# Anforderungen an datenschutzrechtliche Zertifizierungsprogramme

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

---

Version 1.8 (16.04.2021)

## Inhalt


1 Ziel und Einordnung ..... 3
1.1 Ziel ..... 3
1.2 Einordnung in die Regelungssystematik ..... 4
1.3 Prüfverfahren ..... 4
1.4 Basisdokumente ..... 5
2 Zertifizierungskriterien und Anforderungen an einen Zertifizierungsgegenstand ..... 5
2.1 Grundsätzliche Anforderungen ..... 5
2.1.1 Beschreibung des Zertifizierungsgegenstands ..... 5
2.1.2 Angaben des Antragstellers zum Zertifizierungsgegenstand ..... 6
2.1.3 Einhaltung der einschlägigen Datenschutzvorgaben ..... 7
2.2 Artikel 5: Grundsätze für die Verarbeitung personenbezogener Daten ..... 7
2.3 Artikel 6: Rechtmäßigkeit der Verarbeitung ..... 12
2.4 Artikel 25: Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen ..... 20
2.5 Artikel 28: Auftragsverarbeiter ..... 23
2.5.1 Einführende Hinweise ..... 23
2.5.2 Tabellarische Übersicht: Anforderungen, Formen der Umsetzung und Prüfung ..... 23
2.6 Artikel 30: Verzeichnis von Verarbeitungstätigkeiten ..... 26
2.6.1 Einführende Hinweise ..... 26
2.6.2 Tabellarische Übersicht: Anforderungen, Formen der Umsetzung und Prüfung ..... 26
2.7 Artikel 32: Sicherheit der Verarbeitung ..... 29
2.7.1 Einführende Hinweise ..... 29
2.7.2 Tabellarische Übersicht: Anforderungen, Formen der Umsetzung und der Prüfung . 30

2.8 Artikel 33 und 34: Meldung von Verletzungen des Schutzes personenbezogener Daten an die Aufsichtsbehörde und Benachrichtigung der von einer Verletzung betroffenen Person ..... 36
2.8.1 Einführende Hinweise ..... 36
2.8.2 Tabellarische Übersicht: Anforderungen, Formen der Umsetzung und Prüfung ..... 36
2.9 Artikel 35: Datenschutz-Folgenabschätzung ..... 39
2.10 Datenübermittlung an Drittländer oder an intern. Organisationen ..... 41
2.11 Rechte der betroffenen Personen ..... 42
3 Prozesse im Geltungszeitraum der Zertifizierung ..... 43
4 Abkürzungsverzeichnis/Glossar ..... 45

# 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 potentielle Zertifizierungsgegenstände in den Anwendungsbereich von spezialrechtlichen Regelungen fallen.

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] 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.

[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.

## 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.

## 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.

[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.

## 1.4 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.

# 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, in gemeinsamer Verantwortung mit einem anderen Verantwortlichen und alle einbezogenen Auftragsverarbeiter einschließlich sämtlicher Unterauftragsverarbeiter vollzogen werden.

---

[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.

[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.

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

1. welche Verarbeitungsvorgänge mit dem Zertifizierungsgegenstand abgedeckt sind;
2. welche Zwecke mit diesen Verarbeitungsvorgängen abgedeckt werden und weshalb diese Verarbeitungsvorgänge zur Erreichung des Zwecks erforderlich sind;
3. Empfänger bzw. Kategorien von Empfängern;
4. welche Daten im Zusammenhang mit dem Zertifizierungsgegenstand verarbeitet werden und
   a. welche Daten davon besondere Kategorien personenbezogener Daten gem. Art. 9 sind;
   b. welche Daten sich auf strafrechtliche Verurteilungen und Straftaten nach Art. 10 beziehen;
   c. welche Daten sich auf Kinder im Sinn der DSGVO beziehen;
5. wer Auftragsverarbeiter gem. Art. 4 Abs. 8 bzgl. welcher Verarbeitungsvorgänge des Zertifizierungsgegenstands ist;
6. ob im Hinblick auf bestimmte Verarbeitungsvorgänge des Zertifizierungsgegenstands eine gemeinsame Verantwortlichkeit gem. Art. 26 gegeben ist;
7. ob 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.

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

   a. Aufstellung aller Beteiligten – Gruppenbildung ermöglicht Zusammenfassungen (z. B. Kund*innen, Nutzer*innen und Administrator*innen, 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.

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[7] 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 2.10 geregelten Vorgaben zum internationalen Datentransfer und in Kapitel 2.11 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.

## 2.2 Artikel 5: Grundsätze für die Verarbeitung personenbezogener Daten

| *Gesetzliche Tatbestandsmerkmale* | *In den Zertifizierungskriterien zu behandelnde Prüfthemen und deren Umsetzung durch die Kunden[8] der Zertifizierungsstelle[9]* | *Wie prüft die Zertifizierungsstelle die Umsetzung?* |
|---|---|---|
| Art. 5 Abs. 1 lit. a<br>Rechtmäßigkeit, Treu und Glauben, Transparenz | Rechtmäßigkeit, vgl. Kap. 2.3 (Art. 6).<br><br>Verarbeitung nach Treu und Glauben. | Vgl. Kap. 2.3 (Art. 6).<br><br>Vgl. insb. Kap. 2.3 (Art. 6). |

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

[8] Bezeichnet nicht nur die Kunden der Zertifizierungsstelle, sondern auch ggf. Vertragspartner der Kunden (z. B. deren Auftragsverarbeiter).

[9] Zwei Ebenen der Betrachtung: In dieser Spalte werden zu den wichtigsten gesetzlichen Vorgaben die Prüf-themen aufgeführt, die in den Zertifizierungskriterien zu behandeln sind. Daneben erfolgt eine Darstellung der zur Umsetzung durch die Kunden erforderlichen Maßnahmen.

| | | |
|---|---|---|
| | Nachvollziehbarkeit der Verarbeitung, Transparenz für betroffene Personen:<br>Art. 12 ff.<br><br>- Kriterien zur Beurteilung, ob personenbezogene Daten in für die betroffenen Personen nachvollziehbarer Weise verarbeitet werden;<br>- insb. auch Informationen über die Risiken, Vorschriften, Garantien und Rechte sowie darüber, wie diese Rechte geltend gemacht werden können (Erwägungsgrund 39).<br><br>Es ist eine Dokumentation des Prozesses zur Auswahl und Umsetzung technischer und organisatorischer Maßnahmen erforderlich, die die Transparenz der Verarbeitung gewährleisten. (Gewährleistungsziel Transparenz berücksichtigen) | Dokumentenprüfung: Dokumentation der Datenflüsse; Verzeichnis der Verarbeitungstätigkeiten; Informationen nach Art. 13, 14; Dokumentation des Prozesses zur Gewährleistung und Aufrechterhaltung der Transparenz für betroffene Personen.<br><br>Inspektion aller relevanten Geschäftsprozesse und Systeme, Analyse aller Datenflüsse auf Plausibilität.<br><br>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<br>Zweckbindung | Zweckbindung, vgl. insb. Kap. 2.3 (Art. 6).<br><br>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).<br><br>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<br>Datenminimierung | Die Zertifizierungskriterien müssen sich auf den zu führenden Nachweis erstrecken, dass die Verarbeitungstätigkeit in einer datensparsamen Weise durchgeführt wird.<br><br>Die Kriterien müssen die Bewertung dieses Nachweises in Bezug auf die Erfüllung folgender gesetzlicher Vorgaben vorsehen:<br><br>Die Erfüllung der Bedingungen gem. Art. 5 Abs. 1 lit. c:<br><br>a) Kriterien, um die Angemessenheit, die Erheblichkeit und die Notwendigkeit der Verarbeitung der personenbezogenen Daten zu beurteilen,<br><br>b) eine Dokumentation des Prozesses, um zu gewährleisten, dass die Verarbeitung der personenbezogenen Daten jederzeit dem Zweck angemessen und erheblich sowie auf das notwendige Maß beschränkt ist. (Gewährleistungsziel Datenminimierung berücksichtigen.) | Das Zertifizierungsprogramm muss mindestens vorgeben:<br><br>Dokumentenprüfung, juristische Analyse der Unterlagen und Dokumentation gem. Spalte 2<br><br>Das Zertifizierungsprogramm muss mindestens vorgeben, dass der Zertifizierungsdienstleister die folgenden Komponenten der Verarbeitungstätigkeit per Vor-Ort-Begehungen prüft:<br>konkrete Datenbestände und Abgleich mit den Kriterien gem. Spalte 2 a);<br>dies kann sich auf eine Stichprobe beschränken.<br><br>Das Zertifizierungsprogramm muss vorgeben, dass der Zertifizierungsdienstleister die technischen und organisatorischen Maßnahmen dahingehend prüft, dass die Anforderungen zur Gewährleistung der Datenminimierung eingehalten werden (Dokumentenprüfung, methodische Analyse zu Spalte 2 b). |
| Art. 5 Abs. 1 lit. d<br>Richtigkeit | Die Zertifizierungskriterien müssen sich auf den durch den Verantwortlichen zu führenden Nach- | |

| | | |
|---|---|---|
| | weis erstrecken, dass die Verarbeitungstätigkeit dem Grundsatz der Richtigkeit entspricht.<br>Die Kriterien müssen die Bewertung dieses Nachweises in Bezug auf die Erfüllung folgender gesetzlicher Vorgaben vorsehen:<br><br>Die Erfüllung der Bedingungen gem. Art. 5 Abs. 1 lit. d:<br><br>a) Kriterien zur Bestimmung der sachlichen Richtigkeit personenbezogener Daten,<br>b) eine Dokumentation des Prozesses zur Bestimmung der sachlichen Richtigkeit personenbezogener Daten,<br>c) eine Dokumentation des Prozesses zur Auswahl 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). | Das Zertifizierungsprogramm muss mindestens vorgeben: Dokumentenprüfung, juristische Analyse der Unterlagen und Dokumentation gem. Spalte 2.<br><br>Das Zertifizierungsprogramm muss mindestens vorgeben, dass der Zertifizierungsdienstleister die technischen und organisatorischen Maßnahmen dahingehend 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.<br><br>Die Kriterien müssen die Bewertung dieses Nachweises in Bezug auf die Erfüllung der Bedingungen gem. Art. Art. 5 Abs. 1 lit. e vorsehen: | Das Zertifizierungsprogramm muss mindestens vorgeben:<br><br>Dokumentenprüfung, juristische Analyse der Unterlagen und Dokumentation gem. Spalte 2. |

| | | |
|---|---|---|
| | a) Kriterien zur Bestimmung der Identifizierbarkeit einer Person,<br>b) Kriterien zur Bestimmung der für den Zweck der Verarbeitung erforderlichen Dauer der Identifizierbarkeit einer Person,<br>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,<br>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<br>Integrität und Vertraulichkeit | Datenverarbeitung nach dem Grundsatz der Integrität.<br><br>Datenverarbeitung nach dem Grundsatz der Vertraulichkeit.<br><br>Insb. Anforderungen der Art. 24, 25 (vgl. Kap. 2,4), 32 (vgl. Kap. 2.7).<br><br>Es ist eine Dokumentation des Prozesses zur Auswahl und Umsetzung technischer und organisatorischer Maßnahmen erforder- | Insb. Anforderungen der Art. 24, 25 (vgl. Kap. 2.4), 32 (vgl. Kap. 2.7).<br><br>Das Zertifizierungsprogramm muss mindestens vorgeben, dass der Zertifizierungsdienstleister die technischen und organisatorischen |

| | | |
|---|---|---|
| | lich, die die Integrität und Vertraulichkeit der Verarbeitung gewährleisten. (Gewährleistungsziele Integrität und Vertraulichkeit berücksichtigen). | Maßnahmen dahingehend prüft, dass die Anforderungen zur Gewährleistung der Integrität und Vertraulichkeit eingehalten werden (Dokumentenprüfung, methodische Analyse). |
| Art. 5 Abs. 2<br>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)<br>Die Verarbeitung ist nur unter den in Abs. 1 genannten Voraussetzungen rechtmäßig. | a) Darstellung, Prüfung und Dokumentation einer Rechtsgrundlage für die jeweilige Verarbeitung aller personenbezogenen Daten für jeden einzelnen abgrenzbaren Verarbeitungsvorgang; Verarbeitungsvorgänge, die auf derselben Rechtsgrundlage beruhen, können bei der Darstellung, Prüfung und Dokumentation zusammengefasst werden. | a) Dokumentenprüfung, rechtliche Analyse des Vorhandenseins einer Rechtsgrundlage insbesondere anhand 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. |
| | b) Soweit Kunden Verantwortlicher i.S.d. Art. 4 Nr. 7 sind:<br>- Dokumentation von Anweisungen an die Beschäftigten zur vorgelagerten | b) Dokumentenprüfung, rechtliche Analyse der Dokumentation gemäß Spalte 2, z. B. anhand von internen Richtlinien, Dienstanweisungen oder |

| | | |
|---|---|---|
| | 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.<br>- Dokumentation von Strukturen und Zuständigkeiten für die Prüfung einer ausreichenden Rechtsgrundlage (z. B. bei Bedarf Einbindung des Rechts- oder des Datenschutzbereichs oder anderer zuständiger Stellen). | Betriebsvereinbarungen des Verantwortlichen. |
| | 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. | c) 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<br>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<br>- jeden Verarbeitungsvorgang,<br>- jeden Satz personenbezogener Daten,<br>- einen oder mehrere genau bezeichnete Zwecke. | Dokumentenprüfung, rechtliche Analyse der Einwilligung (insb. auf Vollständigkeit, Freiwilligkeit, Aktualität, Übereinstimmung mit Zweck und Verständlichkeit) anhand der Dokumentation gemäß Spalte 2 a). |
| | b) Dabei ist insbesondere zu prüfen, ob sämtliche einschlägige | Inspektion der eingerichteten Abläufe und Maßnahmen zur Einholung der Einwilligung. |

| | | |
|---|---|---|
| | Anforderungen an eine Einwilligung, insbesondere solche aus Art. 7, 8 erfüllt sind, u. a.:<br>- Ist gewährleistet, dass für alle Verarbeitungsvorgänge und –zwecke umfassende und ausreichend deutliche Erklärungen der Betroffenen (und/oder ihrer Vertreter*innen) vor Beginn der Verarbeitung eingeholt und dokumentiert werden?<br>- Ist der Betroffene einwilligungsfähig und sind ggf. Einwilligungen (auch) der vertretungsberechtigten Personen eingeholt worden?<br>- Wurde die Einwilligung freiwillig erklärt (insbesondere unter Beachtung von Über-/Unterordnungsverhältnissen und des Kopplungsverbots für die Verarbeitung)?<br>- Ist die Einwilligung jederzeit widerrufbar und führt sie zur Beendigung der Verarbeitung (oder bestehen z. B. alternative Rechtsgrundlagen für die Verarbeitung)?<br>- Wurde die betroffene Person und ggf. die vertretungsberechtigte(n) Person(en) vor der Erklärung der Einwilligung ausreichend und unter Wahrung des Transparenzgrundsatzes aufgeklärt? | Bei bereits stattfindenden Verarbeitungsvorgängen Stichproben der bestehenden Einwilligungen.<br><br>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.<br><br>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. |
| Art. 6 Abs. 1 lit. b<br>Die Verarbeitung ist für die Erfüllung eines Vertrags, dessen Vertragspartei die betroffene Person ist, oder zur | Benennung, Prüfung und Dokumentation des Vorliegens der folgenden Voraussetzungen:<br><br>a) Vorliegen eines Vertrages mit der betroffenen Person oder | a) Dokumentenprüfung, rechtliche Analyse an- |

| | | |
|---|---|---|
| Durchführung vorvertraglicher Maßnahmen erforderlich, die auf Anfrage der betroffenen Person erfolgt. | 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. | hand von Dokumentation (insbesondere Vertragsmuster, Beschreibungen oder Vermerken zu vorvertraglichen Verhältnissen) des Bestehens eines Vertrages oder eines vorvertraglichen Verhältnisses mit der betroffenen Person. |
| | b) alle verarbeiteten Daten sind zur Vertragserfüllung oder zur Durchführung der vorvertraglichen Maßnahmen erforderlich. | b) 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 Maßnahmen erforderlich. | c) Siehe b). |
| | d) Dokumentation von Strukturen und Abläufen, die zu einem Vertragsschluss oder einem vorvertraglichen Verhältnis führen.<br><br>zu b) bis d) sind insbesondere auch die Anforderungen aus Art. 5 Abs. 1 lit. c zu erfüllen. | d) Dokumentenprüfung der Strukturen und Abläufe gemäß Spalte 2 d) und Inspektion der Abläufe, die zu einem Vertragsschluss oder zu einem vorvertraglichen Verhältnis führen.<br><br>Bei bereits stattfindenden Verarbeitungsvorgängen mindestens stichprobenartige Dokumentenprüfung von abgeschlossenen Verträgen oder eingegangenen vorvertraglichen Verhältnissen. |
| Art. 6 Abs. 1 lit. c<br>Die Verarbeitung ist zur Erfüllung einer rechtlichen Verpflichtung erforderlich, der | Benennung, Prüfung und Dokumentation des Vorliegens der folgenden Voraussetzungen: | |

| | | |
|---|---|---|
| der Verantwortliche unterliegt. | 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 fehlender Eindeutigkeit des Wortlauts inklusive einschlägiger Auslegungsdokumentation wie z. B. Kommentarliteratur, Rechtsgutachten, Rechtsprechung. | a) Dokumentenprüfung, Analyse des Vorliegens einer rechtlichen Verpflichtung des Verantwortlichen anhand der Dokumentation gemäß Spalte 2 a). |
| | b) Alle verarbeiteten Daten sind zur Erfüllung der o. g. rechtlichen Verpflichtung erforderlich. | b) 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.<br><br>zu b) bis c) sind insbesondere auch die Anforderungen aus Art. 5 Abs. 1 lit. c zu erfüllen. | c) Siehe b).<br><br>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. | d) Dokumentenprüfung, rechtliche Analyse zur Beachtung der Regelungen gem. Spalte 2 d). |
| Art. 6 Abs. 1 lit. d<br>Die Verarbeitung ist erforderlich, um lebenswichtige Interessen der betroffenen Person oder einer anderen natürlichen Person zu schützen. | Benennung, Prüfung und Dokumentation der folgenden Voraussetzungen:<br><br>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. | a) Dokumentenprüfung, rechtliche Analyse des Vorliegens lebenswichtiger Interessen einer natürlichen Person anhand der Dokumentation gemäß Spalte 2. |

| | | |
|---|---|---|
| | b) Alle verarbeiteten Daten sind für den Schutz der lebenswichtigen Interessen erforderlich.<br><br>c) Alle Verarbeitungsvorgänge sind für den Schutz der lebenswichtigen Interessen erforderlich.<br><br>Zu b) bis c) sind insbesondere auch die Anforderungen aus Art. 5 Abs. 1 lit. c zu erfüllen. | b) 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.<br><br>c) Siehe b). |
| Art. 6 Abs. 1 lit. e<br>Die Verarbeitung ist für die Wahrnehmung einer Aufgabe erforderlich, die im öffentlichen Interesse liegt oder in Ausübung öffentlicher Gewalt erfolgt, die dem Verantwortlichen übertragen wurde. | Benennung, Prüfung und Dokumentation des Vorliegens folgender Voraussetzungen:<br><br>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.<br><br>b) Alle verarbeiteten Daten sind für die Wahrnehmung der o. g. Aufgabe erforderlich.<br><br>c) Alle Verarbeitungsvorgänge sind für die Wahrnehmung der o. g. Aufgabe erforderlich. | a) 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.<br><br>b) 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.<br><br>c) Siehe b). |

| | | |
|---|---|---|
| | Zu b) bis c) sind insbesondere auch die Anforderungen aus Art. 5 Abs. 1 lit. c zu erfüllen.<br><br>d) Dabei sind insbesondere die Vorgaben des Art. 6 Abs. 2 und 3 sowie eventuell bestehender Sonderregelungen, z.B. in Abhängigkeit des Anwendungskontexts, zu beachten. | d) Dokumentenprüfung, rechtliche Analyse zur Beachtung der Regelungen gem. Spalte 2 d). |
| Art. 6 Abs. 1 lit. f<br>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<br>- die Verarbeitung im berechtigten Interesse des Verantwortlichen oder eines Dritten liegt,<br>- es sich nicht um von Behörden in Erfüllung ihrer Aufgaben vorgenommene Verarbeitungen handelt,<br>- die Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person nicht überwiegen, insbesondere dann, wenn es sich dabei um ein Kind handelt.<br><br>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 hinsichtlich welcher personenbezogenen Daten und welcher Verarbeitungsvorgänge abgewogen werden. | a) 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.<br><br>b) Prüfung und Inspektion des Prozesses der Interessenabwägung. |

| | | |
|---|---|---|
| | | c) Mindestens Stichproben-artige Validierung der Datenflüsse zwischen Systemen und Diensten (zur Erbringung einer (spezifizierten) Dienst-leistung. |
| Art. 6 Abs. 4<br>Bei nachträglicher Verände-rung des Verarbeitungs-zwecks 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 (wirk-same) Einwilligung abgege-ben haben. | a) Dokumentation der Zweckän-derung (von welchem Zweck zu welchem?).<br><br>b) Dokumentation der Begrün-dung der Zweckänderung so-wie Dokumentation der recht-lichen Prüfung der Zulässigkeit der Zweckänderung.<br><br>c) Vorliegen dokumentierter Maßnahmen, damit bevorste-hende Zweckänderungen er-kannt werden und der geän-derte Zweck rechtzeitig ge-prüft und ggf. weitere Vorkeh-rungen getroffen werden kön-nen (wie z. B. die Einholung weiterer Einwilligungen der Betroffenen). | a) Dokumentenprüfung: Prüfung des Vorliegens einer Zweckänderung anhand der Dokumenta-tion gemäß Spalte 2;<br><br>b) Dokumentenprüfung, rechtliche Analyse der Zulässigkeit der Zweck-änderung anhand der Dokumentation gemäß Spalte 2;<br><br>c) Dokumentenprüfung: Prüfung der Maßnahmen zur Erkennung von Zweckänderungen und zum Vorhandensein der sich daran anschließen-den notwendigen Vor-kehrungen anhand der Dokumentation gemäß Spalte 2 sowie mindes-tens stichprobenartige Inspektion dieser Maß-nahmen und Vorkehrun-gen. |

## 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<br>Datenschutz durch Technikgestaltung | Es muss eine datenschutzrechtliche Risikobetrachtung (siehe auch „datenschutzrechtliche Risikobetrachtung“) der Verarbeitungsvorgänge vollzogen und dokumentiert werden.<br><br>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 verbundenen Risiken für die Rechte und Freiheiten natürlicher Personen.<br><br>Es muss eine Beschreibung aller technischen und organisatorischen Maßnahmen zur Wahrung der Datenschutzgrundsätze und Aufnahme notwendiger Garantien,<br><br>- um den Anforderungen der DSGVO zu genügen und<br>- um die Rechte der betroffenen Personen zu schützen<br>bestehen. | Dokumentenprüfung der Risikobetrachtung.<br><br>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“).<br><br>Dokumentenprüfung von Tätigkeitsbeschreibungen oder Arbeitsanweisungen<br><br>Dokumentenprüfung der getroffenen Maßnahmenübersicht und Validierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Minderung des datenschutzrechtlichen Risikos. |

| | | |
|---|---|---|
| Art. 25 Abs. 1<br>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 notwendigen Garantien in die Verarbeitung aufzunehmen, um den Anforderungen dieser Verordnung zu genügen und die Rechte der betroffenen Personen zu schützen. | Es müssen Prozesse bestehen, welche die Berücksichtigung der Datenschutzgrundsätze zum Zeitpunkt der Festlegung der Mittel gewährleisten.<br><br>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 Prozessdokumentation.<br><br>Dokumentenprüfung von exemplarischen Ausschreibungen und Abnahmekriterien für Mittel der Verarbeitung.<br><br>Befragung von Mitarbeitenden über Entscheidungsprozesse in der Designphase der Systeme.<br><br>Dokumentenprüfung der Entscheidungsdokumentation hinsichtlich der angemessenen Abwägung i. S. d. Art. 25 Abs. 1. |
| Art. 25 Abs. 1<br>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).<br><br>Die Festlegung auf bzw. die Entscheidung für geeignete technische und/oder organisatorische Maßnahmen muss dokumentiert | Prüfung hinsichtlich der vollständigen Erfassung aller Verarbeitungstätigkeiten anhand des Verzeichnisses der Verarbeitungstätigkeiten gem. Art. 30 bzw. von Datenflussdiagrammen, Systemübersichten, Prozessbeschreibungen, o. Ä.<br><br>Validierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Minderung des datenschutzrechtlichen Risikos<br><br>Dokumentenprüfung der Entscheidungsdokumenta- |

| | | |
|---|---|---|
| | und begründet werden (vgl. Art. 5 Abs. 1 lit. f i. V. m. Art. 5 Abs. 2). | tion 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.<br><br>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).<br><br>Es muss gewährleistet sein, dass personenbezogene Daten nicht durch die Voreinstellung einer unbestimmten Zahl von natürlichen Personen zugänglich gemacht werden. | Prüfung der Einstellungen einer Standardkonfiguration der Mittel der Verarbeitung, bei der alle nicht erforderlichen Verarbeitungsvorgänge deaktiviert sein müssen.<br><br>Prüfung der Erforderlichkeit von nicht beschränkenden Voreinstellungen anhand der Verarbeitungszwecke.<br><br>Prüfung der dokumentierten Beschränkungen, ob die aufgeführten Gründe einer weitergehenden Datenminimierung entgegenstehen.<br><br>Ermittlung der Verarbeitungsvorgänge, welche personenbezogene Daten an eine unbestimmte Zahl von natürlichen Personen zugänglich machen und anschließende Dokumentenprüfung der festgelegten Voreinstellungen. |

## 2.5 Artikel 28: Auftragsverarbeiter

### 2.5.1 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.

### 2.5.2 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?* |
|---|---|---|
| Auftragsverarbeitung muss im konkreten Einsatz vorliegen und rechtlich zulässig sein. | 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.<br><br>Es ist zu prüfen und zu dokumentieren, ob eine Auftragsverarbeitung oder eine gemeinsame Verantwortung i. S. d. Art. 26 bzw. vorliegt.<br><br>Je nach Einsatzbereich sind die Besonderheiten der Zulässigkeit bzw. ggf. bestehende Einschränkungen zu beachten (z. B. bzgl. Verarbeitung von Personalakten im Auftrag oder auch im Gesundheitsbereich). | Prüfung des Angebotstextes des Auftragsverarbeiters bzw. der Beschreibung seiner Dienstleistung und der übrigen Unterlagen. |
| Art. 28 Abs. 1<br>Hinreichende Garantien für geeignete technische und organisatorische Maßnahmen. | Vorliegen genehmigter Verhaltensregeln (Art. 40) oder<br><br>Zertifizierung (Art. 42) oder | In der Regel alle folgenden Prüfmethoden:<br>- Prüfung von Genehmigungen/Zertifizierungen, |

| | | |
|---|---|---|
| | sonstige Garantien (Audits, Zertifizierungen, Dokumentation, Kontrollmöglichkeiten durch Auftraggeber etc.). | - vor-Ort-Prüfung der technischen und organisatorischen Maßnahmen und<br>- Dokumentenprüfung. |
| Art. 28 Abs. 3<br>Vorliegen eines Auftragsverarbeitungsvertrags (schriftlich/elektronisches Format). | Ausreichende Regelung zu insbesondere den Mindestinhalten gem. Art. 28 Abs. 3:<br>- Gegenstand und Dauer der Verarbeitung (Art. 28 Abs. 3 S. 1);<br>- Art und Zweck der Verarbeitung (Art. 28 Abs. 3 S. 1);<br>- Art der personenbezogenen Daten (Art. 28 Abs. 3 S. 1);<br>- Kategorien von betroffenen Personen (Art. 28 Abs. 3 S. 1);<br>- Dokumentierte Weisungslage für den Auftragsnehmer (Art. 28 Abs. 3 lit. a);<br>- Gewährleistung der Vertraulichkeit oder Verschwiegenheit (Art. 28 Abs. 3 lit. b);<br>- Ergreifen adäquater technischer und organisatorischer Maßnahmen des Auftragsverarbeiters (Art. 28 Abs. 3 lit. c);<br>- Regelung zur Inanspruchnahme von Subunternehmern (Art. 28 Abs. 3 lit. d);<br>- 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)?<br>- Vorgaben zur Unterstützung des Verantwortlichen bei der Einhaltung der Vorgaben aus Art. 32 bis 36 (Art. 28 Abs. 3 lit. f);<br>- Vorgaben zur Löschung/Rückgabe nach Abschluss der vereinbarten Leistung (Art. 28 Abs. 3 lit. g); | - Rechtliche Analyse des Vertrags auf Vollständigkeit und rechtliche Zulässigkeit.<br>- Eingehende rechtliche Prüfung der konkreten vertraglichen Umsetzung und des Vorhandenseins ausreichender technischer und organisatorischer Maßnahmen (vgl. dazu Ausführungen zu Art. 32). |

| | | |
|---|---|---|
| | - Zurverfügungstellung aller erforderlichen Informationen durch Auftragnehmer an den Verantwortlichen zum Nachweis der Pflichten (Art. 28 Abs. 3 lit. h, Art. 5 Abs. 2);<br>- 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;<br>- Vereinbarung einer Informationspflicht des Auftragsverarbeiters, wenn er der Auffassung ist, eine Weisung sei rechtswidrig (Art. 28 Abs. 3 lit. h). | |
| Art. 28 Abs. 4<br>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.<br><br>Ausreichende Garantien bzgl. technischer und organisatorischer Maßnahmen | - Rechtliche Analyse des Vertrags auf Vollständigkeit und Zulässigkeit;<br>- Prüfung der Dokumentation der techn./org. Maßnahmen;<br>- vor-Ort-Prüfung der techn./org. Maßnahmen. |
| Art. 28 Abs. 2<br>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.<br>Dokumentation der Genehmigungen. | - Sofern bereits ein (neuer) Unterauftragnehmer beauftragt wurde, Prüfung, ob entsprechende Unterrichtungen/Genehmigungen erfolgt sind;<br>- Dokumentenprüfung;<br>- Audit der Prozesse. |
| Art. 44<br>Bestehen geeigneter Garantien bei Datenübermittlung an ein Drittland. | Dokumentation der Garantien (vgl. Art. 5). | - Prüfung der Dokumentation (vgl. Art. 5). |
| Art. 33 Abs. 2<br>Sicherstellung einer unverzüglichen Meldung von Datenschutzverstößen, sobald diese | Einrichtung entsprechender Prozesse.<br>Dokumentation. | - Audit der Prozesse;<br>- Durchsicht der Dokumentation. |

| | | |
|---|---|---|
| dem Auftragsverarbeiter bekannt werden. | | |
| Art. 32 Abs. 4, Art. 29<br>Sicherstellung, dass Verarbeitung nur gemäß Weisungslage erfolgt. | Vorhandensein entsprechender Prozesse und Dokumentation der Weisungen | - Prüfung der Dokumentation;<br>- Beschreibung der Prozesse. |

## 2.6 Artikel 30: Verzeichnis von Verarbeitungstätigkeiten

### 2.6.1 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).

### 2.6.2 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?* |
|---|---|---|
| Art 30 Abs. 5<br>Verzeichnis von Verarbeitungstätigkeiten ist erforderlich. | Prüfung der Voraussetzungen:<br>- Anzahl der Mitarbeitenden und ggf. entweder<br>- Risiko für Freiheiten und Rechte natürlicher Personen vorhanden,<br>- nicht nur gelegentliche Verarbeitung, oder<br>- Verarbeitung besonderer Kategorien gem. Art. 9 Abs. 1 oder Art. 10. | Befragung oder Dokumentenprüfung zur Feststellung der Anzahl der Mitarbeitenden.<br><br>Rechtliche und technisch-organisatorische Dokumentenprüfung einer vom Verantwortlichen durchzuführenden Bewertung |

| | | |
|---|---|---|
| | | - des Risikos,<br>- der Häufigkeit und<br>- der betroffenen Kategorien personenbezogener Daten<br>der Verarbeitungstätigkeiten. |
| Art. 30 Abs. 1<br>Verzeichnis ist vollständig. | Das Verzeichnis der Verarbeitungstätigkeiten enthält alle Angaben aus Art. 30 Abs. 1 lit. a-g.<br><br>Prozesse zur Aktualisierung des Verzeichnisses sind etabliert für den Fall, dass<br><br>- Verarbeitungstätigkeiten eingeführt werden,<br>- Verarbeitungstätigkeiten wegfallen,<br>- sich bei bereits aufgeführten Verarbeitungstätigkeiten Angaben entsprechend Art. 30 Abs. 1 lit. a-g ändern.<br><br>Es existieren Prozesse zur dahingehenden Zusammenarbeit zwischen<br><br>- an den Verarbeitungstätigkeiten beteiligten Fachabteilungen,<br>- dem Vertreter des Verantwortlichen sowie<br>- ggf. dem Datenschutzbeauftragten.<br>Entsprechende Zuständigkeiten innerhalb der Organisation sind geklärt. | Dokumentenprüfung des Verzeichnisses der Verarbeitungstätigkeiten.<br><br>Prüfung schriftlich fixierter Prozessbeschreibungen; Audit der Prozesse.<br><br>Dokumentenprüfung von<br><br>- schriftlich fixierten Prozessbeschreibungen,<br>- Organisationsplänen,<br>- Geschäfts-/Aufgabenverteilungsplänen;<br>- ggf. Befragung des Verantwortlichen. |
| Art. 30 Abs. 2<br>Verzeichnis enthält Angaben für Auftragsverarbeiter. | Das Verzeichnis der Verarbeitungstätigkeiten enthält alle Angaben aus Art. 30 Abs. 2 lit. a-d.<br><br>Prozesse zur Aktualisierung des Verzeichnisses sind etabliert für den Fall, dass | Dokumentenprüfung des Verzeichnisses der Verarbeitungstätigkeiten.<br><br>Prüfung schriftlich fixierter Prozessbeschreibungen; Audit der Prozesse. |

| | | |
|---|---|---|
| | - Kategorien von im Auftrag durchgeführten Verarbeitungstätigkeiten eingeführt werden;<br>- Kategorien von im Auftrag durchgeführten Verarbeitungstätigkeiten wegfallen;<br>- sich bei bereits aufgeführten Kategorien von Verarbeitungstätigkeiten Angaben entsprechend Art. 30 Abs. 2 lit. a-d ändern;<br>- zusätzliche Verantwortliche, in deren Auftrag eine Verarbeitung durchgeführt wird, hinzukommen;<br>- Verantwortliche, in deren Auftrag eine Verarbeitung durchgeführt wird, wegfallen;<br>- sich bei bestehenden Verantwortlichen, in deren Auftrag eine Verarbeitung durchgeführt wird, Angaben nach Art. 30 Abs. 2 lit. a-d ändern.<br><br>Es existieren Prozesse zur dahingehenden Zusammenarbeit zwischen<br><br>- an den Verarbeitungstätigkeiten beteiligten Fachabteilungen;<br>- dem Vertreter des Verantwortlichen, der als Auftragsverarbeiter auftritt;<br>- ggf. dem Datenschutzbeauftragten des Verantwortlichen, der als Auftragsverarbeiter auftritt;<br>- den Verantwortlichen, in deren Auftrag eine Verarbeitung durchgeführt wird.<br><br>Entsprechende Zuständigkeiten innerhalb der Organisation sind geklärt. | Dokumentenprüfung von<br><br>- schriftlich fixierten Prozessbeschreibungen;<br>- Organisationsplänen;<br>- Geschäfts-/Aufgabenverteilungsplänen;<br>- ggf. Befragung des Verantwortlichen. |

| | | |
|---|---|---|
| Art. 30 Abs. 3<br>Verzeichnis wird schriftlich geführt. | Die schriftliche Führung des Verzeichnisses ist gegeben.<br><br>Entsprechende Aufbewahrungs-/Speicherorte sind den beteiligten Personen bekannt. | Dokumentenprüfung. |
| Art. 30 Abs. 4<br>Verzeichnis wird auf Anfrage der Aufsichtsbehörde zur Verfügung gestellt. | Prozesse sind etabliert, um<br><br>- die Entgegennahme;<br>- die Bearbeitung;<br>- die Beantwortung unter Zurverfügungstellung des Verzeichnisses der Verarbeitungstätigkeiten<br>einer diesbezüglichen Anfrage einer Aufsichtsbehörde zeitnah sicherzustellen.<br><br>Die Verteilung der entsprechenden Zuständigkeiten innerhalb der Organisation ist geklärt. | Dokumentenprüfung von<br><br>- schriftlich fixierten Prozessbeschreibungen; Audit der Prozesse;<br>- Organisationsplänen;<br>- Geschäfts-/Aufgabenverteilungsplänen;<br>- ggf. Befragung des Verantwortlichen. |

## 2.7 Artikel 32: Sicherheit der Verarbeitung

### 2.7.1 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.[10] Die Erfüllung der entsprechenden datenschutzrecht-

[10] 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

lichen 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.

### 2.7.2 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 für alle erforderlichen Verarbeitungstätigkeiten. | 1. Vollständige, detaillierte Beschreibung aller verarbeiteten Daten bzw. Datenkategorien.<br>2. Risikobasierte Ermittlung des angemessenen Schutzniveaus (insb. unter Berücksichtigung der Erwägungsgründe 38 und 75).<br>3. Berücksichtigung von Risiken, die sich insbesondere durch Vernichtung, Verlust, Veränderung, unbefugte | 1. Dokumentenprüfung, Befragung der Verantwortlichen.<br>2. Prüfung der Konformität der verwendeten Risikomethode mit der DSGVO.<br>Dokumentenprüfung: Korrektheitsprüfung der Risikoermittlung (z. B. nach SDM D3).<br>Dokumentenprüfung, rechtliche Analyse: Abgleich des resultierenden Schutzniveaus mit den Schutzanforderungen der zu verarbeitenden Datenkategorien.<br>3. wie 2. mit der Schwerpunktsetzung auf Vernichtung, Verlust, Veränderung, Offenlegung und |

ISO/IEC 17065“ unter https://www.datenschutzkonferenz-online.de/media/ah/20201008_din17065_Ergaenzungen_deutsch_nach_opinion.pdf).

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

| | | |
|---|---|---|
| | | gen technischen Normen, wie z. B. BSI Grundschutz oder ISO 27001, enthalten.). |
| | 2. Maßnahmen zur Gewährleistung weiterer Ziele nach DSGVO und/oder SDM C1 für die personenbezogenen Daten (in Abhängigkeit zur risikobasierten Ermittlung des Schutzniveaus). | 2. wie 1. |
| | 3. 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, s. auch zu Art. 5 DSGVO). | 3. 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 b<br>Maßnahmen zum Schutz der Systeme und Dienste auf Dauer. | 1. Maßnahmen zur Gewährleistung weiterer Ziele nach DSGVO und/oder SDM C1 (insbesondere Vertraulichkeit, Integrität, Verfügbarkeit, Belastbarkeit) zum Schutz der Systeme und Dienste. | 1. Dokumentenprüfung: Prüfung der Spezifikation und der Schutzkonzepte insb. hinsichtlich des Stands der Technik und der Konsistenz der einzelnen Maßnahmen (insb. Berechtigungskonzept, Identitätsmanagement, Authentifizierung und Autorisierung, Revisions- und |

| | | |
|---|---|---|
| | | Protokollierungs-konzept).<br>Das Schutzniveau der Maßnahmen muss den Schutzanforderungen an das Gesamtsystem entsprechen (z. B. gem. IT-Sicherheits-konzept). Prüfung er-folgt durch einen Ver-gleich.<br><br>Vor-Ort-Begehungen, Validierungsaudits, Be-fragungen: Angemessene Verifika-tion der Maßnah-menumsetzung (siehe oben). |
| | 2. Gewährleistung der Maßnahmen (von Punkt 1) auf Dauer. | 2. 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/Demingkreis).<br><br>Vor-Ort-Begehungen, Validierungsaudits, un-angekündigte Bege-hungen, Befragungen: Verifikation der Um-setzung der entspre-chenden Manage-mentprozesse (z. B. durch Simulation in-terner und externer |

| | | |
|---|---|---|
| | | Vorfälle, wie beabsichtigte Angriffe und unbeabsichtigte Ereignisse und/oder durch Lasttests). |
| Art. 32 Abs. 1 lit. c<br>Maßnahmen zur Sicherstellung der Verfügbarkeit von personenbezogenen Daten im Regelbetrieb sowie bei Zwischenfällen. | 1. Maßnahmen zur Sicherstellung der Verfügbarkeit personenbezogener Daten im Regelbetrieb.<br><br>2. Gewährleistung der Verfügbarkeit bei physischen oder technischen Zwischenfällen. | 1. Dokumentenprüfung: Prüfung der Spezifikation und der relevanten Konzepte (z. B. Überprüfung von Verfügbarkeitsklassen, Service Level Agreements) insb. hinsichtlich des Stands der Technik.<br><br>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.<br><br>Vor-Ort-Begehungen, Validierungsaudits, Befragungen: Angemessene Verifikation der Maßnahmenumsetzung (z. B. nach ITIL Availability Management, KRITIS).<br><br>2. 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<br>Maßnahmen zur Gewährleistung von regelmäßiger Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen. | 1. Gewährleistung, dass alle relevanten Systeme und Prozesse einer regelmäßigen Überprüfung, Bewertung und Evaluierung hinsichtlich der Wirksamkeit der TO-Maßnahmen unterliegen.<br><br>2. Gewährleistung, dass die unter 1. etablierten Maßnahmen bei allen Systemen und Prozessen korrekt (wirksam) umgesetzt sind. | 1. Validierungsaudits: Prüfung entsprechend der Managementsysteme (z. B. nach ISMS, ITIL Service Continuity Management) und der Überwachungssysteme und -prozesse (z. B. Incident-Response, CERT, IDPS).<br><br>2. wie 1. |
| Art. 32 Abs. 4<br>Maßnahmen zur Sicherstellung, dass den Verantwortlichen bzw. den Auftragsverarbeitern unterstellte natürliche Personen diese personenbezogenen Daten grundsätzlich nur | Gewährleistung, dass Vereinbarungen zur Verarbeitung personenbezogener Daten existieren und korrekt sind. | Dokumentenprüfung, rechtliche Analyse: Überprüfung der Rechtmäßigkeit und Korrektheit von internen Richtlinien und Vereinbarungen |

| | | |
|---|---|---|
| auf entsprechende Weisung verarbeiten. | | Dokumentenprüfung, Befragungen:<br>Prüfung, ob die oben genannten Richtlinien und Vereinbarungen der organisatorischen Struktur der Verantwortlichen entsprechen. |

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

### 2.8.1 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.

### 2.8.2 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<br>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.<br><br>Die o. g. Überprüfungen können u. a. durch<br><br>- Dokumentenprüfung;<br>- vor-Ort-Kontrolle;<br>- Mitarbeiterbefragung |

| | | |
|---|---|---|
| | | erfolgen. |
| Art. 33 Abs. 1, Satz 1<br>Verletzung des Schutzes personenbezogener Daten. | Identifikation, Analyse und Bewertung der Schutzverletzung (siehe Definition gem. Art. 4 Nr. 12). | s.o. |
| Art. 33 Abs. 1, Satz 1<br>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“),<br><br>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<br>Meldepflicht des Auftragsverarbeiters an den Verantwortlichen. | Maßnahmen zur Sicherstellung,<br><br>dass der Auftragsverarbeiter die Schutzverletzung an den Verantwortlichen meldet (ggf. Regelung im Auftragsverarbeitungsvertrag). | s.o., insb. Prüfung des Auftragsverarbeitungsvertrages. |
| Art. 33 Abs. 3<br>Inhalt der Meldung. | Maßnahmen zur Sicherstellung einer inhaltlich vollständigen Meldung; ggf. Verwendung aufsichtsbehördlicher Meldeformulare. | s.o. |
| Art. 33 Abs. 3, lit. d<br>Maßnahmen zur Behebung der Verletzung und gegebenenfalls Maßnahmen zur Abmilderung ihrer möglichen nachteiligen Auswirkungen. | Auswahl und Umsetzung der ergriffenen technisch-organisatorischen Maßnahmen.<br><br>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:<br><br>Art. 33 Abs. 4<br>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.<br><br>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 der Fristwahrung führt (Erst- und Nachmeldung).<br><br>Maßnahmen zur Fristwahrung und zur (schrittweisen) Nachreichung der erforderlichen Informationen sind zu ergreifen. | s.o. |
| Art. 33 Abs. 5, Satz 1<br>Dokumentationspflicht. | Dokumentation der Verletzung des Schutzes personenbezogener Daten einschließlich aller im Zusammenhang mit der Verletzung stehenden Fakten, von deren Auswirkungen und der ergriffenen Abhilfemaßnahmen.<br><br>Die Dokumentation muss der Aufsichtsbehörde ermöglichen, die Einhaltung der Bestimmungen des Art. 33 zu überprüfen. | s.o. |
| Art. 34<br>Benachrichtigungspflicht an betroffene Person. | Es muss ein Prozedere festgelegt sein, wie bei Datenschutzverletzungsvorfällen zu verfahren ist, um den Anforderungen der Be- | Die Verfahrensabläufe/Prozesse müssen vgl. Art. 33 überprüft werden können. |

| | | |
|---|---|---|
| | nachrichtigungspflicht an betroffene Personen nachzukommen. Dies umfasst u. a. die Festlegung von Verfahrensschritten und Verantwortlichkeiten. | |
| Art. 34 Abs. 1<br>Verletzung des Schutzes personenbezogener Daten mit voraussichtlich hohem Risiko. | s.o. zu Art. 33. | |
| Art. 34 Abs. 1<br>Frist | s.o. zu Art. 33. | |
| Art. 34 Abs. 2<br>Inhalt der Benachrichtigung | s.o. zu Art. 33. | |
| Art. 34 Abs. 3<br>Ausnahme von der Benachrichtigungspflicht | Prüfung, ob Ausnahmetatbestände vorliegen. | |
| Art. 34<br>Dokumentation der Einhaltung der Anforderungen | Die Dokumentation muss der Aufsichtsbehörde ermöglichen, die Einhaltung der Bestimmungen des Art. 34 zu überprüfen. | |

## 2.9 Artikel 35: Datenschutz-Folgenabschätzung

| *Gesetzliche Tatbestandsmerkmale* | *In den Zertifizierungskriterien zu behandelnde Prüfthemen und deren Umsetzung durch die Kunden der Zertifizierungsstelle* | *Wie prüft die Zertifizierungsstelle die Umsetzung?* |
|---|---|---|
| Art. 35<br>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 je- | Dokumentenprüfung und ggf. Befragung:<br><br>Verantwortlicher und Auftragsverarbeiter haben die DSFA-spezifischen Prüfergebnisse unter Einsatz des Zertifizierungsgegenstands im Anwendungskontext zu |

| | | |
|---|---|---|
| | weiligen Verarbeitungszwecke erfolgen. Maßgeblich ist daher die Erstellung eines Verzeichnisses von Verarbeitungstätigkeiten gem. Art. 30).<br><br>Hierzu ist zu prüfen, ob mindestens ein durch den Zertifizierungsgegenstand abgedeckter Verarbeitungsvorgang in einer der folgenden Listen genannt ist:<br><br>- spezielle Anforderungen aus Art. 35 Abs. 3;<br>- der Liste gem. Art. 35 Abs. 4 (Whitelist)[11];<br>- der Liste gem. Art. 35 Abs. 5 (Blacklist).<br><br>Ebenso ist zu prüfen, ob für den Zertifizierungsgegenstand eine DSFA aus anderen Gründen durchzuführen ist, z. B. weil<br><br>- die Verarbeitung personenbezogener Daten Anforderungen des EDSA in der jeweils aktuellen Fassung (z. B. aus WP248) erfüllt[12];<br>- eine DSFA aufgrund eines Bundes- oder Landesgesetzes oder Spezialgesetzes gefordert wird. | dokumentieren und zu erläutern;<br><br>(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. |
| Art. 35<br>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. | Dokumentenprüfung und ggf. Befragung:<br><br>Verantwortlicher und Auftragsverarbeiter haben die skizzierten Anforderungen unter Einsatz des Zertifizie- |

[11] https://www.datenschutzkonferenz-online.de/media/ah/20181017_ah_DSK_DSFA_Muss-Liste_Version_1.1_Deutsch.pdf.

[12] https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=611236.

| | | |
|---|---|---|
| | Die DSGVO enthält keine expliziten Formvorschriften zur Durchführung der DSFA. In Art. 35 Abs. 7 werden aber Elemente aufgezählt, die die Folgenabschätzung zumindest enthalten muss:<br><br>- Eine systematische Beschreibung der geplanten Verarbeitungsvorgänge und der Zwecke der Verarbeitung, gegebenenfalls einschließlich der von dem Verantwortlichen verfolgten berechtigten Interessen;<br>- eine Bewertung der Notwendigkeit und Verhältnismäßigkeit der Verarbeitungsvorgänge in Bezug auf den Zweck;<br>- eine Bewertung der Risiken für die Rechte und Freiheiten der betroffenen Personen gem. Absatz 1 und<br>- die zur Bewältigung der Risiken geplanten Abhilfemaßnahmen, einschließlich Garantien, Sicherheitsvorkehrungen und Verfahren, durch die der Schutz personenbezogener Daten sichergestellt und der Nachweis dafür erbracht wird, dass diese Verordnung [auch perspektivisch[13]] eingehalten wird, wobei den Rechten und berechtigten Interessen der betroffenen Personen und sonstiger Betroffener Rechnung getragen wird. | rungsgegenstands im Anwendungskontext zu dokumentieren und zu erläutern;<br><br>(optional) Muster einer DSFA für den Einsatz des Zertifizierungsgegenstands unter Berücksichtigung eines oder mehrerer Anwendungskontexte, das durch den Verantwortlichen oder Auftragsverarbeiter, für die die eigene Anwendung des Zertifizierungsgegenstands zu konkretisieren ist.<br><br>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. |

## 2.10 Datenübermittlung an Drittländer oder an intern. Organisationen

Impliziert der Zertifizierungsgegenstand eine Übermittlung personenbezogener Daten an Drittländer oder an internationale Organisationen (nachstehend „Drittlandtransfer“), sind die gesetzlichen Anforderungen an die Rechtmäßigkeit eines solchen Drittlandtransfers aus den Art. 44 bis 49 zu beachten.

[13] 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.

Das bedeutet, dass ein Zertifizierungsprogramm darauf ausgerichtet sein muss, zu prüfen, ob ein Drittlandtransfer Teil des Zertifizierungsgegenstands und rechtlich zulässig ist.

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

1. Die Auseinandersetzung mit der Frage, ob im Rahmen des Zertifizierungsgegenstands ein Drittlandtransfer ausgeschlossen werden kann. Dabei muss die Zertifizierungsstelle beachten, dass es in der Praxis häufig zu derartigen Drittlandtransfers bei der Übermittlung von Daten im Rahmen von Wartung, Pflege und Supports kommt. Oft wird die Relevanz eines solchen Transfers 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 ein Drittlandtransfer ausgeschlossen werden kann, auch solche Leistungen im Blick haben und dies im Rahmen des Zertifizierungsprogramms gezielt überprüfen.

2. Soweit ein Drittlandtransfer im Rahmen des Zertifizierungsgegenstands nicht ausgeschlossen werden kann, müssen Kunden der Zertifizierungsstelle prüfen und dokumentieren (und entsprechend muss die Zertifizierungsstelle überprüfen), auf welcher rechtlichen Grundlage der Drittlandtransfer erfolgt. Dabei ist im Rahmen der sog. 2-Stufen-Prüfung festzustellen und zu dokumentieren, (1) ob unabhängig von spezifischen Anforderungen an den Drittlandtransfer auch alle übrigen Anforderungen an die in Rede stehende Übermittlung eingehalten werden und (2) inwiefern die spezifischen Anforderungen der Art. 44 bis 49 befolgt werden.

Erwartet wird dabei im Hinblick auf die 2. Stufe insbesondere die Darstellung, Prüfung und Dokumentation, auf welcher Übermittlungsgrundlage der Drittlandtransfer, insbesondere auch dem Umfang, der Dauer und dem Zweck nach erfolgt.

In Betracht kommen dabei folgende Grundlagen eines Drittlandtransfers:

1. Ein Angemessenheitsbeschluss der Kommission im Sinne des Art. 45;
2. geeignete Garantien im Sinne des Art. 46 (ggf. i. V. m. 47);
3. (eng auszulegende) Ausnahmen gem. Art. 49,

jeweils unter Beachtung insbesondere der behördlichen Praxis, der Entwicklungen in Bezug auf die Feststellung des angemessenen Schutzniveaus und der Rechtsprechung (wie z. B. des „Schrems II"-Urteils des EuGH[14]).

## 2.11 Rechte der betroffenen Personen

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

[14] Urteil des Europäischen Gerichtshofs vom 16. Juli 2020 (Rechtssache C311/18).

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.[15]

[15] 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/datenschutz/datenschutzmodell/).

# 4 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 (engl. European Data Protection Board) |
| gem. | gemäß |
| IDPS | Intrusion Detection Prevention Systems |
| ISMS | Information Security Management System |
| ITIL | Information Technology Infrastructure Library |
| KRITIS | Kritische Infrastrukturen |
| PDCA-Zyklus | Plan-Do-Check-Act, Deming-Kreis |
| 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.