rechtswidrig (Art. 28 Abs. 3 lit. h).	
Art. 28 Abs. 4 Vertrag mit weiterem Auftragsverarbeiter/Unterauftragnehmer (schriftlich/elektronisches Format).	Abfassen eines Vertrags i. S. d. Vorgaben des Art. 28 Abs. 4 i. V. m. Abs. 3. Ausreichende Garantien bzgl. technischer und organisatorischer Maßnahmen.	- Rechtliche Analyse des Vertrags auf Vollständigkeit und Zulässigkeit; - Prüfung der Dokumentation der technischen/organisatorischen Maßnahmen; - vor-Ort-Prüfung der technischen/organisatorischen Maßnahmen.

Art. 28 Abs. 2 Unterauftragnehmer nur mit schriftlicher Genehmigung.	Vorhandensein eines Prozesses der sicherstellt, dass bei der Planung der Beauftragung eines neuen Unterauftragnehmers eine Unterrichtung des Auftraggebers bzw. Einholung der Genehmigung erfolgt. Dokumentation der Genehmigungen.	- Sofern bereits ein (neuer) Unterauftragnehmer beauftragt wurde, Prüfung, ob entsprechende Unterrichtungen/Genehmigungen erfolgt sind; - Dokumentenprüfung; - Audit der Prozesse.
Art. 44 Bestehen geeigneter Garantien bei Datenübermittlung an ein Drittland.	Dokumentation der Garantien (vgl. Art. 5).	- Prüfung der Dokumentation (vgl. Art. 5).
Art. 33 Abs. 2 Sicherstellung einer unverzüglichen Meldung von Datenschutzverstößen, sobald diese dem Auftragsverarbeiter bekannt werden.	Einrichtung entsprechender Prozesse. Dokumentation.	- Audit der Prozesse, - Durchsicht der Dokumentation.

Art. 32 Abs. 4, Art. 29 Sicherstellung, dass Verarbeitung nur gemäß Weisungslage erfolgt.	Vorhandensein entsprechender Prozesse und Dokumentation der Weisungen	- Prüfung der Dokumentation, - Beschreibung der Prozesse.

2.7 Artikel 30: Verzeichnis von Verarbeitungstätigkeiten

2.7.1 Einführende Hinweise

Die Prüfung der Kriterien des Art. 30 orientiert sich maßgeblich am Merkmal der Vollständigkeit des Verzeichnisses der Verarbeitungstätigkeiten. Das Verzeichnis bildet dabei eine Menge von (Teil-) Ergebnissen aus anderen Prozessen ab, die unter separaten Prüfkriterien betrachtet werden. So kann die Festlegung der Verarbeitungszwecke (Art. 30 Abs. 1 lit. b) oder der technisch-organisatorischen Maßnahmen (Art. 30 Abs. 1 lit. g) nicht erst im Rahmen der Führung dieses Verzeichnisses erfolgen, sondern muss für diese bereits zuvor erfolgt sein.

Bei der Prüfung des Verzeichnisses selbst werden daher insbesondere Prozesse innerhalb der Organisation des Verantwortlichen betrachtet, die dazu beitragen, dass das Verzeichnis als „lebendes" Dokument ständig den tatsächlichen Stand der Verarbeitungstätigkeiten wahrheitsgemäß wiedergibt.

Die besondere Situation von kleinen und Kleinstunternehmen wird dadurch berücksichtigt, dass das Erfordernis zur Führung eines Verzeichnisses der Verarbeitungstätigkeiten ggf. entfallen kann und daher vorab geprüft wird (vgl. Erwägungsgrund 13).

2.7.2 Tabellarische Übersicht: Anforderungen, Formen der Umsetzung und Prüfung

Gesetzliche Tatbestandsmerkmale	*In den Zertifizierungskriterien zu behandelnde Prüfthemen und deren Umsetzung durch die Kunden der Zertifizierungsstelle*	*Wie prüft die Zertifizierungsstelle die Umsetzung?*

Art 30 Abs. 5 Verzeichnis von Verarbeitungstätigkeiten ist erforderlich.	Prüfung der Voraussetzungen: - Anzahl der Mitarbeitenden und ggf. entweder - Risiko für Freiheiten und Rechte natürlicher Personen vorhanden, - nicht nur gelegentliche Verarbeitung, oder - Verarbeitung besonderer Kategorien gem. Art. 9 Abs. 1 oder Art. 10.	Befragung oder Dokumenten-prüfung zur Feststellung der Anzahl der Mitarbeitenden. Rechtliche und technisch-organisatorische Dokumentenprüfung einer vom Verantwortlichen durchzuführenden Bewertung - des Risikos, - der Häufigkeit und - der betroffenen Kategorien personenbezogener Daten der Verarbeitungstätigkeiten.
Art. 30 Abs. 1 Verzeichnis ist vollständig.	Das Verzeichnis der Verarbeitungstätigkeiten enthält alle Angaben aus Art. 30 Abs. 1 lit. a-g. Prozesse zur Aktualisierung des Verzeichnisses sind etabliert für den Fall, dass - Verarbeitungstätigkeiten eingeführt werden, - Verarbeitungstätigkeiten wegfallen, - sich bei bereits aufgeführten	Dokumentenprüfung des Verzeichnisses der Verarbeitungstätigkeiten. Prüfung schriftlich fixierter Prozessbeschreibungen; Audit der Prozesse.

	Verarbeitungstätigkeiten Angaben entsprechend Art. 30 Abs. 1 lit. a-g ändern. Es existieren Prozesse zur dahingehenden Zusammenarbeit zwischen - an den Verarbeitungstätigkeiten beteiligten Fachabteilungen, - dem Vertreter des Verantwortlichen sowie - ggf. dem Datenschutzbeauftragten. Entsprechende Zuständigkeiten innerhalb der Organisation sind geklärt.	Dokumentenprüfung von - schriftlich fixierten Prozessbeschreibungen, - Organisationsplänen, - Geschäfts-/Aufgabenverteilungsplänen; - ggf. Befragung des Verantwortlichen.
Art. 30 Abs. 2 Verzeichnis enthält Angaben für Auftragsverarbeiter.	Das Verzeichnis der Verarbeitungstätigkeiten enthält alle Angaben aus Art. 30 Abs. 2 lit. a-d. Prozesse zur Aktualisierung des Verzeichnisses sind etabliert für den Fall, dass	Dokumentenprüfung des Verzeichnisses der Verarbeitungstätigkeiten. Prüfung schriftlich fixierter Prozessbeschreibungen; Audit der Prozesse.

	- Kategorien von im Auftrag durchgeführten Verarbeitungstätigkeiten eingeführt werden; - Kategorien von im Auftrag durchgeführten Verarbeitungstätigkeiten wegfallen; - sich bei bereits aufgeführten Kategorien von Verarbeitungstätigkeiten Angaben entsprechend Art. 30 Abs. 2 lit. a–d ändern; - zusätzliche Verantwortliche, in deren Auftrag eine Verarbeitung durchgeführt wird, hinzukommen; - Verantwortliche, in deren Auftrag eine Verarbeitung durchgeführt wird, wegfallen; - sich bei bestehenden Verantwortlichen, in deren Auftrag eine Verarbeitung durchgeführt wird, Angaben nach Art. 30 Abs. 2 lit. a–d ändern.	
	Es existieren Prozesse zur dahingehenden Zusammenarbeit zwischen - an den Verarbeitungstätigkeiten beteiligten Fachabteilungen;	Dokumentenprüfung von - schriftlich fixierten Prozessbeschreibungen; - Organisationsplänen; - Geschäfts-/Aufgabenverteilungsplänen;

	- dem Vertreter des Verantwortlichen, der als Auftragsverarbeiter auftritt; - ggf. dem Datenschutzbeauftragten des Verantwortlichen, der als Auftragsverarbeiter auftritt; - den Verantwortlichen, in deren Auftrag eine Verarbeitung durchgeführt wird. Entsprechende Zuständigkeiten innerhalb der Organisation sind geklärt.	- ggf. Befragung des Verantwortlichen.
Art. 30 Abs. 3 Verzeichnis wird schriftlich geführt.	Die schriftliche Führung des Verzeichnisses ist gegeben. Entsprechende Aufbewahrungs-/Speicherorte sind den beteiligten Personen bekannt.	Dokumentenprüfung.
Art. 30 Abs. 4 Verzeichnis wird auf Anfrage der Aufsichtsbehörde zur Verfügung gestellt.	Prozesse sind etabliert, um - die Entgegennahme; - die Bearbeitung;	Dokumentenprüfung von - schriftlich fixierten Prozessbeschreibungen; Audit der Prozesse;

	- die Beantwortung unter Zurverfügungstellung des Verzeichnisses der Verarbeitungstätigkeiten einer diesbezüglichen Anfrage einer Aufsichtsbehörde zeitnah sicherzustellen. Die Verteilung der entsprechenden Zuständigkeiten innerhalb der Organisation ist geklärt.	- Organisationsplänen; - Geschäfts-/Aufgabenverteilungsplänen; - ggf. Befragung des Verantwortlichen.

2.8 Artikel 32: Sicherheit der Verarbeitung

2.8.1 Einführende Hinweise

Art. 32 fordert die Umsetzung von angemessenen technischen und organisatorischen Maßnahmen zum Schutz personenbezogener Daten. Zwecks Überprüfung dieser Maßnahmen ist es zum einen erforderlich, dass alle relevanten Maßnahmen und Prozesse dokumentiert sind und die Dokumentation zur Prüfung vorliegt. Zum anderen muss sichergestellt sein, dass alle relevanten Maßnahmen und Prozesse für angemessene Prüfungen technisch oder physisch zugänglich sind, sodass deren Funktionsweise bewertet werden kann. Bei der Definition der technisch-organisatorischen Maßnahmen ist die Ermittlung des Schutzniveaus maßgeblich. Letzteres muss ebenfalls dokumentiert sowie kontinuierlich überprüft werden.

Bestimmte Anforderungen, die sich aus Art. 32 ergeben, können bereits vollständig oder in Teilen durch das Vorhandensein von geeigneten (IT-Sicherheits-) Zertifizierungen (wie z. B. ISMS nach ISO 27001, BSI Grundschutz), die auch den datenschutzrechtlichen Zertifizierungsgegenstand umfassen, abgedeckt sein, vgl. Ergänzungspapier der DSK.[19] Die Erfüllung der entsprechenden datenschutzrechtlichen Anforderungen durch eine oder mehrere (IT-Sicherheits-) Zertifizierung(en) muss auf Vollständigkeit und Korrektheit geprüft und dokumentiert werden. Eine datenschutzrechtliche Anforderung ist vollständig und korrekt erfüllt, wenn sie eindeutig einer oder mehreren Anforderungen einer (IT-Sicherheits-) Zertifizierung zugeordnet werden kann und die Prüfmethoden, die von einer (IT-Sicherheits-) Zertifizierung zur Erfüllung vorgesehen sind, auch den datenschutzrechtlichen Prüfmethoden entsprechen.

2.8.2 Tabellarische Übersicht: Anforderungen, Formen der Umsetzung und der Prüfung

Gesetzliche Tatbestandsmerkmale	*In den Zertifizierungskriterien zu behandelnde Prüfthemen und deren Umsetzung durch die Kunden der Zertifizierungsstelle*	*Wie prüft die Zertifizierungsstelle die Umsetzung?*
Art. 32 Abs. 1 und Abs. 2 Festlegung des Schutzniveaus	a) Vollständige, detaillierte Beschreibung aller verarbeiteten Daten bzw. Datenkategorien.	Dokumentenprüfung, Befragung der Verantwortlichen.

19 Anerkannt werden solche Zertifizierungen aber nur von akkreditierten Zertifizierungsstellen und nach den in Ziffer 7.4 im Ergänzungspapier der DSK aufgeführten Bedingungen („Anforderungen an eine Akkreditierung gem. Art. 43 i. V. m. DIN EN ISO/IEC 17065“ unter https://www.datenschutzkonferenz-online.de/media/ah/20201008_din17065_Ergaenzungen_deutsch_nach_opinion.pdf).

für alle erforderlichen Verarbeitungstätigkeiten.	b) Risikobasierte Ermittlung des angemessenen Schutzniveaus (insb. unter Berücksichtigung der Erwägungsgründe 38 und 75).	Prüfung der Konformität der verwendeten Risikomethode mit der DSGVO. Dokumentenprüfung: Korrektheitsprüfung der Risikoermittlung (z. B. nach SDM D3). Dokumentenprüfung, rechtliche Analyse: Abgleich des resultierenden Schutzniveaus mit den Schutzanforderungen der zu verarbeitenden Datenkategorien.
	c) Berücksichtigung von Risiken, die sich insbesondere durch Vernichtung, Verlust, Veränderung, unbefugte Offenlegung von bzw. unbefugten Zugang	wie b) mit der Schwerpunktsetzung auf Vernichtung, Verlust, Veränderung, Offenlegung und unbefugten Zugang von Daten.

	zu personenbezogenen Daten (Art. 32 Abs. 2) ergeben können.	
Art. 32 Abs. 1 lit. a und b Maßnahmen zum Schutz personenbezogener Daten.	a) Maßnahmen zur Gewährleistung der Vertraulichkeit von personenbezogenen Daten (insb. Pseudonymisierung und Verschlüsselung).	Dokumentenprüfung: Prüfung der Spezifikation und der Schutzkonzepte insb. hinsichtlich des Stands der Technik und der Konsistenz der einzelnen Maßnahmen. Dokumentenprüfung: Vergleich des Schutzniveaus, welches durch die Schutzmaßnahmen sichergestellt werden sollte mit den datenschutzrechtlichen Schutzanforderungen gem. Art. 32. Vor-Ort-Begehungen, Validierungsaudits, Befragungen: Angemessene Verifikation der Maßnahmenumsetzung. (Eine Verifikation ist angemessen, wenn man davon ausgehen kann, dass alle Maßnahmen nach Konzept/Spezifikation umgesetzt worden sind. Das kann u. a. Technik- und Prozessaudits, wie z. B. Penetrati-

		ons- und Stresstests sowie Auditierungen nach gängigen technischen Normen, wie z. B. BSI Grundschutz oder ISO 27001, enthalten.)
	b) Maßnahmen zur Gewährleistung weiterer Ziele nach DSGVO und/oder SDM C1 für die personenbezogenen Daten (in Abhängigkeit zur risikobasierten Ermittlung des Schutzniveaus).	Siehe a).
	c) eine Dokumentation des Prozesses zur Auswahl und Umsetzung geeigneter technischer und organisatorischer Maßnahmen, die Vertraulichkeit, Integrität und Verfügbarkeit der Verarbeitung gewährleisten (Gewährleistungsziele Verfügbarkeit, Integrität und Vertraulichkeit berücksichtigen, siehe auch zu Art. 5).	Dokumentenprüfung, methodische Analyse: Das Zertifizierungsprogramm muss mindestens vorgeben, dass der Zertifizierungsdienstleister die technischen und organisatorischen Maßnahmen dahingehend prüft, dass die Anforderungen zur Gewährleistung der Verfügbarkeit, Integrität und Vertraulichkeit eingehalten werden.
Art. 32 Abs. 1 lit. b Maßnahmen zum Schutz der Systeme und Dienste auf Dauer.	a) Maßnahmen zur Gewährleistung weiterer Ziele nach DSGVO und/oder SDM C1 (insbesondere Vertraulichkeit, Integrität, Verfügbarkeit, Belastbarkeit) zum Schutz der Systeme und Dienste.	Dokumentenprüfung: Prüfung der Spezifikation und der Schutzkonzepte insb. hinsichtlich des Stands der Technik und der Konsistenz der einzelnen Maßnahmen (insb. Berechtigungskonzept, Identitätsmanagement, Authentifizie-

		rung und Autorisierung, Revisions- und Protokollierungskonzept). Das Schutzniveau der Maßnahmen muss den Schutzanforderungen an das Gesamtsystem entsprechen (z. B. gem. IT-Sicherheitskonzept). Prüfung erfolgt durch einen Vergleich. Vor-Ort-Begehungen, Validierungsaudits, Befragungen: Angemessene Verifikation der Maßnahmenumsetzung (siehe oben).
	b) Gewährleistung der Maßnahmen (von Punkt a) auf Dauer.	Dokumentenprüfung, Befragungen: Prüfung des Betriebs-Kontinuitätskonzepts, z. B. nach BSI 200-4 oder ITIL (insbesondere Prüfung der Vollständigkeit der Abdeckung relevanter Systeme und Prüfung der Einhaltung des PDCA-Prinzips/Deming-kreis). Vor-Ort-Begehungen, Validierungsaudits, unangekündigte Begehungen, Befragungen: Verifikation der Umsetzung der entsprechenden Managementprozesse (z. B. durch Simulation interner und

		externer Vorfälle, wie beabsichtigte Angriffe und unbeabsichtigte Ereignisse und/oder durch Lasttests).
Art. 32 Abs. 1 lit. c Maßnahmen zur Sicherstellung der Verfügbarkeit von personenbezogenen Daten im Regelbetrieb sowie bei Zwischenfällen.	a) Maßnahmen zur Sicherstellung der Verfügbarkeit personenbezogener Daten im Regelbetrieb.	Dokumentenprüfung: Prüfung der Spezifikation und der relevanten Konzepte (z. B. Überprüfung von Verfügbarkeitsklassen, Service Level Agreements) insb. hinsichtlich des Stands der Technik. Das durch die Maßnahmen garantierte Verfügbarkeitsniveau muss den Verfügbarkeitsanforderungen an die verarbeiteten personenbezogenen Daten entsprechen (entsprechend der risikobasierten Festlegung nach Art. 32 Abs. 1). Prüfung erfolgt durch einen Vergleich. Vor-Ort-Begehungen, Validierungsaudits, Befragungen: Angemessene Verifikation der Maßnahmenumsetzung (z. B. nach ITIL Availability Management, KRITIS).

	b) Gewährleistung der Verfügbarkeit bei physischen oder technischen Zwischenfällen.	Dokumentenprüfung: Prüfung der Verfügbarkeits- und Wiederherstellungskonzepte (z. B. nach ISO 2700x). Vor-Ort-Begehungen, Validierungsaudits, unangekündigte Begehungen, Befragungen: Verifikation der in oben genannten Konzepten enthaltenen Maßnahmen und Prozesse (z. B. durch Simulation interner und externer Vorfälle, wie beabsichtigte Angriffe und unbeabsichtigte Ereignisse und/oder durch Lasttests) in Hinblick auf personenbezogene Daten.
Art. 32 Abs. 1 lit. d Maßnahmen zur Gewährleistung von regelmäßiger Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen.	a) Gewährleistung, dass alle relevanten Systeme und Prozesse einer regelmäßigen Überprüfung, Bewertung und Evaluierung hinsichtlich der Wirksamkeit der TO-Maßnahmen unterliegen.	Validierungsaudits: Prüfung entsprechend der Managementsysteme (z. B. nach ISMS, ITIL Service Continuity Management) und der Überwachungssysteme und -prozesse (z. B. Incident-Response, CERT, IDS/IPS).
	b) Gewährleistung, dass die unter a) etablierten Maßnahmen bei allen Systemen und Prozessen korrekt	Siehe a).

	(wirksam) umgesetzt sind.	
Art. 32 Abs. 4 Maßnahmen zur Sicherstellung, dass den Verantwortlichen bzw. den Auftragsverarbeitern unterstellte natürliche Personen diese personenbezogenen Daten grundsätzlich nur auf entsprechende Weisung verarbeiten.	Gewährleistung, dass Vereinbarungen zur Verarbeitung personenbezogener Daten existieren und korrekt sind.	Dokumentenprüfung, rechtliche Analyse: Überprüfung der Rechtmäßigkeit und Korrektheit von internen Richtlinien und Vereinbarungen Dokumentenprüfung, Befragungen: Prüfung, ob die oben genannten Richtlinien und Vereinbarungen der organisatorischen Struktur der Verantwortlichen entsprechen.

2.9 Artikel 33 und 34: Meldung von Verletzungen des Schutzes personenbezogener Daten an die Aufsichtsbehörde und Benachrichtigung der von einer Verletzung betroffenen Person

2.9.1 Einführende Hinweise

Art. 33 und Art. 34 regeln die Meldung an die Aufsichtsbehörde und die Benachrichtigung an die betroffene Person bei Vorliegen einer Verletzung des Schutzes personenbezogener Daten.

Konkret werden hier Inhalt und Frist der Meldung/Benachrichtigung, Dokumentations- und Handlungspflichten sowie mögliche Ausnahmen von der Melde-/Benachrichtigungspflicht geregelt.

2.9.2 Tabellarische Übersicht: Anforderungen, Formen der Umsetzung und Prüfung

Gesetzliche Tatbestandsmerkmale	*In den Zertifizierungskriterien zu behandelnde Prüfthemen und deren Umsetzung durch die Kunden der Zertifizierungsstelle*	*Wie prüft die Zertifizierungsstelle die Umsetzung?*
Art. 33 Meldepflicht an Aufsichtsbehörde.	Es muss ein Prozess zur Operationalisierung festgelegt sein, wie bei Datenschutzverletzungen zu verfahren ist, um den Anforderungen der Meldepflicht nachzukommen. Dies umfasst u. a. die Festlegung von Verfahrensschritten und Verantwortlichkeiten, was die Sensibilisierung aller Beteiligten zur Feststellung von Datenschutzverletzungen im Allgemeinen mit umfasst.	Überprüfung, ob und inwieweit Verfahrensabläufe/Prozesse vorliegen, die im Falle eines Datenschutzvorfalles abzuarbeiten sind und die alle Beteiligten zur Feststellung von Datenschutzverletzungen sensibilisieren. Die o. g. Überprüfungen können u. a. durch - Dokumentenprüfung; - Vor-Ort-Kontrolle; - Mitarbeiterbefragung erfolgen.
Art. 33 Abs. 1, Satz 1 Verletzung des Schutzes	Identifikation, Analyse und Bewertung der Schutzverletzung (siehe Definition gem. Art. 4 Nr. 12).	s.o.

personenbezogener Daten.		
Art. 33 Abs. 1, Satz 1 Ausnahme von der Meldepflicht, wenn voraussichtlich kein Risiko für die Rechte und Freiheiten natürlicher Personen.	Identifikation, Analyse und Bewertung des Risikos (siehe auch „datenschutzrechtliche Risikobetrachtung“).	s.o.
Art. 33 Abs. 1 Satz 1 Frist („unverzüglich und möglichst binnen 72 Stunden“), Art. 33 Abs. 1, Satz 2 Begründungspflicht bei Fristverletzung.	Maßnahmen zur Fristwahrung, zur Feststellung von Fristverletzungen und ggf. zur Begründung.	s.o.
Art. 33 Abs. 2 Meldepflicht des Auftragsverarbeiters an den Verantwortlichen.	Maßnahmen zur Sicherstellung, dass der Auftragsverarbeiter die Schutzverletzung an den Verantwortlichen meldet (ggf. Regelung im Auftragsverarbeitungsvertrag).	s.o., insb. Prüfung des Auftragsverarbeitungsvertrages

Art. 33 Abs. 3 Inhalt der Meldung.	Maßnahmen zur Sicherstellung einer inhaltlich vollständigen Meldung; ggf. Verwendung aufsichtsbehördlicher Meldeformulare.	s.o.
Art. 33 Abs. 3, lit. d Maßnahmen zur Behebung der Verletzung und gegebenenfalls Maßnahmen zur Abmilderung ihrer möglichen nachteiligen Auswirkungen.	Auswahl und Umsetzung der ergriffenen technisch-organisatorischen Maßnahmen. Bzgl. der Maßnahmen ist auf Identifikation, Analyse und Bewertung der Schutzverletzung und des Risikos abzustellen (s.o.).	s.o.
Ausnahme hinsichtlich des Inhalts der Meldung: Art. 33 Abs. 4 Schrittweise Zurverfügungstellung der Informationen.	Informationen werden nach Art. 33 Abs. 4 schrittweise zur Verfügung gestellt. Die Meldefrist nach Art. 33 Abs. 1, Satz 1 muss grundsätzlich auch dann gewahrt werden, wenn die erforderlichen Mindestinformationen nach Abs. 3 nicht fristwahrend zur gleichen Zeit vorliegen. Für diesen Fall „kann“ der erforderliche Inhalt/Umfang der Meldung schrittweise zur Verfügung gestellt werden, was zu einem faktischen „muss“ der schrittweisen Zurverfügungstellung der Informationen zu Gunsten	s.o.

	der Fristwahrung führt (Erst- und Nachmeldung). Maßnahmen zur Fristwahrung und zur (schrittweisen) Nachreichung der erforderlichen Informationen sind zu ergreifen.	
Art. 33 Abs. 5, Satz 1 Dokumentationspflicht.	Dokumentation der Verletzung des Schutzes personenbezogener Daten einschließlich aller im Zusammenhang mit der Verletzung stehenden Fakten, von deren Auswirkungen und der ergriffenen Abhilfemaßnahmen. Die Dokumentation muss der Aufsichtsbehörde ermöglichen, die Einhaltung der Bestimmungen des Art. 33 zu überprüfen.	s.o.
Art. 34 Benachrichtigungspflicht an betroffene Person.	Es muss ein Prozedere festgelegt sein, wie bei Datenschutzverletzungsvorfällen zu verfahren ist, um den Anforderungen der Benachrichtigungspflicht an betroffene Personen nachzukommen. Dies umfasst u. a. die Festlegung von Verfahrensschritten und Verantwortlichkeiten.	Die Verfahrensabläufe/Prozesse müssen vgl. Art. 33 überprüft werden können.

Art. 34 Abs. 1 Verletzung des Schutzes personenbezogener Daten mit voraussichtlich hohem Risiko.	s.o. zu Art. 33	
Art. 34 Abs. 1 Frist.	s.o. zu Art. 33	
Art. 34 Abs. 2 Inhalt der Benachrichtigung.	s.o. zu Art. 33	
Art. 34 Abs. 3 Ausnahme von der Benachrich-tigungspflicht.	Prüfung, ob Ausnahmetatbestände vorliegen.	
Art. 34 Dokumentation der Einhaltung der Anforderungen.	Die Dokumentation muss der Aufsichtsbehörde ermöglichen, die Einhaltung der Bestimmungen des Art. 34 zu überprüfen.	

2.10 Artikel 35: Datenschutz-Folgenabschätzung

Gesetzliche	*In den Zertifizierungskriterien zu behandelnde*	*Wie prüft die Zertifizierungsstelle die Umsetzung?*

Tatbestandsmerkmale	*Prüfthemen und deren Umsetzung durch die Kunden der Zertifizierungsstelle*	
Art. 35 Erforderlichkeitsprüfung	Verpflichtung zur Datenschutz-Folgenabschätzung (DSFA) bei einem potentiell hohen Risiko unter Einsatz des Zertifizierungsgegenstands im Anwendungskontext (die Ermittlung der Erforderlichkeit wird in aller Regel über die **Beschreibung der geplanten Verarbeitungsvorgänge** und der jeweiligen Verarbeitungszwecke erfolgen. Maßgeblich ist daher die Erstellung eines Verzeichnisses von Verarbeitungstätigkeiten gem. Art. 30). Hierzu ist zu prüfen, ob mindestens ein durch den Zertifizierungsgegenstand abgedeckter Verarbeitungsvorgang in einer der folgenden Listen genannt ist: - spezielle Anforderungen aus Art. 35 Abs. 3; - der Liste gem. Art. 35 Abs. 4 (Whitelist);	Dokumentenprüfung und ggf. Befragung: Verantwortlicher und Auftragsverarbeiter haben die DSFA-spezifischen Prüfergebnisse unter Einsatz des Zertifizierungsgegenstands im Anwendungskontext zu dokumentieren und zu erläutern; (optional) Muster einer DSFA für den Einsatz des Zertifizierungsgegenstands unter Berücksichtigung eines oder mehrerer Anwendungskontexte, das durch den Verantwortlichen oder Auftragsverarbeiter, für die eigene Anwendung des Zertifizierungsgegenstands zu konkretisieren ist.

	- der Liste gem. Art. 35 Abs. 5 (Blacklist). Ebenso ist zu prüfen, ob für den Zertifizierungsgegenstand eine DSFA aus anderen Gründen durchzuführen ist, z. B. weil - die Verarbeitung personenbezogener Daten Anforderungen des EDSA in der jeweils aktuellen Fassung (z. B. aus WP248) erfüllt; - eine DSFA aufgrund eines Bundes- oder Landesgesetzes oder Spezialgesetzes gefordert wird.	
Art. 35 Mindestanforderungen	Die formellen Anforderungen an die Durchführung einer DSFA ergeben sich aus der DSGVO, speziell aus Art. 35 sowie den Erwägungsgründen 84, 90, 91, 92 und 93. Die verwendete Methode steht dem Verantwortlichen grundsätzlich frei. Die DSGVO enthält keine expliziten Formvorschriften zur Durchführung der DSFA. In Art. 35 Abs. 7 werden	Dokumentenprüfung und ggf. Befragung: Verantwortlicher und Auftragsverarbeiter haben die skizzierten Anforderungen unter Einsatz des Zertifizierungsgegenstands im Anwendungskontext zu dokumentieren und zu erläutern; (optional) Muster einer DSFA für den Einsatz des Zerti-

	aber Elemente aufgezählt, die die Folgenabschätzung zumindest enthalten muss: - Eine systematische Beschreibung der geplanten Verarbeitungsvorgänge und der Zwecke der Verarbeitung, gegebenenfalls einschließlich der von dem Verantwortlichen verfolgten berechtigten Interessen; - eine Bewertung der Notwendigkeit und Verhältnismäßigkeit der Verarbeitungsvorgänge in Bezug auf den Zweck; - eine Bewertung der Risiken für die Rechte und Freiheiten der betroffenen Personen gem. Absatz 1 und die zur Bewältigung der Risiken geplanten Abhilfemaßnahmen, einschließlich Garantien, Sicherheitsvorkehrungen und Verfahren, durch die der Schutz personenbezogener Daten sichergestellt und der	fizierungsgegenstands unter Berücksichtigung eines oder mehrerer Anwendungskontexte, das durch den Verantwortlichen oder Auftragsverarbeiter, für die die eigene Anwendung des Zertifizierungsgegenstands zu konkretisieren ist. Hinweis bei hohen Restrisiken: Ergibt eine DSFA, dass trotz technischer und organisatorischer Maßnahmen zur Risikoeindämmung weiterhin ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen besteht (Restrisiko), muss nach Art. 36 der Verantwortliche die zuständige Aufsichtsbehörde konsultieren.

	Nachweis dafür erbracht wird, dass diese Verordnung [auch perspektivisch[20]] eingehalten wird, wobei den Rechten und berechtigten Interessen der betroffenen Personen und sonstiger Betroffener Rechnung getragen wird.	

2.11 Artikel 44ff.: Übermittlung personenbezogener Daten an Drittländer

2.11.1 Einführende Hinweise

Impliziert der Zertifizierungsgegenstand eine Übermittlung personenbezogener Daten an Drittländer oder an internationale Organisationen (nachstehend „Drittlandübermittlung“), sind die gesetzlichen Anforderungen an die Rechtmäßigkeit einer solchen Drittlandübermittlung aus den Art. 44 bis 49 zu beachten. Das bedeutet, dass ein Zertifizierungsprogramm darauf ausgerichtet sein muss, zu prüfen, ob eine Drittlandübermittlung Teil des Zertifizierungsgegenstands ist und ob sie rechtlich zulässig ist.[21]

Daraus ergeben sich folgende zwingende Inhalte eines Zertifizierungsprogramms, die als Zertifizierungskriterien zu behandeln sind:

20 Eine DSFA ist kein einmaliger Vorgang und ist – orientiert an einer veränderten Risikolage oder bei wesentlichen Änderungen im Verfahren erneut durchzuführen. Insoweit wird ein iterativer Prozess der Überprüfung und Anpassung empfohlen.

21 Für die Zertifizierung als Transfertool i.S.v. Art 46 Abs. 2 lit. f, siehe Guideline on certification as tools for transfers (Nr. nachtragen nach EDSA-Plenum)

1. Ausschluss einer Drittlandübermittlung?

   Die Zertifizierungsstelle muss zunächst überprüfen, ob im Rahmen des Zertifizierungsgegenstands eine Drittlandübermittlung ausgeschlossen werden kann. Dabei muss die Zertifizierungsstelle beachten, dass es in der Praxis bei der Übermittlung von Daten im Rahmen von Wartung, Pflege und Support häufig zu Drittlandübermittlungen kommt. Oft wird die Relevanz einer solchen Übermittlung übersehen, insbesondere dann, wenn Wartungs-, Pflege- und Supportleistungen nicht den Schwerpunkt des Zertifizierungsgegenstands darstellen oder die Übermittlung zwar im Standardfall nicht vorgesehen ist, aber in Ausnahmefällen erforderlich sein kann. Daher müssen Zertifizierungsstellen und Programmeigner bei der Abfrage, inwiefern eine Drittlandübermittlung ausgeschlossen werden kann, auch solche Leistungen, sowie die Tätigkeiten von Unterauftragsverarbeitern im Blick haben und dies im Rahmen des Zertifizierungsprogramms gezielt überprüfen.

2. Zwei-Stufen-Prüfung

   Soweit eine Drittlandübermittlung im Rahmen des Zertifizierungsgegenstands nicht ausgeschlossen werden kann, müssen die Kunden der Zertifizierungsstelle prüfen und dokumentieren (und entsprechend muss die Zertifizierungsstelle überprüfen), auf welcher rechtlichen Grundlage die Drittlandübermittlung erfolgt. Dabei ist im Rahmen der sog. Zwei-Stufen-Prüfung festzustellen und zu dokumentieren, (1) ob unabhängig von spezifischen Anforderungen an die Drittlandübermittlung nach Kapitel 5 DSGVO die übrigen Bestimmungen der DSGVO in Bezug auf die in Rede stehende Verarbeitung eingehalten werden und (2) inwiefern die spezifischen Anforderungen der Art. 44 bis 49 befolgt werden.

Erwartet wird dabei im Hinblick auf die zweite Stufe insbesondere die Darstellung, Prüfung und Dokumentation, auf welcher Übermittlungsgrundlage die Drittlandübermittlung, erfolgt. Außerdem ist die Bildung von konkreten Anwendungsfällen[22] als zusätzliche Anwendungshilfe erforderlich. Die Anwendungsfälle sollten in eine Methodik eingebunden sein, die eine nachvollziehbare, belastbare und reproduzierbare Bewertung des zu zertifizierenden Sachverhalts sicherstellt.

In Betracht kommen folgende Grundlagen einer Drittlandübermittlung:

1. Ein Angemessenheitsbeschluss der Kommission im Sinne des Art. 45 Abs. 1, 3;
2. geeignete Garantien im Sinne des Art. 46 Abs. 1 (ggf. i. V. m. 47)[23];

jeweils unter Beachtung insbesondere der Veröffentlichungen der Datenschutzaufsichtsbehörden auf nationaler und europäischer Ebene, der Entwicklungen in Bezug auf die Feststellung des angemessenen Schutzniveaus und der Rechtsprechung (wie z. B. des „Schrems II"-Urteils des EuGH[24]). Art. 49 kommt in der Regel nicht als Rechtsgrundlage für eine wiederkehrende Datenübermittlung in ein Drittland in Frage.[25]

---

22 Hierfür sind die Empfehlungen des EDSA im Papier Empfehlungen 01/2020 zu Maßnahmen zur Ergänzung von Übermittlungstools zur Gewährleistung des unionsrechtlichen Schutzniveaus für personenbezogene Daten heranzuziehen und die darin beschriebenen Fälle ggf. weiter zu konkretisieren.

23 Darunter fallen u. a. verbindliche interne Datenschutzvorschriften gem. Art. 47 DS-GVO, von der Kommission erlassene Standardvertragsklauseln, von einer Aufsichtsbehörde angenommene Standarddatenschutzklauseln, genehmigte Verhaltensregeln nach Art. 40 DS-GVO.

24 Urteil des Europäischen Gerichtshofs vom 16. Juli 2020 (Rechtssache C311/18).

25 Leitlinien 2/2018 zu den Ausnahmen nach Art. 49 der Verordnung 2016/679, angenommen am 25. Mai 2018, S. 4.

2.11.2 Prüfschritte

Möglich sind zwei Konstellationen:

1. Der Verantwortliche ist Datenexporteur: Der Verantwortliche hat die Voraussetzungen von Kapitel 5 des DSGVO zu erfüllen
2. Der Auftragsverarbeiter ist Datenexporteur und hat die Voraussetzungen von Kapitel 5 DSGVO zu erfüllen. Der Verantwortliche muss aber zumindest inzident die Voraussetzungen von Kapitel 5 DSGVO prüfen (Art. 28 Abs. 1 und 3 lit. a).

Prüfschritte	*In den Zertifizierungskriterien zu behandelnde Prüfthemen und deren Umsetzung durch die Kunden der Zertifizierungsstelle*	*Wie prüft die Zertifizierungsstelle die Umsetzung?*
Geplante Datenübermittlungen kennen	Darstellung und Dokumentation aller jener Verarbeitungstätigkeiten, in deren Kontext die Übermittlung personenbezogener Daten in ein Drittland erfolgt. Die Darstellung muss erkennen lassen, welche Datenarten betroffen sind, welche Drittländer beteiligt sind (auch im Transit) und welche Technologien genutzt werden.	Prüfung der grafischen Darstellung, Dokumentenprüfung, insbesondere der Dokumente im Zusammenhang mit den Informationspflichten gem. Art. 13, 14 (beim Verantwortlichen); Prüfung des Verzeichnisses der Verarbeitungstätigkeiten gem. Art. 30; Prüfung der verwendeten bzw. geplanten Dienstleistungen und deren tatsächliche Datenflüsse[26].

26 Etwa Drittanbieter auf der Webseite, Hosting Provider, Content Delivery Networks, Internet-Sicherheitsdienste, Geolocation, Customer Relations Management-Systeme etc.

Prüfung eines angemessenen Übermittlungsinstruments (entspricht Art. 44)	Darstellung der ausgewählten Übermittlungsinstrumente aus den Art. 45, 46 und Darstellung der dieser Auswahl zugrundeliegenden Prüfung a) Vorhandensein eines Angemessenheitsbeschlusses der Europäischen Kommission für das Zielland Liegt ein Angemessenheitsbeschluss vor, ist dessen Fortbestehen regelmäßig zu überprüfen und ein Notfallplan zu entwerfen, falls dieser aufgehoben wird. Ohne Angemessenheitsbeschluss sind b) und die weiteren Punkte der Tabelle zu prüfen. b) Übermittlung aufgrund eines Übermittlungsinstruments nach Art. 46 Abs. 2 lit. a bis f oder Abs. 3 lit. a oder b, jeweils i. V. m. Art. 46 Abs. 1 (durchsetzbare Rechte und wirksame	Dokumentenprüfung (inkl. Prüfung von Prozessbeschreibungen).

	Rechtsbehelfe).	
Weitere Prüfung, falls kein Angemessenheitsbeschluss vorliegt Beurteilung der Rechtslage und Praxis im Zielland.	Abgleich des Schutzniveaus für personenbezogene Daten im Drittland[27] mit dem Schutzniveau im Geltungsbereich der DSGVO; Identifizierung der Tatsachen, die dazu führen, dass das Schutzniveau im Zielland als im Vergleich zur EU bzw. dem EWR niedriger anzusehen ist, sodass die Übermittlung ggf. nur mithilfe ergänzender Maßnahmen zulässig ist. Es muss nachgewiesen werden, dass das Schutzniveau in Bezug auf den konkreten Zertifizierungsgegenstand bei Anwendung des gewählten Übermittlungsinstruments angemessen ist[28]. Die Analyse der Rechtslage und Praxis im Zielland muss den Vorgaben der Empfehlungen 01/2020 entsprechen und das Schutzniveau muss den Anforderungen der	Prüfung von Prozessbeschreibungen; Rechtliche Prüfung der Dokumentation und der Rechtslage und Praxis im Drittland, auf Grundlage der (nicht abschließend aufgelisteten) Informationsquellen nach Anhang 3 der Empfehlungen 1/2020.

27 In der Praxis wird sich eine Eingrenzung des Zertifizierungsgegenstands auf bestimmte Drittländer empfehlen, deren Rechtslage zu beurteilen und zu überwachen sind.
28 Urteil des Europäischen Gerichtshofs vom 16. Juli 2020 (Rechtssache C311/18).

	Empfehlungen 02/2020 zu den wesentlichen europäischen Garantien in Bezug auf Überwachungsmaßnahmen genügen.	
Auswahl und Anwendung der ergänzenden Maßnahmen.	Prozesse zur Auswahl geeigneter ergänzender Maßnahmen im Rahmen der vom EDSA entwickelten Anwendungsfälle[29] ausgehend von den identifizierten Lücken bei dem Schutz personenbezogener Daten im Zielland (inkl. aller Transitländer und Zwischenstationen). Falls ergänzende Maßnahmen möglich sind: Umsetzung in Form der vom EDSA in den Anwendungsfällen entwickelten Maßnahmen[30].	Prüfung der Dokumente und der technisch-organisatorischen Maßnahmen (Pseudonymisierung, Verschlüsselung)
Vorliegen komplementärer Maßnahmen beim	Es besteht die Grundannahme, dass sämtliche ergänzende Maßnahmen, die beim Exporteur ergriffen	Prüfung von Prozessbeschreibungen und Dokumentenprüfung

29 Siehe Anhang 2 der Empfehlungen 01/2020 zu Maßnahmen zur Ergänzung von Übermittlungstools zur Gewährleistung des unionsrechtlichen Schutzniveaus für personenbezogene Daten.

30 Siehe Anhang 2 der Empfehlungen 01/2020 zu Maßnahmen zur Ergänzung von Übermittlungstools zur Gewährleistung des unionsrechtlichen Schutzniveaus für personenbezogene Daten.

Datenimporteur	werden, zu den Gegebenheiten des Importeurs passen (und wirksam sein) müssen. Insbesondere muss eine Prüfung dahingehend erfolgen, ob ergänzende Maßnahmen des Importeurs erforderlich sind und entsprechende Weisungen bezüglich ergänzender Maßnahmen des Importeurs erfolgt sind. Im Fall, dass als Übermittlungsinstrument die Zertifizierung gem. 46 Abs. 3 lit. f DSGVO gewählt wird, müssen zusätzlich die Anforderungen an die Wirksamkeit der ergänzenden Maßnahmen gemäß „GL Certification as tools for transfer“[31] erfüllt sein, das heißt: Prüfung, ob das Zertifikat des Importeurs zu den Daten und Anwendungsfällen des Exporteurs passt.	Vorlage des AVV oder der schriftlichen Weisungen; Prüfung der Umsetzung der Weisungen beim Importeur. Vorlage des Zertifikats des Importeurs;
Ggf. förmliche Verfahrensschritte	Einbindung der zuständigen Aufsichtsbehörde mit dem Ziel der Genehmigung in Fällen des Art. 46 Abs. 3.	Prüfung von Prozessbeschreibungen und Dokumentenprüfung.

31 Siehe Punkt 3.2.7 der GL: Additional safeguards concerning the exporter und Annex I der Guidelines on certification as tools for transfers (Entwurf Stand Mai 2022).

Regelmäßige Überwachung und Neubewertung	Prozesse zur regelmäßigen Evaluation der Entwicklung der Rechtslage und Praxis im Drittland und damit einhergehend der Auswirkungen auf das Schutzniveau für personenbezogene Daten; für den Fall des Absinkens des Schutzniveaus muss es einen Notfallplan geben.	Prüfung von Prozessbeschreibungen, Dokumentenprüfung. Inaugenscheinnahme und Prüfung der Umsetzung wie bei den vorhergehenden Schritten.

2.12 Rechte der betroffenen Personen

Folgende Betroffenenrechte sind in einem Zertifizierungsprogramm zwingend als Zertifizierungskriterien zu behandeln:

1. Transparenz und Modalitäten für die Ausübung der Rechte der betroffenen Person gem. Art. 12;
2. Informationspflicht bei Erhebung von personenbezogenen Daten gem. Art. 13 und 14;
3. Auskunftsrecht der betroffenen Person gem. Art. 15;
4. Recht auf Berichtigung gem. Art. 16;
5. Recht auf Löschung („Recht auf Vergessenwerden“) gem. Art. 17;
6. Recht auf Einschränkung der Verarbeitung gem. Art. 18;
7. Mitteilungspflicht im Zusammenhang mit der Berichtigung oder Löschung personenbezogener Daten oder der Einschränkung der Verarbeitung gem. Art. 19;
8. Recht auf Datenübertragbarkeit gem. Art. 20;
9. Widerspruchsrecht gem. Art. 21;
10. automatisierte Entscheidungen im Einzelfall einschließlich Profiling gem. Art. 22.

Sollte einer der aufgeführten Punkte für den betrachteten Zertifizierungsgegenstand nicht einschlägig sein, ist eine Begründung zu liefern, warum dies für den konkreten Zertifizierungsgegenstand nicht erforderlich ist.

3 Prozesse im Geltungszeitraum der Zertifizierung

Damit ein Zertifizierungsprogramm angewendet werden kann, müssen Kriterien durch die zuständige unabhängige Aufsichtsbehörde genehmigt werden. Dazu müssen den Zertifizierungsgegenstand umschließende Prozesse definiert und implementiert sowie organisatorische Maßnahmen ergriffen werden. Als Teil des in der Organisation verankerten Datenschutzmanagements sollen diese Prozesse sicherstellen, dass die DSGVO-Konformität des Zertifizierungsgegenstands über den gesamten Geltungszeitraum der datenschutzrechtlichen Zertifizierung hinweg gewahrt ist. Diesen Prozessen kommt im Zusammenhang mit einer datenschutzrechtlichen Zertifizierung dabei also eine Art Doppelfunktion zu. Zum einen sind sie Bestandteil des organisationseigenen Datenschutzmanagements, zum anderen sind sie jedoch auch, aus der Perspektive der Zertifizierung, integraler Bestandteil des Zertifizierungsgegenstands. Als solches sind sie im Zertifizierungsverfahren Gegenstand der datenschutzrechtlichen Prüfung und Bewertung durch die Zertifizierungsstelle und damit von der erteilten Zertifizierung umfasst, dies eben jedoch nur, soweit sie sich auf den Zertifizierungsgegenstand beziehen. Eine Zertifizierung des gesamten organisationseigenen Datenschutzmanagements erfolgt hier also gerade nicht.

Um eine hinreichende Prüfung und dauerhafte Funktionsfähigkeit dieser Prozesse und damit auch eine, über den Gültigkeitszeitraum der Zertifizierung andauernde, valide und nachprüfbare Siegelaussage gewährleisten zu können, sind in diesem Zusammenhang klar getrennte Zuständigkeiten und Verantwortlichkeiten zu definieren und zu gewährleisten. Hierfür sind die Aufgaben der Zertifizierungsstelle und der Inhaber eines Datenschutzsiegels oder -prüfzeichens konkret voneinander abzugrenzen. Sie sind so darzustellen, dass sowohl die Zuständigkeiten und die Verantwortlichkeiten der jeweiligen Zertifizierungsstelle als auch der Inhaber eines Datenschutzsiegels oder -prüfzeichens daraus eindeutig hervorgehen.

Zu den zu zertifizierenden datenschutzrechtlichen Prozessen gehören mindestens die folgenden Prozesse:

- Datenschutzspezifische Verwaltungsprozesse, die die Beziehung der Zertifizierungsstelle zum Inhaber eines Datenschutzsiegels oder -prüfzeichens beschreiben (u. a. Sicherstellung der Bereitstellung der Kontaktdaten der konkreten Ansprechpartner einschließlich ihrer Befugnisse auf beiden Seiten,),
- Prozesse zur dauerhaften Einhaltung der datenschutzrechtlichen Grundsätze gem. Art. 5;
- Datenschutz-spezifische Prozesse zur Wahrung der Betroffenenrechte gem. Art. 12 bis Art. 22;
- Prozesse zur datenschutzrechtlichen Risikobetrachtung gem. Art. 30 i. V. m. Art. 35 und 36;
- Prozesse zum Umgang mit Verletzungen des Schutzes personenbezogener Daten gem. Art. 33 und 34
  - mit Identifikation, Analyse, technischer Bewertung und rechtlicher Beurteilung damit einhergehender Risiken der Schutzverletzung beim Inhaber eines Datenschutzsiegels oder -prüfzeichens und
  - mit der Auswahl und Umsetzung infolgedessen ergriffener technisch-organisatorischer Maßnahmen gem. Art. 33 Abs. 3 lit. d;
- Realisierung technisch-organisatorischer Maßnahmen aus Prozesssicht, die ggf. durch IT-gestützte Prozesse kontrolliert und überwacht werden können und unter Berücksichtigung und Anwendung von Art. 25 und 32 umzusetzen sind;
- Darstellung der validen, prozessgestützten Transformation datenschutzrechtlicher Anforderungen in Systeme und Dienste, für die eine geeignete und angemessene Form der technischen Bewertung sicherzustellen sowie eine ggf. sich wiederholende rechtliche Beurteilung zu gewährleisten ist.[32]

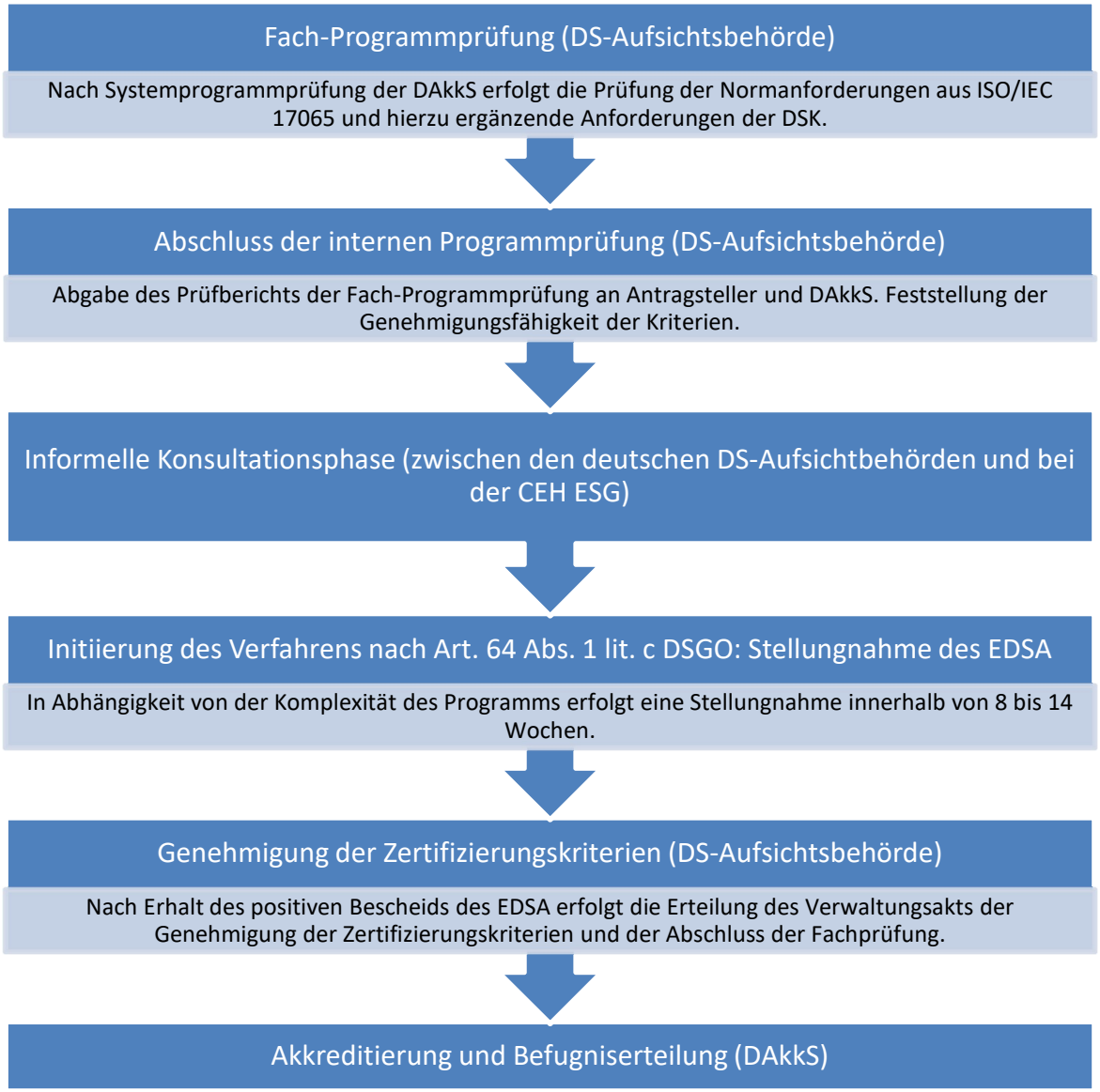
32 Eine solche Bewertung der durch Transformation der datenschutzrechtlichen Anforderungen abgeleiteten Prozesse ist im Zertifizierungsprogramm ebenso darzulegen. Eine mögliche Anleitung zur Durchführung einer solchen

Transformation bietet das Standard-Datenschutzmodell (siehe auch https://www.datenschutz-mv.de/daten-schutz/datenschutzmodell/).

4 Grafiken zum Ablauf der Verfahren (nationales und europäisches Siegel)

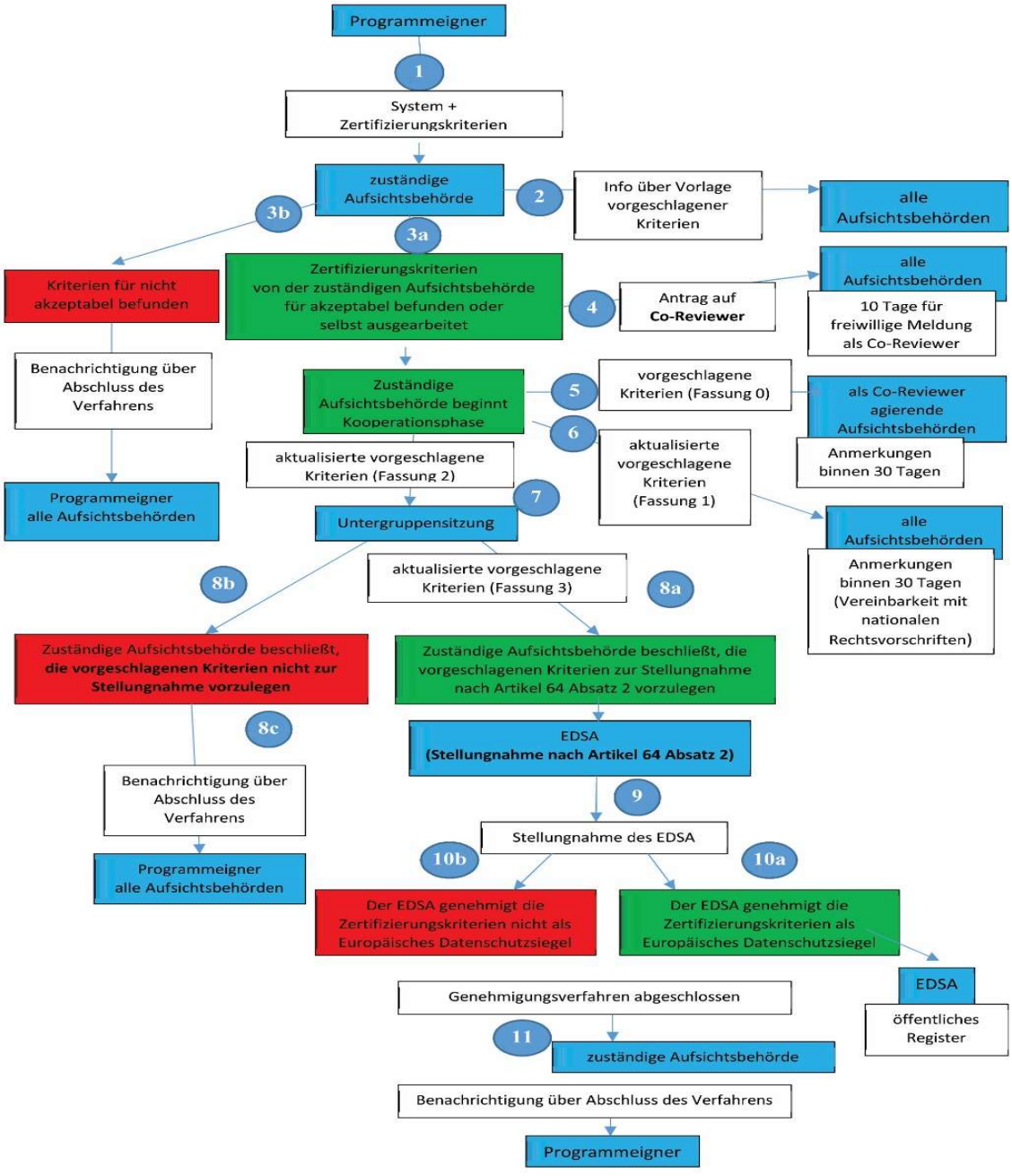
4.1 Abbildung Verfahrensablauf bei der Aufsichtsbehörde für nationale Kriterien

Die folgende Abbildung enthält den weiteren Ablauf im Rahmen des nationalen Verfahrens zur Siegelerteilung.



4.2 Abbildung Verfahrensablauf bei der Aufsichtsbehörde für das europäische Siegel

Zur weiteren Übersicht im Rahmen des europäischen Siegels folgt hier eine Abbildung zum weiteren Verfahrensablauf in diesem Bereich (Prozessübersicht des EDSA-internen Verfahrens zur Genehmigung von zu einem Europäischen Datenschutzsiegel führenden Zertifizierungskriterien).



Quelle: https://edpb.europa.eu/our-work-tools/our-documents/procedure/edpb-document-procedure-approval-certification-criteria-edpb_de

5 Abkürzungsverzeichnis/Glossar

AEUV	Vertrag über die Arbeitsweise der Europäischen Union
AkkStelleG	Akkreditierungsstellengesetz
Art.	Artikel
BDSG	Bundesdatenschutzgesetz
BSI	Bundesamt für Sicherheit in der Informationstechnik
CERT	Computer Emergency Response Team
DAkkS	Deutsche Akkreditierungsstelle GmbH
DSFA	Datenschutz-Folgenabschätzung (Art. 35 DSGVO)
DSK	Datenschutzkonferenz
DSGVO	Datenschutz-Grundverordnung
EDSA	Europäischer Datenschutzausschuss
gem.	gemäß
IDS	Intrusion Detection System
IPS	Intrusion Prevention System
ISMS	Information Security Management System
ITIL	Information Technology Infrastructure Library
KRITIS	Kritische Infrastrukturen
PDCA-Prinzip	Plan-Do-Check-Act, Demingkreis
SDM	Standard-Datenschutzmodell

Für das Glossar wird auf Anhang 1 des DSK Ergänzungspapiers zu „Anforderungen zur Akkreditierung gemäß Art. 43 Abs. 3 DS-GVO i. V. m. DIN EN ISO/IEC 17065“ verwiesen.