European Privacy Seal

– privacy at its best

EuroPriSe-Kriterienkatalog

für die Zertifizierung von Verarbeitungsvorgängen von Auftragsverarbeitern (Anwendungsbereich: DE)

v3.0

EuroPriSe-Kriterienkatalog

Verarbeitungsvorgänge von Auftragsverarbeitern

(v3.0 – Veröffentlichungsdatum: Vertraulicher Entwurf, noch nicht veröffentlicht)

Änderungsgrund bzw. -gründe für die Erstellung dieser neuen Version:

- Umsetzung der Empfehlungen des Europäischen Datenschutzausschusses (EDSA) in seiner Stellungnahme 25/2022 zum Kriterienkatalog für Auftragsverarbeiter der EuroPriSe Cert GmbH.

EuroPriSe Cert GmbH

Joseph-Schumpeter-Allee 25 – D-53227 Bonn

Inhaltsverzeichnis

Einleitung

Dieses Dokument beinhaltet die EuroPriSe-Zertifizierungskriterien für ein nationales Zertifizierungsprogramm für Deutschland zur Zertifizierung von Verarbeitungsvorgängen von Auftragsverarbeitern.[1] Gegenstand von Zertifizierungen, auf die dieser Kriterien- bzw. Anforderungskatalog Anwendung findet, sind Verarbeitungsvorgänge, die in Produkten, Prozessen und Dienstleistungen oder mit Hilfe von (auch mehreren) Produkten und Dienstleistungen erbracht werden, und bezüglich derer der Zertifizierungskunde als Auftragsverarbeiter einzustufen ist.

Der Anwendungsbereich dieses Kriterienkatalogs ist nicht auf bestimmte Arten von Verarbeitungsvorgängen beschränkt. Vielmehr ermöglicht die einer Evaluation nach EuroPriSe zugrundeliegende (bzw. zu legende) Methodik[2] eine Zertifizierung jeglicher Verarbeitungsvorgänge von Auftragsverarbeitern. Es handelt sich hierbei folglich um einen allgemeingültigen methodischen Ansatz, auf dessen Grundlage eine Vielzahl sehr verschiedener Verarbeitungsvorgänge zertifiziert werden können. Deshalb ist es von fundamentaler Bedeutung, dass die methodischen Vorgaben beachtet werden, weil nur so eine einheitliche Anwendung der Zertifizierungskriterien und ein vergleichbares Maß an Prüftiefe über verschiedene Zertifizierungsverfahren hinweg sichergestellt werden können. Letztlich geht es hier darum, ein möglichst hohes Maß an Vergleichbarkeit und Reproduzierbarkeit der erteilten Zertifizierungen und ihrer Ergebnisse zu garantieren.[3]

Verarbeitungsvorgänge von Auftragsverarbeitern können nur für einen einzelnen oder einige wenige Kunden/Auftraggeber[4] erbracht werden. Häufig wird es aber um Verarbeitungsvorgänge gehen, die von einer Vielzahl von Auftraggebern in Anspruch genommen werden.[5] Nicht zuletzt deshalb spielen im Rahmen einer Zertifizierung nach EuroPriSe nicht nur die gesetzlichen Verpflichtungen des Zertifizierungskunden als Auftragsverarbeiter[6] eine Rolle, sondern es wird stets auch im Sinne einer weiten Auslegung

[1] Die Anforderungen, die an Verarbeitungsvorgänge von Verantwortlichen zu stellen sind, sind nicht Gegenstand des vorliegenden Dokuments, sondern werden in einem eigenständigen Kriterienkatalog für Verarbeitungsvorgänge von Verantwortlichen aufgelistet. Grundsätzliche Informationen zu den Beteiligten eines Zertifizierungsverfahrens und verbindliche Regeln zum Ablauf eines solchen Verfahrens sind der Verfahrensordnung für die Zertifizierung von Verarbeitungsvorgängen von Verantwortlichen und Auftragsverarbeitern zu entnehmen, die gegenwärtig in der Version 2.1 vorliegt.

[2] Die methodischen Anforderungen, bei denen es sich um Anforderungen an die Konformitätsbewertungstätigkeit handelt, sind Gegenstand eines separaten Dokuments. Dieses Kompendium der Methodik von Evaluationen nach EuroPriSe für Verarbeitungsvorgänge von Auftragsverarbeitern (kurz: Methodik-Kompendium AV) liegt gegenwärtig in der Version 2.1 vor. Es wird ergänzt durch das Dokument „EuroPriSe-Matrix zu Evaluierungsarten und – methoden gemäß ISO/IEC 17067 T. 6.5.1 lit. b) und g)“ (kurz: Matrix Evaluationsmethoden AV). Dieses Dokument liegt gegenwärtig ebenfalls in der Version 2.1 vor.

[3] Dies stellt im Kontext des europäischen Datenschutzrechts deshalb eine besondere Herausforderung dar, weil hier die Auslegung unbestimmter Rechtsbegriffe (z. B. „angemessene technische und organisatorische Maßnahmen“) und die Vornahme von Interessenabwägungen eine wichtige Rolle spielen.

[4] In der Regel wird es sich bei diesen um Verantwortliche im Sinne des Art. 4 Nr. 7 DSGVO handeln.

[5] z. B. SaaS-Dienstleitungen zur Speicherung bzw. zum Austausch von Dokumenten und Daten in der – öffentlichen – Cloud

[6] Die Verantwortung für die Einhaltung der Vorschriften der DSGVO liegt beim Verantwortlichen (vgl. Artt. 5 Abs. 2, 24 DSGVO). Den Auftragsverarbeiter treffen hingegen „nur“ spezifische gesetzliche Verpflichtungen wie die Pflicht zum Führen eines Verzeichnisses von Verarbeitungstätigkeiten (Art. 30 Abs. 2 DSGVO), die Pflicht zur Benennung eines

der Grundsätze Datenschutz durch Technikgestaltung und Datenschutz durch datenschutzfreundliche Voreinstellungen geprüft, ob der Auftragsverarbeiter seinen Kunden die datenschutzkonforme Inanspruchnahme der zu zertifizierenden Verarbeitungsvorgänge leicht macht[7].

Es ist wichtig klarzustellen, dass Unterauftragsverarbeiter, die von einem Auftragsverarbeiter, der eine Zertifizierung beantragt, eingesetzt werden, nicht im Rahmen des EuroPriSe-Zertifizierungsprogramms zertifiziert werden können. Vielmehr sind nur die vom Verarbeiter durchgeführten Verarbeitungsvorgänge Gegenstand der Zertifizierung.

Dieses Dokument listet die Zertifizierungskriterien für Verarbeitungsvorgänge von Auftragsverarbeitern auf. Die Kriterien werden als solche durch die Überschriften "Anforderung in Kürze" und "Anforderung im Detail" kenntlich gemacht.

Darüber hinaus gibt es Orientierungshilfen dazu, wie diese Anforderungen im Hinblick auf einen konkreten Zertifizierungsgegenstand anzuwenden bzw. auszulegen sind. Insoweit werden auf Ebene der einzelnen Anforderungen insbesondere einschlägige Urteile des Europäischen Gerichtshofs (EuGH) und höchstrichterliche Rechtsprechung auf mitgliedstaatlicher Ebene[8] sowie relevante Veröffentlichungen des Europäischen Datenschutzausschusses (EDSA) und von nationalen Datenschutzaufsichtsbehörden[9] aufgelistet. Diese Hinweise sind nicht Bestandteil der Zertifizierungskriterien als solcher. Sie sind vielmehr lediglich als eine Orientierungshilfe für die Nutzer dieses Kriterienkatalogs gedacht. Dies bedeutet, dass im Rahmen eines jeden Zertifizierungsverfahrens eine tagesaktuelle Analyse der rechtlichen Rahmenbedingungen durchzuführen und im Evaluationskonzept des Evaluationsteams der Zertifizierungsstelle und später auch in dessen Prüfbericht zu dokumentieren ist.[10] Nur so kann sichergestellt werden, dass im Rahmen eines Zertifizierungsverfahrens aktuelle Rechtsprechung und Veröffentlichungen von Datenschutzaufsichtsbehörden in der jeweils aktuell gültigen Fassung berücksichtigt werden. Entsprechendes gilt auch für die Ermittlung des zum Zeitpunkt eines Zertifizierungsverfahrens geltenden Stands der Technik.

Hinweis: Dieses Dokument enthält Hyperlinks auf diverse Leitlinien des EDSA. Die meisten dieser Leitlinien liegen in einer deutschen Übersetzung vor. Wo dies nicht der Fall ist, wird der englische Titel des jeweiligen Dokuments angegeben und auf die englischsprachige Version des Dokuments verlinkt.

Datenschutzbeauftragten (Art. 37 DSGVO), die Pflicht zur Implementierung angemessener technischer und organisatorischer Maßnahmen (Art. 32 DSGVO) oder auch bestimmte Pflichten gegenüber dem Verantwortlichen (vgl. etwa Art. 33 Abs. 2 DSGVO). Übermittelt der Auftragsverarbeiter personenbezogene Daten in Drittländer oder an internationale Organisationen, so muss er auch die Einhaltung der in Kapitel V der DSGVO niedergelegten Grundsätze sicherstellen. Schließlich ist nicht nur der Verantwortliche, sondern auch der Auftragsverarbeiter dafür verantwortlich, dass es einen Vertrag oder einen anderen Rechtsakt gibt, der die Auftragsverarbeitung regelt (Art. 28 Abs. 3 DSGVO).

[7] Hierzu vgl. insbesondere Kapitel 1.5 dieses Kriterienkatalogs.

[8] In dieser Version des Kriterienkatalogs wird dies auf Entscheidungen deutscher oberster Gerichte beschränkt.

[9] In dieser Version des Kriterienkatalogs wird dies auf Veröffentlichungen der Datenschutzkonferenz (DSK), des Gremiums der deutschen Datenschutzaufsichtsbehörden, beschränkt.

[10] Ausführliche Informationen hierzu enthält Kapitel 5 des Methodik-Kompendiums AV (vgl. obige Fn. 2).

Sofern vorhanden, werden zu jeder Anforderung auch bereichsspezifische nationale Rechtsvorschriften aufgeführt, die im Hinblick auf die betreffende Anforderung (gegebenenfalls) zu berücksichtigen sind.[11]

Schließlich enthält dieses Dokument auch Orientierungshilfen zur Überprüfung der Einhaltung jeder einzelnen Anforderung. So wird etwa stets aufgelistet, welche Dokumente für die rechtliche und technische Evaluation einer Anforderung typischerweise relevant sind und welche Evaluationsmethoden im Hinblick auf eine Anforderung als geeignet bzw. unverzichtbar erscheinen. Nähere Informationen zu Letzterem lassen sich der Matrix Evaluationsmethoden AV entnehmen.[12] Auch insoweit gilt aber, dass die finale Festlegung der zu prüfenden Dokumente und der zur Anwendung zu bringenden Evaluationsmethoden stets im Hinblick auf den konkreten Zertifizierungsgegenstand erfolgen muss und im Evaluationskonzept zu dokumentieren ist.[13]

Orientierungshilfen werden stets als solche bezeichnet und darstellungstechnisch besonders hervorgehoben.

Der Anforderungskatalog ist in drei zentrale Komplexe unterteilt: Anforderungen aus rechtlicher Sicht, Anforderungen aus technisch-organisatorischer Sicht und Rechte der betroffenen Personen. Nähere Informationen zu dieser Aufteilung finden sich zu Beginn des nächsten Kapitels dieses Dokuments.

Das vorliegende Dokument richtet sich in erster Linie an die folgenden Adressaten:

- Auftragsverarbeiter, die eine Zertifizierung nach EuroPriSe anstreben,
- Datenschutzexperten, die gegebenenfalls von einem solchen Auftragsverarbeiter damit beauftragt werden, ihn bei der Vorbereitung auf eine Evaluation nach EuroPriSe zu unterstützen,
- Mitarbeiter der EuroPriSe-Zertifizierungsstelle, die für die Durchführung der rechtlichen und technischen Evaluation bzw. für die Bewertung der Ergebnisse einer solchen Prüfung und/oder die Zertifizierungsentscheidung verantwortlich sind, und
- Mitarbeiter der zuständigen Aufsichtsbehörde, die deren Kompetenzen im Hinblick auf Zertifizierungen, die von Zertifizierungsstellen im Sinne des Art. 43 DSGVO erteilt werden, ausüben.

[11] In dieser Version des Dokuments beschränkt sich die Auflistung bereichsspezifischer nationaler Vorschriften auf solche des deutschen Rechts. Auch hierbei handelt es sich letztlich lediglich um eine Hilfestellung, die nicht von der Durchführung einer tagesaktuellen Analyse der rechtlichen Rahmenbedingungen und deren Dokumentation entbindet.

[12] Vgl. hierzu schon obige Fn. 2.

[13] Vgl. insoweit Kapitel 3 und Kapitel 8-12 des Methodik-Kompendiums AV.

EuroPriSe-Zertifizierungskriterien für Verarbeitungsvorgänge von Auftragsverarbeitern

Dieser Kriterienkatalog enthält die Zertifizierungskriterien für Verarbeitungsvorgänge von Auftragsverarbeitern.

Er ist in drei Kapitel unterteilt:

- Kapitel 1: Anforderungen aus rechtlicher Sicht
- Kapitel 2: Anforderungen aus technisch-organisatorischer Sicht
- Kapitel 3: Rechte der betroffenen Personen

Kapitel 1 adressiert die Anforderungen, die aus rechtlicher Sicht an Verarbeitungsvorgänge von Auftragsverarbeitern zu stellen sind. Neben eher formalen Anforderungen wie der Pflicht zur Benennung eines Datenschutzbeauftragten oder zum Führen eines Verzeichnisses von Verarbeitungstätigkeiten sind insbesondere auch die rechtlichen Anforderungen im Hinblick auf das Verhältnis Verantwortlicher – Auftragsverarbeiter sowie auf das Verhältnis Auftragsverarbeiter – weitere(r) Auftragsverarbeiter (sofern einschlägig) Gegenstand dieses Kapitels. Darüber hinaus sind im Rahmen einer rechtlichen Evaluierung auch Anforderungen bezüglich spezieller Verarbeitungsvorgänge wie z. B. einer Übermittlung personenbezogener Daten in Drittländer (sofern einschlägig) zu betrachten. Ebenfalls Gegenstand dieses Kapitels sind Anforderungen, die im Sinne einer weiten Auslegung der Grundsätze Datenschutz durch Technikgestaltung und Datenschutz durch datenschutzfreundliche Voreinstellungen vom Zertifizierungskunden Maßnahmen verlangen, die dessen Auftraggebern (sprich: den Verantwortlichen) die rechtskonforme Inanspruchnahme der Verarbeitungsvorgänge leicht machen.

Das zweite Kapitel enthält die Anforderungen, die aus technisch-organisatorischer Sicht an Verarbeitungsvorgänge von Auftragsverarbeitern zu stellen sind. Die Einhaltung dieser Anforderungen ist nicht nur im Hinblick auf den Zertifizierungskunden selbst, sondern auch im Hinblick auf weitere Auftragsverarbeiter zu überprüfen. Dabei ist insbesondere auch den Ergebnissen der in Vorbereitung der Evaluation durchzuführenden Risikoanalyse[14] Rechnung zu tragen.

Gegenstand des dritten Kapitels sind schließlich die Rechte der betroffenen Personen. Die hier aufgelisteten Anforderungen betreffen die Pflicht des Zertifizierungskunden als Auftragsverarbeiter, die Verantwortlichen dabei zu unterstützen, ihrer Verpflichtung zur Beantwortung von Anträgen auf Wahrnehmung der in Kapitel III der DSGVO genannten Rechte der betroffenen Personen nachzukommen.

Nachfolgend wird das Schlüsselwort MUSS verwendet. MUSS bezeichnet eine zwingende Anforderung.

[14] Vgl. hierzu Kapitel 4 des Methodik-Kompendiums AV.

1. Anforderungen aus rechtlicher Sicht

Dieses Kapitel ist wie folgt strukturiert:

- Allgemeine Anforderungen an Auftragsverarbeiter,
- Anforderungen im Hinblick auf Art. 28 DSGVO (Verhältnis Auftragsverarbeiter – Verantwortlicher),
- Anforderungen im Hinblick auf Art. 28 DSGVO (Verhältnis Auftragsverarbeiter – weiterer Auftragsverarbeiter),
- Anforderungen bzgl. spezieller Arten von Verarbeitungsvorgängen und
- Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen.

1.1. Allgemeine Anforderungen an Auftragsverarbeiter

1.1.1. Verzeichnis der Verarbeitungstätigkeiten

Anforderung in Kürze:

Der Auftragsverarbeiter MUSS in jedem Fall ein Verzeichnis von Verarbeitungstätigkeiten gem. Art. 30 Abs. 2 DSGVO führen, unabhängig davon, ob die Ausnahmevorschrift des Art. 30 Abs. 5 DSGVO greift. Er MUSS zudem Prozesse zur stetigen Aktualisierung des Verzeichnisses etabliert haben.

Orientierungshilfe

Relevante Artikel der DSGVO:

Art. 30 Abs. 2-5 DSGVO

Hintergrund:

Art. 30 DSGVO verpflichtet neben dem Verantwortlichen und ggf. den Vertretern von nicht in der EU niedergelassenen Verantwortlichen oder Auftragsverarbeitern auch den Auftragsverarbeiter dazu, ein Verzeichnis von Verarbeitungstätigkeiten zu führen, die seiner Zuständigkeit unterliegen. Diese Pflicht zum Führen eines Verarbeitungsverzeichnisses dient dem Nachweis der Einhaltung der DSGVO (vgl. Erwägungsgrund 82 der DSGVO).

Für den erfolgreichen Abschluss einer Zertifizierung von Verarbeitungsvorgängen nach EuroPriSe genügt es, wenn die Evaluation und die nachfolgende Bewertung zum Ergebnis haben, dass der Auftragsverarbeiter ein Verarbeitungsverzeichnis führt, das sich auf die zu zertifizierenden Verarbeitungsvorgänge bezieht, sowie Prozesse zur stetigen Aktualisierung dieses Verzeichnisses etabliert hat, und insoweit alle nachfolgend unter „Details“ aufgelisteten Einzelanforderungen erfüllt werden[15].

[15] Eine Überprüfung, ob der Auftragsverarbeiter seine Verpflichtung nach Art. 30 Abs. 2 DSGVO auch im Hinblick auf Verarbeitungsvorgänge erfüllt, die nicht vom ToE umfasst sind, findet im Rahmen einer solchen Zertifizierung hingegen nicht statt. Dies deshalb, da ja nur bestimmte Verarbeitungsvorgänge, nicht aber die Organisation als Ganzes bzw. deren Datenschutzmanagementsystem Gegenstand der Zertifizierung sind.

Ende der Orientierungshilfe

Anforderung im Detail:

Voraussetzungen für die / Ausnahmen von der Anwendbarkeit der Anforderung:

Diese Anforderung gilt immer, auch wenn die Ausnahmevorschrift des Art. 30 Abs. 5 DSGVO greifen sollte.

Details zum Gegenstand der Anforderung:

Folgende Einzelanforderungen müssen erfüllt sein:

1. Das Verzeichnis von Verarbeitungstätigkeiten, das sich auf die zu zertifizierenden Verarbeitungsvorgänge bezieht, MUSS schriftlich geführt werden, was auch in einem elektronischen Format erfolgen kann.

2. Das Verzeichnis MUSS den Namen und die Kontaktdaten des Auftragsverarbeiters sowie gegebenenfalls seines Vertreters (vgl. Art. 27 DSGVO) und/oder eines etwaigen Datenschutzbeauftragten (Art. 37 ff. DSGVO) enthalten. Insoweit MÜSSEN jeweils Angaben zur postalischen, telefonischen und elektronischen Erreichbarkeit gemacht werden.

3. Das Verzeichnis muss den Namen und die Kontaktdaten jedes Verantwortlichen, in dessen Auftrag der Auftragsverarbeiter tätig ist, sowie gegebenenfalls seines Vertreters (vgl. Art. 27 DSGVO) und/oder eines etwaigen Datenschutzbeauftragten (Art. 37 ff. DSGVO) enthalten.[16] Auch insoweit MÜSSEN jeweils Angaben zur postalischen, telefonischen und elektronischen Erreichbarkeit gemacht werden.

4. Das Verzeichnis MUSS die Kategorien von Verarbeitungen enthalten, die Gegenstand der Zertifizierung nach EuroPriSe sind.[17]

5. Das Verzeichnis MUSS – sofern einschlägig – Informationen zu Übermittlungen von personenbezogenen Daten an ein Drittland oder an eine internationale Organisation, einschließlich der Angabe des betreffenden Drittlands oder der betreffenden internationalen Organisation enthalten. Werden Daten an ein Drittland übermittelt, MÜSSEN zudem die konkreten Datenempfänger im Drittland angegeben werden. Erfolgen die Übermittlungen auf Grundlage des Art. 49 Abs. 1 UAbs. 2 DSGVO, ist auch die Dokumentierung der vorgesehenen geeigneten Garantien aufzuführen.

6. Das Verzeichnis MUSS eine allgemeine Beschreibung der technischen und organisatorischen Maßnahmen (TOM) gem. Art. 32 Abs. 1 DSGVO enthalten, die im Hinblick auf die zu zertifizierenden Verarbeitungsvorgänge getroffen worden sind. Insoweit genügt der spezifische Verweis auf ein separates Dokument, in dem die TOM beschrieben werden.

[16] Da wo der Zertifizierungskunde als Subunternehmer tätig wird (falls überhaupt), muss er nur seine direkten Auftraggeber benennen, nicht hingegen auch die dahinterstehende weitere Kette bis zu den Verantwortlichen zurück.

[17] Andere Verarbeitungstätigkeiten, die der Zertifizierungskunde ggf. auch im Auftrag der Verantwortlichen erbringt, sind für das konkrete Zertifizierungsverfahren hingegen irrelevant, und können deshalb weggelassen bzw. im Verzeichnis geschwärzt werden.

7. Der Auftragsverarbeiter MUSS Prozesse zur stetigen Aktualisierung des Verzeichnisses etabliert haben für den Fall, dass

- Kategorien von im Auftrag durchgeführten Verarbeitungstätigkeiten eingeführt werden bzw. wegfallen,
- zusätzliche Verantwortliche, in deren Auftrag eine Verarbeitung durchgeführt wird, hinzukommen bzw. wegfallen,
- sich bei bereits aufgeführten Kategorien von Verarbeitungstätigkeiten und / oder bestehenden Verantwortlichen, in deren Auftrag eine Verarbeitung durchgeführt wird, Angaben nach Art. 30 Abs. 2 lit. a)-d) DSGVO ändern.

8. Der Auftragsverarbeiter MUSS Prozesse etabliert haben, die die Zusammenarbeit der im Hinblick auf die Aktualisierung des Verzeichnisses (vgl. obige Nr. 7) relevanten Akteure regeln (zu nennen sind insoweit: Fachabteilungen des Auftragsverarbeiters, die an den zu zertifizierenden Verarbeitungstätigkeiten beteiligt sind, ggf. der Vertreter und/oder der Datenschutzbeauftragte des Auftragsverarbeiters und Verantwortliche, in deren Auftrag die Verarbeitungsvorgänge durchgeführt werden).

Ggf.: Relevantes Nationales Recht:

N/A

Orientierungshilfe

Relevante Dokumente:

1. Verzeichnis der Verarbeitungstätigkeiten

2. Ggf. separate Dokumente:
Auflistung der Verantwortlichen und Beschreibung der implementierten TOM

Relevante Evaluationsmethoden:

Dokumentenprüfung, Interviews

Anwendungs-/Auslegungshilfen:

- Art. 29 WP (vom EDSA bestätigt): POSITION PAPER on the derogations from the obligation to maintain records of processing activities pursuant to Article 30(5) GDPR
- DE: Kurzpapier Nr. 1 der DSK
- DE: Hinweise zum Verzeichnis von Verarbeitungstätigkeiten, Art. 30 DS-GVO der DSK
- DE: Muster eines Verzeichnisses von Verarbeitungstätigkeiten eines Auftragsverarbeiters der DSK

Ende der Orientierungshilfe

1.1.2. Benennung eines Datenschutzbeauftragten

Anforderung in Kürze:

Der Auftragsverarbeiter MUSS einen Datenschutzbeauftragten benannt und dies dokumentiert haben, wenn ihn nach Art. 37 DSGVO oder nach ggf. einschlägigen nationalen Rechtsnormen eine Benennungspflicht trifft. In diesem Fall MUSS der Auftragsverarbeiter

auch die Anforderungen an die fachlichen Qualifikationen des DSB sowie die unten unter "Anforderung im Detail" aufgeführten organisatorischen Anforderungen einhalten.

Orientierungshilfe

Relevante Artikel der DSGVO:

Art. 37 ff. DSGVO

Hintergrund:

Art. 37 Abs. 1 DSGVO verpflichtet neben dem Verantwortlichen auch den Auftragsverarbeiter dazu, unter bestimmten Voraussetzungen einen Datenschutzbeauftragten (DSB) zu benennen. Dieser soll den Auftragsverarbeiter als interne Kontrollinstanz bei der Überwachung der Einhaltung der DSGVO unterstützen (vgl. Erwägungsgrund 97 der DSGVO). Wegen der Öffnungsklausel zur Benennungspflicht (Art. 37 Abs. 4 S. 1, 2 Hs. DSGVO) spielt für die Beantwortung der Frage, ob diese Anforderung eingehalten wird, auch nationales Recht eine Rolle.

Ende der Orientierungshilfe

Anforderung im Detail:

Voraussetzungen für die / Ausnahmen von der Anwendbarkeit der Anforderung:

Der Auftragsverarbeiter MUSS einen Datenschutzbeauftragten benennen, wenn zumindest eine der folgenden Aussagen zutrifft:

1. Der Auftragsverarbeiter ist eine Behörde oder öffentliche Stelle nach Maßgabe des nationalen Rechts, mit Ausnahme von Gerichten, die im Rahmen ihrer justiziellen Tätigkeit handeln.
2. Die Kerntätigkeit[18] des Auftragsverarbeiters besteht in der Durchführung von Verarbeitungsvorgängen, die aufgrund ihrer Art, ihres Umfangs und/oder ihrer Zwecke eine umfangreiche regelmäßige und systematische Überwachung von betroffenen Personen erforderlich macht.

   Eine Überwachung ist "regelmäßig", wenn eines oder mehrere der folgenden Merkmale gegeben sind:

   - fortlaufend oder in bestimmten Abständen während eines bestimmten Zeitraums vorkommend;
   - immer wieder oder wiederholt zu bestimmten Zeitpunkten auftretend;
   - ständig oder regelmäßig stattfindend.

   Eine Überwachung ist „systematisch“, wenn eines oder mehrere der folgenden Merkmale gegeben sind:

   - systematisch vorkommend;
   - vereinbart, organisiert oder methodisch;

[18] Als „Kerntätigkeit“ lassen sich die wichtigsten Arbeitsabläufe betrachten, die zur Erreichung der Ziele des Auftragsverarbeiters erforderlich sind. Dazu gehören auch sämtliche Tätigkeiten, bei denen die Verarbeitung von Daten einen untrennbaren Bestandteil der Tätigkeit des Auftragsverarbeiters darstellt.

- im Rahmen eines allgemeinen Datenerfassungsplans erfolgend;
- im Rahmen einer Strategie erfolgend.

Eine „umfangreiche Verarbeitung“ liegt vor, wenn eines oder mehrere der folgenden Merkmale gegeben sind:

- Die Zahl der betroffenen Personen ist groß – entweder als bestimmte Zahl oder als Anteil an der maßgeblichen Bevölkerung;
- Das Datenvolumen und/oder das Spektrum an in Bearbeitung befindlichen Daten ist groß;
- Die Dauer oder Permanenz der Datenverarbeitungstätigkeit ist groß bzw. lang;
- Die geografische Ausdehnung der Verarbeitungstätigkeit ist groß.

3. Die Kerntätigkeit[19] des Auftragsverarbeiters besteht in der umfangreichen Verarbeitung besonderer Kategorien von Daten oder von personenbezogenen Daten über strafrechtliche Verurteilungen und Straftaten.

   Zum Begriff der "umfangreichen Verarbeitung" siehe die vorhergehende Aufzählungsnummer.

4. Der Auftragsverarbeiter unterliegt dem Recht eines oder mehrerer Mitgliedstaaten, das ihn dazu verpflichtet, einen Datenschutzbeauftragten zu benennen (vgl. insoweit die Angaben unter „Relevantes Nationales Recht“).

Details zum Gegenstand der Anforderung:

1. Die Benennung des Datenschutzbeauftragten MUSS dokumentiert werden.
2. Der Auftragsverarbeiter MUSS den Datenschutzbeauftragten auf der Grundlage der folgenden beruflichen Qualifikationen benennen:
   - Fachkompetenz auf dem Gebiet des nationalen und europäischen Datenschutzrechts und der Datenschutzpraxis, einschließlich eines umfassenden Verständnisses der DS-GVO
   - Verständnis der jeweils durchgeführten Verarbeitungsvorgänge
   - Kenntnisse in den Bereichen IT und Datensicherheit
   - Kenntnis der jeweiligen Branche und Einrichtung
   - die Fähigkeit, eine Datenschutzkultur innerhalb der Einrichtung zu fördern.
3. Der Auftragsverarbeiter MUSS
   - die Kontaktdaten des Datenschutzbeauftragten veröffentlichen und damit sicherstellen, dass die betroffenen Personen den DSB kontaktieren können;
   - die Kontaktdaten des Datenschutzbeauftragten an die zuständige Aufsichtsbehörde übermitteln und damit sicherstellen, dass die Aufsichtsbehörden den behördlichen Datenschutzbeauftragten kontaktieren können.

[19] Vgl. die vorangegangene Fußnote.

4. Der Auftragsverarbeiter MUSS sicherstellen, dass der Datenschutzbeauftragte:
    - von Anfang an in alle Fragen des Schutzes personenbezogener Daten einbezogen wird, insbesondere in Bezug auf die zu zertifizierenden Verarbeitungsvorgänge;
    - über Zeit, finanzielle Mittel und Zugang zu Ausrüstung/Abteilungen und Dokumenten verfügt, um seine Aufgaben zu erfüllen und sein Fachwissen aufrechtzuerhalten;
    - unabhängig handeln kann, keine Anweisungen bzgl. der Ausübung seiner gesetzlichen Aufgaben erhält und wegen der Erfüllung dieser Aufgaben nicht abberufen oder benachteiligt wird;
    - regelmäßig und direkt dem leitenden Management des Auftragsverarbeiters Bericht erstatten kann;
    - nicht an Aufgaben und Pflichten beteiligt ist, die dazu führen, dass er den Zweck und die Mittel der Verarbeitung personenbezogener Daten bestimmt, und somit zu einem Interessenkonflikt führen würden;
    - mit der zuständigen Aufsichtsbehörde zusammenarbeitet und als zentrale Anlaufstelle fungiert, um den Zugang der Aufsichtsbehörden zu Dokumenten und Informationen sowie die Ausübung ihrer Untersuchungs-, Korrektur- und Beratungsbefugnisse zu erleichtern (vgl. hierzu auch nachfolgendes Kapitel 1.1.4).

Ggf.: Relevantes Nationales Recht:

DE: § 38 Abs. 1 BDSG sieht eine Benennungspflicht für nichtöffentliche Stellen vor, wenn zumindest eine der nachfolgenden Konstellationen vorliegt: Der Auftragsverarbeiter

- beschäftigt in der Regel mindestens 20 Personen ständig mit der automatisierten Verarbeitung personenbezogener Daten,
- nimmt Verarbeitungen vor, die einer Datenschutzfolgen-Abschätzung unterliegen, oder
- verarbeitet personenbezogene Daten geschäftsmäßig zum Zweck der Übermittlung, der anonymisierten Übermittlung oder für Zwecke der Markt- oder Meinungsforschung.

Orientierungshilfe

Relevante Dokumente:

1. Nachweis bzgl. der Benennung eines Datenschutzbeauftragten (z. B. Benennungsurkunde)

2. Soweit vorhanden: Dokumentation der vom Auftragsverarbeiter durchgeführten Analyse, ob eine Pflicht zur Benennung eines Datenschutzbeauftragten vorliegt

Relevante Evaluationsmethoden:

Dokumentenprüfung, Interviews

Anwendungs-/Auslegungshilfen:

- Art. 29 WP (vom EDSA bestätigt): Leitlinien in Bezug auf Datenschutzbeauftragte („DSB“) (WP 243 rev. 01) (vgl. Kapitel 2: „Benennung eines DSB“)
- DE: Kurzpapier Nr. 12 der DSK

Ende der Orientierungshilfe

1.1.3. Benennung eines Vertreters in der Europäischen Union

Anforderung in Kürze:

Hat der Auftragsverarbeiter keine Niederlassung in der Europäischen Union (EU) bzw. dem Europäischen Wirtschaftsraum (EWR), MUSS er schriftlich einen Vertreter in der EU benannt haben, wenn im Hinblick auf die zu zertifizierenden Verarbeitungsvorgänge der räumliche Anwendungsbereich der DSGVO nach deren Art. 3 Abs. 2 eröffnet ist und keiner der beiden in Art. 27 Abs. 2 DSGVO aufgelisteten Ausnahmefälle vorliegt.

Orientierungshilfe

Relevante Artikel der DSGVO:

Art. 3 Abs. 2, Art. 4 Nr. 17 und Art. 27 DSGVO

Hintergrund:

Art. 27 Abs. 1 DSGVO verpflichtet neben dem Verantwortlichen auch den Auftragsverarbeiter, der keine Niederlassung in der EU hat, grundsätzlich zur Benennung eines Vertreters in der EU, wenn er betroffenen Personen in der Union Waren oder Dienstleistungen anbietet oder wenn er das Verhalten betroffener Personen in der EU beobachtet. Dies dient der Durchsetzung des Marktortprinzips und damit der Geltung und Durchsetzung der DSGVO in Drittländern. Konkret soll dieser Vertreter es als Anlaufstelle des Auftragsverarbeiters in der EU einerseits den betroffenen Personen ermöglichen, ihre Rechte wirksam geltend zu machen, und andererseits die Aufsichtsbehörden in die Lage versetzen, ihre Aufsichtsmaßnahmen effektiv durchzusetzen.

Im Rahmen einer Zertifizierung nach EuroPriSe ist in Fällen, in denen der Auftragsverarbeiter keine Niederlassung in der EU / dem EWR hat, bereits zu Beginn des Zertifizierungsverfahrens zu prüfen, ob die DSGVO auf die zu zertifizierenden Verarbeitungsvorgänge überhaupt Anwendung findet. Ist dies nicht der Fall, kommt eine Zertifizierung im Sinne des Art. 42 f. DSGVO nicht in Betracht. Anderenfalls ist die vorliegende Anforderung grundsätzlich[20] anwendbar.

Ende der Orientierungshilfe

Anforderung im Detail:

Voraussetzungen für die / Ausnahmen von der Anwendbarkeit der Anforderung:

Ist der Auftragsverarbeiter nicht in der EU niedergelassen, MUSS er grundsätzlich einen Vertreter in der EU benennen, wenn er personenbezogene Daten von Personen, die sich in der Union befinden, verarbeitet, und die Verarbeitung mit zumindest einer der beiden nachfolgenden Konstellationen im Zusammenhang steht:

[20] Die in Art. 27 Abs. 2 DSGVO aufgelisteten Ausnahmefälle bleiben unberührt (s.u.).

1. Der Auftragsverarbeiter bietet betroffenen Personen in der Union Waren oder Dienstleistungen an,
2. Der Auftragsverarbeiter beobachtet das Verhalten betroffener Personen, soweit ihr Verhalten in der Union erfolgt.

Die Benennungspflicht besteht allerdings dann nicht, wenn zumindest eine der beiden nachfolgenden Ausnahmen einschlägig ist (vgl. Art. 27 Abs. 2 DSGVO):

1. Die zu zertifizierenden Verarbeitungsvorgänge
   - erfolgen nur gelegentlich[21],
   - haben keine umfangreiche Verarbeitung besonderer Kategorien personenbezogener Daten oder personenbezogener Daten über strafrechtliche Verurteilungen und Straftaten zum Gegenstand und
   - führen unter Berücksichtigung der Art, der Umstände, des Umfangs und der Zwecke der Verarbeitung voraussichtlich nicht zu einem Risiko für die Rechte und Freiheiten natürlicher Personen.
2. Bei dem Auftragsverarbeiter handelt es sich um eine Behörde oder öffentliche Stelle.

Details zum Gegenstand der Anforderung:

Folgende Einzelanforderungen MÜSSEN erfüllt sein:

1. Der Auftragsverarbeiter MUSS den Vertreter in der EU schriftlich benennen.
2. Der von dem Auftragsverarbeiter benannte Vertreter MUSS in einem der Mitgliedstaaten niedergelassen sein, in denen die betroffenen Personen, deren personenbezogene Daten im Zusammenhang mit den ihnen angebotenen Waren oder Dienstleistungen verarbeitet werden oder deren Verhalten beobachtet wird, sich befinden.
3. Der Auftragsverarbeiter MUSS den Vertreter in der EU damit beauftragt haben, zusätzlich zu ihm selbst oder an seiner Stelle insbesondere für Aufsichtsbehörden und betroffene Personen bei sämtlichen Fragen im Zusammenhang mit den betreffenden Verarbeitungsvorgängen zur Gewährleistung der Einhaltung der DSGVO als Anlaufstelle zu dienen. Er muss dies auch entsprechend dokumentiert haben.

Darüber hinaus ist darauf hinzuweisen, dass

- bei jeder Übermittlung im Sinne von Art. 44 DSGVO an einen außerhalb der EU oder des EWR niedergelassenen Auftragsverarbeiter die in Kapitel V der DSGVO festgelegten Verpflichtungen in vollem Umfang eingehalten werden müssen;
- das vorliegende Zertifizierungsprogramm kein Programm im Sinne von Art. 46 Abs. 2 lit. f) DSGVO ist;
- falls die Zertifizierung erteilt wird, der Auftragsverarbeiter nicht dazu berechtigt ist, die Zertifizierung in einer Weise zu verwenden, die den Eindruck erwecken könnte,

[21] Hier ist darauf hinzuweisen, dass es sehr unwahrscheinlich ist, dass ein Auftragsverarbeiter Verarbeitungsvorgänge zertifizieren lässt, die nur gelegentlich erfolgen.

dass die Zertifizierung selbst ein Übermittlungsinstrument im Sinne von Art. 46 Abs. 2 lit. f) DSGVO ist.

Ggf.: Relevantes Nationales Recht:

N/A

Orientierungshilfe

Relevante Dokumente:

Nachweis bzgl. der schriftlichen Benennung eines Vertreters und seiner Beauftragung in Übereinstimmung mit Art. 27 Abs. 4 DSGVO (z. B. Benennungsurkunde)

Relevante Evaluationsmethoden:

Dokumentenprüfung, Interviews

Anwendungs-/Auslegungshilfen:

- EDSA: Leitlinien 3/2018 zum räumlichen Anwendungsbereich der DSGVO (Artikel 3) (vgl. Kapitel 4: „Vertreter von nicht in der Union niedergelassenen Verantwortlichen oder Auftragsverarbeitern“)
- DE: Kurzpapier Nr. 7 der DSK

Ende der Orientierungshilfe

1.1.4. Zusammenarbeit mit der Aufsichtsbehörde

Anforderung in Kürze:

Der Auftragsverarbeiter MUSS der Verpflichtung zur Zusammenarbeit mit der zuständigen Aufsichtsbehörde nachkommen, wie nachstehend unter "Anforderung im Detail" dargelegt.

Orientierungshilfe

Relevante Artikel der DSGVO:

Art. 31 DSGVO

Hintergrund:

Art. 31 DSGVO verpflichtet neben dem Verantwortlichen auch den Auftragsverarbeiter und ggf. dessen Vertreter dazu, auf Anfrage mit der zuständigen Aufsichtsbehörde bei der Erfüllung ihrer Aufgaben zusammenzuarbeiten. Hat der Auftragsverarbeiter einen DSB benannt, so wird dieser Ansprechpartner der Aufsichtsbehörde sein (vgl. insoweit auch Art. 39 Abs. 1 lit. d) DSGVO). Hat der Auftragsverarbeiter mangels gesetzlicher Verpflichtung hingegen keinen Datenschutzbeauftragten benannt, so muss er mindestens eine Person benennen, die für die Bearbeitung von Anfragen der zuständigen Aufsichtsbehörde verantwortlich ist.

Ende der Orientierungshilfe

Anforderung im Detail:

Voraussetzungen für die / Ausnahmen von der Anwendbarkeit der Anforderung:

Diese Anforderung ist stets anwendbar.

Details zum Gegenstand der Anforderung:

1. Der Auftragsverarbeiter MUSS mindestens eine Person benennen, die für die Zusammenarbeit mit der zuständigen Aufsichtsbehörde zuständig ist. Ist der Auftragsverarbeiter verpflichtet, einen Datenschutzbeauftragten zu benennen (vgl. hierzu bereits Kapitel 1.1.2), MUSS er die Anforderungen der nachstehenden Option 1 einhalten. Ist der Auftragsverarbeiter nicht verpflichtet, einen DSB zu benennen, MUSS er entweder die Anforderungen von Option 1 oder die von Option 2 einhalten.

   Option 1 (DSB):

   Der Auftragsverarbeiter MUSS

   a) einen Datenschutzbeauftragten benennen, der als zentrale Anlaufstelle für die Zusammenarbeit mit der zuständigen Aufsichtsbehörde fungiert;

   b) die Kontaktdaten des Datenschutzbeauftragten an die zuständige Aufsichtsbehörde übermitteln;

   c) der zuständigen Aufsichtsbehörde Änderungen mitteilen, falls ein neuer Datenschutzbeauftragter ernannt werden sollte.

   Option 2 (andere Anlaufstelle als der DSB):

   Der Auftragsverarbeiter MUSS

   a) einen Mitarbeiter oder einen Dienstleister benennen, der als zentrale Anlaufstelle für die zuständige Aufsichtsbehörde fungiert und für alle Aufgaben im Zusammenhang mit der Zusammenarbeit mit der Aufsichtsbehörde verantwortlich ist;

   b) in der Kommunikation mit den Aufsichtsbehörden und der Öffentlichkeit deutlich machen, dass es sich bei dieser Person nicht um einen Datenschutzbeauftragten handelt.

2. Der Auftragsverarbeiter MUSS die Kontaktdaten der zentralen Anlaufstelle für die Zusammenarbeit mit der zuständigen Aufsichtsbehörde veröffentlichen, um sicherzustellen, dass die Aufsichtsbehörden sie direkt erreichen können.

3. Der Auftragsverarbeiter MUSS durch einen implementierten Prozess sicherstellen, dass der DSB / die andere zentrale Anlaufstelle mit der zuständigen Aufsichtsbehörde zusammenarbeitet, als Anlaufstelle für Fragen im Zusammenhang mit der Verarbeitung personenbezogener Daten fungiert und der Aufsichtsbehörde den Zugang zu Dokumenten und Informationen sowie die Ausübung ihrer Untersuchungs-, Korrektur- und Beratungsbefugnisse ermöglicht.

Ggf.: Relevantes Nationales Recht:

N/A

Orientierungshilfe

Relevante Dokumente:

Arbeitsanweisung o.ä.

Relevante Evaluationsmethoden:

Dokumentenprüfung, Interviews

Anwendungs-/Auslegungshilfen:

N/A

Ende der Orientierungshilfe

1.2. Anforderungen im Hinblick auf Art. 28 DSGVO (Verhältnis Auftragsverarbeiter - Verantwortlicher)

1.2.1. Vorhandensein von Vertragsklauseln, die alle Anforderungen des Art. 28 DSGVO erfüllen

Anforderung in Kürze:

Szenario 1: Auftragsverarbeiter wird für eine Vielzahl von Verantwortlichen tätig

Der Auftragsverarbeiter MUSS eine Vorlage für einen Auftragsverarbeitungsvertrag mit seinen Auftraggebern (Verantwortlichen) vorhalten, die alle Anforderungen des Art. 28 DSGVO erfüllt. Zum Nachweis hierfür ist die Vertragsvorlage bei der Zertifizierungsstelle vorzulegen. In Betracht kommen insoweit individuell erstellte Vorlagen und Standardvertragsklauseln[22] (vgl. Art. 28 Abs. 6-8 DSGVO).

Darüber hinaus MUSS der Verarbeiter der Zertifizierungsstelle tatsächliche Verträge vorlegen, die auf der Vorlage basieren und von beiden Parteien unterzeichnet sind.

Es ist notwendig klarzustellen, dass die Vorlage für einen Auftragsverarbeitungsvertrag das Recht des Verantwortlichen unberührt lässt, die Klauseln nach Art. 28 DSGVO mit dem Auftragsverarbeiter auszuhandeln, ohne dass dies Auswirkungen auf die Zertifizierung hat.

Szenario 2: Auftragsverarbeiter wird nur für einen / einige wenige Verantwortliche(n) tätig

Der Auftragsverarbeiter MUSS mit jedem Verantwortlichen einen Vertrag geschlossen haben, der die Anforderungen des Art. 28 DSGVO erfüllt. Zum Nachweis hierfür ist jeweils der unterschriebene Vertrag[23] bei der Zertifizierungsstelle vorzulegen.

Orientierungshilfe

Relevante Artikel der DSGVO:

Art. 28 DSGVO

Hintergrund:

Art. 28 DSGVO regelt die inhaltlichen Anforderungen an eine Auftragsverarbeitung. Ein zentraler Aspekt ist insoweit das Erfordernis eines Auftragsverarbeitungsvertrags sowie die an diesen in inhaltlicher und formaler Hinsicht zu stellenden Anforderungen.

Zu Szenario 1 (s.o.):

Auftragsverarbeiter werden regelmäßig für eine Vielzahl von Kunden / Auftraggebern (Verantwortlichen) tätig. Wollte man im Rahmen einer Zertifizierung prüfen, ob mit allen

[22] Im Juni 2021 veröffentlichte die Europäische Kommission Standardvertragsklauseln gemäß Art. 28 Abs. 7 DSGVO, die die Anforderungen an Verträge zwischen Verantwortlichen und Auftragsverarbeitern gemäß Art. 28 Abs. 3 und 4 DSGVO erfüllen. Diese Klauseln finden sich im Anhang des entsprechenden Durchführungsbeschlusses (EU) 2021/915 der Kommission, der seit 27.06.2021 wirksam ist.

[23] Vorgelegt werden müssen nur die aus Datenschutzsicht relevanten Vertragsklauseln. Falls der jeweilige Vertrag noch weitere, datenschutzfremde Klauseln enthält, müssen diese nicht vorgelegt bzw. können die entsprechenden Passagen geschwärzt werden.

Kunden Auftragsverarbeitungsverträge geschlossen worden sind, die die Vorgaben von Art. 28 DSGVO einhalten, wäre dies regelmäßig mit einem Aufwand verbunden, der den wirtschaftlichen Rahmen einer Zertifizierung sprengen würde. Deshalb wird vorliegend ein anderer Ansatz verfolgt: Im Sinne einer weiten Auslegung der Grundsätze Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen wird von den Zertifizierungskunden verlangt, dass diese ihren Auftraggebern die datenschutzkonforme Inanspruchnahme der zu zertifizierenden Verarbeitungsvorgänge so leicht wie möglich machen.

Konkret heißt das: Um seinen Kunden die datenschutzkonforme Inanspruchnahme möglichst leicht zu machen, hat der Auftragsverarbeiter eine Vertragsvorlage zu erstellen, die alle rechtlichen Anforderungen des Art. 28 DSGVO erfüllt, was dann im Rahmen des Zertifizierungsverfahrens zu verifizieren ist. Alternativ hierzu kann der Auftragsverarbeiter auch auf Standardvertragsklauseln zurückgreifen (vgl. Art. 28 Abs. 6-8 DSGVO).

Im Rahmen eines Zertifizierungsverfahrens wird insoweit folgendes geprüft (vgl. hierzu auch die Matrix Evaluationsmethoden AV unter 1.2.1):

Falls eine individuell erstellte Vertragsvorlage verwendet wird:

- Inhaltliche Prüfung der Vertragsvorlage als solcher;
- Exemplarische Prüfung konkreter Verträge, die auf der Vertragsvorlage basieren.

Falls Standardvertragsklauseln verwendet werden:

- Prüfung, ob die Standardvertragsklauseln übernommen und keine dazu in Widerspruch stehenden Klauseln aufgenommen worden sind[24];
- Prüfung, ob der Auftragsverarbeiter ausfüllungsbedürftige Annexe / Freitextfelder, in denen z. B. die in Rede stehenden Verarbeitungsvorgänge zu beschreiben sind, ausgefüllt hat;
- Exemplarische Prüfung konkreter Verträge, die auf den verwendeten Standardvertragsklauseln basieren.

Wichtig:

Das Vorhalten einer Vertragsvorlage bedeutet nicht, dass diese dann auch stets (unverändert) zum Einsatz kommen wird bzw. gar kommen muss.[25] In jedem Fall ist stets zu gewährleisten, dass es der Verantwortliche ist, der über Zwecke und wesentliche Mittel der Verarbeitung entscheidet.[26]

[24] Ist dies der Fall, so ist keine weitere inhaltliche Überprüfung der Klauseln als solcher erforderlich.

[25] Vielmehr wird der finale Vertragstext üblicher Weise zwischen den Parteien ausgehandelt werden. Ganz grundsätzlich gilt, dass der Verantwortliche, falls er in Erwägung zieht, vom Auftragsverarbeiter gestellte Vertragsklauseln zu akzeptieren, diese vorab im Hinblick auf Art. 28 DSGVO bewerten muss. Akzeptiert er die Vertragsklauseln und nimmt er den Dienst in Anspruch, übernimmt er damit auch die volle Verantwortung für die Einhaltung der DSGVO. Diese Bewertung wird ihm nicht nur leicht gemacht, wenn der Auftragsverarbeiter Standardvertragsklauseln gem. Art. 28 Abs. 6-8 DSGVO verwendet, sondern auch, wenn dessen individuell erstellte Vertragsvorlage Gegenstand einer Zertifizierung nach EuroPriSe gewesen ist, da im Rahmen eines solchen Zertifizierungsverfahrens ausdrücklich geprüft wird, ob die Vertragsvorlage alle in Art. 28 DSGVO aufgelisteten Anforderungen erfüllt.

[26] Versuchte der Auftragsverarbeiter, seinem Vertragspartner mit Hilfe der Vertragsvorlage Entscheidungen bzw. Festlegungen insbesondere zu Art und Zweck(en) der Verarbeitung, die nur einem Verantwortlichen zustehen, zu

Zu Szenario 2 (s.o.):

Wird ein Zertifizierungskunde ausnahmsweise exklusiv nur für einen oder einige wenige Kunden tätig, ist im Rahmen einer Zertifizierung hingegen zu überprüfen, ob der Auftragsverarbeiter mit jedem Verantwortlichen einen Auftragsverarbeitungsvertrag geschlossen hat, der die Anforderungen des Art. 28 DSGVO erfüllt.

Ende der Orientierungshilfe

Anforderung im Detail:

Voraussetzungen für die / Ausnahmen von der Anwendbarkeit der Anforderung:

Diese Anforderung ist nicht anwendbar, wenn die in Rede stehende Auftragsverarbeitung nicht auf der Grundlage eines Vertrags, sondern auf der Grundlage eines anderen Rechtsinstruments nach dem Unionsrecht oder dem Recht der Mitgliedstaaten erfolgt.

Details zum Gegenstand der Anforderung:

Zu Szenario 1 (Standardvertragsklauseln):

Der Auftragsverarbeiter MUSS die Standardvertragsklauseln übernehmen und sicherstellen, dass keine dazu in Widerspruch stehenden Klauseln aufgenommen werden. Er MUSS die ausfüllungsbedürftigen Annexe / Freitextfelder der Standardvertragsklauseln ausfüllen.

Der Auftragsverarbeiter MUSS in einer Arbeitsanweisung o.ä. regeln, wie sichergestellt wird, dass die Vorgaben des Art. 28 DSGVO eingehalten werden, wenn die Standardvertragsklauseln im Einzelfall nicht abgeschlossen werden, weil der Verantwortliche mit deren Verwendung nicht einverstanden ist.

Zu Szenario 1 (Vertragsvorlage) und zu Szenario 2 (Verträge mit dem/n Verantwortlichen):

1. Der Vertrag bzw. die Vertragsvorlage MUSS den Auftragsverarbeiter in Bezug auf den Verantwortlichen binden und Festlegungen treffen bezüglich:

   a) Gegenstand und Dauer der Verarbeitung

      Der Gegenstand der Verarbeitung MUSS spezifiziert werden. Insoweit kann auf die relevanten Passagen eines eventuellen „Hauptvertrags“ (im Sinne einer Leistungsvereinbarung / Service Level Agreement - SLA) verwiesen werden. Ein solcher Verweis MUSS dann aber so konkret sein, dass diese Passagen ohne weiteres aufgefunden werden können.

      Der genaue Zeitraum oder die Kriterien, nach denen er bestimmt wird, MÜSSEN angegeben werden. Dies ist insbesondere dann gewährleistet, wenn entweder der geplante Beginn und das Ende der Verarbeitung angegeben werden oder festgelegt wird, dass das Auftragsverhältnis für unbestimmte Zeit eingegangen wird, wobei im letzteren Fall dann auch Angaben zur Kündigungsfrist zu machen sind.

   b) Art und Zweck der Verarbeitung

diktieren, wäre er im Erfolgsfall (Abschluss der Vereinbarung ohne Änderungen) ggf. selbst als (gemeinsam) Verantwortlicher anzusehen. Dies hätte zur Konsequenz, dass eine Zertifizierung auf der Grundlage dieses Kriterienkatalogs nicht in Betracht kommt.

Die Beschreibung der Art und des Zwecks MUSS in Abhängigkeit der spezifischen Verarbeitungstätigkeit erfolgen.

c) Art der personenbezogenen Daten

Insoweit MUSS insbesondere auch angegeben werden, ob besondere Kategorien personenbezogener Daten (vgl. Art. 9 DSGVO) verarbeitet werden, und, falls ja, welche besonderen Kategorien genau betroffen sind (z. B. Gesundheitsdaten oder genetische Daten). Werden personenbezogene Daten über strafrechtliche Verurteilungen und Straftaten oder Verkehrs- und/oder Standortdaten i. S. d. ePrivacy-Richtlinie verarbeitet, MUSS dies ebenfalls angegeben werden.

d) Kategorien betroffener Personen

Pauschalangaben wie „Vertrags- oder Geschäftspartner" sind zu vermeiden. Stattdessen MÜSSEN konkrete Kategorien benannt werden[27], wie z. B.: Kunden, Lieferanten, Interessenten, Nutzer eines Dienstes, Abonnenten, Besucher, Passanten, Patienten oder Beschäftigte. Je höher das Risiko der betreffenden Datenverarbeitung, desto genauer MÜSSEN die Kategorien bezeichnet werden.

e) Pflichten und Rechte des Verantwortlichen

Die Pflichten des Verantwortlichen ergeben sich insbesondere aus den Kapiteln III und IV der DSGVO. Im Hinblick auf seine Rechte sind insbesondere Weisungs- und Kontrollrechte zu nennen.

2. Der Vertrag bzw. die Vertragsvorlage MUSS außerdem noch folgendes vorsehen:

a) Der Auftragsverarbeiter verarbeitet personenbezogene Daten nur auf dokumentierte Weisung[28] des Verantwortlichen (dies auch in Bezug auf eine Übermittlung personenbezogener Daten an ein Drittland oder an eine internationale Organisation), soweit er nicht durch das Recht der Union oder der Mitgliedstaaten[29], dem er unterliegt, hierzu verpflichtet ist, und dass er, wenn er einer solchen Verpflichtung unterliegt, dem Verantwortlichen diese rechtlichen Anforderungen vor der Verarbeitung mitteilt, sofern das betreffende Recht eine solche Mitteilung nicht wegen eines wichtigen öffentlichen Interesses verbietet.

b) Der Auftragsverarbeiter gewährleistet, dass sich die zur Verarbeitung der personenbezogenen Daten befugten Personen zur Vertraulichkeit verpflichtet haben oder einer gesetzlichen Verschwiegenheitspflicht unterliegen.

Sind gesetzliche Geheimhaltungspflichten oder Berufsgeheimnisse und besondere Amtsgeheimnisse, die nicht auf gesetzlichen Vorschriften beruhen, einschlägig, ist zusätzlich Kapitel 1.4.1 dieses Kriterienkatalogs zu beachten, wonach der Vertrag / die Vertragsvorlage die entsprechende Geheimhaltungspflicht adressieren MUSS. Soweit das anwendbare Unions- bzw.

[27] Etwas anderes gilt nur dann, wenn sich die Kategorien betroffener Personen aufgrund der Art der betreffenden Verarbeitungsvorgänge nicht eingrenzen lassen.

[28] Weisungen sind dokumentiert, wenn ihr Inhalt in elektronischer oder schriftlicher Form festgehalten wird. Damit sind auch mündliche Weisungen zulässig, sofern sie nachträglich dokumentiert werden.

[29] In Betracht kommen insoweit insbesondere Vorschriften des jeweiligen nationalen Rechts zur inneren Sicherheit: Beispiel im Hinblick auf DE: § 22 a Abs. 5 BPolG.

mitgliedstaatliche Recht vorsieht, dass der Auftragsverarbeiter von dem Verantwortlichen im Hinblick auf die einschlägige Geheimhaltungspflicht zur Verschwiegenheit zu verpflichten und auf die Konsequenzen eines eventuellen Verstoßes gegen diese Pflicht hinzuweisen ist, MUSS auch dies Gegenstand des Vertrags / der Vertragsvorlage sein.

c) Der Auftragsverarbeiter ergreift alle gemäß Art. 32 DSGVO erforderlichen Maßnahmen. Konkret bedeutet dies folgendes:

   Der Vertrag / die Vertragsvorlage MUSS Informationen über die zu treffenden bzw. bereits implementierten Maßnahmen enthalten oder auf ein separates Dokument, in dem die TOM aufgelistet werden, verweisen.[30] Die Vertragsklauseln MÜSSEN eine Verpflichtung des Auftragsverarbeiters vorsehen, vor wesentlichen Änderungen der Maßnahmen die Zustimmung des für die Verarbeitung Verantwortlichen einzuholen, sowie eine regelmäßige Überprüfung der TOM durchzuführen, um ihre Angemessenheit im Hinblick auf die Risiken, die sich im Laufe der Zeit entwickeln können, zu gewährleisten.

d) Der Auftragsverarbeiter hält die in Art. 28 Abs. 2 und Abs. 4 Satz 1 DSGVO genannten Bedingungen für die Inanspruchnahme der Dienste eines weiteren Auftragsverarbeiters ein.

   Insoweit kommen verschiedene Varianten in Betracht. Der Auftragsverarbeiter MUSS zu der im Einzelfall einschlägigen Variante Festlegungen im Vertrag / der Vertragsvorlage treffen:

   Variante 1: Der Einsatz weiterer Auftragsverarbeiter wird generell ausgeschlossen.

   Variante 2: Der Auftragsverarbeiter nimmt weitere Auftragsverarbeiter nur nach vorheriger gesonderter schriftlicher (elektronisches Format genügt) Genehmigung des Verantwortlichen in Anspruch.

   Variante 3: Der Verantwortliche erteilt eine allgemeine schriftliche (elektronisches Format genügt) Genehmigung für den Einsatz weiterer Auftragsverarbeiter. In diesem Fall informiert der Auftragsverarbeiter den Verantwortlichen über jede beabsichtigte Änderung in Bezug auf die Hinzuziehung oder die Ersetzung anderer Auftragsverarbeiter, wodurch der Verantwortliche die Möglichkeit erhält, gegen derartige Änderungen Einspruch zu erheben.

   Ist der Vertrag / die Vertragsvorlage darauf ausgelegt, zum Zeitpunkt der Unterzeichnung der Vereinbarung bestimmte weitere Auftragsverarbeiter zuzulassen, MUSS eine Liste der zugelassenen weiteren Auftragsverarbeiter in den Vertrag oder einen Anhang dazu aufgenommen werden.

e) Der Auftragsverarbeiter unterstützt den Verantwortlichen angesichts der Art der Verarbeitung nach Möglichkeit mit technischen und organisatorischen Maßnahmen dabei, seiner Pflicht zur Beantwortung von Anträgen auf

[30] Unabhängig hiervon ist eine erfolgreiche Zertifizierung stets nur dann möglich, wenn die entsprechenden Maßnahmen implementiert worden sind (vgl. Kapitel 2 weiter unten in diesem Dokument).

Wahrnehmung der in Kapitel III der DSGVO genannten Rechte der betroffenen Person nachzukommen. [31]

Während die Unterstützung in einigen Konstellationen lediglich in der unverzüglichen Weiterleitung der eingegangenen Anfragen bestehen kann und/oder den Verantwortlichen in die Lage versetzt, die betreffenden personenbezogenen Daten direkt zu extrahieren und zu verwalten, können dem Auftragsverarbeiter unter bestimmten Umständen spezifischere, technische Aufgaben übertragen werden. Dies ist insbesondere dann der Fall, wenn der Auftragsverarbeiter dazu in der Lage ist, die personenbezogenen Daten zu extrahieren und zu verwalten.

In diesem Zusammenhang ist zu berücksichtigen, inwieweit der Verantwortliche tatsächlich auf die Unterstützung des Auftragsverarbeiters in Bezug auf die Rechte der betroffenen Person angewiesen ist.

Solche Klauseln sollten mit der Verantwortung des Verantwortlichen in Bezug auf die Rechte der betroffenen Person im Einklang stehen und diese Verantwortung nicht unangemessen auf den Auftragsverarbeiter übertragen.

f) Der Auftragsverarbeiter unterstützt den Verantwortlichen unter Berücksichtigung der Art der Verarbeitung und der ihm zur Verfügung stehenden Informationen bei der Einhaltung der in den Art. 32 bis 36 DSGVO genannten Pflichten.

Konkret geht es insoweit um die Unterstützung des Verantwortlichen im Hinblick auf die folgenden Pflichten:

- Pflicht, technische und organisatorische Maßnahmen zu treffen;
- Pflicht, Verletzungen des Schutzes personenbezogener Daten an die Aufsichtsbehörde und an die betroffenen Personen zu melden;
- Pflicht eine Datenschutz-Folgenabschätzung durchzuführen, wenn dies erforderlich ist, und die Aufsichtsbehörde zu konsultieren, wenn das Ergebnis der DSFA zeigt, dass ein hohes Risiko besteht, das nicht gemindert werden kann.

g) Es ist vorzusehen, dass der Auftragsverarbeiter nach Abschluss der Erbringung der Verarbeitungsleistungen alle personenbezogenen Daten nach Wahl des Verantwortlichen entweder löscht oder zurückgibt und die vorhandenen Kopien löscht, sofern nicht nach dem Unionsrecht oder dem Recht der Mitgliedstaaten eine Verpflichtung zur Speicherung der personenbezogenen Daten besteht.

Im Ergebnis MUSS insoweit sichergestellt werden, dass nach Abschluss der Erbringung der Verarbeitungsleistungen beim Auftragsverarbeiter keine personenbezogenen Daten zurückbleiben, die ihm zwecks Auftragserfüllung überlassen worden sind und für die keine gesetzlichen Speicherpflichten (mehr) bestehen. Dies beinhaltet auch die Löschung / Rückgabe eventuell angefertigter Kopien.

h) Es ist vorzusehen, dass der Auftragsverarbeiter dem Verantwortlichen alle erforderlichen Informationen zum Nachweis der Einhaltung der in Art. 28 DSGVO

[31] Die dem Auftragsverarbeiter möglichen Unterstützungsleistungen richten sich nach der Art der Verarbeitung. Vgl. insoweit auch Kapitel 3 dieses Kriterienkatalogs.

niedergelegten Pflichten zur Verfügung stellt[32] und Überprüfungen[33] – einschließlich Inspektionen – , die vom Verantwortlichen oder einem anderen von diesem beauftragten Prüfer durchgeführt werden, ermöglicht und dazu beiträgt.

i) Der Auftragsverarbeiter informiert den Verantwortlichen unverzüglich, falls er der Auffassung ist, dass eine Weisung gegen die DSGVO oder gegen andere Datenschutzbestimmungen der Union oder der Mitgliedstaaten verstößt.

3. Die folgende weitere Anforderung betrifft nur Szenario 1 (Vertragsvorlage): Der Auftragsverarbeiter MUSS in einer Arbeitsanweisung o.ä. regeln, wie sichergestellt wird, dass die Vorgaben des Art. 28 DSGVO eingehalten werden, wenn die Vertragsvorlage im Einzelfall nicht verwendet wird, weil der Verantwortliche hiermit nicht einverstanden ist.

Ggf.: Relevantes Nationales Recht:

1. Ggf.: §§ zu anderen Rechtsinstrumenten (→ Art. 28 Abs. 3 S. 1 DSGVO)
2. Ggf.: §§ des Rechts der inneren Sicherheit etc. (→ Art. 28 Abs. 3 S. 2 lit. a) DSGVO)
3. Ggf.: Gesetzliche Speicherpflichten (→ Art. 28 Abs. 3 S. 2 lit. g) DSGVO)
4. Ggf.: Nationales Recht, das im Hinblick auf die Rechtmäßigkeit einer Weisung relevant ist (→ Art. 28 Abs. 3 S. 3 DSGVO)

Orientierungshilfe

Relevante Dokumente:

Auftragsverarbeitungsvertrag zwischen dem Auftragsverarbeiter (Zertifizierungskunden) und den Verantwortlichen, die die zu zertifizierenden Verarbeitungsvorgänge in Anspruch nehmen / beauftragen bzw. eine entsprechende Vertragsvorlage, wobei es sich hierbei auch um (an den relevanten Stellen ausgefüllte) Standardvertragsklauseln handeln kann.

Arbeitsanweisung (Einhaltung Art. 28 DSGVO bei Nichtverwendung der Vertragsvorlage)

Relevante Evaluationsmethoden:

Dokumentenprüfung, Interviews

Anwendungs-/Auslegungshilfen:

- EDSA: Leitlinien 07/2020 zu den Begriffen „Verantwortlicher“ und „Auftragsverarbeiter“ in der DSGVO (vgl. Teil 2, Kapitel 1: „Beziehung zwischen Verantwortlichem und Auftragsverarbeiter“)
- DE: Kurzpapier Nr. 13 der DSK

Ende der Orientierungshilfe

[32] Vgl. hierzu auch Kapitel 1.2.2 dieses Kriterienkatalogs (unter Details zum Gegenstand der Anforderung, Nr. 8).

[33] Hier ist zu regeln, wie der Auftragsverarbeiter Überprüfungen durch den Verantwortlichen oder von diesem beauftragte Dritte ermöglicht und wie er (aktiv) dazu beiträgt. Umfasst hiervon sind Überprüfungen vor Ort und / oder Einsichtnahmen in IT-Systeme und Verfahren.

1.2.2. Umsetzung der vertraglich vereinbarten Pflichten: Verantwortlichkeiten, Prozesse, Arbeitsanweisungen

Anforderung in Kürze:

Der Auftragsverarbeiter MUSS Maßnahmen zur Umsetzung der vertraglich vereinbarten bzw. in der Vertragsvorlage vorgesehenen Pflichten implementiert haben (vgl. nachfolgend unter „Anforderung im Detail“).

Orientierungshilfe

Relevante Artikel der DSGVO:

Art. 28 DSGVO

Hintergrund:

Beschränkte sich eine Zertifizierung auf die Überprüfung der vertraglichen Vereinbarungen zwischen einem Auftragsverarbeiter und dem/n Verantwortlichen (bzw. auf die entsprechende Vertragsvorlage), ließe aber außer Betracht, ob der Auftragsverarbeiter die zur Umsetzung der vertraglichen Verpflichtungen erforderlichen Maßnahmen implementiert hat, käme ihr nur eine geringe Aussagekraft zu. Deshalb ist im Rahmen einer Zertifizierung von Verarbeitungsvorgängen von Auftragsverarbeitern nach EuroPriSe auch zu prüfen, ob der Auftragsverarbeiter die zur Umsetzung der vertraglich vereinbarten bzw. in der Vertragsvorlage vorgesehenen Pflichten erforderlichen Weichenstellungen vorgenommen hat. Den Maßstab für diese Prüfung stellen die jeweiligen Vertragsklauseln dar, so dass die nachfolgend aufgelisteten Anforderungen stets im Hinblick auf diese zu konkretisieren sind. Flankiert werden die Anforderungen durch die in Kapitel 2 dieses Dokuments aufgelisteten Anforderungen bezüglich technisch-organisatorischer Maßnahmen, die im Hinblick auf Art. 32 DSGVO und die Gewährleistungsziele des Datenschutzes für Verarbeitungsvorgänge von Auftragsverarbeitern stets bzw. in der Regel von Belang sind.

Ende der Orientierungshilfe

Anforderung im Detail:

Voraussetzungen für die / Ausnahmen von der Anwendbarkeit der Anforderung:

Diese Anforderung ist bei einer Zertifizierung von Verarbeitungsvorgängen von Auftragsverarbeitern stets anwendbar.

Details zum Gegenstand der Anforderung:

Der Auftragsverarbeiter MUSS Maßnahmen zur Einhaltung bzw. Umsetzung der vertraglich vereinbarten Pflichten implementiert haben. Konkret sind bei der Überprüfung der Einhaltung der nachfolgend aufgelisteten einzelnen Anforderungen insbesondere Dokumente zu betrachten, die Verantwortlichkeiten und Prozesse festlegen bzw. Arbeitsanweisungen oder Verschwiegenheitspflichten von Mitarbeitern des Auftragsverarbeiters zum Gegenstand haben.

Im Einzelnen MUSS der Auftragsverarbeiter nachweisen, dass er Maßnahmen zur Einhaltung der vertraglichen Vereinbarungen zu folgenden Themenkomplexen getroffen hat:

1. Verarbeitung personenbezogener Daten nur auf dokumentierte Weisung des Verantwortlichen, soweit er nicht einer entgegenstehenden Verpflichtung durch das

Recht der Union oder der Mitgliedstaaten unterliegt.

Der Auftragsverarbeiter MUSS insoweit insbesondere Festlegungen dazu treffen, welche Personen / Abteilungen zur Entgegennahme von Weisungen des Verantwortlichen befugt sind.

2. Vertraulichkeitsverpflichtung der zur Verarbeitung der personenbezogenen Daten befugten Personen bzw. Vorliegen einer gesetzlichen Verschwiegenheitspflicht dieser Personen.

   Insoweit MUSS der Auftragsverarbeiter aktuell in Gebrauch befindliche Vorlagen für Verschwiegenheits- bzw. Geheimhaltungsverpflichtungen des zuständigen Personals bei der Zertifizierungsstelle einreichen.

3. Ergreifen aller gemäß Art. 32 DSGVO erforderlichen Maßnahmen (→ dies ist Gegenstand der Anforderungen des Kapitels 2 dieses Kriterienkatalogs).

4. Einhaltung der Bedingungen für die Inanspruchnahme der Dienste eines weiteren Auftragsverarbeiters.[34]

   Der Auftragsverarbeiter MUSS Zuständigkeiten / Verantwortlichkeiten und Prozesse in Arbeitsanweisungen und/oder sonstigen Dokumenten spezifizieren. Diese MÜSSEN den insoweit getroffenen vertraglichen Vereinbarungen mit dem/den Verantwortlichen entsprechen – vgl. hierzu obiges Kapitel 1.2.1.2.d).

5. Unterstützung des Verantwortlichen bei der Beantwortung von Anträgen auf Wahrnehmung von Betroffenenrechten.[35]

   Die in diesem Zusammenhang erforderlichen Aktivitäten ergeben sich aus den einschlägigen Vertragsklauseln mit dem/den Verantwortlichen – vgl. hierzu obiges Kapitel 1.2.1.2.e).[36]

6. Unterstützung des Verantwortlichen bei der Einhaltung der Pflichten gem. Art. 32-36 DSGVO.

   Die in diesem Zusammenhang erforderlichen Aktivitäten ergeben sich aus den einschlägigen Vertragsklauseln mit dem/den Verantwortlichen – vgl. hierzu obiges Kapitel 1.2.1.2.f). Insoweit ist wie folgt zu differenzieren:

- Art. 32 DSGVO: Dies ist Gegenstand von Kapitel 2 dieses Kriterienkatalogs.
- Art. 33 f. DSGVO: Der Auftragsverarbeiter MUSS Maßnahmen getroffen haben, die gewährleisten, dass er dem Verantwortlichen ihm bekannt gewordene Verletzungen

[34] Im Hinblick auf tatsächlich eingesetzte weitere Auftragsverarbeiter ist dann außerdem zu prüfen, ob im konkreten Fall weitere Anforderungen eingehalten werden. So ist zu prüfen, ob die vertraglichen Verpflichtungen im Verhältnis Verantwortlicher – Auftragsverarbeiter an den weiteren Auftragsverarbeiter „durchgereicht werden" (vgl. Art. 28 Abs. 4 S. 1 DSGVO) und ob dieser technische und organisatorische Maßnahmen im Sinne des Art 32 DSGVO implementiert hat. Dies ist Gegenstand des nächsten Kapitels sowie von Kapitel 2 dieses Kriterienkatalogs.

[35] Dies ist Gegenstand von Kapitel 3 dieses Kriterienkatalogs.

[36] Während die Unterstützung lediglich darin bestehen kann, alle eingegangenen Anfragen umgehend weiterzuleiten und/oder dem Verantwortlichen die Möglichkeit zu geben, die einschlägigen personenbezogenen Daten direkt zu extrahieren und zu verwalten, werden dem Auftragsverarbeiter unter bestimmten Umständen spezifischere technische Aufgaben übertragen, insbesondere, wenn er in der Lage ist, die personenbezogenen Daten zu extrahieren und zu verwalten (EDSA, Leitlinien 07/2020).

des Schutzes personenbezogener Daten unverzüglich meldet (vgl. Art. 33 Abs. 2 DSGVO). Auch die Maßnahmen, die der Auftragsverarbeiter zur Umsetzung der vertraglich vereinbarten Pflichten zur Unterstützung des Verantwortlichen bei der Benachrichtigung betroffener Personen nach Art. 34 DSGVO sowie ggf. zu weiteren relevanten Unterstützungspflichten getroffen hat, sind Gegenstand dieser Anforderung.

- Art. 35 f. DSGVO: Der Auftragsverarbeiter MUSS auch insoweit alle für die Umsetzung der vertraglich vereinbarten Pflichten erforderlichen Maßnahmen getroffen haben. Sind Verantwortliche bei bestimmungsgemäßer Inanspruchnahme der zu zertifizierenden Verarbeitungsvorgänge dazu verpflichtet, eine Datenschutz-Folgenabschätzung durchzuführen, MUSS der Auftragsverarbeiter zudem im Sinne einer weiten Auslegung der Grundsätze Datenschutz durch Technikgestaltung und Datenschutz durch datenschutzfreundliche Voreinstellungen eine exemplarische DSFA durchführen[37], deren Ergebnisse dokumentieren und diese den Verantwortlichen zur Verfügung stellen (hierdurch erbringt der Auftragsverarbeiter Vorarbeiten, die die Verantwortlichen bei der Einhaltung ihrer Pflichten gemäß Art. 35 DSGVO unterstützen, wodurch der Auftragsverarbeiter seinerseits eine Hilfestellung in Erfüllung des Art. 28 Abs. 3 S. 2 lit. f) DSGVO leistet).

7. Löschung oder Zurückgabe aller personenbezogenen Daten nach Abschluss der Erbringung der Verarbeitungsleistungen, sofern die Daten nicht Gegenstand gesetzlicher Speicherpflichten nach dem Unionsrecht oder dem Recht der Mitgliedstaaten sind.[38]

8. Zur Verfügung stellen aller erforderlichen Informationen zum Nachweis der Einhaltung des Art. 28 DSGVO sowie Ermöglichung und aktive Unterstützung von Überprüfungen – einschließlich Inspektionen –, die vom Verantwortlichen oder einem anderen von diesem beauftragten Prüfer durchgeführt werden.

   Im Hinblick auf die Bereitstellung aller erforderlichen Informationen zum Nachweis der Einhaltung von Art. 28 DSGVO MUSS der Auftragsverarbeiter die folgenden Unterlagen bei der Zertifizierungsstelle einreichen:

   a) „TOM-Dokument“ – Beschreibung der implementierten technischen und organisatorischen Maßnahmen,

   b) Arbeitsanweisungen / Prozessbeschreibungen zur Sicherstellung der Einhaltung der Klauseln des (Muster-)Auftragsverarbeitungsvertrags:

      a. Dokument zum Umgang mit Weisungen des Verantwortlichen

      b. Nachweis über die Verpflichtung zur Vertraulichkeit

      c. Arbeitsanweisung zur Inanspruchnahme weiterer Auftragsverarbeiter

[37] Auch wenn hier von einer exemplarischen DSFA die Rede ist, bedeutet dies natürlich nicht, dass der Auftragsverarbeiter selbst eine DSFA gemäß Art. 35 DSGVO durchführen muss. Gemeint ist vielmehr, dass der Auftragsverarbeiter bereits vor Beauftragung durch einen konkreten Verantwortlichen ein Dokument zu den Risiken der zu zertifizierenden Verarbeitungsvorgänge erstellt, welches er dem Verantwortlichen dann nach Beauftragung zur Verfügung stellt. Der Verantwortliche wird also durch die Vorarbeiten des Auftragsverarbeiters bei der Durchführung einer DSFA unterstützt.

[38] Die technischen Anforderungen, die bzgl. einer Löschung zu beachten sind, sind Gegenstand von Kapitel 2.1.6 dieses Kriterienkatalogs.

d. Arbeitsanweisung zu Anfragen betroffener Personen

e. Arbeitsanweisung zu Verletzungen des Schutzes personenbezogener Daten

c) Relevante Dokumente bzw. Informationen zum Themenkomplex „weitere Auftragsverarbeiter“ (sofern einschlägig – vgl. auch Kapitel 1.3),

a. Liste weiterer Auftragsverarbeiter (Unterauftragnehmer) mit ToE-Relevanz und deren Standorte

b. Dokument zur Vorgehensweise bei der Auswahl weiterer Auftragsverarbeiter im Allgemeinen

c. Dokument/e zum Nachweis der sorgfältigen Auswahl jedes weiteren Auftragsverarbeiters

d. Unterschriebene Auftragsverarbeitungsverträge mit weiteren Auftragsverarbeitern

d) Relevante Dokumente bzw. Informationen zum Themenkomplex „Übermittlung personenbezogener Daten in ein Drittland“ (sofern einschlägig – vgl. auch Kapitel 1.4.2),

a. Ergebnisse eines / mehrerer Transfer Impact Assessments

b. Andere Dokumente im Zusammenhang mit einer Übermittlung personenbezogener Daten in ein Drittland

i. Verbindliche interne Datenschutzvorschriften und Nachweis ihrer Genehmigung

ii. Verwendete Standarddatenschutzklauseln

iii. Verhaltensregeln und Nachweis ihrer Genehmigung

iv. Dokumente bezüglich einer Zertifizierung gemäß Art. 42 DSGVO

v. Dokumente, die sich auf eine der Ausnahmeregelungen gemäß Art. 49 DSGVO beziehen

vi. Nachweise über getroffene zusätzliche Maßnahmen

d) Ggf. relevante Protokolldaten, durch die die Einhaltung der Vorgaben der DSGVO dokumentiert wird,

e) Ggf. Informationen zur Einhaltung genehmigter Verhaltensregeln bzw. Zertifizierungsverfahren,

f) Ggf. Informationen zu sonstigen relevanten Zertifizierungen / Überprüfungen

9. Information des Verantwortlichen, falls der Auftragsverarbeiter der Auffassung ist, dass eine Weisung gegen die DSGVO oder gegen andere Datenschutzbestimmungen der Union oder der Mitgliedstaaten verstößt.

   Der vom Auftragsverarbeiter insoweit definierte Prozess muss auch festlegen, wie konkret mit Weisungen umgegangen wird, deren Umsetzung zu offenkundigen Rechtsverstößen und/oder schwerwiegenden Verletzungen des Persönlichkeitsrechts der betroffenen Personen führt.

Ggf.: Relevantes Nationales Recht:

1. Ggf.: §§ zu anderen Rechtsinstrumenten (→ Art. 28 Abs. 3 S. 1 DSGVO)

2. Ggf.: §§ des Rechts der inneren Sicherheit etc. (→ Art. 28 Abs. 3 S. 2 lit. a) DSGVO)
3. Ggf.: Gesetzliche Speicherpflichten (→ Art. 28 Abs. 3 S. 2 lit. g) DSGVO)
4. Ggf.: Nationales Recht, das im Hinblick auf die Rechtmäßigkeit einer Weisung relevant ist (→ Art. 28 Abs. 3 S. 3 DSGVO)

Orientierungshilfe

Relevante Dokumente:

1. Auftragsverarbeitungsvertrag zwischen dem Auftragsverarbeiter (Zertifizierungskunden) und den Verantwortlichen, die die zu zertifizierenden Verarbeitungsvorgänge in Anspruch nehmen/beauftragen bzw. eine entsprechende Vertragsvorlage, wobei es sich hierbei auch um (an den relevanten Stellen ausgefüllte) Standardvertragsklauseln handeln kann.
2. Weitere in diesem Zusammenhang relevante Dokumente wie insbesondere:

   a) Datenschutzkonzept

   b) Beschreibung der technischen und organisatorischen Maßnahmen

   c) Relevante Arbeitsanweisungen, Prozessbeschreibungen etc.

   d) Vorlagen für Verschwiegenheits- bzw. Geheimhaltungsverpflichtungen des zuständigen Personals des Auftragsverarbeiters

   e) Relevante Dokumente bzw. Informationen zum Themenkomplex „weitere Auftragsverarbeiter“ (sofern einschlägig)

   f) Relevante Dokumente bzw. Informationen zum Themenkomplex „Übermittlung personenbezogener Daten in Drittländer“ (sofern einschlägig),

   g) Ggf. relevante Protokolldaten, durch die die Einhaltung der Vorgaben der DSGVO dokumentiert wird,

   h) Ggf. Informationen zur Einhaltung genehmigter Verhaltensregeln bzw. Zertifizierungsverfahren

   i) Ggf. Informationen zu sonstigen relevanten Zertifizierungen / Überprüfungen

Relevante Evaluationsmethoden:

Dokumentenprüfung, Interviews

Anwendungs-/Auslegungshilfen:

- EDSA: Leitlinien 07/2020 zu den Begriffen „Verantwortlicher“ und „Auftragsverarbeiter“ in der DSGVO (vgl. Teil 2, Kapitel 1: „Beziehung zwischen Verantwortlichem und Auftragsverarbeiter“)
- DE: Kurzpapier Nr. 13 der DSK

Ende der Orientierungshilfe

1.3. Anforderungen im Hinblick auf Art. 28 DSGVO (Verhältnis Auftragsverarbeiter – weiterer Auftragsverarbeiter)

Dieses Unterkapitel ist immer dann anwendbar, wenn der Zertifizierungskunde (Auftragsverarbeiter) weitere Auftragsverarbeiter in Anspruch nimmt. Der Begriff "weiterer

Auftragsverarbeiter" bezieht sich auf Fälle, in denen der Zertifizierungskunde einen weiteren Auftragsverarbeiter einschaltet.

Da nur dann eine verlässliche Aussage dazu getroffen werden kann, ob das EU-Datenschutzrecht bei den zu zertifizierenden Verarbeitungsvorgängen eingehalten wird, wenn auch die weiteren Auftragsverarbeiter mit betrachtet werden, sind die nachfolgenden Anforderungen in solchen Fällen stets anwendbar.[39]

Zunächst ist aber zu klären, ob vom Auftragsverarbeiter eingeschaltete Dienstleister überhaupt als weitere Auftragsverarbeiter i. S. v. Art. 28 Abs. 2 und 4 DSGVO einzustufen sind.

Orientierungshilfe

Qualifikation eingeschalteter Dienstleister als weitere Auftragsverarbeiter

Zunächst ist aber zu klären, ob vom Auftragsverarbeiter eingeschaltete Dienstleister überhaupt als weitere Auftragsverarbeiter i. S. v. Art. 28 Abs. 2 und 4 DSGVO einzustufen sind.

Weitere Auftragsverarbeiter, die personenbezogene Daten im (Unter-)Auftrag verarbeiten, sind von Dienstleistern, die der Auftragsverarbeiter einschaltet, und die lediglich weisungsgebundene Dienstleistungen anderer Art erbringen, abzugrenzen. Dabei ist eine Auftragsverarbeitung bereits dann zu prüfen, wenn für den Sub-Dienstleister bei der Erbringung der Dienstleistung die Möglichkeit eines Zugriffs auf personenbezogene Daten besteht.

Besonders praxisrelevant ist insoweit die Frage, wann von einem Rechenzentrum erbrachte Dienstleistungen dazu führen, dass dieses als weiterer Auftragsverarbeiter zu qualifizieren ist. Ebenfalls hohe praktische Relevanz hat die Frage, ob eine Prüfung bzw. (Fern-)Wartung von IT-Systemen als Auftragsverarbeitung einzustufen ist. Insoweit gilt folgendes:

a) Dienstleistungen eines Rechenzentrums

Stellt das Rechenzentrum lediglich infrastrukturelle Dienstleistungen und Betriebsunterstützung bereit, wird die Hardware aber vom Kunden (konkret: dem Auftragsverarbeiter) gestellt (sog. Housing), ist das Rechenzentrum nicht als weiterer Auftragsverarbeiter zu qualifizieren. es sei denn, das Housing umfasst gemeinsam genutzte Netzwerkdienste einschließlich aktiver Netzwerkausrüstung zum Anschluss der Hardware des Kunden an das Netzwerk.

Werden hingegen über das Housing hinausgehende Hosting-Dienstleistungen erbracht (z. B. Server-Hosting, Web-Hosting oder E-Mail-Hosting), liegt insoweit eine Auftragsverarbeitung vor.

b) Prüfung bzw. (Fern-)Wartung von IT-Systemen

[39] Grundsätzlich sind alle eingeschalteten weiteren Auftragsverarbeiter zu betrachten. Nimmt der Auftragsverarbeiter die Dienstleistungen mehrerer weiterer Auftragsverarbeiter, die gleichartige Tätigkeiten ausüben (z. B. Übersetzungsbüros), in Anspruch, kann im Rahmen eines Zertifizierungsverfahrens gegebenenfalls eine exemplarische Prüfung (nähere Betrachtung nur eines bzw. einiger dieser weiteren Auftragsverarbeiter im Rahmen der Evaluierung) ausreichen. Dies allerdings nur dann, wenn dies im Evaluationskonzept entsprechend kenntlich gemacht worden ist.

Wird eine Prüfung bzw. (Fern-)Wartung von IT-Systemen vereinbart und besteht für den Dienstleister insoweit die Möglichkeit einer Verarbeitung personenbezogener Daten, liegt eine Auftragsverarbeitung vor. Nimmt der Dienstleister hingegen lediglich eine technische Prüfung oder Wartung der entsprechenden Infrastruktur (Strom, Kühlung, Heizung) vor, ist nicht von einer Auftragsverarbeitung auszugehen.

An dieser Stelle ist erneut darauf hinzuweisen, dass im Rahmen eines Zertifizierungsverfahrens stets eine konkrete Betrachtung des Einzelfalls unter Berücksichtigung aller maßgeblichen Details der einschlägigen Anwendungs- bzw. Auslegungshilfen zu erfolgen hat.

Relevante Dokumente:

ToE-Beschreibung bzw. Prüfbericht

Relevante Evaluationsmethoden:

Dokumentenprüfung, Interviews

Anwendungs-/Auslegungshilfen:

- Rechtsprechung des EuGH zur gemeinsamen Verantwortlichkeit: Rechtssachen C-210/16, C-25/17 und C-40/17
- EDSA: Leitlinien 07/2020 zu den Begriffen „Verantwortlicher“ und „Auftragsverarbeiter“ in der DSGVO (vgl. Teil 1, Kapitel 1-4)
- DE: Kurzpapier Nr. 13 der DSK (insbesondere auch zum Thema Wartung und Fernzugriffe)

Ende der Orientierungshilfe

1.3.1. Auswahl weiterer Auftragsverarbeiter im Hinblick auf Garantien zur Wahrung des Datenschutzes

Anforderung in Kürze:

Der Auftragsverarbeiter MUSS einen Prozess festgelegt und dokumentiert haben (z. B. in einer Arbeitsanweisung / Prozessbeschreibung), wie bei der Auswahl weiterer Auftragsverarbeiter zu verfahren ist.

Der Auftragsverarbeiter MUSS für jeden weiteren Auftragsverarbeiter, der an der Erbringung der zu zertifizierenden Verarbeitungsvorgänge beteiligt ist, nachweisen, dass er diesen im Hinblick auf Garantien zur Wahrung des Datenschutzes ausgewählt hat (wie nachstehend unter „Anforderung im Detail“ näher ausgeführt).

Orientierungshilfe

Relevante Artikel der DSGVO:

Art. 28 Abs. 1 DSGVO

Ende der Orientierungshilfe

Anforderung im Detail:

Voraussetzungen für die / Ausnahmen von der Anwendbarkeit der Anforderung:

Diese Anforderung ist bei einer Zertifizierung von Verarbeitungsvorgängen von Auftragsverarbeitern anwendbar, wenn der Auftragsverarbeiter auf weitere Auftragsverarbeiter zurückgreift, die an der Erbringung der zu zertifizierenden Verarbeitungsvorgänge beteiligt sind.

Details zum Gegenstand der Anforderung:

Möchte der Auftragsverarbeiter die Dienste weiterer Auftragsverarbeiter in Anspruch nehmen, dann MUSS er sich bei deren Auswahl davon überzeugen, dass sie Garantien dafür bieten, dass technische und organisatorische Maßnahmen so durchgeführt werden, dass die Verarbeitung im Einklang mit den Anforderungen der DSGVO erfolgt und den Schutz der Rechte der betroffenen Personen gewährleistet. Als Kriterien bei der Auswahl eines potentiellen weiteren Auftragsverarbeiters sind insbesondere dessen Fachwissen, Zuverlässigkeit und Ressourcen zu berücksichtigen (vgl. Erwägungsgrund 81 S. 1 der DSGVO), daneben können auch dessen finanzielle Stabilität und Reputation Berücksichtigung finden.

Die Einhaltung genehmigter Verhaltensregeln oder eines genehmigten Zertifizierungsverfahrens durch einen weiteren Auftragsverarbeiter kann als Faktor herangezogen werden, um dessen sorgfältige Auswahl durch den Auftragsverarbeiter nachzuweisen (vgl. Erwägungsgrund 81 S. 2 der DSGVO).[40] Nachweisrelevant sein können aber auch anerkannte internationale Zertifizierungen wie die ISO/IEC 27000er-Reihe, Ergebnisse externer oder interner Audits, Kontrollmöglichkeiten bzw. Prüfrechte des Auftragsverarbeiters, vertragliche Zusicherungen, individuelle Sicherheitskonzepte, TOM-Dokumente oder andere Dokumente, die im Hinblick auf das Vorliegen von Garantien relevant ein können (z. B. eine Informationssicherheitsrichtlinie oder ein Verzeichnis der Verarbeitungstätigkeiten).

Der Auftragsverarbeiter MUSS aus den oben aufgelisteten Nachweismöglichkeiten solche auswählen, die den Risiken, die mit den Verarbeitungstätigkeiten des weiteren Auftragsverarbeiters verbunden sind, gerecht werden.

Anmerkung: Die Auswahl der Unterauftragsverarbeiter muss immer auf der Grundlage mehrerer der oben genannten Elemente erfolgen. Es reicht dagegen nicht aus, sich nur auf eines dieser Elemente zu stützen.

Wichtig:

Im Rahmen von Kapitel 2 erfolgt dann eine Prüfung der bei weiteren Auftragsverarbeitern implementierten technischen und organisatorischen Maßnahmen im Hinblick auf die dort aufgelisteten, konkreten Anforderungen (soweit diese hinsichtlich der vom jeweiligen weiteren Auftragsverarbeiter erbrachten Leistungen relevant sind).

Ggf.: Relevantes Nationales Recht:

N/A

Orientierungshilfe

Relevante Dokumente:

[40] Dies natürlich stets unter der Voraussetzung, dass die vom weiteren Auftragsverarbeiter für den Auftragsverarbeiter erbrachten Leistungen vom Geltungsbereich der Zertifizierung bzw. Verhaltensregeln abgedeckt werden.

1. Relevante Arbeitsanweisungen, Prozessbeschreibungen etc.

2. Ggf. Verhaltensregeln nebst Nachweis bzgl. deren Genehmigung

3. Ggf. Unterlagen zu einer Zertifizierung nach Art. 42 DSGVO

4. Ggf. Unterlagen zu einer anerkannten internationalen Zertifizierung (z. B. ISO/IEC 2700er Reihe)

5. Ggf. Unterlagen zu den Ergebnissen eines externen oder internen Audits

6. Ggf. Kontrollmöglichkeiten des Auftragsverarbeiters / vertragliche Zusicherungen

7. Ggf. individuelle Sicherheitskonzepte / TOM-Dokumente

8. Ggf. andere relevante Dokumente wie eine Informationssicherheitsleitlinie oder ein Verzeichnis der Verarbeitungstätigkeiten

Relevante Evaluationsmethoden:

Dokumentenprüfung, Interviews

Anwendungs-/Auslegungshilfen:

- EDSA: Leitlinien 07/2020 zu den Begriffen „Verantwortlicher“ und „Auftragsverarbeiter“ in der DSGVO (vgl. Teil 2, Unterkapitel 1.1: „Auswahl des Auftragsverarbeiters“)
- DE: Kurzpapier Nr. 13 der DSK

Ende der Orientierungshilfe

1.3.2. Vorhandensein unterschriebener AV-Verträge mit allen weiteren Auftragsverarbeitern

Anforderung in Kürze:

Der Auftragsverarbeiter MUSS mit allen weiteren Auftragsverarbeitern Verträge geschlossen haben, die diesen dieselben Datenschutzpflichten auferlegen, die in dem Vertrag / den Verträgen zwischen dem / den Verantwortlichen und dem Auftragsverarbeiter festgelegt sind. Zum Nachweis hierfür ist jeweils der unterschriebene Vertrag[41] bei der Zertifizierungsstelle vorzulegen.

Orientierungshilfe

Relevante Artikel der DSGVO:

Art. 28 DSGVO

Hintergrund:

Die DSGVO verlangt ihrem Wortlaut nach, dass jedem weiteren Auftragsverarbeiter im Wege eines Vertrags dieselben Datenschutzpflichten auferlegt werden, die in dem

[41] Vorgelegt werden müssen nur die aus Datenschutzsicht relevanten Vertragsklauseln. Falls der jeweilige Vertrag noch weitere, datenschutzfremde Klauseln enthält, müssen diese nicht vorgelegt bzw. können die entsprechenden Passagen geschwärzt werden.

Vertrag zwischen dem Verantwortlichen und dem Auftragsverarbeiter festgelegt sind. Dies bedeutet aber nicht, dass dem weiteren Auftragsverarbeiter zwingend identische vertragliche Regelungen auferlegt werden müssen.[42] Sachgerecht ist es insoweit vielmehr zu verlangen, dass die Datenschutzpflichten und die zu implementierenden technischen und organisatorischen Maßnahmen im Hinblick auf die vom weiteren Auftragsverarbeiter durchzuführenden (Verarbeitungs-)Tätigkeiten festgelegt werden, wobei sicherzustellen ist, dass die dem weiteren Auftragsverarbeiter auferlegten Pflichten in ihrer Substanz denen des Auftragsverarbeiters vergleichbar sind. Letztlich ist entscheidend, dass das zwischen dem Verantwortlichen und dem Auftragsverarbeiter vereinbarte Schutzniveau durch die Einschaltung weiterer Auftragsverarbeiter nicht abgesenkt wird.

Ende der Orientierungshilfe

Anforderung im Detail:

Voraussetzungen für die / Ausnahmen von der Anwendbarkeit der Anforderung:

Diese Anforderung ist bei einer Zertifizierung von Verarbeitungsvorgängen von Auftragsverarbeitern anwendbar, wenn der Auftragsverarbeiter auf weitere Auftragsverarbeiter zurückgreift.

Details zum Gegenstand der Anforderung:

1. Der Auftragsverarbeiter MUSS mit jedem weiteren Auftragsverarbeiter einen AV-Vertrag geschlossen haben, der verbindliche Regelungen zu den folgenden Aspekten enthält:

a) Gegenstand und Dauer der Verarbeitung

Der Gegenstand des Vertrags MUSS spezifiziert werden. Insoweit kann es genügen, wenn auf die relevanten Passagen eines eventuellen „Hauptvertrags“ (im Sinne einer Leistungsvereinbarung / Service Level Agreement - SLA) verwiesen wird. Ein solcher Verweis MUSS dann aber so konkret sein, dass diese Passagen ohne weiteres aufgefunden werden können.

Der genaue Zeitraum oder die Kriterien, nach denen er bestimmt wird, MÜSSEN angegeben werden. Dies ist insbesondere dann gewährleistet, wenn entweder der geplante Beginn und das Ende der Verarbeitung angegeben werden oder festgelegt wird, dass das Auftragsverhältnis für unbestimmte Zeit eingegangen wird, wobei im letzteren Fall dann auch Angaben zur Kündigungsfrist zu machen sind. Diese Angaben zur Dauer der Verarbeitung richten sich nach den einschlägigen Bestimmungen des Auftragsverarbeitungsvertrags zwischen dem Verantwortlichen und dem Auftragsverarbeiter / der entsprechenden Vertragsvorlage.

b) Art und Zweck der Verarbeitung

Die Beschreibung der Art und des Zwecks MUSS in Abhängigkeit der spezifischen Verarbeitungstätigkeit erfolgen.

c) Art der personenbezogenen Daten

Insoweit MUSS insbesondere auch angegeben werden, ob besondere Kategorien personenbezogener Daten (vgl. Art. 9 DSGVO) verarbeitet werden, und falls ja,

[42] So „passen“ die zwischen dem Verantwortlichen und dem Auftragsverarbeiter vereinbarten vertraglichen Regelungen z. B. nicht ohne weiteres 1:1 auf das Verhältnis zwischen dem Auftragsverarbeiter und einem von diesem unterbeauftragten Call Center oder Rechenzentrum.

welche besonderen Kategorien genau betroffen sind (z.B. Gesundheitsdaten oder genetische Daten). Werden personenbezogene Daten über strafrechtliche Verurteilungen und Straftaten oder Verkehrs- und/oder Standortdaten i. S. d. ePrivacy-Richtlinie verarbeitet, MUSS dies ebenfalls angegeben werden.

d) Kategorien betroffener Personen

Pauschalangaben wie „Vertrags- oder Geschäftspartner“ sind zu vermeiden. Stattdessen MÜSSEN konkrete Kategorien benannt werden[43], wie z. B.: Kunden, Lieferanten, Interessenten, Nutzer eines Dienstes, Abonnenten, Besucher, Passanten, Patienten oder Beschäftigte. Je höher das Risiko der betreffenden Datenverarbeitung, desto genauer müssen die Kategorien bezeichnet werden.

e) Pflichten und Rechte des Auftragsverarbeiters im Verhältnis zum weiteren Auftragsverarbeiter

Im Hinblick auf die Rechte des Auftragsverarbeiters im Verhältnis zum weiteren Auftragsverarbeiter sind insbesondere Weisungs- und Kontrollrechte zu nennen.

2. Der Vertrag MUSS außerdem noch folgendes vorsehen:

a) Der weitere Auftragsverarbeiter verarbeitet personenbezogene Daten nur auf dokumentierte Weisung[44] des Auftragsverarbeiters (dies auch in Bezug auf eine Übermittlung personenbezogener Daten an ein Drittland oder an eine internationale Organisation), soweit er nicht durch das Recht der Union oder der Mitgliedstaaten[45], dem er unterliegt, hierzu verpflichtet ist, und dass er, wenn er einer solchen Verpflichtung unterliegt, dem Auftragsverarbeiter diese rechtlichen Anforderungen vor der Verarbeitung mitteilt, sofern das betreffende Recht eine solche Mitteilung nicht wegen eines wichtigen öffentlichen Interesses verbietet,

b) Der weitere Auftragsverarbeiter gewährleistet, dass sich die zur Verarbeitung der personenbezogenen Daten befugten Personen zur Vertraulichkeit verpflichtet haben oder einer gesetzlichen Verschwiegenheitspflicht unterliegen.

Sind gesetzliche Geheimhaltungspflichten oder Berufsgeheimnisse und besondere Amtsgeheimnisse, die nicht auf gesetzlichen Vorschriften beruhen, einschlägig, ist zusätzlich Kapitel 1.4.1 dieses Kriterienkatalogs zu beachten, wonach der Vertrag die entsprechende Geheimhaltungspflicht adressieren MUSS. Soweit das anwendbare Unions- bzw. mitgliedstaatliche Recht vorsieht, dass der weitere Auftragsverarbeiter im Hinblick auf die einschlägige Geheimhaltungspflicht zur Verschwiegenheit zu verpflichten und auf die Konsequenzen eines eventuellen Verstoßes gegen diese Pflicht hinzuweisen ist, MUSS auch dies Gegenstand des Vertrags sein.

[43] Etwas anderes gilt nur dann, wenn sich die Kategorien betroffener Personen aufgrund der Art der betreffenden Verarbeitungsvorgänge nicht eingrenzen lassen.

[44] Weisungen sind dokumentiert, wenn ihr Inhalt in elektronischer oder schriftlicher Form festgehalten wird. Damit sind auch mündliche Weisungen zulässig, sofern sie nachträglich dokumentiert werden.

[45] In Betracht kommen insoweit insbesondere Vorschriften des jeweiligen nationalen Rechts zur inneren Sicherheit: Beispiel im Hinblick auf DE: § 22 a Abs. 5 BPolG.

c) Der weitere Auftragsverarbeiter ergreift alle gemäß Art. 32 DSGVO erforderlichen Maßnahmen. Konkret bedeutet dies folgendes:

Der Vertrag MUSS Informationen über die zu treffenden bzw. bereits implementierten Maßnahmen enthalten oder auf ein separates Dokument, in dem die TOM aufgelistet werden, verweisen.[46] Er MUSS eine Verpflichtung des weiteren Auftragsverarbeiters vorsehen, vor wesentlichen Änderungen der Maßnahmen die Zustimmung des Auftragsverarbeiters einzuholen, sowie eine regelmäßige Überprüfung der TOM durchzuführen, um ihre Angemessenheit im Hinblick auf Risiken, die sich im Lauf der Zeit entwickeln können, zu gewährleisten.

d) Der weitere Auftragsverarbeiter hält die in Art. 28 Abs. 2 und Abs. 4 Satz 1 DSGVO genannten Bedingungen für die Inanspruchnahme der Dienste eines zusätzlichen weiteren Auftragsverarbeiters ein.

Insoweit kommen verschiedene Varianten in Betracht. Der Vertrag MUSS zu der im Einzelfall einschlägigen Variante Festlegungen treffen:

Variante 1: Der Einsatz zusätzlicher weiterer Auftragsverarbeiter wird generell ausgeschlossen.

Variante 2: Der weitere Auftragsverarbeiter nimmt zusätzliche weitere Auftragsverarbeiter nur nach vorheriger gesonderter schriftlicher (elektronisches Format genügt) Genehmigung des Auftragsverarbeiters in Anspruch.

Variante 3: Der Auftragsverarbeiter erteilt eine allgemeine schriftliche (elektronisches Format genügt) Genehmigung für den Einsatz zusätzlicher weiterer Auftragsverarbeiter. In diesem Fall informiert der weitere Auftragsverarbeiter den Auftragsverarbeiter über jede beabsichtigte Änderung in Bezug auf die Hinzuziehung oder die Ersetzung zusätzlicher weiterer Auftragsverarbeiter, wodurch der Auftragsverarbeiter die Möglichkeit erhält, gegen derartige Änderungen Einspruch zu erheben.

Ist der Vertrag darauf ausgelegt, zum Zeitpunkt der Unterzeichnung der Vereinbarung bestimmte zusätzliche weitere Auftragsverarbeiter zuzulassen, MUSS eine Liste der zugelassenen weiteren Auftragsverarbeiter in den Vertrag oder einen Anhang dazu aufgenommen werden.

e) Der weitere Auftragsverarbeiter unterstützt den Auftragsverarbeiter angesichts der Art der Verarbeitung nach Möglichkeit mit technischen und organisatorischen Maßnahmen dabei, den Verantwortlichen dabei zu unterstützen, seiner Pflicht zur Beantwortung von Anträgen auf Wahrnehmung der in Kapitel III der DSGVO genannten Rechte der betroffenen Person nachzukommen.[47]

f) Der weitere Auftragsverarbeiter unterstützt den Auftragsverarbeiter unter Berücksichtigung der Art der Verarbeitung und der ihm zur Verfügung stehenden Informationen dabei, den Verantwortlichen bei der Einhaltung der in den Art. 32 bis 36 DSGVO genannten Pflichten zu unterstützen.

[46] Unabhängig hiervon ist eine erfolgreiche Zertifizierung nur dann möglich, wenn die entsprechenden Maßnahmen implementiert worden sind (vgl. Kapitel 2 weiter unten in diesem Dokument).

[47] Die dem weiteren Auftragsverarbeiter möglichen Unterstützungsleistungen richten sich nach der Art der Verarbeitung.

Konkret geht es insoweit um die Unterstützung des Auftragsverarbeiters bei der Unterstützung des Verantwortlichen im Hinblick auf die folgenden Pflichten:

- Pflicht, technische und organisatorische Maßnahmen zu treffen.
- Pflicht, Verletzungen des Schutzes personenbezogener Daten an die Aufsichtsbehörde und an die betroffenen Personen zu melden.
- Pflicht, eine Datenschutz-Folgenabschätzung durchzuführen, wenn dies erforderlich ist, und die Aufsichtsbehörde zu konsultieren, wenn das Ergebnis der DSFA zeigt, dass ein hohes Risiko besteht, das nicht gemindert werden kann.

g) Der Vertrag MUSS vorsehen, dass der weitere Auftragsverarbeiter nach Abschluss der Erbringung der Verarbeitungsleistungen alle personenbezogenen Daten nach Wahl des Auftragsverarbeiters entweder löscht oder zurückgibt und die vorhandenen Kopien löscht, sofern nicht nach dem Unionsrecht oder dem Recht der Mitgliedstaaten eine Verpflichtung zur Speicherung der personenbezogenen Daten besteht.

   Anmerkung hierzu: Die Wahl des Auftragsverarbeiters MUSS in Übereinstimmung mit der von dem Verantwortlichen seinerseits gegenüber dem Auftragsverarbeiter getroffenen Wahl erfolgen.[48]

   Im Ergebnis MUSS insoweit sichergestellt werden, dass nach Abschluss der Erbringung der Verarbeitungsleistungen beim weiteren Auftragsverarbeiter keine personenbezogenen Daten zurückbleiben, die ihm zwecks Auftragserfüllung überlassen worden sind und für die keine gesetzlichen Speicherpflichten (mehr) bestehen. Dies beinhaltet auch die Löschung / Rückgabe eventuell angefertigter Kopien.

h) Es ist vorzusehen, dass der weitere Auftragsverarbeiter dem Auftragsverarbeiter alle erforderlichen Informationen zum Nachweis der Einhaltung der in Art. 28 DSGVO niedergelegten Pflichten zur Verfügung stellt[49] und Überprüfungen[50] – einschließlich Inspektionen – , die vom Auftragsverarbeiter oder einem anderen von diesem beauftragten Prüfer bzw. gegebenenfalls auch direkt vom Verantwortlichen durchgeführt werden, ermöglicht und dazu beiträgt.

i) Der weitere Auftragsverarbeiter informiert den Auftragsverarbeiter unverzüglich, falls er der Auffassung ist, dass eine Weisung gegen die DSGVO oder gegen andere Datenschutzbestimmungen der Union oder der Mitgliedstaaten verstößt.

Ggf.: Relevantes Nationales Recht:

[48] Vgl. insoweit Kapitel 1.2.1.

[49] Unter Informationen in diesem Sinne fallen alle Dokumente/Daten, die es dem Auftragsverarbeiter ermöglichen, die Einhaltung der DSGVO durch den weiteren Auftragsverarbeiter zu überprüfen. Zu nennen sind etwa ein Datenschutzkonzept (sofern vorhanden), ein Dokument, in dem die getroffenen technischen und organisatorischen Maßnahmen beschrieben werden, Informationen zu eventuellen weiteren Auftragsverarbeitern und eventuellen Übermittlungen an Drittländer sowie Protokolldaten, die Aufschluss über die Einhaltung bestimmter Vorschriften der DSGVO geben.

[H] Insoweit ist zu regeln, wie der weitere Auftragsverarbeiter Überprüfungen durch den Auftragsverarbeiter oder von diesem beauftragte Dritte bzw. gegebenenfalls auch direkt durch den Verantwortlichen ermöglicht und wie er (aktiv) dazu beiträgt. Umfasst hiervon sind Überprüfungen vor Ort und / oder Einsichtnahmen in IT-Systeme und Verfahren.

1. Ggf.: §§ zu anderen Rechtsinstrumenten (→ Art. 28 Abs. 3 S. 1 DSGVO)

2. Ggf.: §§ des Rechts der inneren Sicherheit etc. (→ Art. 28 Abs. 3 S. 2 lit. a) DSGVO)

3. Ggf.: Gesetzliche Speicherpflichten (→ Art. 28 Abs. 3 S. 2 lit. g) DSGVO)

4. Ggf.: Nationales Recht, das im Hinblick auf die Rechtmäßigkeit einer Weisung relevant ist (→ Art. 28 Abs. 3 S. 3 DSGVO)

Orientierungshilfe

Relevante Dokumente:

Verträge zur Auftragsverarbeitung zwischen dem Auftragsverarbeiter (Zertifizierungskunden) und von ihm in Anspruch genommenen weiteren Auftragsverarbeitern.

Relevante Evaluationsmethoden:

Dokumentenprüfung, Interviews

Anwendungs-/Auslegungshilfen:

- EDSA: Leitlinien 07/2020 zu den Begriffen „Verantwortlicher“ und „Auftragsverarbeiter“ in der DSGVO (vgl. Teil 2, Kapitel 1: „Beziehung zwischen Verantwortlichem und Auftragsverarbeiter“)
- DE: Kurzpapier Nr. 13 der DSK

Ende der Orientierungshilfe

1.3.3. Umsetzung der vertraglich vereinbarten Pflichten: Verantwortlichkeiten, Prozesse, Arbeitsanweisungen

Anforderung in Kürze:

Der Auftragsverarbeiter MUSS Maßnahmen zur Umsetzung der vertraglich vereinbarten Pflichten implementiert haben.

Orientierungshilfe

Relevante Artikel der DSGVO:

Art. 28 DSGVO

Hintergrund:

Auch im Verhältnis Auftragsverarbeiter zu weiterem Auftragsverarbeiter ist zu prüfen, ob der Auftragsverarbeiter wirksame Maßnahmen zur Umsetzung der vertraglichen Regelungen getroffen hat. So muss er etwa Personen bzw. Abteilungen benannt haben, die zu Weisungen gegenüber dem jeweiligen weiteren Auftragsverarbeiter befugt sind, und in Übereinstimmung mit den entsprechenden Passagen des Vertrags festgelegt haben, in welcher Form Weisungen zu erfolgen haben bzw. zu dokumentieren sind.

Da Auftragsverarbeiter in der Praxis oftmals auf mehrere weitere Auftragsverarbeiter zurückgreifen, würde es den Rahmen einer Zertifizierung sprengen, bezüglich aller weiteren Auftragsverarbeiter zu prüfen, ob diese alle Verantwortlichkeiten und Prozesse, die zur Umsetzung der vertraglichen Regelungen erforderlich sind, spezifiziert und zum Gegenstand verbindlicher Arbeitsanweisungen gemacht haben. Deshalb ist die

Umsetzung der vertraglichen Pflichten im Sinne dieses Kapitels nur im Hinblick auf den Auftragsverarbeiter selbst zu prüfen.

Im Rahmen einer Zertifizierung zu betrachten sind allerdings die technischen und organisatorischen Maßnahmen, die die weiteren Auftragsverarbeiter im Hinblick auf Art. 32 DSGVO und die Gewährleistungsziele des Datenschutzes getroffen haben. Dies ist Gegenstand des Kapitels 2 dieses Kriterienkatalogs.

Ende der Orientierungshilfe

Anforderung im Detail:

Voraussetzungen für die / Ausnahmen von der Anwendbarkeit der Anforderung:

Diese Anforderung ist bei einer Zertifizierung von Verarbeitungsvorgängen von Auftragsverarbeitern anwendbar, wenn der Auftragsverarbeiter auf weitere Auftragsverarbeiter zurückgreift.

Details zum Gegenstand der Anforderung:

Der Auftragsverarbeiter MUSS nachweisen, dass er Maßnahmen zur Einhaltung bzw. Umsetzung der vertraglichen Vereinbarungen mit den weiteren Auftragsverarbeitern zu folgenden Themenkomplexen getroffen hat:

1. Verarbeitung personenbezogener Daten nur auf dokumentierte Weisung des Auftragsverarbeiters, soweit der weitere Auftragsverarbeiter nicht einer entgegenstehenden Verpflichtung durch das Recht der Union oder der Mitgliedstaaten unterliegt.

   Der Auftragsverarbeiter MUSS festlegen, welche Personen bzw. Abteilungen im Verhältnis zu dem weiteren Auftragsverarbeiter weisungsbefugt sind. Zudem ist in einer Arbeitsanweisung o.ä. in Übereinstimmung mit den vertraglichen Regelungen festzulegen, inwieweit eine Berechtigung zur Erteilung von Einzelweisungen besteht und wie (d.h. in welcher Form) diese zu erteilen und zu dokumentieren sind.

2. Einhaltung der Bedingungen für die Inanspruchnahme der Dienste zusätzlicher weiterer Auftragsverarbeiter, wie zwischen dem Auftragsverarbeiter und dem weiteren Auftragsverarbeiter vertraglich vereinbart – vgl. hierzu obiges Kapitel 1.3.2.2.d).

   Der Auftragsverarbeiter MUSS festlegen, welche Personen oder Abteilungen dazu befugt sind, die Inanspruchnahme zusätzlicher weiterer Auftragsverarbeiter durch den weiteren Auftragsverarbeiter gesondert zu genehmigen bzw. hiergegen Einspruch zu erheben, es sei denn, dass die Beauftragung weiterer Auftragsverarbeiter vertraglich ausgeschlossen worden ist.

3. Unterstützung des Auftragsverarbeiters bei der Unterstützung des Verantwortlichen bei der Beantwortung von Anträgen auf Wahrnehmung von Betroffenenrechten, wie zwischen dem Auftragsarbeiter und dem weiteren Auftragsverarbeiter vertraglich vereinbart – vgl. hierzu obiges Kapitel 1.3.2.2.e).

   Der Auftragsverarbeiter MUSS festlegen, welche Personen bzw. Abteilungen insoweit Ansprechpartner des weiteren Auftragsverarbeiters sind und diesem gegenüber die entsprechenden Unterstützungsleistungen einfordern dürfen.

4. Unterstützung des Auftragsverarbeiters bei der Unterstützung des Verantwortlichen bei der Einhaltung der Pflichten gem. Art. 32-36 DSGVO, wie zwischen dem Auftragsarbeiter und dem weiteren Auftragsverarbeiter vertraglich vereinbart – vgl.

hierzu obiges Kapitel 1.3.2.2.f).

Der Auftragsverarbeiter MUSS festlegen, welchen Personen bzw. Abteilungen der weitere Auftragsverarbeiter eine Verletzung des Schutzes personenbezogener Daten zu melden hat und wie mit solchen Meldungen umzugehen ist (→ Information des/r Verantwortlichen etc.). Sofern das Thema Datenschutz-Folgenabschätzung einschlägig ist, müssen Verantwortlichkeiten und Prozesse auch im Hinblick auf die Einforderung, die Entgegennahme und die Berücksichtigung von diesbezüglichen Unterstützungsleistungen des weiteren Auftragsverarbeiters festgelegt werden.

5. Löschung oder Zurückgabe aller personenbezogenen Daten nach Abschluss der Erbringung der Verarbeitungsleistungen, sofern die Daten nicht Gegenstand gesetzlicher Speicherpflichten nach dem Unionsrecht oder dem Recht der Mitgliedstaaten sind.

   Der Auftragsverarbeiter MUSS auch insoweit Maßnahmen zur Umsetzung der vertraglichen Regelungen treffen.[51]

6. Information des Auftragsverarbeiters, falls der weitere Auftragsverarbeiter der Auffassung ist, dass eine Weisung gegen die DSGVO oder gegen andere Datenschutzbestimmungen der Union oder der Mitgliedstaaten verstößt.

   Der Auftragsverarbeiter MUSS festlegen, welche Personen bzw. Abteilungen der weitere Auftragsverarbeiter zu informieren hat, wenn er der Auffassung ist, dass eine Weisung des Auftragsverarbeiters gegen Datenschutzbestimmungen verstößt, und wie hiermit umzugehen ist.

Ggf.: Relevantes Nationales Recht:

1. Ggf.: §§ zu anderen Rechtsinstrumenten (→ Art. 28 Abs. 3 S. 1 DSGVO)

2. Ggf.: §§ des Rechts der inneren Sicherheit etc. (→ Art. 28 Abs. 3 S. 2 lit. a) DSGVO)

3. Ggf.: Gesetzliche Speicherpflichten (→ Art. 28 Abs. 3 S. 2 lit. g) DSGVO)

4. Ggf.: Nationales Recht, das im Hinblick auf die Rechtmäßigkeit einer Weisung relevant ist (→ Art. 28 Abs. 3 S. 3 DSGVO)

Orientierungshilfe

Relevante Dokumente:

1. Verträge zur Auftragsverarbeitung zwischen dem Auftragsverabeiter (Zertifizierungskunden) und von ihm in Anspruch genommenen weiteren Auftragsverarbeitern.
2. Weitere in diesem Zusammenhang relevante Dokumente wie insbesondere relevante Arbeitsanweisungen, Prozessbeschreibungen etc.

Relevante Evaluationsmethoden:

Dokumentenprüfung, Interviews

[51] z. B. Festlegungen dazu, welche Personen bzw. Abteilungen dazu befugt sind, den weiteren Auftragsverarbeiter in Übereinstimmung mit der vom Verantwortlichen insoweit getroffenen Wahl dazu aufzufordern, personenbezogene Daten zu löschen oder zurückzugeben, und/oder die Vorlage von Protokollen zur Löschung/Vernichtung personenbezogener Daten zu verlangen.

Anwendungs-/Auslegungshilfen:

- EDSA: Leitlinien 07/2020 zu den Begriffen „Verantwortlicher“ und „Auftragsverarbeiter“ in der DSGVO (vgl. Teil 2, Kapitel 1: „Beziehung zwischen Verantwortlichem und Auftragsverarbeiter“)
- DE: Kurzpapier Nr. 13 der DSK

Ende der Orientierungshilfe

1.4. Anforderungen bzgl. spezieller Arten von Verarbeitungsvorgängen

Die nachfolgenden Anforderungen betreffen die folgenden Themenbereiche:

- Gesetzliche Geheimhaltungspflichten / Berufs- und besondere Amtsgeheimnisse und
- Übermittlung personenbezogener Daten in Drittländer.

1.4.1. Gesetzliche Geheimhaltungspflichten sowie Berufsgeheimnisse und besondere Amtsgeheimnisse, die nicht auf gesetzlichen Vorschriften beruhen

Anforderung in Kürze:

Werden die zu zertifizierenden Verarbeitungsvorgänge ausschließlich bzw. mehrheitlich (> 50%) von Verantwortlichen in Anspruch genommen, die nach EU- oder relevantem mitgliedstaatlichem Recht besonderen Geheimhaltungspflichten unterliegen, so MUSS der Auftragsverarbeiter dem im Verhältnis zu den Verantwortlichen und zu eventuellen weiteren Auftragsverarbeitern Rechnung tragen.[52]

Orientierungshilfe

Relevante Artikel der DSGVO:

Art. 28 Abs. 3 S. 2 lit. b) sowie Art. 9 Abs. 2 lit. i), Art. 9 Abs. 2 lit. h) i. V. m. Abs. 3, Art. 14 Abs. 5 lit. d) und Art. 90 DSGVO

Hintergrund:

Das Datenschutzrecht weist einen engen Zusammenhang zu gesetzlichen Geheimhaltungspflichten sowie zu Geheimhaltungspflichten, die aus Berufs- und besonderen Amtsgeheimnissen resultieren, auf. Das EU-Datenschutzrecht selbst begründet keine solchen besonderen Geheimhaltungspflichten, sondern verweist lediglich in einigen Vorschriften auf Berufsgeheimnisse und gleichwertige Geheimhaltungspflichten, die sich aus EU- und aus mitgliedstaatlichem Recht ergeben können, wobei Letzteres de facto die Regel ist. Die DSGVO verfolgt insoweit das Ziel, die

[52] Auch wenn die Zertifizierung auf Grundlage dieses Kriterienkatalogs (nur) dem Nachweis dient, dass EU-Datenschutzrecht bei Verarbeitungsvorgängen von Auftragsverarbeitern eingehalten wird, wäre es wegen des engen Zusammenhangs, den das EU-Datenschutzrecht zu den besonderen Geheimhaltungspflichten aufweist, inakzeptabel, wenn im Rahmen der Zertifizierung eventuell einschlägige Geheimhaltungspflichten (z. B. bei Verarbeitungsvorgängen im Gesundheitsbereich) nicht mitbetrachtet werden würden.

Vorschriften des europäischen Datenschutzrechts mit den auf Ebene der Mitgliedstaaten existierenden besonderen Geheimhaltungspflichten in Einklang zu bringen.

Beide Rechtsmaterien gelten parallel. Das bedeutet, dass auf Verarbeitungen, bezüglich derer sowohl besondere Geheimhaltungspflichten als auch die datenschutzrechtlichen Vorgaben zu beachten sind, beide Rechtsgebiete unabhängig voneinander Anwendung finden. Ist eine Datenverarbeitung zwar datenschutzrechtlich zulässig, verstößt sie aber gegen eine besondere Geheimhaltungspflicht, so ist sie insgesamt unzulässig. Ein solcher Verstoß kann u.a. auch daraus resultieren, dass personenbezogene Daten, die Gegenstand einer Geheimhaltungspflicht sind, einem Auftragsverarbeiter gegenüber offengelegt werden, der selbst nicht zur Geheimhaltung verpflichtet (worden) ist.

Aus den obigen Gesichtspunkten ergibt sich, dass es geboten ist, besondere Geheimhaltungspflichten, die gegebenenfalls im Hinblick auf zu zertifizierende Verarbeitungsvorgänge von Auftragsverarbeitern bestehen, im Rahmen einer Zertifizierung nach EuroPriSe mit zu betrachten.

Ende der Orientierungshilfe

Anforderung im Detail:

Voraussetzungen für die / Ausnahmen von der Anwendbarkeit der Anforderung:

Diese Anforderung ist nur dann anwendbar, wenn die zu zertifizierenden Verarbeitungsvorgänge ausschließlich bzw. mehrheitlich (> 50%) von Verantwortlichen in Anspruch genommen werden, die besonderen Geheimhaltungspflichten unterliegen.

Details zum Gegenstand der Anforderung:

Insoweit ist zwischen den nachfolgend beschriebenen Konstellationen zu unterscheiden:

1. Im Verhältnis zum Verantwortlichen, der einer besonderen Geheimhaltungspflicht unterliegt, gilt folgendes:

   - Die vom Auftragsverarbeiter vorzuhaltende Vorlage für einen Vertrag zur Auftragsverarbeitung bzw. die mit einzelnen Verantwortlichen geschlossenen Verträge[53] MÜSSEN die besondere Geheimhaltungspflicht adressieren.[54]
   - Soweit das anwendbare Unions- bzw. mitgliedstaatliche Recht vorsieht, dass der Auftragsverarbeiter von dem Verantwortlichen im Hinblick auf die einschlägige Geheimhaltungspflicht zur Verschwiegenheit zu verpflichten und auf die Konsequenzen eines eventuellen Verstoßes gegen diese Pflicht hinzuweisen ist, MUSS dies auch Gegenstand der vom Auftragsverarbeiter vorzuhaltenden Vorlage für einen Vertrag zur Auftragsverarbeitung bzw. der mit einzelnen Verantwortlichen geschlossenen Verträge sein.

[53] Vgl. hierzu Kapitel 1.2.1 dieses Kriterienkatalogs.

[54] Da diese Materie größtenteils auf nationaler Ebene geregelt ist, ist diese Anforderung relativ unbestimmt formuliert. Ihre konkrete Ausgestaltung in der Praxis richtet sich dann nach den Vorgaben, die das nationale Recht in diesem Bereich vorsieht. Dies jedenfalls solange, wie keine Anhaltspunkte dafür ersichtlich sind, dass hierdurch datenschutzrechtliche Bestimmungen in unzulässiger Weise eingeschränkt werden.

2. Im Verhältnis zu weiteren Auftragsverarbeitern (insbesondere Unterauftragsverarbeitern), denen gegenüber personenbezogene Daten, die einer besonderen Geheimhaltungspflicht unterliegen, offengelegt werden, gilt folgendes:

- Die einschlägige besondere Geheimhaltungspflicht MUSS in dem jeweiligen Vertrag zur Auftragsverarbeitung adressiert werden.[55]
- Soweit dies nach Unions- bzw. mitgliedstaatlichem Recht erforderlich ist, MUSS der Auftragsverarbeiter weitere Auftragsverarbeiter, die an den zu zertifizierenden Verarbeitungsvorgängen mitwirken, im Hinblick auf die einschlägige Geheimhaltungspflicht zur Verschwiegenheit verpflichten und sie auf die Konsequenzen eines eventuellen Verstoßes gegen diese Pflicht hinweisen.
- Gegebenenfalls MÜSSEN weitere Anforderungen des EU- bzw. mitgliedstaatlichen Rechts beachtet werden.

Relevantes Nationales Recht:

DE: § 203 StGB, §§ 1 Abs. 2 S. 3 sowie 22 und 29 BSDG[56]

Orientierungshilfe

Relevante Dokumente:

1. Auftragsverarbeitungsvertrag zwischen dem Auftragsverarbeiter (Zertifizierungskunden) und den Verantwortlichen, die die zu zertifizierenden Verarbeitungsvorgänge in Anspruch nehmen/beauftragen bzw. eine entsprechende Vertragsvorlage, wobei es sich hierbei auch um (an den relevanten Stellen ausgefüllte) Standardvertragsklauseln handeln kann.

2. Verträge, die der Auftragsverarbeiter mit weiteren Auftragsverarbeitern geschlossen hat, denen gegenüber personenbezogene Daten, die Gegenstand einer Geheimhaltungspflicht sind, offengelegt werden

3. Ggf. weitere Dokumente bzw. entsprechende Vorlagen, in denen der Auftragsverarbeiter bzw. weitere Auftragsverarbeiter im Hinblick auf die einschlägige Geheimhaltungspflicht zur Verschwiegenheit verpflichtet werden

Relevante Evaluationsmethoden:

Dokumentenprüfung, Interviews

Anwendungs-/Auslegungshilfen:

- DE: Kurzpapier Nr. 13 der DSK (zu 203 StGB)

Ende der Orientierungshilfe

[55] Vgl. hierzu die vorangegangene Fußnote sowie Kapitel 1.3.2 dieses Kriterienkatalogs.

[56] - Beispiele für gesetzliche Geheimhaltungspflichten sind § 43a Abs. 2 BRAO und § 62 StBerG.
- Beispiele für Berufsgeheimnisse, denen keine gesetzlichen Geheimhaltungspflichten zugrunde liegen, sind die ärztliche Schweigepflicht (vgl. § 9 MBO-Ä) oder die in den entsprechenden landesrechtlichen Berufsordnungen normierte Schweigepflicht für Psychotherapeuten.
- Beispiele für (gesetzlich geregelte) Amtsgeheimnisse sind das Steuergeheimnis (§ 30 AO) und das Sozialgeheimnis (§ 35 SGB V).

1.4.2. Übermittlung personenbezogener Daten in Drittländer

Zunächst ist darauf hinzuweisen, dass das EuroPriSe-Zertifizierungsprogramm für Auftragsverarbeiter selbst keine Zertifizierung gemäß Art. 46 Abs. 2 lit. f) DSGVO ist, die für die internationale Übermittlung personenbezogener Daten bestimmt ist, und daher keine angemessenen Garantien im Rahmen der Übermittlung personenbezogener Daten an Drittländer oder internationale Organisationen gemäß den in Art. 46 Abs. 2 lit. f) genannten Bedingungen bietet. Folglich muss der Auftragsverarbeiter (Zertifizierungsantragsteller) den/die Verantwortlichen darüber informieren, dass das EuroPriSe-Zertifizierungsprogramm für Auftragsverarbeiter selbst kein Übermittlungsinstrument im Sinne von Art. 46 Abs. 2 lit. f) DSGVO ist. Die unten aufgeführten spezifischen Anforderungen gelten nur, wenn der Auftragsverarbeiter personenbezogene Daten an einen Datenimporteur in einem Drittland übermittelt.

1.4.2.1. Vorliegen eines Angemessenheitsbeschlusses / geeigneter Garantien

Anforderung in Kürze:

Wenn die zu zertifizierenden Verarbeitungsvorgänge eine Übermittlung personenbezogener Daten an bzw. in Drittländer bzw. an internationale Organisationen beinhalten, MUSS der Auftragsverarbeiter die in Kapitel V der DSGVO niedergelegten Bedingungen einhalten.

Orientierungshilfe

Relevante Artikel der DSGVO:

Art. 44 ff. DSGVO

Hintergrund:

Eine Übermittlung personenbezogener Daten in Drittländer wird im Rahmen von zu zertifizierenden Verarbeitungsvorgängen von Auftragsverarbeitern insbesondere dann vorkommen, wenn der Auftragsverarbeiter auf die Dienstleistungen weiterer Auftragsverarbeiter, die außerhalb der EU / des EWR und damit in einem Drittland i. S. v. Art. 44 ff. DSGVO ansässig sind, zurückgreift. Nicht zuletzt im Kontext des Cloud Computings sind oft mehrere solcher Übermittlungen bzw. Weiterübermittlungen zu beobachten, da in vielen Fällen weitere Auftragsverarbeiter, die in Drittländern angesiedelt sind (z. B. Betreiber von Rechenzentren oder Unternehmen, die Support- und/oder Fernwartungsdienstleistungen erbringen), involviert sind.

Zu einer Übermittlung personenbezogener Daten in Drittländer kann es aber auch dann kommen, wenn der Auftragsverarbeiter innerhalb der EU bzw. des EWR ansässig ist (d. h. dort eine Niederlassung hat), die zu zertifizierenden Verarbeitungsvorgänge im Rahmen der Tätigkeiten dieser Niederlassung erfolgen und die Verarbeitungsvorgänge zumindest auch von Verantwortlichen, die außerhalb der EU bzw. des EWR ansässig sind, in Anspruch genommen werden, und dies auch Gegenstand des Zertifizierungsgegenstands (ToE) sein soll.[57] In einer solchen Konstellation ist zu prüfen, ob und inwieweit es im Rahmen der Verarbeitungsvorgänge zu einer Übermittlung personenbezogener Daten in Drittländer kommt.

[57] Das ToE könnte in einem solchen Fall aber ggf. auch auf Verarbeitungsvorgänge, die (nur) für Verantwortliche in der EU erbracht werden, beschränkt werden.

Schließlich kann eine Übermittlung in ein Drittland auch dann in Betracht kommen, wenn der Auftragsverarbeiter in einem solchen niedergelassen ist, die DSGVO gemäß Art. 3 Abs. 2 auf ihn Anwendung findet und ein die Verarbeitungsvorgänge in Anspruch nehmender, in der EU bzw. dem EWR ansässiger Verantwortlicher personenbezogene Daten zwecks Nutzung für die zu zertifizierenden Verarbeitungsvorgänge an den Auftragsverarbeiter im Drittland übermittelt[58] oder wenn ein weiterer Auftragsverarbeiter in der EU/dem EWR personenbezogene Daten an den Auftragsverarbeiter im Drittland (rück)übermittelt.

Ende der Orientierungshilfe

Anforderung im Detail:

Voraussetzungen für die / Ausnahmen von der Anwendbarkeit der Anforderung:

Diese Anforderung ist nur dann anwendbar, wenn die Inanspruchnahme der zu zertifizierenden Verarbeitungsvorgänge durch den Verantwortlichen zu einer Übermittlung personenbezogener Daten in Drittländer bzw. an internationale Organisationen führt.

Details zum Gegenstand der Anforderung:

Der Auftragsverarbeiter MUSS ein sogenanntes Transfer Impact Assessment (TIA) durchgeführt haben und der Zertifizierungsstelle die Ergebnisse zur Verfügung stellen. Bei der Durchführung des TIA sind die Empfehlungen 01/2020 des EDSA zu Maßnahmen zur Ergänzung von Übermittlungstools zur Gewährleistung des unionsrechtlichen Schutzniveaus für personenbezogene Daten zu beachten.

Der Auftragsverarbeiter MUSS sicherstellen, dass im Hinblick auf jede eventuelle Übermittlung personenbezogener Daten in Drittländer bzw. an internationale Organisationen sichergestellt ist, dass die Bedingungen des Kapitels V der DSGVO eingehalten werden, damit das durch die DSGVO gewährleistete Schutzniveau für natürliche Personen nicht untergraben wird.

Als Legitimation für eine Übermittlung personenbezogener Daten in Drittländer kommen nach Kapitel V der DSGVO insbesondere die folgenden Optionen in Betracht:

1. Angemessenheitsbeschluss der EU-Kommission gem. Art. 45 DSGVO[59],
2. Verbindliche interne Datenschutzvorschriften gem. Art. 46 Abs. 2 lit. b) i. V. m. Art. 47 DSGVO[60],

[58] So z. B. bei Webanalysediensten, wenn IP-Adressen ungekürzt an den Auftragsverarbeiter im Drittland übermittelt werden.

[59] Vgl. hierzu: https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_de. Auf Grundlage des Art. 45 DSGVO sind bislang Angemessenheitsbeschlüsse zu Japan und zum Vereinigten Königreich (UK) erlassen worden. Relevant sind aber auch die auf der Grundlage von Art. 25 Abs. 6 der RL 95/46/EG erlassenen Angemessenheitsbeschlüsse, die gem. Art. 45 Abs. 9 DSGVO bis auf weiteres in Kraft bleiben. Hierbei handelt es sich um Angemessenheitsbeschlüsse bzgl. Andorra, Argentinien, Guernsey, Faröer Inseln, Isle of Man, Israel, Jersey, Kanada (begrenzter Anwendungsbereich: Kommerzielle Organisationen), Neuseeland, Republik Korea, Schweiz und Uruguay. Stand: 10/2022

[60] Dieses Instrument kommt insbesondere im Verhältnis Auftragsverarbeiter zu weiterer Auftragsverarbeiter in Betracht. Dies aber nur dann, wenn beide derselben Unternehmensgruppe angehören oder derselben Gruppe von Unternehmen, die eine gemeinsame Wirtschaftstätigkeit ausüben, und wenn verbindliche interne Datenschutzvorschriften in Bezug auf

3. Standarddatenschutzklauseln gem. Art. 46 Abs. 2 lit. c) und d) DSGVO[61],
4. Genehmigte Verhaltensregeln gem. Art. 40 DSGVO[62],
5. Ein genehmigter Zertifizierungsmechanismus gem. Art. 42 DSGVO[63],
6. Einer der Ausnahmetatbestände nach Art. 49 DGSVO ist einschlägig.

   Wenn eine der Ausnahmen gemäß Art. 49 einschlägig ist, MUSS der Auftragsverarbeiter der Zertifizierungsstelle spezifische Informationen darüber zur Verfügung stellen, in welchen Situationen und unter welchen Bedingungen er sich auf die spezifische Ausnahme berufen wird.

Der Auftragsverarbeiter MUSS die Wahl eines bestimmten Übermittlungsinstruments gemäß Kapitel V der DSGVO begründen und dokumentieren.

Im Hinblick auf die in Art. 46 DSGVO vorgesehenen Übermittlungsinstrumente und insbesondere im Hinblick auf Standarddatenschutzklauseln ist folgendes zu beachten:

Hier MUSS im Einzelfall und gegebenenfalls in Zusammenarbeit mit dem Empfänger personenbezogener Daten im Drittland geprüft (und dokumentiert) werden, ob das Recht oder die Praxis des Drittlandes die Wirksamkeit der in den Übermittlungsinstrumenten nach Art. 46 DSGVO enthaltenen angemessenen Garantien beeinträchtigt.[64] Ist dies der Fall, MUSS der Auftragsverarbeiter ergänzende Maßnahmen treffen (und dokumentieren), um diese Schutzlücken zu schließen und das Schutzniveau auf das vom EU-Recht geforderte Niveau zu bringen. In Betracht kommen insoweit technische Maßnahmen, organisatorische

diese(s) Unternehmen(sgruppe) genehmigt worden sind. Es ist zudem stets darauf zu achten, dass die zu zertifizierenden Verarbeitungsvorgänge, die der Kunde als Auftragsverarbeiter erbringt, vom Anwendungsbereich der Binding Corporate Rules (BCR) umfasst sind. Grundsätzliche Voraussetzung hierfür ist zunächst einmal, dass es sich bei den verbindlichen internen Datenschutzvorschriften um sog. "BCR for Processors" handelt (vgl. insoweit auch Art. 4 Abs. 20 DSGVO). Gem. Art. 26 Abs. 2 RL 95/46/EG genehmigte verbindliche interne Datenschutzvorschriften bleiben nach Art. 46 Abs. 5 S. 1 DSGVO bis auf weiteres gültig. Eine Liste aller Unternehmen, deren BCR vor dem 25.05.2018 genehmigt worden sind, stellt die EU-Kommission im Internet bereit. Eine Liste aller Unternehmen, deren BCR seither genehmigt worden sind, findet sich auf der Website des EDSA: https://edpb.europa.eu/our-work-tools/accountability-tools/bcr_en.

[61] Im Juni 2021 veröffentlichte die Europäische Kommission Standarddatenschutzklauseln gemäß Art. 46 Abs. 2 lit. c) DSGVO für Übermittlungen personenbezogener Daten von Verantwortlichen oder Auftragsverarbeitern in der EU/im EWR (oder anderweitig der DSGVO unterliegend) an Verantwortliche oder Auftragsverarbeiter mit Sitz außerhalb der EU/des EWR (und nicht der DSGVO unterliegend). Diese Klauseln finden sich im Anhang des entsprechenden Durchführungsbeschlusses (EU) 2021/914 der Kommission, der seit dem 27.06.2021 wirksam ist. Sie werden die Standardvertragsklauseln ersetzen, die unter der vorherigen Datenschutzrichtlinie 95/46/EG verabschiedet wurden. Vgl. insoweit auch Art. 46 Abs. 5 DSGVO sowie Art. 4 Abs. 4 des Durchführungsbeschlusses, wonach die bisherigen Standardvertragsklauseln noch bis zum 27. Dezember 2022 geeignete Garantien im Sinne des Art. 46 Abs. 1 DSGVO bieten, sofern die Verarbeitungsvorgänge, die Gegenstand des Vertrags sind, unverändert bleiben und die Anwendung der Klauseln gewährleistet, dass die Übermittlung personenbezogener Daten geeigneten Garantien unterliegt (insoweit müssen im Hinblick auf das Schrems II-Urteil des EuGH (C-311/18) gegebenenfalls auch noch ergänzende Maßnahmen getroffen werden – die bloße Vereinbarung der Klauseln allein genügt in einem solchen Fall nicht). Diese Übergangsvorschrift erfasst alle Verträge, die vor dem 27. September 2021 auf Grundlage der Entscheidung 2001/497/EG oder des Beschlusses 2010/87/EU geschlossen wurden.

[62] zusammen mit rechtsverbindlichen und durchsetzbaren Verpflichtungen des Verantwortlichen oder des Auftragsverarbeiters in dem Drittland zur Anwendung der geeigneten Garantien

[63] vgl. die vorangegangene Fußnote

[64] Diese spezifische Risikoanalyse wird oft auch als „Transfer Impact Assessment" bezeichnet.

Maßnahmen und zusätzliche vertragliche Maßnahmen, wobei es im Einzelfall erforderlich sein kann, verschiedene dieser Maßnahmen zu kombinieren.

Bei der Implementierung zusätzlicher Maßnahmen sind die Empfehlungen 01/2020 des EDSA zu Maßnahmen zur Ergänzung von Übermittlungstools zur Gewährleistung des unionsrechtlichen Schutzniveaus für personenbezogene Daten zu beachten.

Wichtig:

Vertragliche und organisatorische Maßnahmen allein werden in der Regel nicht ausreichen, um den Zugriff von Behörden des Drittlandes auf personenbezogene Daten zu verhindern, denn es wird Situationen geben, in denen nur technische Maßnahmen einen solchen Zugriff verhindern oder unwirksam machen können.

Relevantes Nationales Recht:

Ggf. nationales Recht auf der Grundlage von Artt. 49 Abs. 1 lit. d) und g) sowie Abs. 5, 85 Abs. 2 DSGVO

Orientierungshilfe

Relevante Dokumente:

1. Ggf. verbindliche interne Datenschutzvorschriften nebst Nachweis bzgl. deren Genehmigung

2. Ggf. verwendete Standarddatenschutzklauseln

3. Ggf. Verhaltensregeln nebst Nachweis bzgl. deren Genehmigung

4. Ggf. Unterlagen zu einer Zertifizierung nach Art. 42 DSGVO

5. Ggf. ein Formular für eine Einwilligungserklärung, relevante Vertragsunterlagen etc. (Art. 49 DSGVO)

6. Ggf. Nachweise im Hinblick auf vom Auftragsverarbeiter implementierte ergänzende Maßnahmen

Relevante Evaluationsmethoden:

Dokumentenprüfung, Interviews

Anwendungs-/Auslegungshilfen:

- EuGH: Schrems II (C-311/18)
- EDSA (zu Schrems II):
  - Empfehlungen 01/2020 zu Maßnahmen zur Ergänzung von Übermittlungstools zur Gewährleistung des unionsrechtlichen Schutzniveaus für personenbezogene Daten (v2.0 des Dokuments liegt bislang nur in englischer Sprache vor – abrufbar hier)
  - Empfehlungen 02/2020 zu den wesentlichen europäischen Garantien in Bezug auf Überwachungsmaßnahmen
  - Häufig gestellte Fragen zum Urteil des Gerichtshofs der Europäischen Union in der Rechtssache C-311/18 – Data Protection Commissioner gegen Facebook Ireland Ltd und Maximillian Schrems
- EDSA (sonstiges):

- Leitlinien 2/2018 zu den Ausnahmen nach Artikel 49 der Verordnung 2016/679

  An dieser Stelle ist auf die folgende Aussage des EDSA zur Anwendbarkeit von Art. 49 DSGVO hinzuweisen: "Bei den Ausnahmeregelungen nach Artikel 49 handelt es sich also um Ausnahmen von dem allgemeinen Grundsatz, dass personenbezogene Daten nur dann an Drittländer übermittelt werden dürfen, wenn in diesem Drittland ein angemessenes Schutzniveau besteht oder geeignete Garantien vorgesehen wurden und den betroffenen Personen durchsetzbare und wirksame Rechte eingeräumt werden, damit sie ihre Grundrechte und Garantien weiterhin in Anspruch nehmen können. Im Einklang mit den Grundsätzen des Europäischen Rechts sind die Ausnahmen deshalb restriktiv auszulegen, damit die Ausnahme nicht zur Regel wird. Diese Sichtweise wird auch vom Wortlaut des Titels des Artikels 49 gestützt, wonach die Ausnahmeregelungen nur in bestimmten Fällen Anwendung finden ("Ausnahmen für bestimmte Fälle").

- Art. 29 WP (vom EDSA bestätigt): Diverse Dokumente zum Thema Binding Corporate Rules[65]

DE: Kurzpapier Nr. 4 der DSK

Use Cases:

Dieses Dokument stellt mittels der nachstehend aufgeführten Anwendungsfälle (Use Cases) zusätzliche Anwendungshilfen für die obige Anforderung 2.4.2 bereit.[66] Diese Use Cases betreffen die Übermittlung personenbezogener Daten in die Drittländer X, Y and Z. Sie basieren auf den vom EDSA in seinen Empfehlungen 01/2020 beschriebenen Use Cases 1, 2 und 6. Der Schwerpunkt der hier bereitgestellten Informationen liegt auf den Schritten 3 und 4 des vom EDSA in diesen Empfehlungen vorgeschlagenen Ablauf- bzw. Prüfplans.

Use Case 1: Ende-zu-Ende-verschlüsselte Speicherung personenbezogener Daten in einer Cloud, die von einem in X ansässigen Anbieter gehostet wird

Sachverhalt / Relevante Drittstaatenübermittlungen:

Ein in der EU ansässiger Auftragsverarbeiter (Datenexporteur)[67] bietet seinen Kunden (den für die Verarbeitung Verantwortlichen) die Möglichkeit, personenbezogene Daten in einer öffentlichen Cloud zu speichern, die von einem in X ansässigen Anbieter

[65] WP 256 rev.01, 257 rev.01, 263 rev.01, 264 und 265 zu BCR beziehen sich auf die Rechtslage unter der DSGVO (vgl. Art. 47) und sind allesamt vom EDSA bestätigt worden.

[66] Da dieser Kriterienkatalog nur Verarbeitungsvorgänge von Auftragsverarbeitern betrifft, sind die an dieser Stelle aufgelisteten Anwendungsfälle so gewählt, dass es sich bei den jeweiligen Datenexporteuren stets um Auftragsverarbeiter handelt. Die nachfolgenden Ausführungen betreffen ausschließlich das Thema Übermittlung personenbezogener Daten in Drittstaaten. Andere datenschutzrechtliche Fragestellungen, die sich aus den Anwendungsfällen ergeben können, werden nicht betrachtet.

[67] Der Klarstellung halber: Der Datenexporteur ist keine Tochtergesellschaft eines in X ansässigen Unternehmens.

(Datenimporteur) betrieben wird[68]. Der Speicherdienst kann für die Speicherung aller Arten von Daten (einschließlich personenbezogener Daten im Allgemeinen und besonderer Kategorien personenbezogener Daten) genutzt werden. Die entsprechenden Server befinden sich ausschließlich in X.

An der Erbringung des Dienstes sind keine anderen Stellen beteiligt und es finden auch keine Weiterübermittlungen statt. Schon an dieser Stelle ist festzuhalten, dass der Auftragsverarbeiter eine anspruchsvolle, dem Stand der Technik entsprechende Ende-zu-Ende-Verschlüsselung implementiert hat.

Zwischenergebnis:

Es erfolgt eine Übermittlung personenbezogener Daten von der EU nach X, da der vom Auftragsverarbeiter angebotene Dienst die Speicherung personenbezogener Daten auf Servern in X zum Gegenstand hat.[69]

Übermittlungsinstrument:

Bezüglich des Übermittlungsinstruments haben sich Datenexporteur und Datenimporteur auf die Standarddatenschutzklauseln 2021/914/EU geeinigt. Insoweit wurden weder Änderungen an den Klauseln als solchen vorgenommen noch zusätzliche Maßnahmen ergriffen, die direkt oder indirekt im Widerspruch zu den Klauseln stehen.

Zwischenergebnis:

Einschlägiges Übermittlungsinstrument sind vorliegend Standarddatenschutzklauseln gemäß Art. 46 Abs. 2 lit. c) DSGVO.

Wirksamkeit des Übermittlungsinstruments:

Rechtsvorschriften und/oder Praktiken des Drittlands

Als Nächstes müssen alle Rechtsvorschriften / Praktiken des Drittlands ermittelt werden, die die Wirksamkeit der geeigneten Garantien des einschlägigen Übermittlungsinstruments (hier: der Standarddatenschutzklauseln) im konkreten Fall beeinträchtigen könnten.

Hauptgegenstand dieser rechtlichen Prüfung sind die in dem jeweils einschlägigen Drittland geltenden Gesetze, die die Offenlegung personenbezogener Daten gegenüber Behörden vorschreiben oder diesen den Zugriff auf die Daten erlauben. Es wird insoweit noch einmal ausdrücklich darauf hingewiesen, dass diese Prüfung im Hinblick auf die konkret in Rede stehende Übermittlung personenbezogener Daten in das Drittland vorzunehmen ist.

Im vorliegenden Fall unterliegt der Datenimporteur einem Gesetz, das die elektronische Überwachung im Bereich der nationalen Sicherheit und der Auslandsaufklärung regelt. Dieses Gesetz („Gesetz A“) gilt für Anbieter elektronischer Kommunikationsdienste. Als ein Anbieter von Infrastructure-as-a-Service-Dienstleistungen wie Datenspeicher und

[68] Konkret erbringt der Datenimporteur Infrastructure as a Service-Dienstleistungen wie Datenspeicher und Rechenkapazität.

[69] An dieser Stelle ist aber darauf hinzuweisen, dass es bereits dann zu einer Übermittlung personenbezogener Daten nach X kommen würde, wenn sich die Server ausschließlich in der EU befänden, der Cloud-Anbieter jedoch zu Wartungs- oder Supportzwecken auf die Daten zugreifen könnte.

Rechenkapazität in einer öffentlichen Cloud ist der Datenimporteur als Anbieter eines elektronischen Kommunikationsdienstes nach dem einschlägigen nationalen Recht von X einzustufen[70], weshalb Gesetz A vorliegend anwendbar ist. Der Datenimporteur hat zudem bestätigt, dass er in der Vergangenheit Anfragen nach Datenzugriff von Behörden aus X erhalten hat.

Datenschutzniveau im Drittland

Nun ist zu prüfen, ob das im Drittland bestehende Datenschutzniveau dem in der EU garantierten Niveau der Sache nach gleichwertig ist. Auch diese Prüfung ist im Hinblick auf die konkret in Rede stehende Übermittlung personenbezogener Daten in das Drittland vorzunehmen.

Hierbei kann auf die Empfehlungen 02/2020 des EDSA zu den wesentlichen europäischen Garantien in Bezug auf Überwachungsmaßnahmen zurückgegriffen werden. Zu klären ist demnach, ob die im vorangegangenen Schritt ermittelten Rechtsvorschriften und/oder Praktiken des Drittlandes den Anforderungen der nachfolgend aufgelisteten wesentlichen europäischen Garantien genügen:

- Auf klaren, präzisen und zugänglichen Vorschriften beruhende Datenverarbeitung,
- Nachweis der Erforderlichkeit und Angemessenheit im Hinblick auf die verfolgten legitimen Ziele,
- Vorhandensein eines unabhängigen Aufsichtsmechanismus und
- Vorhandensein wirksamer Rechtsbehelfe für den Bürger.

Im vorliegenden Fall genügt es hier festzustellen, dass der Europäische Gerichtshof im Hinblick auf Gesetz A bereits entschieden hat, dass insoweit in X kein dem in der EU der Sache nach gleichwertiges Datenschutzniveau besteht: “Demzufolge lässt Gesetz A in keiner Weise erkennen, dass für die darin enthaltene Ermächtigung zur Durchführung von Überwachungsprogrammen zum Zweck der Auslandsaufklärung Einschränkungen bestehen. Genauso wenig ist erkennbar, dass für potenziell von diesen Programmen erfasste Nicht-X-Personen Garantien existieren. Unter diesen Umständen ist diese Vorschrift nicht geeignet, ein Schutzniveau zu gewährleisten, das dem durch die Charta der Grundrechte der Europäischen Union (GrCh) – in ihrer Auslegung durch die insoweit relevante Rechtsprechung, wonach eine gesetzliche Grundlage für Eingriffe in Grundrechte, um dem Grundsatz der Verhältnismäßigkeit zu genügen, den Umfang, in dem die Ausübung des betreffenden Rechts eingeschränkt wird, selbst festlegen sowie klare und präzise Regeln für die Tragweite und die Anwendung der betreffenden Maßnahme vorsehen und Mindesterfordernisse aufstellen muss – garantierten Niveau der Sache nach gleichwertig ist.” (zitiert aus dem entsprechenden Urteil des EuGH, das sich mit der Rechtslage in X befasst).

Zwischenergebnis:

Die im konkreten Fall einschlägigen Rechtsvorschriften und/oder Praktiken des Drittlandes X genügen den wesentlichen europäischen Garantien nicht und sind damit

[70] Zu den Anbietern elektronischer Kommunikationsdienste nach diesem Recht zählen u.a. auch Anbieter sogenannter „Remote-Computing-Dienste“, die die Bereitstellung von Computerspeicher- oder -verarbeitungsdiensten für die Öffentlichkeit über ein elektronisches Kommunikationssystem zum Gegenstand haben. Der Datenimporteur ist aufgrund der von ihm angebotenen IaaS-Dienstleistungen als Anbieter eines solchen „Remote-Computing-Dienstes“ anzusehen.

nicht geeignet, ein Schutzniveau zu gewährleisten, das dem in der EU garantierten Niveau der Sache nach gleichwertig ist. Folglich sind die Standarddatenschutzklauseln nicht wirksam, und es ist zu prüfen, ob wirksame zusätzliche Maßnahmen getroffen worden sind (siehe unten).

Vorhandensein wirksamer zusätzlicher Maßnahmen:

An dieser Stelle ist zu prüfen, ob zusätzliche Maßnahmen getroffen worden sind, die als Ergänzung zu den in dem betreffenden Übermittlungsinstrument (hier: den Standarddatenschutzklauseln) enthaltenen Garantien gewährleisten könnten, dass die übermittelten personenbezogenen Daten in dem Drittland ein Schutzniveau genießen, das dem in der EU garantierten Schutzniveau der Sache nach gleichwertig ist.

Im vorliegenden Fall hat der Auftragsverarbeiter zusätzliche technische Maßnahmen ergriffen. Genauer gesagt hat er eine anspruchsvolle, dem Stand der Technik entsprechende Ende-zu-Ende-Verschlüsselung eingeführt. Darüber hinaus hat der Auftragsverarbeiter keine weiteren zusätzlichen Maßnahmen ergriffen.

In Bezug auf die implementierte Ende-zu-Ende-Verschlüsselung hat der Auftragsverarbeiter im Einzelnen sichergestellt, dass[71]

- vor der Übermittlung eine leistungsfähige Verschlüsselungsmethode verwendet wird,
- der Verschlüsselungsalgorithmus und seine Parametrisierung dem Stand der Technik entsprechen und die nötige Robustheit aufweisen,
- die Verschlüsselungsstärke den spezifischen Zeitraum berücksichtigt, für den die Vertraulichkeit der verschlüsselten personenbezogenen Daten sicherzustellen ist,
- der Verschlüsselungsalgorithmus fehlerfrei durch ordnungsgemäß gepflegte Software implementiert ist,
- die Schlüssel zuverlässig verwaltet werden und
- die Kontrolle über die Schlüssel allein beim Datenexporteur liegt.

Dies bedeutet, dass die implementierte Ende-zu-Ende-Verschlüsselung alle Anforderungen erfüllt, die der EDSA in seinen Empfehlungen 01/2020 aufführt (vgl. dort Anwendungsfall 1 - Randnummer 84). Zusammen mit den Garantien, die in dem entsprechenden Übermittlungsinstrument (konkret: den Standarddatenschutzklauseln) enthalten sind, stellt diese Verschlüsselungslösung sicher, dass die übermittelten personenbezogenen Daten im Drittland ein Schutzniveau genießen, das dem in der EU garantierten Schutzniveau der Sache nach gleichwertig ist.

Da die implementierte Ende-zu-Ende-Verschlüsselungslösung als solche (zusammen mit den Standarddatenschutzklauseln) bereits ein solches Schutzniveau bietet, müssen hier keine weiteren zusätzlichen Maßnahmen ergriffen werden (mit anderen Worten: eine Kombination mehrerer zusätzlicher Maßnahmen ist nicht erforderlich).

Zwischenergebnis:

[71] Auflistung in (teilweise) verkürzter Form gegenüber den Empfehlungen 01/2020 des EDSA (vgl. dort Anwendungsfall 1 - Randnummer 84). Im Ergebnis soll hier aber davon ausgegangen werden, dass der Auftragsverarbeiter alle in den Empfehlungen aufgelisteten Anforderungen vollumfänglich einhält.

Der Auftragsverarbeiter hat zusätzliche (technische) Maßnahmen implementiert, die zusammen mit den in den Standarddatenschutzklauseln enthaltenen Garantien sicherstellen, dass die übermittelten personenbezogenen Daten im Drittland ein Schutzniveau genießen, das dem in der EU garantierten Schutzniveau der Sache nach gleichwertig ist.

Endergebnis:

Die Übermittlung personenbezogener Daten nach X ist im vorliegenden Fall zulässig.

Use Case 2: Übermittlung pseudonymisierter Gesundheitsdaten an einen in Y ansässigen spezialisierten Dienstleister

Sachverhalt / Relevante Drittstaatenübermittlungen:

Ein in der EU ansässiger Auftragsverarbeiter (Datenexporteur) soll für eine große medizinische Einrichtung (Verantwortlicher), die ebenfalls in der EU ansässig ist, Gesundheitsdaten analysieren, um bestimmte Korrelationen zu finden, die die Entwicklung neuer Behandlungsmethoden ermöglichen könnten. Zu diesem Zweck erhält der Auftragsverarbeiter personenbezogene Daten zu mehr als 10.000 Patienten. Bestimmte Analysevorgänge werden allerdings nicht vom Auftragsverarbeiter selbst, sondern von einem hierauf spezialisierten Unternehmen, das seinen Sitz in Y hat, durchgeführt.[72] Dieses Unternehmen (Datenimporteur) gehört zu einer Unternehmensgruppe, die vom Auftragsverarbeiter beherrscht wird.

An der Erbringung des Dienstes sind keine anderen Stellen beteiligt und es finden auch keine Weiterübermittlungen statt. Schon an dieser Stelle ist anzumerken, dass der Auftragsverarbeiter die Gesundheitsdaten pseudonymisiert, bevor er sie an den Datenimporteur übermittelt.

Zwischenergebnis:

Es erfolgt eine Übermittlung personenbezogener Daten von der EU nach Y.

Übermittlungsinstrument:

Der Auftragsverarbeiter hat der zuständigen Aufsichtsbehörde verbindliche interne Datenschutzvorschriften für Auftragsverarbeiter („Binding Corporate Rules for Processors“) vorgelegt, die von dieser nach Durchlaufen des entsprechenden Verfahrens genehmigt worden sind. Die hier in Rede stehende Übermittlung personenbezogener Daten nach Y wird vom materiellen Geltungsbereich der BCR umfasst.

Zwischenergebnis:

Als Übermittlungsinstrument kommen vorliegend verbindliche unternehmensinterne Datenschutzvorschriften für Auftragsverarbeiter gemäß Art. 47 DSGVO zum Einsatz.

Wirksamkeit des Übermittlungsinstruments:

Rechtsvorschriften und/oder Praktiken des Drittlands

Als Nächstes müssen alle Rechtsvorschriften / Praktiken des Drittlands ermittelt werden, die die Wirksamkeit der geeigneten Garantien des einschlägigen

[72] Die Analysevorgänge werden in Y auf eigenen Computersystemen des spezialisierten Unternehmens durchgeführt.

Übermittlungsinstruments (hier: der BCR für Auftragsverarbeiter) im konkreten Fall beeinträchtigen könnten.

Hauptgegenstand dieser rechtlichen Prüfung sind die in dem jeweils einschlägigen Drittland geltenden Gesetze, die die Offenlegung personenbezogener Daten gegenüber Behörden vorschreiben oder diesen den Zugriff auf die Daten erlauben. Es wird insoweit noch einmal ausdrücklich darauf hingewiesen, dass diese Prüfung im Hinblick auf die konkret in Rede stehende Übermittlung personenbezogener Daten in das Drittland vorzunehmen ist.

Im vorliegenden Fall unterliegt der Datenimporteur einem Gesetz („Gesetz B“), das die Zentralregierung oder die Regierung eines Bundesstaates dazu ermächtigt, eine Behörde der zuständigen Regierung anzuweisen, Informationen abzufangen, zu überwachen oder zu entschlüsseln, die in einer Computerressource[73] erzeugt, übertragen, empfangen oder gespeichert werden. Voraussetzung hierfür ist, dass die anweisende Stelle davon überzeugt ist, dass dies im Interesse der Souveränität oder Integrität von Y, seiner Verteidigung, der Sicherheit des Staates, der freundschaftlichen Beziehungen zu ausländischen Staaten, der öffentlichen Ordnung oder zur Verhinderung der Anstiftung zur Begehung einer diesbezüglichen erkennbaren Straftat oder zur Ermittlung einer Straftat notwendig oder zweckmäßig ist. Gleichzeitig werden Teilnehmer, Vermittler oder für die Computerressource verantwortliche Personen dazu verpflichtet, auf Ersuchen einer der oben genannten Behörden alle Erleichterungen und technische Unterstützung zu gewähren, um

(a) Zugang zu der Computerressource, die solche Informationen erzeugt, überträgt, empfängt oder speichert, zu gewähren oder den Zugang zu ihr zu sichern oder

(b) die Informationen abzufangen, zu überwachen oder zu entschlüsseln oder

(c) die in der Computerressource gespeicherten Informationen bereitzustellen.

Sofern die Voraussetzungen von Gesetz B vorliegen, können die zuständigen Stellen letztlich Informationen aus jeglichen Computerressourcen in ihren Besitz bringen. Folglich ist diese Vorschrift im vorliegenden Fall (potentiell) einschlägig.

In Ausübung der Befugnisse, die ihr durch Gesetz B übertragen worden sind, hat die Zentralregierung von Y eine einschlägige Verordnung („Verordnung C“) erlassen. Diese enthält u.a. Regeln dazu, wer Abhör- und Überwachungsanweisungen erlassen darf, wie diese Anweisungen auszuführen sind, wie lange sie in Kraft bleiben und an wen Daten weitergegeben werden dürfen sowie eine Verpflichtung dazu, alternative Mittel zur Informationsbeschaffung in Betracht zu ziehen. Zudem besagt eine weitere Regel, dass ein Überprüfungsausschuss, der sich aus ranghohen Mitgliedern der Zentral- bzw. Landesregierung (“secretaries to the government“) zusammensetzt, mindestens einmal alle zwei Monate zusammentreten muss, um alle Fälle von Abhören, Überwachung und Entschlüsselung zu überprüfen.

Der Oberste Gerichtshof von Y hat in einem Urteil das Recht auf Privatsphäre („Privacy“) als eine Ausprägung der Verfassung von Y und damit als Grundrecht anerkannt. Dem Gerichtshof zufolge umfasst dieses Recht unter anderem auch das Recht auf informationelle Selbstbestimmung (“informational privacy“). Das Grundrecht auf

[73] Der Begriff Computerressource bezeichnet hier einen Computer, ein Computersystem, ein Computernetz, Daten, eine Computerdatenbank oder Software.

Privatsphäre gilt auch für EU-Bürger. Der Gerichtshof hat in seinem Urteil Grundsätze wie "Rechtmäßigkeit, legitimes Ziel, Verhältnismäßigkeit und Verfahrensgarantien" im Rahmen des Rechts auf Privatsphäre als verbindlich anerkannt. Diese gesetzlichen Rechte gelten ebenfalls auch für EU-Bürger.

Y hat bislang kein umfassendes allgemeines Datenschutzgesetz.

Datenschutzniveau im Drittland

Nun ist zu prüfen, ob das im Drittland bestehende Datenschutzniveau dem in der EU garantierten Niveau der Sache nach gleichwertig ist. Auch diese Prüfung ist im Hinblick auf die konkret in Rede stehende Übermittlung personenbezogener Daten in das Drittland vorzunehmen.

Hierbei kann auf die Empfehlungen 02/2020 des EDSA zu den wesentlichen europäischen Garantien in Bezug auf Überwachungsmaßnahmen zurückgegriffen werden. Zu klären ist demnach, ob die im vorangegangenen Schritt ermittelten Rechtsvorschriften und/oder Praktiken des Drittlandes den Anforderungen der nachfolgend aufgelisteten wesentlichen europäischen Garantien genügen:

- Auf klaren, präzisen und zugänglichen Vorschriften beruhende Datenverarbeitung,
- Nachweis der Erforderlichkeit und Angemessenheit im Hinblick auf die verfolgten legitimen Ziele,
- Vorhandensein eines unabhängigen Aufsichtsmechanismus und
- Vorhandensein wirksamer Rechtsbehelfe für den Bürger.

An dieser Stelle kann keine ausführliche Analyse der in Y geltenden Rechtslage erfolgen, da dies den Rahmen eines Kriterienkatalogs sprengen würde. Es soll aber auf Folgendes hingewiesen werden:

Es fehlt im Recht von Y an einer expliziten Beschreibung der Personengruppen, die überwacht werden können. Eine solche ist aber nach der Rechtsprechung des Europäischen Gerichtshof für Menschenrechte (EGMR) erforderlich.[74] Somit ist fraglich, ob die Datenverarbeitung auf klaren, präzisen und zugänglichen Vorschriften beruht.

Die oben vorgestellten Überprüfungsausschüsse setzen sich aus ranghohen Mitgliedern der Zentral- bzw. Landesregierung (“secretaries to the government“) zusammen. Deshalb ist zu bezweifeln, dass es sich hierbei um einen unabhängigen Aufsichtsmechanismus handelt.

Zudem ist erneut darauf hinzuweisen, dass es in Y bislang kein allgemeines, umfassendes Datenschutzrecht gibt. Derzeit gibt es in Y auch keine unabhängige Datenschutzaufsichtsbehörde.

Zwischenergebnis:

Es bestehen erhebliche Zweifel daran, dass die im konkreten Fall einschlägigen Rechtsvorschriften und/oder Praktiken des Drittlandes Y den wesentlichen europäischen Garantien genügen und dass sie dazu geeignet sind, ein Schutzniveau zu gewährleisten, das dem in der EU garantierten Niveau der Sache nach gleichwertig ist. Folglich wird

[74] EGMR, 29. Juni 2006, Weber und Saravia (54934/00), Rn. 95. Vgl. hierzu auch die Empfehlungen 01/2020 des EDSA, Randnummer 30.

vorliegend davon ausgegangen, dass die verbindlichen internen Datenschutzvorschriften für Auftragsverarbeiter nicht wirksam sind, weshalb zu prüfen ist, ob wirksame zusätzliche Maßnahmen getroffen worden sind (siehe unten).

Vorhandensein wirksamer zusätzlicher Maßnahmen:

An dieser Stelle ist zu prüfen, ob zusätzliche Maßnahmen getroffen worden sind, die als Ergänzung zu den in dem betreffenden Übermittlungsinstrument (hier: den BCR für Auftragsverarbeiter) enthaltenen Garantien gewährleisten könnten, dass die übermittelten personenbezogenen Daten in dem Drittland ein Schutzniveau genießen, das dem in der EU garantierten Schutzniveau der Sache nach gleichwertig ist.

Im vorliegenden Fall hat der Auftragsverarbeiter zusätzliche technische Maßnahmen getroffen, die darin bestehen, die Gesundheitsdaten vor deren Übermittlung nach Y zu pseudonymisieren. Dabei ersetzt er Patientennamen durch zufällig generierte Kennnummern („Identifier“) und Angaben zu Alter, Größe und Gewicht durch Angaben zur Zugehörigkeit zu einer bestimmten Gruppe („Cluster“ - z. B Alter: 20-29 Jahre oder Gewicht: 70-79 kg). Die Gruppen sind dabei so gewählt, dass die Daten als solche (auch in einer Gesamtschau aller vorhandenen Informationen) nicht mehr einer spezifischen betroffenen Person zugeordnet werden können. Es werden nicht zuletzt auch keine Informationen zu Krankheiten und deren Umständen gespeichert, die so einzigartig sind, dass es im Bereich des Möglichen liegen könnte, hierdurch Rückschlüsse auf die Identität einzelner Patienten zu ziehen. Schließlich betreffen die Daten nicht die Nutzung von Informationsdiensten.[75]

Der Auftragsverarbeiter speichert die zusätzlichen Informationen, mittels derer die pseudonymisierten Daten (wieder) einer spezifischen Person zugeordnet werden können, in einer dedizierten, nach dem aktuellen Stand der Technik abgesicherten Datenbank, die sich auf Servern innerhalb der EU befindet, und über die er die alleinige Kontrolle hat.[76]

Über die Pseudonymisierung hinaus hat der Auftragsverarbeiter keine weiteren zusätzlichen Maßnahmen ergriffen.

Aus den obigen Ausführungen ergibt sich, dass der Auftragsverarbeiter in Bezug auf die implementierte Pseudonymisierung Folgendes sichergestellt hat:[77]

- Er übermittelt die personenbezogenen Daten in solcher Weise, dass sie ohne Hinzuziehung zusätzlicher Informationen keiner spezifischen betroffenen Person zugeordnet werden können,
- die zusätzlichen Informationen werden allein von ihm und separat gehalten, und zwar in einem Mitgliedstaat der EU,

[75] Hierzu vgl. Anwendungsfall 2 – Randnummern 86 ff. der Empfehlungen 01/2020 des EDSA.

[76] Auch wenn der Datenimporteur zur selben Unternehmensgruppe gehört wie der Auftragsverarbeiter, verfügt er nicht über technische Berechtigungen, um auf diese Datenbank zuzugreifen. Auf Seiten des Auftragsverarbeiters gibt es eine Arbeitsanweisung, durch die die Mitarbeiter dazu angewiesen werden, Mitarbeitern anderer Unternehmen der Unternehmensgruppe unter keinen Umständen die Möglichkeit eines Zugriffs auf diese Datenbank einzuräumen bzw. die in der Datenbank gespeicherten zusätzlichen Informationen an diese weiterzugeben oder sie auf sonstige Weise diesen gegenüber offenzulegen.

[77] Auflistung in (teilweise) verkürzter Form gegenüber den Empfehlungen 01/2020 des EDSA (vgl. dort Anwendungsfall 2 - Randnummer 85). Im Ergebnis soll hier aber davon ausgegangen werden, dass der Auftragsverarbeiter alle in den Empfehlungen aufgelisteten Anforderungen vollumfänglich einhält.

- die Offenlegung oder die unerlaubte Verwendung der zusätzlichen Informationen wird durch geeignete technische und organisatorische Garantien verhindert, und es ist gewährleistet, dass die Kontrolle über den Datenspeicher, der die Re-Identifizierung anhand der zusätzlichen Informationen ermöglicht, allein beim Auftragsverarbeiter liegt,
- er hat durch gründliche Analyse der betreffenden Daten, unter Berücksichtigung sämtlicher Informationen, die den Behörden im Empfängerland zur Verfügung stehen mögen, festgestellt, dass die pseudonymisierten personenbezogenen Daten keiner identifizierten oder identifizierbaren natürlichen Person zugeordnet werden können, selbst wenn sie mit derartigen Informationen abgeglichen werden sollten.

Dies bedeutet, dass die implementierte Pseudonymisierung alle Anforderungen erfüllt, die der EDSA in seinen Empfehlungen 01/2020 aufführt (vgl. dort Anwendungsfall 2 - Randnummer 85).[78] Zusammen mit den Garantien, die in dem entsprechenden Übermittlungsinstrument (d. h. den verbindlichen internen Datenschutzvorschriften für Auftragsverarbeiter) enthalten sind, stellt diese Pseudonymisierungslösung sicher, dass die übermittelten personenbezogenen Daten im Drittland ein Schutzniveau genießen, das dem in der EU garantierten Schutzniveau der Sache nach gleichwertig ist.

Da die implementierte Pseudonymisierungslösung als solche (zusammen mit den BCR für Auftragsverarbeiter) bereits ein solches Schutzniveau bietet, müssen hier keine weiteren zusätzlichen Maßnahmen ergriffen werden (mit anderen Worten: eine Kombination mehrerer zusätzlicher Maßnahmen ist nicht erforderlich).

Zwischenergebnis:

Der Auftragsverarbeiter hat zusätzliche (technische) Maßnahmen implementiert, die zusammen mit den in den verbindlichen internen Datenschutzvorschriften für Auftragsverarbeiter enthaltenen Garantien sicherstellen, dass die übermittelten personenbezogenen Daten im Drittland ein Schutzniveau genießen, das dem in der EU garantierten Schutzniveau der Sache nach gleichwertig ist.

Endergebnis:

Die Übermittlung personenbezogener Daten nach Y ist im vorliegenden Fall zulässig.

Use Case 3: Übermittlung von Verbraucherdaten an ein in Z ansässiges Callcenter

Sachverhalt / Relevante Drittstaatenübermittlungen:

Ein in der EU ansässiges Callcenter (Auftragsverarbeiter / Datenexporteur) erbringt für einen ebenfalls in der EU ansässigen Online-Versandhändler (Verantwortlicher) Dienstleistungen in den Bereichen Kundendienst, Beschwerdemanagement und

[78] Es ist darauf hinzuweisen, dass Teilnehmer, Vermittler oder für die Computerressource verantwortliche Personen nach Gesetz B dazu verpflichtet sind, die befugten Stellen auf deren Anweisung bei der Entschlüsselung verschlüsselter Informationen zu unterstützen. Nach Verordnung C bezeichnet "Entschlüsselung" den Prozess der Umwandlung von Informationen in unverständlicher Form in eine verständliche Form mittels einer mathematischen Formel, eines Codes, eines Kennworts oder eines Algorithmus oder einer Kombination davon. Ob diese Legaldefinition auch die Offenlegung zusätzlicher Informationen nach Art. 4 Nr. 5 DSGVO umfasst, kann dahin gestellt bleiben, da im vorliegenden Fall der Auftragsverarbeiter die alleinige Kontrolle über diese Informationen bzw. die entsprechende Datenbank hat.

Markforschung. Hierzu kann der Auftragsverarbeiter auf personenbezogene Daten[79] von mehr als 100.000 Verbrauchern zugreifen, die auf Servern in der EU gespeichert sind.[80] Bei der Erbringung der Dienstleistungen lässt sich der Auftragsverarbeiter bei Bedarf (z. B. bei Belastungsspitzen) durch ein anderes Callcenter (Datenimporteur) unterstützen, das seinen Sitz in Z hat. Zu diesem Zweck erhält auch der Datenimporteur Zugriff auf (potentiell) alle personenbezogenen Daten im Klartext.

An der Erbringung des Dienstes sind keine anderen Stellen beteiligt und es finden auch keine Weiterübermittlungen statt.

Zwischenergebnis:

Der Datenimporteur greift per Fernzugriff auf die personenbezogenen Daten von Verbrauchern zu, weshalb eine Übermittlung personenbezogener Daten von der EU nach Z vorliegt.[81]

Übermittlungsinstrument:

Bezüglich des Übermittlungsinstruments haben sich Datenexporteur und Datenimporteur auf von einer Aufsichtsbehörde angenommene Standarddatenschutzklauseln, die von der Europäischen Kommission gemäß dem Prüfverfahren nach Art. 93 Abs. 2 DSGVO genehmigt wurden, geeinigt. Insoweit wurden weder Änderungen an den Klauseln als solchen vorgenommen noch zusätzliche Maßnahmen ergriffen, die direkt oder indirekt im Widerspruch zu den Klauseln stehen.

Zwischenergebnis:

Einschlägiges Übermittlungsinstrument sind vorliegend Standarddatenschutzklauseln gemäß Art. 46 Abs. 2 lit. d) DSGVO.

Wirksamkeit des Übermittlungsinstruments:

Rechtsvorschriften und/oder Praktiken des Drittlands

Als Nächstes müssen alle Rechtsvorschriften / Praktiken des Drittlands ermittelt werden, die die Wirksamkeit der geeigneten Garantien des einschlägigen Übermittlungsinstruments (hier: der Standarddatenschutzklauseln) im konkreten Fall beeinträchtigen könnten.

Hauptgegenstand dieser rechtlichen Prüfung sind die in dem jeweils einschlägigen Drittland geltenden Gesetze, die die Offenlegung personenbezogener Daten gegenüber Behörden vorschreiben oder diesen den Zugriff auf die Daten erlauben. Es wird insoweit noch einmal ausdrücklich darauf hingewiesen, dass diese Prüfung im Hinblick auf die konkret in Rede stehende Übermittlung personenbezogener Daten in das Drittland vorzunehmen ist.

Im vorliegenden Fall unterliegt der Datenimporteur einem Gesetz („Gesetz D“), das die Überwachung der Kommunikation sowohl im Rahmen von Strafverfahren als auch

[79] Hierbei handelt es sich um Name, Adresse, weitere Kontaktdaten, demografische Daten und Vertragsdaten.

[80] Bei der Verarbeitung dieser personenbezogenen Daten hat das Callcenter (Auftragsverarbeiter) keine wesentlichen eigenen Entscheidungsspielräume.

[81] Vgl. hierzu Randnummer 13 der Empfehlungen 01/2020 des EDSA.

außerhalb dieses Rahmens, insbesondere im Zusammenhang mit "Ereignissen oder Aktivitäten, die die nationale, militärische, wirtschaftliche oder ökologische Sicherheit gefährden", regelt.[82] Für die Zwecke dieses Anwendungsfalls liegt der Schwerpunkt der Betrachtung auf Letzterem.

Zu den operativen Suchaktivitäten gemäß Gesetz D gehören u.a. die Überwachung des Post-, Telegraphen-, Telefon- und sonstigen Nachrichtenverkehrs sowie die Erhebung von Daten aus technischen Kommunikationskanälen. Da es in diesem Anwendungsfall um ein Callcenter geht, konzentrieren sich die folgenden Ausführungen auf das Abhören der telefonischen Kommunikation.[83]

Die entsprechenden operativen Suchaktivitäten können nach Erhalt von Informationen (u.a.) über Ereignisse oder Aktivitäten, die die nationale, militärische, wirtschaftliche oder ökologische Sicherheit von Z gefährden, auf der Grundlage eines Gerichtsbeschlusses durchgeführt werden.

Unter der Voraussetzung, dass die Anforderungen von Gesetz D erfüllt sind, können die mit operativen Suchaktivitäten befassten Behörden personenbezogene Daten in ihren Besitz bringen, die durch die Überwachung von Telefongesprächen gewonnen wurden. Daher ist dieses Gesetz im vorliegenden Fall (potenziell) einschlägig.

An dieser Stelle ist darauf hinzuweisen, dass der Europäische Gerichtshof für Menschenrechte (EGMR) festgestellt hat, dass die Rechtsvorschriften von Z über das Abhören der Kommunikation keine angemessenen und wirksamen Garantien gegen Willkür und die Gefahr von Missbrauch bieten.

Angesichts mehrerer von ihm festgestellter Mängel[84] befand der Gerichtshof, dass das Recht von Z nicht den Anforderungen an die „Qualität des Rechts“ entspricht und nicht geeignet ist, den „Eingriff“ auf das zu beschränken, was „in einer demokratischen Gesellschaft notwendig“ ist. Aus diesem Grund bejahte der EGMR eine Verletzung von Art. 8 der Europäischen Menschenrechtskonvention (EMRK).

Kurzer Überblick über die Rechtsquellen des Datenschutzrechts von Z:

Zwei Artikel der Verfassung von Z bilden die verfassungsrechtliche Grundlage für den Datenschutz.[85]

Z hat das Übereinkommen von 1981 zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten (Übereinkommen 108) ratifiziert. Z hat das Protokoll zur Änderung des Übereinkommens zum Schutz des Menschen bei der

[82] Da es hier um personenbezogene Daten von EU-Bürgern geht, ist darauf hinzuweisen, dass die Staatsangehörigkeit und die Nationalität kein Hindernis für die Einleitung operativer Suchaktivitäten auf dem Territorium von Z darstellen, es sei denn, ein Bundesgesetz sieht etwas Anderes vor.

[83] Es ist davon auszugehen, dass bei Telefongesprächen zwischen dem Callcenter und den Verbrauchern persönliche Daten über letztere zur Sprache kommen, die der jeweilige Mitarbeiter während des Gesprächs entweder von den Servern in der EU abruft oder neu erhebt und dann auf den Servern in der EU speichert.

[84] Diese Mängel werden weiter unten im Detail vorgestellt.

[85] Am wichtigsten für diesen Anwendungsfall ist der folgende Artikel: „Jeder hat das Recht auf das Geheimnis des Schriftverkehrs, von Telefongesprächen, postalischen, telegraphischen und anderen Mitteilungen. Eine Einschränkung dieses Rechts ist nur aufgrund einer gerichtlichen Entscheidung zulässig.“

automatischen Verarbeitung personenbezogener Daten (Vertrag 223) unterzeichnet, hat es aber noch nicht ratifiziert.

Gesetzliche Regelungen zum Datenschutz finden sich im Gesetz über personenbezogene Daten von Z.

Die wichtigste Aufsichtsbehörde für den Datenschutz ist der Föderale Dienst für die Aufsicht im Bereich der Kommunikation, Informationstechnologie und Massenkommunikation.

Datenschutzniveau im Drittland

Nun ist zu prüfen, ob das im Drittland bestehende Datenschutzniveau dem in der EU garantierten Niveau der Sache nach gleichwertig ist. Auch diese Prüfung ist im Hinblick auf die konkret in Rede stehende Übermittlung personenbezogener Daten in das Drittland vorzunehmen.

Hierbei kann auf die Empfehlungen 02/2020 des EDSA zu den wesentlichen europäischen Garantien in Bezug auf Überwachungsmaßnahmen zurückgegriffen werden. Zu klären ist demnach, ob die im vorangegangenen Schritt ermittelten Rechtsvorschriften und/oder Praktiken des Drittlandes den Anforderungen der nachfolgend aufgelisteten wesentlichen europäischen Garantien genügen:

- Auf klaren, präzisen und zugänglichen Vorschriften beruhende Datenverarbeitung,
- Nachweis der Erforderlichkeit und Angemessenheit im Hinblick auf die verfolgten legitimen Ziele,
- Vorhandensein eines unabhängigen Aufsichtsmechanismus und
- Vorhandensein wirksamer Rechtsbehelfe für den Bürger.

An dieser Stelle kann keine ausführliche Analyse der in Z geltenden Rechtslage erfolgen, da dies den Rahmen eines Kriterienkatalogs sprengen würde. Es soll aber auf Folgendes hingewiesen werden: Im seinem Urteil über die gesetzlichen Bestimmungen von Z über die Überwachung der Kommunikation hat der EGMR Mängel in den (damaligen) Gesetzen und Praktiken von Z zur Überwachung des Fernmeldeverkehrs festgestellt. Diese Mängel betrafen alle europäischen Grundgarantien, wie im Folgenden dargelegt wird:

Klare, präzise und zugängliche Vorschriften:

- Die Voraussetzungen, unter denen die Behörden zu geheimen Überwachungsmaßnahmen befugt sind, sind nicht klar genug definiert;

Erforderlichkeit und Angemessenheit:

- Die Regelungen zur Beendigung heimlicher Überwachungsmaßnahmen bieten keine ausreichenden Garantien gegen willkürliche Eingriffe;
- Das innerstaatliche Recht erlaubt die automatische Speicherung offensichtlich irrelevanter Daten;

Unabhängiger Aufsichtsmechanismus:

- Die Genehmigungsverfahren sind nicht geeignet, um sicherzustellen, dass geheime Überwachungsmaßnahmen nur dann angeordnet werden, wenn sie "in einer demokratischen Gesellschaft notwendig sind";

- Die Aufsicht über Überwachungsmaßnahmen erfüllt nicht die Anforderungen an Unabhängigkeit, Befugnisse und Zuständigkeiten, die für eine wirksame und kontinuierliche Kontrolle, eine öffentliche Prüfung und die Wirksamkeit in der Praxis ausreichen;

Wirksame Rechtsbehelfe:

- Die Wirksamkeit der Rechtsbehelfe wird dadurch untergraben, dass die Abhörmaßnahmen zu keinem Zeitpunkt mitgeteilt werden und kein angemessener Zugang zu den Unterlagen über die Abhörmaßnahmen besteht.

Aus den obigen Ausführungen wird deutlich, dass die Rechtsvorschriften und Praktiken von Z zum Zeitpunkt des Urteils des EGMR nicht den wesentlichen europäischen Garantien entsprachen. Seitdem haben sich die Gesetze und Praktiken in dieser Hinsicht nicht zum Besseren hin geändert. Vielmehr wurden neue Gesetze eingeführt, die den Geheimdiensten noch mehr Befugnisse einräumen und umfangreiche Speicherpflichten für Telekommunikationsanbieter vorsehen. Hier sind insbesondere mehrere Gesetze zur Terrorismusbekämpfung zu nennen:

Die entsprechenden Gesetzesänderungen sehen unter anderem vor, dass Telekommunikationsanbieter Textnachrichten, Sprachinformationen, Bilder, Töne, Videos und andere Nachrichten von Nutzern von Kommunikationsdiensten (Inhaltsdaten) sechs Monate lang und die dazugehörigen Metadaten drei Jahre lang speichern müssen. Telekommunikationsunternehmen sind verpflichtet, diese Inhalts- und Metadaten sowie "andere erforderliche Informationen" auf Anfrage und ohne Gerichtsbeschluss an die die zuständigen Behörden weiterzugeben.

Es sei außerdem auch darauf hingewiesen, dass die wichtigste Aufsichtsbehörde für den Datenschutz in Z nicht nur für die Datenschutzaufsicht zuständig ist, sondern daneben auch eine Vielzahl anderer Aufgaben (einschließlich der Zensur von Massenmedien in Z) wahrnimmt, und dass diese Behörde dem Ministerium für digitale Entwicklung, Kommunikation und Massenmedien untersteht. Daher ist es zumindest fraglich, ob diese Aufsichtsbehörde bei der Wahrnehmung der Aufgaben als Datenschutzaufsichtsbehörde unabhängig handelt.

Zwischenergebnis:

Es bestehen erhebliche Zweifel daran, dass die im konkreten Fall einschlägigen Rechtsvorschriften und/oder Praktiken des Drittlandes Z den wesentlichen europäischen Garantien genügen und dass sie dazu geeignet sind, ein Schutzniveau zu gewährleisten, das dem in der EU garantierten Niveau der Sache nach gleichwertig ist. Folglich wird vorliegend davon ausgegangen, dass die Standarddatenschutzklauseln nicht wirksam sind, weshalb zu prüfen ist, ob wirksame zusätzliche Maßnahmen getroffen worden sind (siehe unten).

Vorhandensein wirksamer zusätzlicher Maßnahmen:

An dieser Stelle ist zu prüfen, ob zusätzliche Maßnahmen getroffen worden sind, die als Ergänzung zu den in dem betreffenden Übermittlungsinstrument (hier: den Standardvertragsklauseln) enthaltenen Garantien gewährleisten könnten, dass die übermittelten personenbezogenen Daten in dem Drittland ein Schutzniveau genießen, das dem in der EU garantierten Schutzniveau der Sache nach gleichwertig ist.

Dem EDSA zufolge wird es Situationen geben, insbesondere wenn der Zugriff zu Überwachungszwecken erfolgt, in denen es nur mit technischen Maßnahmen möglich ist, den Zugriff staatlicher Stellen im Drittland auf personenbezogene Daten zu verhindern

oder ineffektiv zu machen.[86] Der vorliegende Anwendungsfall ist ein solcher Fall. Es ist daher zu prüfen, ob der Auftragsverarbeiter wirksame technische zusätzliche Maßnahmen ergriffen hat.

Die in Rede stehenden personenbezogenen Daten werden nicht in Übereinstimmung mit den entsprechenden Anforderungen des EDSA verschlüsselt oder pseudonymisiert.[87] Vielmehr hat der Datenimporteur Zugriff auf die personenbezogenen Daten im Klartext, und es gibt keine wirksamen technischen Maßnahmen, die das Abhören von Telefongesprächen zwischen dem Datenimporteur und Verbrauchern verhindern. Daher sind vorliegend keine wirksamen technischen Zusatzmaßnahmen vorhanden.[88]

Zwischenergebnis:

Der Auftragsverarbeiter hat keine zusätzlichen (technischen) Maßnahmen implementiert, die zusammen mit den in den Standardvertragsklauseln enthaltenen Garantien sicherstellen, dass die übermittelten personenbezogenen Daten im Drittland ein Schutzniveau genießen, das dem in der EU garantierten Schutzniveau der Sache nach gleichwertig ist.

Endergebnis:

Die Übermittlung personenbezogener Daten nach Z ist im vorliegenden Fall unzulässig.

Ende der Orientierungshilfe

1.4.2.2. Weisungsgebundenheit im Hinblick auf Übermittlung personenbezogener Daten in Drittländer

Anforderung in Kürze:

Der Auftragsverarbeiter darf personenbezogene Daten nur dann in Drittländer übermitteln, wenn dies in Übereinstimmung mit den Weisungen des Verantwortlichen geschieht. Der entsprechende Auftragsverarbeitungsvertrag bzw. die vom Auftragsverarbeiter verwendete Vertragsvorlage MUSS hierzu Regelungen treffen.

Orientierungshilfe

Relevante Artikel der DSGVO:

Art. 28 Abs. 3 S. 2 lit. a) DSGVO

Hintergrund:

Ein Auftragsverarbeitungsvertrag muss u.a. vorsehen, dass der Auftragsverarbeiter personenbezogene Daten grundsätzlich[89] nur auf dokumentierte Weisung des Verantwortlichen verarbeitet. Entsprechendes gilt gem. Art. 28 Abs. 4 Satz 1 DSGVO auch für Verträge zwischen einem Auftragsverarbeiter und weiteren Auftragsverarbeitern.

[86] Siehe Randnummer 53 der Empfehlungen 01/2020 des EDSA.

[87] Siehe Anwendungsfall 1 (Randnummer 84) und Anwendungsfall 2 (Randnummern 85 ff.) der Empfehlungen 01/2020 des EDSA.

[88] Dies folgt aus Randnummer 93 und Anwendungsfall 6 (Randnummern 94 ff.) der Empfehlungen 01/2020 des EDSA.

[89] Etwas anderes gilt nur dann, wenn der Auftragsverarbeiter durch EU- oder mitgliedstaatliches Recht zu einer bestimmten Verarbeitung verpflichtet ist.

In diesem Zusammenhang MUSS auch festgelegt werden, ob eine Verarbeitung in einem Drittland außerhalb der Union oder durch eine internationale Organisation erfolgen darf.

Ende der Orientierungshilfe

Anforderung im Detail:

Voraussetzungen für die / Ausnahmen von der Anwendbarkeit der Anforderung:

Diese Anforderung ist nur dann anwendbar, wenn die Inanspruchnahme der zu zertifizierenden Verarbeitungsvorgänge durch den Verantwortlichen zu einer Übermittlung personenbezogener Daten in Drittländer bzw. an internationale Organisationen führt.

Details zum Gegenstand der Anforderung:

Übermittelt der Auftragsverarbeiter im Rahmen der zu zertifizierenden Verarbeitungsvorgänge personenbezogene Daten in Drittländer, so MÜSSEN die vom Auftragsverarbeiter verwendete Vorlage für einen Vertrag nach Art. 28 Abs. 3 DSGVO bzw. die mit einzelnen Verantwortlichen abgeschlossenen Verträge einen Passus enthalten, der regelt, dass und inwieweit bzw. unter welchen Voraussetzungen ihm dies gestattet ist. Entsprechendes gilt ggf. auch für Verträge zwischen dem Auftragsverarbeiter und weiteren Auftragsverarbeitern.

Relevantes Nationales Recht:

N/A

Orientierungshilfe

Relevante Dokumente:

1. Auftragsverarbeitungsvertrag zwischen dem Auftragsverarbeiter (Zertifizierungskunden) und den Verantwortlichen, die die zu zertifizierenden Verarbeitungsvorgänge in Anspruch nehmen/beauftragen bzw. eine entsprechende Vertragsvorlage, wobei es sich hierbei auch um (an den relevanten Stellen ausgefüllte) Standardvertragsklauseln handeln kann.

2. Verträge, die der Auftragsverarbeiter mit weiteren Auftragsverarbeitern geschlossen hat

Relevante Evaluationsmethoden:

Dokumentenprüfung, Interviews

Anwendungs-/Auslegungshilfen:

N/A

Ende der Orientierungshilfe

1.5. Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen

Dieses Kapitel betrifft Anforderungen, die auf die Grundsätze Datenschutz durch Technikgestaltung und Datenschutz durch datenschutzfreundliche Voreinstellungen zurückzuführen sind. Die DSGVO verpflichtet unmittelbar nur den Verantwortlichen zur Beachtung dieser Grundsätze. Da dieser die Grundsätze aber nicht nur bei der Auswahl von (IT-)Produkten, sondern auch bei der Auswahl geeigneter Auftragsverarbeiter zu berücksichtigen hat, sind auch Auftragsverarbeiter mittelbar Adressat des insoweit

einschlägigen Art. 25 DSGVO.[90] Deshalb ist im Rahmen einer Zertifizierung von Verarbeitungsvorgängen von Auftragsverarbeitern zu prüfen, ob die zu zertifizierenden Verarbeitungsvorgänge den Grundsätzen Datenschutz durch Technikgestaltung und Datenschutz durch datenschutzfreundliche Voreinstellungen gerecht werden.

1.5.1. Datenschutz durch Technikgestaltung

Anforderung in Kürze:

Der Auftragsverarbeiter MUSS dem Grundsatz Datenschutz durch Technikgestaltung Rechnung tragen. Dies kann er entweder tun, indem er selbst technische und organisatorische Maßnahmen trifft, die dafür ausgelegt sind, die Datenschutzgrundsätze des Art. 5 DSGVO umzusetzen, oder indem er es den Verantwortlichen durch die Gestaltung der zu zertifizierenden Verarbeitungsvorgänge ermöglicht, im Hinblick auf diese solche Maßnahmen zu treffen. Er MUSS im Sinne einer kontinuierlichen Verbesserung in einem Managementsystem Prozesse implementieren, die die Berücksichtigung des Grundsatzes Datenschutz durch Technikgestaltung sowohl zum Zeitpunkt der Auswahl bzw. Festlegung der Mittel (Planungsphase) als auch zum Zeitpunkt der eigentlichen Verarbeitung gewährleisten. Die jeweiligen Vorgänge und Ergebnisse sind zu dokumentieren.

Konkrete Maßnahmen, die insoweit erforderlich sind, sind Gegenstand von Kapitel 2 dieses Kriterienkatalogs (technische und organisatorische Maßnahmen).

Orientierungshilfe

Relevante Artikel der DSGVO:

Art. 25 Abs. 1 i. V. m. Art. 5 DSGVO

Ende der Orientierungshilfe

Anforderung im Detail:

Voraussetzungen für die / Ausnahmen von der Anwendbarkeit der Anforderung:

Diese Anforderung ist stets anwendbar. Je nach der Art der zu zertifizierenden Verarbeitungsvorgänge kommen insoweit unterschiedliche Maßnahmen in Betracht. Deshalb sind die zu treffenden Maßnahmen stets im Hinblick auf den konkreten Zertifizierungsgegenstand zu bestimmen.

Details zum Gegenstand der Anforderung:

Der Auftragsverarbeiter MUSS die zu zertifizierenden Verarbeitungsvorgänge so gestalten, dass sie dafür ausgelegt sind, die nachfolgend aufgelisteten Datenschutzgrundsätze des Art. 5 DSGVO umzusetzen:

- Rechtmäßigkeit;
- Verarbeitung nach Treu und Glauben;
- Transparenz;

[90] Vgl. insoweit auch Erwägungsgrund 78 der DSGVO.

- Zweckbindung;
- Datenminimierung;
- Richtigkeit;
- Speicherbegrenzung;
- Integrität und Vertraulichkeit;
- Rechenschaftspflicht.

Zu berücksichtigen sind insoweit der Stand der Technik, die Implementierungskosten, die Art, der Umfang, die Umstände und die Zwecke der Verarbeitung sowie die unterschiedliche Eintrittswahrscheinlichkeit und Schwere der mit der Verarbeitung verbundenen Risiken für die Rechte und Freiheiten natürlicher Personen.

Die Festlegung auf bzw. die Entscheidung für technische und / oder organisatorische Maßnahmen in der Planungsphase der Verarbeitungsvorgänge bzw. bei deren letztmaliger Weiterentwicklung / letztmaligem Review MUSS im Hinblick auf den Grundsatz Datenschutz durch Technikgestaltung dokumentiert und begründet werden (sogenannte Entscheidungsdokumentation).

Im Rahmen eines Zertifizierungsverfahrens wird insoweit durch eine Dokumentenprüfung und/oder durch Interviews die getroffene Abwägung überprüft. Ebenfalls überprüft wird, ob Prozesse im Sinne eines fortlaufenden Prüfzyklus implementiert worden sind, die die Berücksichtigung des Grundsatzes Datenschutz durch Technikgestaltung gewährleisten (vgl. hierzu auch die Matrix Evaluationsmethoden AV unter 1.5.1).

Ggf.: Relevantes Nationales Recht:

N/A

Orientierungshilfe

Relevante Dokumente:

- ToE-Beschreibung (MUSS)
- „TOM-Dokument“ – Beschreibung der implementierten technischen und organisatorischen Maßnahmen (MUSS)
- Ggf. Entscheidungsdokumentation
- Ggf. Datenschutzmerkblatt

Relevante Evaluationsmethoden:

Dokumentenprüfung, Interviews

Anwendungs-/Auslegungshilfen:

- EDSA: Leitlinien 4/2019 zu Artikel 25 Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen (vgl. insbesondere Kapitel 2.1 und 3)

Ende der Orientierungshilfe

1.5.2. Datenschutz durch datenschutzfreundliche Voreinstellungen

Anforderung in Kürze:

Der Auftragsverarbeiter MUSS dem Grundsatz Datenschutz durch datenschutzfreundliche Voreinstellungen Rechnung tragen. Dies kann er entweder tun, indem er selbst technische und organisatorische Maßnahmen trifft, die sicherstellen, dass durch Voreinstellung nur personenbezogene Daten, deren Verarbeitung für den jeweiligen bestimmten Verarbeitungszweck erforderlich ist, verarbeitet werden, oder indem er es den Verantwortlichen durch die Gestaltung der zu zertifizierenden Verarbeitungsvorgänge ermöglicht, solche Maßnahmen zu treffen. Er MUSS im Sinne einer kontinuierlichen Verbesserung in einem Managementsystem Prozesse implementieren, die die Berücksichtigung des Grundsatzes Datenschutz durch datenschutzfreundliche Voreinstellungen sowohl zum Zeitpunkt der Auswahl bzw. Festlegung der Mittel (Planungsphase) als auch zum Zeitpunkt der eigentlichen Verarbeitung gewährleisten. Die jeweiligen Vorgänge und Ergebnisse sind zu dokumentieren.

Konkrete Maßnahmen, die insoweit erforderlich sind, sind Gegenstand von Kapitel 2 dieses Kriterienkatalogs (technische und organisatorische Maßnahmen).

Orientierungshilfe

Relevante Artikel der DSGVO:

Art. 25 Abs. 2 i. V. m. Art. 5 DSGVO

Ende der Orientierungshilfe

Anforderung im Detail:

Voraussetzungen für die / Ausnahmen von der Anwendbarkeit der Anforderung:

Diese Anforderung ist stets anwendbar. Je nach der Art der zu zertifizierenden Verarbeitungsvorgänge kommen insoweit unterschiedliche Maßnahmen in Betracht. Deshalb sind die zu treffenden Maßnahmen stets im Hinblick auf den konkreten Zertifizierungsgegenstand zu bestimmen.

Details zum Gegenstand der Anforderung:

Der Auftragsverarbeiter MUSS die zu zertifizierenden Verarbeitungsvorgänge so gestalten, dass sichergestellt ist, dass durch Voreinstellungen nur personenbezogene Daten, deren Verarbeitung für den jeweiligen bestimmten Verarbeitungszweck erforderlich ist, verarbeitet werden. Dies gilt für die Menge der erhobenen personenbezogenen Daten, den Umfang ihrer Verarbeitung, ihre Speicherfrist und ihre Zugänglichkeit. Insbesondere MUSS sichergestellt sein, dass personenbezogene Daten durch Voreinstellungen nicht ohne Eingreifen der betroffenen Person einer unbestimmten Zahl von natürlichen Personen zugänglich gemacht werden.

Die insoweit zu treffenden Maßnahmen sind auf die Umsetzung der Datenschutzgrundsätze des Art. 5 DSGVO auszurichten:

- Rechtmäßigkeit;
- Verarbeitung nach Treu und Glauben;
- Transparenz;
- Zweckbindung;

- Datenminimierung;
- Richtigkeit;
- Speicherbegrenzung;
- Integrität und Vertraulichkeit;
- Rechenschaftspflicht.

Ggf.: Relevantes Nationales Recht:

N/A

Orientierungshilfe

Relevante Dokumente:

- ToE-Beschreibung (MUSS)
- „TOM-Dokument" – Beschreibung der implementierten technischen und organisatorischen Maßnahmen (MUSS)
- Ggf. Datenschutzmerkblatt

Relevante Evaluationsmethoden:

Dokumentenprüfung, Interviews, Prüfung einer Standardkonfiguration, Ermittlung möglicher Optionen der öffentlichen Zugänglichmachung

Anwendungs-/Auslegungshilfen:

- EDSA: Leitlinien 4/2019 zu Artikel 25 Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen (vgl. insbesondere Kapitel 2.2 und 3)

Ende der Orientierungshilfe

1.5.3. Zurverfügungstellung eines Datenschutzmerkblatts

Bei dieser Anforderung handelt es sich um eine spezielle Anforderung, die aus den Grundsätzen Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen (DPbDD) abgeleitet worden sind.

Anforderung in Kürze:

Der Auftragsverarbeiter MUSS den Verantwortlichen ein Datenschutzmerkblatt zur Verfügung stellen, durch das diese einen kurzen Überblick über ihre wichtigsten datenschutzrechtlichen Pflichten bei der Inanspruchnahme der zu zertifizierenden Verarbeitungsvorgänge erhalten.

Orientierungshilfe

Relevante Artikel der DSGVO:

Art. 25 DSGVO i.V.m. Art. 5 DSGVO

Hintergrund:

Verantwortlich für die Rechtmäßigkeit der Verarbeitung ist der Verantwortliche. Der Auftragsverarbeiter kann die zu zertifizierenden Verarbeitungsvorgänge im Hinblick auf

die Grundsätze des DPbDD aber so gestalten, dass sie dafür ausgelegt sind, die Datenschutzgrundsätze des Art. 5 DSGVO umzusetzen.

In der Praxis bieten Auftragsverarbeiter oft sehr spezifische Verarbeitungsvorgänge an, für die gegebenenfalls bereichsspezifische Rechtsvorschriften auf EU- bzw. mitgliedstaatlicher Ebene gelten. Vielfach entwickeln solche spezialisierten Auftragsverarbeiter insoweit eine höhere Expertise (auch bezüglich der rechtlichen Rahmenbedingungen) als die, die typischer Weise zunächst bei einem Verantwortlichen vorhanden ist. In einem solchen Fall wird dem Verantwortlichen die Umsetzung der Datenschutzgrundsätze des Art. 5 DSGVO leicht gemacht, wenn ihm vorab ein Merkblatt ausgehändigt wird, welches die wichtigsten rechtlichen und technisch-organisatorischen Rahmenbedingungen auflistet, die bei der Inanspruchnahme der Verarbeitungsvorgänge zu beachten sind.

Ende der Orientierungshilfe

Anforderung im Detail:

Voraussetzungen für die / Ausnahmen von der Anwendbarkeit der Anforderung:

Diese Anforderung findet keine Anwendung auf Verarbeitungsvorgänge von Auftragsverarbeitern, die von deren Auftraggebern (Verantwortlichen) zu drei oder mehr Zwecken in Anspruch genommen werden. Dies deshalb, weil ein Datenschutzmerkblatt in einem solchen Fall nur Allgemeinplätze enthalten könnte und deshalb im Hinblick auf die Grundsätze des DPbDD keinen Mehrwert haben würde. In einem solchen Fall genügt es vielmehr, wenn der Auftragsverarbeiter den Verantwortlichen aussagekräftige Informationen zu den von ihm getroffenen technischen und organisatorischen Maßnahmen zur Verfügung stellt.

Details zum Gegenstand der Anforderung:

Die Formulierungen in einem solchen Datenschutzmerkblatt müssen kurz und prägnant gehalten sein.[91] Die Schwelle zu einer individuellen Rechtsberatung darf nicht überschritten werden.

Das Merkblatt MUSS Informationen zu folgenden Themen enthalten, sofern diese im Einzelfall relevant sind:

1. Klarstellung der Rollen: Zertifizierungskunde = Auftragsverarbeiter, Auftraggeber des Zertifizierungskunden = Verantwortlicher (immer relevant),

2. Hinweis auf spezielle Arten von Verarbeitungsvorgängen und die für diese geltenden rechtlichen Rahmenbedingungen (sofern einschlägig),

3. Benennung der zentralen technischen und organisatorischen Maßnahmen, die der Auftragsverarbeiter getroffen hat, und Verweis auf einschlägige Dokumente, die nähere Informationen zu diesen und weiteren TOM enthalten (immer relevant)

[91] Im Normallfall ist es möglich, alle relevanten Hinweise in einem ein- bis zweiseitigen Dokument unterzubringen. Die von dem Auftragsverarbeiter ggf. beauftragten Datenschutzexperten, die diesen auf die Evaluierung durch die Zertifizierungsstelle vorbereiten, dürfen den Auftragsverarbeiter bei der Erstellung eines solchen Dokuments unterstützen.

4. Benennung spezifischer technisch-organisatorischer Maßnahmen, die der Verantwortliche bei Inanspruchnahme der Verarbeitungsvorgänge zu treffen hat (sofern einschlägig),

5. Sonstige Hinweise, die für eine datenschutzkonforme Inanspruchnahme der Verarbeitungsvorgänge durch den Verantwortlichen relevant sind, insbesondere

- Benennung der Unterstützungsleistungen des Auftragsverarbeiters im Hinblick auf die Beantwortung von Anträgen auf Wahrnehmung von Betroffenenrechten und die Einhaltung der Pflichten des Verantwortlichen nach Artt. 32 – 36 DSGVO sowie Verweis auf die relevanten Vertragsklauseln (immer relevant),
- Voreinstellungen und diesbezügliche Konfigurationsmöglichkeiten des Verantwortlichen mit Datenschutzrelevanz (sofern einschlägig),
- Sonstige Hinweise, die für eine datenschutzkonforme Inanspruchnahme von Bedeutung sind (sofern einschlägig).

Ggf.: Relevantes Nationales Recht:

N/A

Orientierungshilfe

Relevante Dokumente:

Datenschutzmerkblatt

Relevante Evaluationsmethoden:

Dokumentenprüfung, Interviews

Anwendungs-/Auslegungshilfen:

N/A, da sich die insoweit in Betracht kommenden Dokumente nicht sinnvoll eingrenzen lassen

Ende der Orientierungshilfe

2. Technische und organisatorische Maßnahmen: Begleitende Maßnahmen zum Schutz der betroffenen Person

Dieses Kapitel behandelt **technische und organisatorische Maßnahmen**, die der Auftragsverarbeiter bzw. von ihm eingesetzte weitere Auftragsverarbeiter treffen MÜSSEN, um ein dem sich aus den zu zertifizierenden Verarbeitungsvorgängen ergebenden Risiko für die Rechte und Freiheiten der betroffenen Personen angemessenes Schutzniveau zu gewährleisten (vgl. Art. 32 Abs. 1 DSGVO).

Bei der Bearbeitung der einzelnen Anforderungen dieses Kapitels und insbesondere bei der Bewertung der Qualität der implementierten technischen und organisatorischen Maßnahmen MÜSSEN die folgenden Fragen deshalb stets mit bedacht werden:

- Sind die getroffenen technischen und organisatorischen Maßnahmen dazu geeignet, ein den identifizierten Risiken für die Rechte und Freiheiten der betroffenen Personen angemessenes Schutzniveau zu gewährleisten?
- Unterstützen die getroffenen technischen und organisatorischen Maßnahmen die Anforderungen an den Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen (siehe Kapitel 1.5 dieses Dokuments)?

Angemessen sind technische Maßnahmen grundsätzlich nur dann, wenn sie dem aktuellen Stand der Technik entsprechen. Folglich ist vor Beginn einer technischen Evaluation stets der aktuelle Stand der Technik im Hinblick auf die vom Auftragsverarbeiter bzw. weiteren Auftragsverarbeitern implementierten technischen Maßnahmen und deren datenschutzfreundliche Voreinstellungen zu ermitteln. Insoweit orientiert sich EuroPriSe insbesondere an dem Dokument „Handreichung zum „Stand der Technik“ von ENISA und TeleTrust[92], auf das auch der EDSA in seinen „Leitlinien 4/2019 zu Artikel 25 Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen“ Bezug nimmt.[93]

Bevor die Einhaltung der spezifischen Anforderungen dieses Kapitels bzw. die Angemessenheit der jeweils relevanten Maßnahmen überprüft wird, sind aber zunächst die folgenden Fragen zu beantworten (vgl. Art. 32 Abs. 2 DSGVO)[94]:

- Welche Risiken für die Rechte und Freiheiten der betroffenen Personen bestehen im Hinblick auf die bestimmungsgemäße oder tatsächliche Inanspruchnahme der zu zertifizierenden Verarbeitungsvorgänge durch den oder die Verantwortlichen (insbesondere durch unbeabsichtigte(n) oder unrechtmäßige(n) Vernichtung, Verlust, Veränderung oder durch unbefugte Offenlegung beziehungsweise unbefugten Zugang zu personenbezogenen Daten, die übermittelt, gespeichert oder auf andere Art verarbeitet werden)?

[92] https://www.teletrust.de/publikationen/broschueren/stand-der-technik/. Entsprechende Ausführungen zum Stand der Technik in der IT-Sicherheit sind aber stets im Hinblick darauf, dass im Rahmen einer Datenschutzzertifizierung die Rechte der betroffenen Personen im Vordergrund stehen müssen, kritisch zu hinterfragen.

[93] Leitlinien 4/2019 zu Artikel 25 Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen (vgl. S. 8, Fn. 9 + 10).

[94] Vgl. hierzu Kapitel 4 des Methodik-Kompendiums AV.

- Kann die Verwirklichung dieser Risiken zu physischen, materiellen oder immateriellen Schäden für die betroffenen Personen führen?

Bei der Beantwortung der Fragen sind Art, Umfang, Umstände und Zwecke der jeweiligen Verarbeitung zu berücksichtigen. Risiken für die Rechte und Freiheiten betroffener Personen sind anhand einer objektiven Bewertung zu beurteilen. Im Ergebnis ist festzustellen, ob die in Rede stehenden Verarbeitungsvorgänge ein Risiko oder ein hohes Risiko bergen. Die EuroPriSe-Methodik orientiert sich bei der Klassifizierung der Risiken an der Methode des Standard-Datenschutzmodells der DSK in der jeweils gültigen Fassung.[95] Schließlich ist auf der Grundlage der für die Rechte und Freiheiten der betroffenen Personen ermittelten Risiken eine Einstufung der jeweiligen Verarbeitungsvorgänge in eine der beiden Schutzbedarfsklassen normal oder hoch vorzunehmen.

Technische und organisatorische Maßnahmen können im Hinblick auf Daten, Systeme und Prozesse, die Gegenstand der zu zertifizierenden Verarbeitungsvorgänge sind, von Belang sein. Sofern einzelne der nachfolgenden Anforderungen für mehr als eines dieser Elemente relevant sind, ist im Rahmen einer Evaluierung entsprechend zu differenzieren.

Zu betrachten sind die vom Auftragsverarbeiter bzw. weiteren Auftragsverarbeitern implementierten technischen und organisatorischen Maßnahmen. Dies beinhaltet auch Maßnahmen, die Bestandteil einer IT-Komponente sind, auf die bei der Durchführung der zu zertifizierenden Verarbeitungsvorgänge zurückgegriffen wird (z. B. Verschlüsselungs- oder Authentifizierungsfunktionalitäten).

Im Hinblick auf den Grundsatz der Transparenz MUSS die Dokumentation, die den Verantwortlichen, die die zu zertifizierenden Verarbeitungsvorgänge in Anspruch nehmen, zur Verfügung gestellt wird, diese über relevante technische und organisatorische Maßnahmen, für deren Implementierung sie selbst Sorge tragen müssen, informieren (z. B. Maßnahmen zur Zutrittskontrolle hinsichtlich der Büroräume eines Verantwortlichen). Dies gilt allerdings nur dann, wenn eine entsprechende Information im konkreten Fall von entscheidender Bedeutung ist.

Wenn sich der Auftragsverarbeiter bei der Erbringung seines Dienstes auf weitere Auftragsverarbeiter (Subdienstleister) stützt, so MUSS geprüft werden, ob auch für diese angemessene technische und organisatorische Maßnahmen vertraglich festgelegt worden sind. Dies kann auch die Prüfung von Verträgen mit weiteren Subdienstleistern hinsichtlich der dort festgelegten TOM zur Folge haben, je nach Kritikalität der unterbeauftragten Dienstleistung. Die Erforderlichkeit einer Prüfung der technisch-organisatorischen Maßnahmen in geeigneter Form auch bei Subdienstleistern ergibt sich aus der Risikobetrachtung der ausgelagerten Teilprozesse im Verhältnis zum eigentlichen ToE.

2.1. Allgemeine Pflichten

Dieses Kapitel beinhaltet Anforderungen, die allgemeine Pflichten wie die Pflicht zur Verhinderung eines unautorisierten Zugangs zu Daten, Programmen, technischen Einrichtungen / Geräten bzw. Systemen sowie zu Betriebsstätten / relevanten Räumlichkeiten, die Pflicht zur Ergreifung von Maßnahmen zur Sicherstellung der Netzwerk- und Transportsicherheit, die Pflicht zur Implementierung von Maßnahmen zur Verhinderung eines unbeabsichtigten Verlusts personenbezogener Daten oder die Pflicht zur

[95] https://www.datenschutzzentrum.de/uploads/sdm/SDM-Methode_V2.0b.pdf

Gewährleistung einer sicheren Entsorgung und Löschung personenbezogener Daten betreffen.

2.1.1. Verhinderung eines unautorisierten Zugangs zu Daten, Programmen, Geräten und Räumlichkeiten

Anforderung in Kürze:

Der Auftragsverarbeiter MUSS sicherstellen, dass sowohl der Zutritt zu Räumlichkeiten wie auch der Zugang zu Daten, Programmen und technischen Geräten bzw. Systemen für nicht autorisierte Personen ausgeschlossen ist. Im Einzelnen MÜSSEN die nachfolgend aufgelisteten spezifischen (Unter-)Anforderungen 2.1.1.1 bis 2.1.1.6 eingehalten werden.

Orientierungshilfe

Relevante Artikel der DSGVO:

Art. 5 Abs. 1 lit. f) und Art. 32 Abs. 1 lit. b) DSGVO

Einführung / Überblick:

Die Verhinderung eines unautorisierten Zugangs zu Daten etc. ist eine der Schlüsselmaßnahmen, um einen Verlust der Integrität, der Vertraulichkeit und der Verfügbarkeit personenbezogener Daten zu verhindern. Der Zugang zu Daten etc. ist sowohl auf einer physischen als auch auf einer logischen Ebene zu regulieren: Physischer Zugang meint hierbei den Zutritt zu Gebäuden und Räumen sowie zu Hardware, Kommunikationsleitungen, Datenträgern etc., wohingegen der Begriff des logischen Zugangs den (nicht-physischen) Zugang zu Daten, Software, Funktionen etc. bezeichnet. Aus technischer Sicht ist der Begriff des Zugangs nicht auf den Zugang durch natürliche Personen beschränkt, sondern beinhaltet auch den Zugang durch Hardware (z. B. Zugangskontrolle von Netzwerkkomponenten wie beispielsweise Routern) und Software (z. B. Zugriff von Datenbanktreibern auf Datenbanken).

Ende der Orientierungshilfe

2.1.1.1. Kontrolle des physischen Zugangs (Zutritts)

Anforderung in Kürze:

Der Auftragsverarbeiter MUSS durch Maßnahmen sicherstellen, dass sowohl der Zutritt zu Räumlichkeiten wie auch der Zugang zu technischen Geräten bzw. Systemen für nicht autorisierte Personen ausgeschlossen ist, bzw. sicherstellen, dass relevante weitere Auftragsverarbeiter solche Maßnahmen getroffen haben.

Orientierungshilfe

Relevanter Artikel der DSGVO:

Art. 5 Abs. 1 lit. f) und Art. 32 Abs. 1 lit. b) DSGVO

Einführung / Überblick:

Die Kontrolle des physischen Zugangs betrifft die tatsächlich stattfindende („reallife") Verarbeitung personenbezogener Daten. Folglich müssen alle Verarbeitungsvorgänge sowie die insoweit jeweils relevanten Betriebsstätten / Räumlichkeiten im Hinblick auf die Umsetzung physischer Zugangskontrollmaßnahmen evaluiert werden.

Ende der Orientierungshilfe

Anforderung im Detail:

Der Auftragsverarbeiter MUSS nachweisen, dass

- die von ihm bzw. von relevanten weiteren Auftragsverarbeitern (z.B. Rechenzentren) ergriffenen Maßnahmen einen unautorisierten Zugang zu Gebäuden, Räumen, Hardware, Archiven, transportablen Medien, Ausdrucken etc. verhindern,
- diese Maßnahmen das bestehende bzw. ein angenommenes Risiko für die Rechte und Freiheiten der betroffenen Personen berücksichtigen,
- Maßnahmen zum Einsatz kommen, die den Zugang durch Personen bzw. Hard- und Software (rückverfolgbar) erfassen. Im Hinblick auf die daraus resultierenden personenbezogenen Daten (Logdaten) ist das Kapitel 2.1.2 einschlägig.

Orientierungshilfe

Evaluationsmethoden:

Typischerweise kommen die folgenden Evaluationsmethoden zur Anwendung:

- Audit vor Ort zur Wirksamkeitskontrolle
- Interview mit Vorgesetzten und Mitarbeitern
- Dokumentenprüfung
- Berücksichtigung relevanter anderer Zertifizierungen

Dokumente:

Typischerweise sind insoweit insbesondere die folgenden Dokumente relevant:

- Einschlägige Zertifizierungen Dritter mit zugehörigen Prüfberichten
- Risikoanalyse des Auftragsverarbeiters
- Prozessbeschreibungen
- Einschlägige Policy und Regelungen
- Schulungsunterlagen für Mitarbeiter

Prüftools/Anwendungshilfen:

Als Leitfaden bei Überprüfungen können die einschlägigen Prüfbausteine des BSI[96] herangezogen werden. In diesen wird sowohl der Stand der Technik reflektiert als auch nach Maßnahmen entsprechend der Risikoklassen unterschieden. Darüber hinaus bietet ENISA einschlägige Unterstützung an und zusammen mit TeleTrusT liefert sie eine praxisbezogene Handreichung[97] zum Stand der Technik.

[96] In der Rubrik „Publikationen“ werden einschlägige technische Richtlinien und Standards angeboten und laufend aktualisiert: https://www.bsi.bund.de/DE/Publikationen/TechnischeRichtlinien/technischerichtlinien_node.html

[97] Insoweit orientiert sich EuroPriSe insbesondere an dem folgenden Dokument von ENISA und TeleTrust: Handreichung Stand der Technik in der IT-Sicherheit (https://www.teletrust.de/publikationen/broschueren/stand-der-technik/).

Ende der Orientierungshilfe

2.1.1.2. Zugang zu transportablen Medien und mobilen Geräten

Anforderung in Kürze:

Der Auftragsverarbeiter MUSS durch Maßnahmen sicherstellen, dass der Zugang zu transportablen (Speicher-) Medien und mobilen IT-Geräten für nicht autorisierte Personen ausgeschlossen ist, bzw. sicherstellen, dass relevante weitere Auftragsverarbeiter solche Maßnahmen getroffen haben.

Orientierungshilfe

Relevante Artikel der DSGVO:

Art. 5 Abs. 1 lit. f) und Art. 32 Abs. 1 lit. b) DSGVO

Einführung / Überblick:

Die Kontrolle des (physischen) Zugangs zu transportablen Medien, auf denen personenbezogene Daten gespeichert werden (CDs/DVDs, USB-Sticks, externe Festplatten, Bänder etc.), ist von entscheidender Bedeutung, weil logische Zugangskontrollen wie z. B. Lese- und Schreibberechtigungen im Zusammenhang mit Dateien oder Datenbanktabellen häufig (leicht) umgangen werden können, wenn der Angreifer erst einmal Zugriff auf diese Medien hat. Gleiches gilt für mobile Geräte (Laptops, Tablets, Smartphones etc.), auf denen personenbezogene Daten gespeichert werden.

Ende der Orientierungshilfe

Anforderung im Detail:

Falls die Inanspruchnahme der zu zertifizierenden Verarbeitungsvorgänge die Speicherung personenbezogener Daten auf transportablen Datenträgern zur Folge hat bzw. haben kann, MUSS der Auftragsverarbeiter nachweisen, dass:

- transportable Medien sicher (bspw. in zugriffsbeschränkten Archiven) verwahrt,
- auch Ausdrucke sicher verwahrt,
- Medien und ihre Inhalte inventarisiert,
- die Weitergabe von Medien dokumentiert / protokolliert werden.

Orientierungshilfe

Evaluationsmethoden:

Typischerweise kommen die folgenden Evaluationsmethoden zur Anwendung:

- Audit vor Ort zur Wirksamkeitskontrolle

Entsprechende Ausführungen zum Stand der Technik in der IT-Sicherheit sind aber stets im Hinblick darauf, dass im Rahmen einer Datenschutzzertifizierung die Rechte der betroffenen Personen im Vordergrund stehen müssen, kritisch zu hinterfragen.

- Interview mit Vorgesetzten und Mitarbeitern
- Dokumentenprüfung
- Berücksichtigung relevanter anderer Zertifizierungen

Dokumente:

Typischerweise sind insoweit insbesondere die folgenden Dokumente relevant:

- Einschlägige Zertifizierungen Dritter mit zugehörigen Prüfberichten
- Risikoanalyse des Auftragsverarbeiters
- Prozessbeschreibungen
- Einschlägige Policies und Regelungen
- Schulungsunterlagen für Mitarbeiter

Prüftools/Anwendungshilfen:

Als Leitfaden bei Überprüfungen können die einschlägigen Prüfbausteine des BSI herangezogen werden. In diesen wird sowohl der Stand der Technik reflektiert als auch nach Maßnahmen entsprechend der Risikoklassen unterschieden. Darüber hinaus bietet ENISA einschlägige Unterstützung an und zusammen mit TeleTrusT liefert sie eine praxisbezogene Handreichung zum Stand der Technik.

Ende der Orientierungshilfe

2.1.1.3. Zugang zu Daten, Programmen und Geräten

Anforderung in Kürze:

Der Auftragsverarbeiter MUSS durch Maßnahmen sicherstellen, dass der Zugang zu Daten, Programmen und Geräten für nicht autorisierte Personen ausgeschlossen ist, bzw. sicherstellen, dass relevante weitere Auftragsverarbeiter solche Maßnahmen getroffen haben.

Orientierungshilfe

Relevante Artikel der DSGVO:

Art. 5 Abs. 1 lit. f) und Art. 32 Abs. 1 lit. b) DSGVO

Einführung / Überblick:

Der Zugang zu Daten und Programmen wird häufig nicht mittels physischer, sondern mittels logischer Mechanismen kontrolliert: Typische Zugriffskontrollmechanismen sind die Vergabe von Berechtigungen zum Lesen und Schreiben auf Dateien oder die Verwendung von Software oder Softwarefunktionalitäten, die innerhalb des Betriebssystems, des Datenbankmanagementsystems oder einer Applikation verankert sind. Die Granularität der Kontrollmechanismen ist zu evaluieren, wobei stets zu bedenken ist, dass eine einfache Handhabung eines solchen Systems wichtig ist. Weiterhin MUSS die Qualität der Implementierung evaluiert werden. Dies gilt vor allem für webbasierte Anwendungen.

Die Kontrolle des Zugangs zu Geräten kann entweder auf einer logischen Ebene (z. B. durch BIOS-Passwörter oder durch PIN-Codes für Festnetz- oder Mobiltelefone) oder auf

einer physikalischen Ebene (beispielsweise durch elektromechanische Verriegelungen) erfolgen.

Ende der Orientierungshilfe

Anforderung im Detail:

Der Auftragsverarbeiter MUSS nachweisen, dass Zugangs- / Zugriffskontrollmechanismen der zur Erbringung des Dienstes eingesetzten IT-Produkte wie nachfolgend aufgeführt verwendet werden. Er muss jederzeit den Überblick haben, durch welche Personen oder Rollen die Zugangs- / Zugriffsrechte verwaltet werden. Des Weiteren MUSS er sicherstellen, dass

- Eingesetzte Geräte oder Systeme Funktionen zur Zugangskontrolle bieten wie mechanische Schlösser, PIN-Codes oder Passwortschutz,
- SW-Systeme Funktionen zur Zugangskontrolle wie z. B. ein rollenbasiertes Berechtigungskonzept bei SAP Modulen bieten,
- Zugriffsrechte mit Granularität vergeben werden,
- dies sowohl im Hinblick auf den Umfang der jeweiligen Berechtigungen (Lesen, Verändern, Übermitteln, Drucken etc.) als auch hinsichtlich der jeweiligen Daten (Datei, Datensatz, Feld, Tabelle etc.) der Fall ist,
- es spezielle Rollen für die Administration von Zugriffsrechten gibt (z. B. für die Vergabe / den Entzug von Berechtigungen, das Einrichten von Gruppen und Rollen oder die Konfiguration von Rollen für Benutzerkonten),
- die Administration von Zugangs- / Zugriffsrechten von der technischen Administration (z. B. Erstellung von Backups, Programmiertätigkeiten oder Second-Level-Support) getrennt wird (z. B. durch Delegierung),
- der Zugang / Zugriff in jeder Verarbeitungsphase kontrolliert wird,
- Maßnahmen ergriffen worden sind, um die unbefugte Manipulation von Daten durch Nutzer zu verhindern (insbesondere getestete Maßnahmen gegen SQL Injections),
- Maßnahmen zur Überprüfung der Eingaben von Nutzern ergriffen worden sind (insbesondere getestete Maßnahmen zur Verhinderung von XXS-Angriffen).

Orientierungshilfe

Evaluationsmethoden:

Typischerweise kommen die folgenden Evaluationsmethoden zur Anwendung:

- Audit vor Ort zur Wirksamkeitskontrolle
- Interviews mit Vorgesetzten und Mitarbeitern
- Dokumentenprüfung
- Berücksichtigung relevanter anderer Zertifizierungen
- Testzugang

Dokumente:

Typischerweise sind insoweit insbesondere die folgenden Dokumente relevant:

- Einschlägige Zertifizierungen Dritter mit zugehörigen Prüfberichten
- Risikoanalyse des Auftragsverarbeiters
- Prozessbeschreibungen
- Einschlägige Policies und Regelungen
- Schulungsunterlagen für Mitarbeiter
- Ggf. Verträge mit weiteren Auftragsverarbeitern (insbes.: Vorgaben zu TOM)

Prüftools/Anwendungshilfen:

Als Leitfaden bei Überprüfungen können die einschlägigen Prüfbausteine des BSI herangezogen werden. In diesen wird sowohl der Stand der Technik reflektiert als auch nach Maßnahmen entsprechend der Risikoklassen unterschieden. Darüber hinaus bietet ENISA einschlägige Unterstützung an und zusammen mit TeleTrusT liefert sie eine praxisbezogene Handreichung zum Stand der Technik.

Ende der Orientierungshilfe

2.1.1.4. Identifikation und Authentifizierung

Anforderung in Kürze:

Der Auftragsverarbeiter MUSS durch Maßnahmen sicherstellen, dass Personen, bevor sie Zugang zu Daten, Programmen, Geräten und Räumlichkeiten erhalten, identifiziert und authentifiziert werden, bzw. sicherstellen, dass relevante weitere Auftragsverarbeiter solche Maßnahmen getroffen haben.

Orientierungshilfe

Relevante Artikel der DSGVO:

Art. 5 Abs. 1 lit. f) und Art. 32 Abs. 1 lit. b) DSGVO

Einführung / Überblick:

Voraussetzung für die Zugangs- / Zugriffserteilung ist stets eine erfolgreiche Identifikation und Authentifizierung der Nutzer. Gleiches gilt für Hardware und Software. Typische Mechanismen hierfür sind die Verwendung von Loginnamen und Passwörtern, biometrischen Systemen, Sicherheitstoken und kryptographischen Schlüsseln (Zertifikaten). Auch zufällig erzeugte Identifikatoren wie beispielsweise Sitzungsschlüssel für webbasierte Anwendungen werden zur Identifikation und Authentifizierung verwendet.

Ende der Orientierungshilfe

Anforderung im Detail:

Der Auftragsverarbeiter MUSS nachweisen, dass:

- die zu zertifizierenden Verarbeitungsvorgänge durch Identifikations- und Authentifizierungsmaßnahmen abgesichert sind,
- Maßnahmen ergriffen wurden, um (weitere) wiederholte Identifikations- und Authentisierungsversuche nach einer bestimmten Anzahl von gescheiterten Versuchen zu unterbinden,

- diese Gegenmaßnahmen (z. B. das Verlangsamen des Identifikationsprozesses oder die temporäre bzw. dauerhafte Deaktivierung der Benutzerkonten) das bestehende bzw. ein angenommenes Risiko berücksichtigen,
- falls die Identifikation und Authentifizierung mit Hilfe von Token (z. B. Karten, Schlüsseln oder Zertifikaten) erfolgt, diese gegen Nachbildung (Klonen) und unberechtigten Zugriff gesichert sind.

Orientierungshilfe

Evaluationsmethoden:

Typischerweise kommen die folgenden Evaluationsmethoden zur Anwendung:

- Audit vor Ort zur Wirksamkeitskontrolle
- Interviews mit Vorgesetzten und Mitarbeitern
- Dokumentenprüfung
- Berücksichtigung relevanter anderer Zertifizierungen
- Testzugang

Dokumente:

Typischerweise sind insoweit insbesondere die folgenden Dokumente relevant:

- Einschlägige Zertifizierungen Dritter mit zugehörigen Prüfberichten
- Risikoanalyse des Auftragsverarbeiters
- Prozessbeschreibungen
- Einschlägige Policies und Regelungen
- Schulungsunterlagen für Mitarbeiter
- Nutzerhandbuch
- Ggf. Verträge mit weiteren Auftragsverarbeitern (insbes.: Vorgaben zu TOM)

Prüftools / Anwendungshilfen:

Als Leitfaden bei Überprüfungen können die einschlägigen Prüfbausteine des BSI herangezogen werden. In diesen wird sowohl der Stand der Technik reflektiert als auch nach Maßnahmen entsprechend der Risikoklassen unterschieden. Darüber hinaus bietet ENISA einschlägige Unterstützung an und zusammen mit TeleTrusT liefert sie eine praxisbezogene Handreichung zum Stand der Technik.

Ende der Orientierungshilfe

2.1.1.5. Nutzung von Passwörtern

Anforderung in Kürze:

Der Auftragsverarbeiter MUSS durch Maßnahmen einen Passwortschutz sicherstellen bzw. sicherstellen, dass relevante weitere Auftragsverarbeiter solche Maßnahmen getroffen haben.

Orientierungshilfe

Relevante Artikel der DSGVO:

Art. 5 Abs. 1 lit. f) und Art. 32 Abs. 1 lit. b) DSGVO

Einführung / Überblick:

Werden Passwörter zur Authentifizierung von Nutzern (oder Maschinen) verwendet, so sind spezifische Sicherheitsaspekte zu berücksichtigen. Zu diesen gehören insbesondere solche, die die Verwaltung, die Änderung und den Widerruf / das Ungültig-Erklären von Passwörtern betreffen. Die Wahl der Passwortkomplexität, der Mechanismen zur Änderung von Passwörtern und der Maßnahmen zur sicheren Speicherung von Passwörtern hat unter Berücksichtigung der jeweiligen Umstände zu erfolgen. Dazu kann auch die technische Lösung einer Mehr-Faktor-Authentifizierung gehören.

Ende der Orientierungshilfe

Anforderung im Detail:

Der Auftragsverarbeiter MUSS nachweisen, dass:

- Prozesse implementiert und wirksam sind, die eine vertrauliche und unverfälschte Zuweisung, Verteilung und Speicherung von Passwörtern sicherstellen,
- eine Änderung verwendeter Passwörter in regelmäßigen Abständen verlangt / technisch erzwungen wird,
- auch Passwörter zur Authentifizierung von Hard- oder Software (z. B. Authentisierungscodes für WLAN-Hardware oder Datenbankzugänge von Webservern) geändert werden,
- eine dem Stand der Technik entsprechende Qualität von Passwörtern (z. B. im Hinblick auf Länge und Komplexität) verlangt / technisch erzwungen wird,
- unterstützende Mechanismen der (eingesetzten) Software (z. B. des Betriebssystems) für die Kontrolle der Passwortqualität und –Lebensdauer verwendet werden,
- Vorkehrungen für den Fall getroffen sind, dass ein Nutzer sein Passwort vergessen hat (Zuweisung eines neuen Passworts)
- eine Mehr-Faktor-Authentifizierungstechnik zum Einsatz kommt, falls nach dem Stand der Technik angemessen.

Orientierungshilfe

Evaluationsmethoden:

Typischerweise kommen die folgenden Evaluationsmethoden zur Anwendung:

- Audit vor Ort zur Wirksamkeitskontrolle
- Interviews mit Vorgesetzten und Mitarbeitern
- Dokumentenprüfung
- Berücksichtigung relevanter anderer Zertifizierungen
- Testzugang

Dokumente:

Typischerweise sind insoweit insbesondere die folgenden Dokumente relevant:

- Einschlägige Zertifizierungen Dritter mit zugehörigen Prüfberichten
- Risikoanalyse des Auftragsverarbeiters
- Prozessbeschreibungen
- Einschlägige Policy und Regelungen
- Schulungsunterlagen für Mitarbeiter
- Nutzerhandbuch
- Ggf. Verträge mit weiteren Auftragsverarbeitern (insbes.: Vorgaben zu TOM)

Prüftools / Anwendungshilfen:

Als Leitfaden bei Überprüfungen können die einschlägigen Prüfbausteine des BSI herangezogen werden. In diesen wird sowohl der Stand der Technik reflektiert als auch nach Maßnahmen entsprechend der Risikoklassen unterschieden. Darüber hinaus bietet ENISA einschlägige Unterstützung an und zusammen mit TeleTrusT liefert sie eine praxisbezogene Handreichung zum Stand der Technik.

Ende der Orientierungshilfe

2.1.1.6. Organisation und Dokumentation von Zugangskontrollen

Anforderung in Kürze:

Der Auftragsverarbeiter MUSS durch Maßnahmen Zugangskontrollen sicherstellen, dokumentieren und managen bzw. sicherstellen, dass relevante weitere Auftragsverarbeiter solche Maßnahmen getroffen haben.

Orientierungshilfe

Relevante Artikel der DSGVO:

Art. 5 Abs. 1 lit. f) und Art. 32 Abs. 1 lit. b) DSGVO

Einführung / Überblick:

Die Zugangs- und Zugriffskontrolle muss verwaltet werden. Dies beinhaltet die Festlegung und Dokumentation von Zugriffsrechten und die technische Implementierung und Konfiguration von Zugangskontrollen. Betroffen sind insoweit alle Arten der Zugangskontrolle (physisch und logisch) und auch Fälle, in denen das Management von Zugangs- und Zugriffsberechtigungen und das von Authentifizierungsmethoden nur schwer voneinander getrennt werden können (wie beispielsweise bei der Verwendung mechanischer Schlüssel, wo Zugangsberechtigungen nur durch das Einziehen der entsprechenden Schlüssel widerrufen werden können).

Ende der Orientierungshilfe

Anforderung im Detail:

Der Auftragsverarbeiter MUSS nachweisen, dass:

- die Zugangs- und Zugriffsrechte organisiert, eindeutig dokumentiert und für jeden berechtigten Nutzer nachvollziehbar sind,

- die Regeln für die Administration von Zugangs- und Zugriffsrechten implementiert und dokumentiert sind,
- Zugangs- und Zugriffsrechte widerrufen werden, sofern nicht länger benötigt,
- Token, die zur Authentifizierung verwendet werden (beispielsweise Schlüssel, Smartcards, oder Hardware-Sicherheitstoken), ebenfalls Bestandteil der Inventarisierung sind.

Orientierungshilfe

Evaluationsmethoden:

Typischerweise kommen die folgenden Evaluationsmethoden zur Anwendung:

- Audit vor Ort zur Wirksamkeitskontrolle
- Interviews mit Vorgesetzten und Mitarbeitern
- Dokumentenprüfung
- Berücksichtigung relevanter anderer Zertifizierungen
- Testzugang

Dokumente:

Typischerweise sind insoweit insbesondere die folgenden Dokumente relevant:

- Einschlägige Zertifizierungen Dritter mit zugehörigen Prüfberichten
- Risikoanalyse des Auftragsverarbeiters
- Prozessbeschreibungen
- Einschlägige Policies und Regelungen
- Schulungsunterlagen für Mitarbeiter
- Nutzerhandbuch
- (Auszug) Inventarliste
- Ggf. Verträge mit weiteren Auftragsverarbeitern (insbes.: Vorgaben zu TOM)

Prüftools / Anwendungshilfen:

Als Leitfaden bei Überprüfungen können die einschlägigen Prüfbausteine des BSI herangezogen werden. In diesen wird sowohl der Stand der Technik reflektiert als auch nach Maßnahmen entsprechend der Risikoklassen unterschieden. Darüber hinaus bietet ENISA einschlägige Unterstützung an und zusammen mit TeleTrusT liefert sie eine praxisbezogene Handreichung zum Stand der Technik.

Ende der Orientierungshilfe

2.1.2. Protokollierung (Logging) der Verarbeitung personenbezogener Daten

Anforderung in Kürze:

Der Auftragsverarbeiter MUSS durch Maßnahmen eine Protokollierung der Verarbeitung personenbezogener Daten sicherstellen bzw. sicherstellen, dass relevante weitere Auftragsverarbeiter solche Maßnahmen getroffen haben. Im Einzelnen MÜSSEN die

nachfolgend aufgelisteten spezifischen (Unter-)Anforderungen 2.1.2.1 und 2.1.2.2 eingehalten werden.

Orientierungshilfe

Relevante Artikel der DSGVO:

Art. 5 Abs. 1 lit. a) + Abs. 2 und Art. 32 Abs. 1 DSGVO

Einführung / Überblick:

Die Protokollierung des Zugriffs auf personenbezogene Daten und ihrer (weiteren) Verarbeitung ist eine wichtige Maßnahme, um die Nachprüfbarkeit (Revisionsfähigkeit) der Verarbeitung sicherzustellen. Logdateien und Protokolldaten enthalten üblicherweise personenbezogene Daten, die sich sowohl auf die betroffenen Personen (Personen, deren Daten zur bestimmungsgemäßen oder tatsächlichen Inanspruchnahme der Verarbeitungsvorgänge verarbeitet werden) als auch auf die Personen, die diese Daten verarbeiten (z. B. Mitarbeiter des Service-Providers), beziehen. Zu letzteren können in bestimmten Fällen auch die betroffenen Personen selbst gehören (z. B., wenn diese einen Selbstbedienungsdienst („self service“) in Anspruch nehmen, der es ihnen beispielsweise ermöglicht, ihre eigenen Daten zu berichtigen).

Ende der Orientierungshilfe

2.1.2.1. Protokollierungsmechanismen (Loggingmechanismen)

Anforderung in Kürze:

Der Auftragsverarbeiter MUSS Protokollierungsmechanismen implementiert haben bzw. sicherstellen, dass relevante weitere Auftragsverarbeiter solche Mechanismen implementiert haben.

Orientierungshilfe

Relevante Artikel der DSGVO:

(Art. 5 Abs. 1 lit. a) + Abs. 2 und Art. 32 Abs. 1 DSGVO

Einführung / Überblick:

Die Protokollierung des Zugriffs auf personenbezogene Daten und ihrer (weiteren) Verarbeitung ist eine wichtige Maßnahme, um die Nachprüfbarkeit (Revisionsfähigkeit) der Verarbeitung sicherzustellen.

Ende der Orientierungshilfe

Anforderung im Detail:

Der Auftragsverarbeiter MUSS nachweisen, dass:

- im Hinblick auf die zu zertifizierenden Verarbeitungsvorgänge Loggingmechanismen vorhanden sind, die die Überarbeitung / Ergänzung / Berichtigung der verarbeiteten personenbezogenen Daten zum Gegenstand haben,
- darin die Möglichkeit der Nachverfolgung von Lese-, Speicher-, Änderungs- und Übermittlungsvorgängen ebenso eingeschlossen ist wie die Möglichkeit, die Identität der Nutzer, die diese Aktionen durchgeführt haben und den Zeitpunkt, zu dem diese Aktionen stattgefunden haben, aufzuzeichnen,

- das Logging im Hinblick auf seinen Detaillierungsgrad konfiguriert werden kann (z. B. indem das Logging auf schreibende / einfügende Aktionen beschränkt wird) bzw. es so konfiguriert ist, dass das bestehende bzw. ein angenommenes Risiko berücksichtigt ist,
- die Speicherdauer der Protokolldaten konfiguriert werden kann bzw. so konfiguriert ist, dass das bestehende bzw. ein angenommenes Risiko und der Zweck der Verarbeitung berücksichtigt sind,
- verschiedene Arten von Protokolldaten (z. B. hinsichtlich der Verarbeitung / Übermittlung personenbezogener Daten oder der Vergabe von Zugangsberechtigungen), die in ein- und demselben Logfile gespeichert werden, so gespeichert sind, dass gegebenenfalls unterschiedliche Speicherfristen (z. B. zwei Jahre für den Zugriff auf personenbezogene Daten und fünf Jahre für die Vergabe von Zugangsberechtigungen) zur Anwendung kommen können oder diese verschiedenen Arten von Protokolldaten in unterschiedlichen Logfiles gespeichert werden,
- die Protokolldaten (manipulationssicher) durch Eingaben der Nutzer (z. B. die Angabe eines Aktenzeichens, um einen Zugriff auf Daten zu rechtfertigen) ergänzt werden können,
- eine einfache Auswertung der Protokolldaten im Hinblick auf definierte Fragestellungen möglich ist (z. B. alle Änderungen der Datei XXX, alle Dateizugriffe zwischen 23:00 und 03:00 Uhr oder alle durch den Nutzer YYY durchgeführten oder angestoßenen Übermittlungen),
- falls keine automatisierten Loggingfunktionalitäten im Rahmen der Erbringung eines Dienstes durchgeführt werden (bzw. durch den Nutzer durchgeführt werden können), manuelle Loggingmechanismen vorhanden sind (z.B. Mechanismen, die auf Papier zurückgreifen, „Besucherbuch“).

Orientierungshilfe

Evaluationsmethoden:

Typischerweise kommen die folgenden Evaluationsmethoden zur Anwendung:

- Audit vor Ort zur Wirksamkeitskontrolle
- Interviews mit Vorgesetzten und Mitarbeitern
- Dokumentenprüfung
- Berücksichtigung relevanter anderer Zertifizierungen
- Testzugang
- Prüfung der Logdateien

Dokumente:

Typischerweise sind insoweit insbesondere die folgenden Dokumente relevant:

- Einschlägige Zertifizierungen Dritter mit zugehörigen Prüfberichten
- Risikoanalyse des Auftragsverarbeiters
- Prozessbeschreibungen

- Einschlägige Policies und Regelungen
- Ggf. Verträge mit weiteren Auftragsverarbeitern (insbes.: Vorgaben zu TOM)

Prüftools / Anwendungshilfen:

Als Leitfaden bei Überprüfungen können die einschlägigen Prüfbausteine des BSI herangezogen werden. In diesen wird sowohl der Stand der Technik reflektiert als auch nach Maßnahmen entsprechend der Risikoklassen unterschieden. Darüber hinaus bietet ENISA einschlägige Unterstützung an und zusammen mit TeleTrusT liefert sie eine praxisbezogene Handreichung zum Stand der Technik.

Ende der Orientierungshilfe

2.1.2.2. Betrieb der Protokollierungsmechanismen (Loggingmechanismen)

Anforderung in Kürze:

Der Auftragsverarbeiter MUSS Maßnahmen für den Betrieb der Protokollierungsmechanismen implementiert haben bzw. sicherstellen, dass relevante weitere Auftragsverarbeiter solche Mechanismen implementiert haben.

Orientierungshilfe

Relevante Artikel der DSGVO:

Art. 5 Abs. 1 lit. a) + Abs. 2 und Art. 32 Abs. 1 DSGVO

Einführung / Überblick:

Aufgrund der Einstufung von Protokolldaten als personenbezogene Daten muss die Verarbeitung von Protokolldaten durch technische und organisatorische Maßnahmen abgesichert werden.

Ende der Orientierungshilfe

Anforderung im Detail:

Der Auftragsverarbeiter MUSS nachweisen, dass:

- die Speicherdauer so konfiguriert ist, dass sie sich mit den maßgeblichen Sicherheitspolicies und den anwendbaren Datenschutzbestimmungen im Einklang befindet,
- Protokolldaten regelmäßig durch den Datenschutz- oder den IT-Sicherheitsbeauftragten überprüft werden,
- Protokolldaten nach Ablauf der Speicherdauer sicher entsorgt / (wirklich) gelöscht werden,
- falls die Protokollierung blockiert / deaktiviert wurde, dies seinerseits protokolliert wird.

Orientierungshilfe

Evaluationsmethoden:

Typischerweise kommen die folgenden Evaluationsmethoden zur Anwendung:

- Audit vor Ort zur Wirksamkeitskontrolle
- Interviews mit Vorgesetzten und Mitarbeitern
- Dokumentenprüfung
- Berücksichtigung relevanter anderer Zertifizierungen
- Testzugang

Dokumente:

Typischerweise sind insbesondere die folgenden Dokumente relevant:

- Einschlägige Zertifizierungen Dritter mit zugehörigen Prüfberichten
- Risikoanalyse des Auftragsverarbeiters
- Prozessbeschreibungen
- Einschlägige Policies und Regelungen
- Schulungsunterlagen für Mitarbeiter
- Ggf. Verträge mit weiteren Auftragsverarbeitern (insbes.: Vorgaben zu TOM)

Prüftools / Anwendungshilfen:

Als Leitfaden bei Überprüfungen können die einschlägigen Prüfbausteine des BSI herangezogen werden. In diesen wird sowohl der Stand der Technik reflektiert als auch nach Maßnahmen entsprechend der Risikoklassen unterschieden. Darüber hinaus bietet ENISA einschlägige Unterstützung an und zusammen mit TeleTrusT liefert sie eine praxisbezogene Handreichung zum Stand der Technik.

Ende der Orientierungshilfe

2.1.3. Netzwerk- und Transportsicherheit

Anforderung in Kürze:

Der Auftragsverarbeiter MUSS sicherstellen, dass die Transportsicherheit der Daten gegeben und die eigenen Netze sicher betrieben werden, bzw. sicherstellen, dass relevante weitere Auftragsverarbeiter solche Maßnahmen getroffen haben. Vgl. auch nachfolgend unter „Anforderung im Detail:“.

Orientierungshilfe

Relevante Artikel der DSGVO:

Art. 5 Abs. 1 lit. f) und Art. 32 Abs. 1 lit. b) DSGVO

Einführung / Überblick:

Die Netzwerk- und Transportsicherheit betrifft die Sicherheit der IT-Infrastruktur und die Sicherheit der übertragenen oder transportierten Daten. Während der erste Aspekt üblicher Weise die gesamte Infrastruktur betrifft, kann der zweite Aspekt Gegenstand spezifischer Regelungen sein, die in Abhängigkeit von der Art der übertragenen Daten, vom Empfänger usw. Anwendung finden.

Ende der Orientierungshilfe

Anforderung im Detail:

Der Auftragsverarbeiter MUSS nachweisen, dass:

- die Sicherheit von Remotezugängen, mittels derer auf Daten oder auf Unternehmensnetzwerke zugegriffen werden kann, vergleichbar ist mit der, die für interne Zugriffe gewährleistet wird (typische Maßnahmen sind Verschlüsselung, VPN, Mehr-Faktor-Authentifizierung etc.),
- die Übertragung über öffentliche Netzwerke (z. B. das Internet) verschlüsselt erfolgt,
- falls eine Verbindung zwischen einem internen und einem externen Netzwerk besteht, das interne Netzwerk vom externen / öffentlichen Netzwerk abgeschottet ist (beispielsweise durch Firewalls),
- im Falle einer Firewall die entsprechenden Firewall-Regeln für eine sichere Trennung der Netzwerke sorgen,
- die Teile des Netzwerks, die sowohl von intern als auch von extern erreichbar sind (z. B. Proxies, Mailserver etc.), besonders abgeschottet sind (beispielsweise durch eine demilitarisierte Zone – DMZ),
- das interne Netzwerk gegen Schadsoftware gesichert ist, die z. B. über externe Verbindungen (Links) oder durch das Anschließen mobiler Geräte übertragen wird.

Orientierungshilfe

Evaluationsmethoden:

Typischerweise kommen die folgenden Evaluationsmethoden zur Anwendung:

- Audit vor Ort zur Wirksamkeitskontrolle
- Interviews mit Vorgesetzten und Mitarbeitern
- Dokumentenprüfung
- Berücksichtigung relevanter anderer Zertifizierungen
- Testzugang

Dokumente:

Typischerweise sind insbesondere die folgenden Dokumente relevant:

- Einschlägige Zertifizierungen Dritter mit zugehörigen Prüfberichten
- Risikoanalyse des Auftragsverarbeiters
- Prozessbeschreibungen
- Einschlägige Policies und Regelungen
- Schulungsunterlagen für Mitarbeiter
- Netzwerktopologie
- Ggf. Verträge mit weiteren Auftragsverarbeitern (insbes.: Vorgaben zu TOM)

Prüftools / Anwendungshilfen:

Als Leitfaden bei Überprüfungen können die einschlägigen Prüfbausteine des BSI herangezogen werden. In diesen wird sowohl der Stand der Technik reflektiert als auch

nach Maßnahmen entsprechend der Risikoklassen unterschieden. Darüber hinaus bietet ENISA einschlägige Unterstützung an und zusammen mit TeleTrusT liefert sie eine praxisbezogene Handreichung zum Stand der Technik.

Gängige Prüftools wie

- https://www.ssllabs.com/ssltest/
- https://webbkoll.dataskydd.net/de
- https://owasp.org/www-project-top-ten/

Ende der Orientierungshilfe

2.1.4. Mechanismen zur Verhinderung eines unbeabsichtigten Datenverlusts; Sicherungs- & Wiederherstellungsmechanismen (Backup & Recovery)

Anforderung in Kürze:

Der Auftragsverarbeiter MUSS sicherstellen, dass Mechanismen zur Verhinderung eines unbeabsichtigten Datenverlustes bereitstehen, bzw. sicherstellen, dass relevante weitere Auftragsverarbeiter solche Maßnahmen getroffen haben. Im Einzelnen müssen die nachfolgend aufgelisteten spezifischen (Unter-)Anforderungen 2.1.4.1 bis 2.1.4.4 eingehalten werden.

Orientierungshilfe

Relevante Artikel der DSGVO:

Art. 5 Abs. 1 lit. f) und Art. 32 Abs. 1 lit. b)+c) DSGVO

Einführung / Überblick:

Neben der Integrität und Vertraulichkeit personenbezogener Daten ist bzw. kann auch deren Verfügbarkeit ein wichtiges Gewährleistungsziel sein. Insoweit geht es aber nicht nur um die Verfügbarkeit von Daten, sondern auch um die Verfügbarkeit der Verarbeitungsvorgänge des Auftragsverarbeiters (inklusive der zugehörigen Hardware und Software). Eine Standardmaßnahme ist hier die Erstellung von Sicherungskopien (Backups), die durch geeignete Maßnahmen zur Aufbewahrung / Lagerung und weitere organisatorische Maßnahmen (z. B. Recovery-Tests) zu ergänzen ist. Andere Maßnahmen, die insbesondere im Hinblick auf geschäfts- oder sonstige kritische Daten (z. B. Gesundheitsdaten) relevant sind, sind auf Hardwareredundanz gerichtete Maßnahmen (z. B. Cold Standby oder Hot Standby), Datenspiegelungen (z. B. mit Hilfe von RAID-Systemen oder Datenreplikation) oder der Einsatz redundanter Rechenzentren. Gerade bei ToEs, die mehrere Verarbeitungsvorgänge zum Gegenstand haben, müssen gegebenenfalls ganze Prozesse (inklusive der zugehörigen Daten und Hardware, aber auch persönlichen Knowhows und Kenntnissen etc.) gesichert werden, um Verletzungen der Verfügbarkeit durch Störfälle oder Datenverluste zu minimieren.

Jedoch ist die Verfügbarkeit im Datenschutzkontext nie „Selbstzweck“, sondern immer mit Blick auf den tatsächlichen ToE zu bewerten. Sind personenbezogene Daten vollständig „verschwunden”, ist dies sicherlich vom Geschäftsstandpunkt eines Auftragsverarbeiters schädlich, unter Umständen jedoch nicht immer aus Sicht der betroffenen Person, wie man am Beispiel „Adressensammlung zu Werbezwecken“ sehen kann.

Ende der Orientierungshilfe

2.1.4.1. Allgemeine Maßnahmen

Anforderung in Kürze:

Der Auftragsverarbeiter MUSS sicherstellen, dass generelle Vorsorgemaßnahmen gegen unbeabsichtigten Datenverlust getroffen worden und wirksam sind.

Orientierungshilfe

Relevante Artikel der DSGVO:

Art. 5 Abs. 1 lit. f) und Art. 32 Abs. 1 lit. b) DSGVO

Einführung / Überblick:

Siehe oben (Kapitel 2.1.4)

Ende der Orientierungshilfe

Anforderung im Detail:

Der Auftragsverarbeiter MUSS nachweisen, dass:

- Maßnahmen gegen Feuer, Wasser, starke elektromagnetische Felder etc. ergriffen worden sind,
- Maßnahmen gegen einen Stromausfall getroffen worden sind,
- ein Verfügbarkeits- / Redundanzkonzept vorhanden ist (optional oder verpflichtend[98]),

Orientierungshilfe

Evaluationsmethoden:

Typischerweise kommen die folgenden Evaluationsmethoden zur Anwendung:

- Audit vor Ort zur Wirksamkeitskontrolle
- Interviews mit Vorgesetzten und Mitarbeitern
- Dokumentenprüfung
- Berücksichtigung relevanter anderer Zertifizierungen
- Testzugang

Dokumente:

Typischerweise sind insoweit insbesondere die folgenden Dokumente relevant:

- Einschlägige Zertifizierungen Dritter mit zugehörigen Prüfberichten
- Risikoanalyse des Auftragsverarbeiters

[98] Die Entscheidung darüber, ob ein Verfügbarkeits- / Redundanzkonzept optional ist oder zwingend vorliegen muss, hängt von den konkreten Umständen des jeweiligen Einzelfalls ab.

- Prozessbeschreibungen
- Backup Konzept
- Einschlägige Policies und Regelungen
- Schulungsunterlagen für Mitarbeiter
- Ggf. Verträge mit weiteren Auftragsverarbeitern (insbes.: Vorgaben zu TOM)

Prüftools / Anwendungshilfen:

Als Leitfaden bei Überprüfungen können die einschlägigen Prüfbausteine des BSI herangezogen werden. In diesen wird sowohl der Stand der Technik reflektiert als auch nach Maßnahmen entsprechend der Risikoklassen unterschieden.

Ende der Orientierungshilfe

2.1.4.2. Sicherungsmechanismen (Backup)

Anforderung in Kürze:

Der Auftragsverarbeiter MUSS sicherstellen, dass Sicherungsmechanismen wirksam sind.

Orientierungshilfe

Relevante Artikel der DSGVO:

Art. 5 Abs. 1 lit. f) und Art. 32 Abs. 1 lit. b)+c) DSGVO

Einführung / Überblick:

Siehe oben (Kapitel 2.1.4)

Ende der Orientierungshilfe

Anforderung im Detail:

Der Auftragsverarbeiter MUSS nachweisen, dass:

- im Rahmen der Auftragsverarbeitung auch Sicherungsdateien von einem Löschkonzept behandelt werden,
- Backups in einer Frequenz erstellt werden, die im Einklang mit insoweit anwendbaren Rechtsvorschriften oder internen Sicherheitsregelungen steht (sofern vorhanden),
- Hilfsmittel zur Verfügung stehen, um das fehlerfreie Funktionieren der implementierten Sicherungsverfahren zu testen (z. B. zur Verifizierung der Fehlerfreiheit / Lesbarkeit von Sicherungskopien),
- die Archivierung personenbezogener Daten von der Erstellung von Sicherungskopien getrennt ist.

Orientierungshilfe

Evaluationsmethoden:

Typischerweise kommen die folgenden Evaluationsmethoden zur Anwendung:

- Audit vor Ort zur Wirksamkeitskontrolle
- Interviews mit Vorgesetzten und Mitarbeitern

- Dokumentenprüfung
- Berücksichtigung relevanter anderer Zertifizierungen
- Testzugang

Dokumente:

Typischerweise sind insbesondere die folgenden Dokumente relevant:

- Einschlägige Zertifizierungen Dritter mit zugehörigen Prüfberichten
- Risikoanalyse des Auftragsverarbeiters
- Prozessbeschreibungen
- Backup Konzept
- Einschlägige Policies und Regelungen
- Schulungsunterlagen für Mitarbeiter
- Ggf. Verträge mit weiteren Auftragsverarbeitern (insbes.: Vorgaben zu TOM)

Prüftools / Anwendungshilfen:

Als Leitfaden bei Überprüfungen können die einschlägigen Prüfbausteine des BSI herangezogen werden. In diesen wird sowohl der Stand der Technik reflektiert als auch nach Maßnahmen entsprechend der Risikoklassen unterschieden. Darüber hinaus bietet ENISA einschlägige Unterstützung an und zusammen mit TeleTrusT liefert sie eine praxisbezogene Handreichung zum Stand der Technik.

Ende der Orientierungshilfe

2.1.4.3. Speicherung von Sicherungskopien

Anforderung in Kürze:

Der Auftragsverarbeiter MUSS sicherstellen, dass Sicherungskopien sicher aufbewahrt werden.

Orientierungshilfe

Relevante Artikel der DSGVO:

Art. 5 Abs. 1 lit. f) und Art. 32 Abs. 1 lit. b)+c) DSGVO

Einführung / Überblick:

Siehe oben (Kapitel 2.1.4)

Ende der Orientierungshilfe

Anforderung im Detail:

Der Auftragsverarbeiter MUSS nachweisen, dass:

- Sicherungsdateien sicher aufbewahrt / gelagert werden (z. B. in feuersicheren Safes oder in anderen Brandabschnitten),
- Sicherungsdateien gegen unberechtigte Zugänge / Zugriffe gesichert sind (z. B. durch Verschlüsselung, insbesondere bei Speicherung in der Cloud, Lagerung in Safes).

Orientierungshilfe

Evaluationsmethoden:

Typischerweise kommen die folgenden Evaluationsmethoden zur Anwendung:

- Audit vor Ort zur Wirksamkeitskontrolle
- Interviews mit Vorgesetzten und Mitarbeitern
- Dokumentenprüfung
- Berücksichtigung relevanter anderer Zertifizierungen
- Testzugang

Dokumente:

Typischerweise sind insbesondere die folgenden Dokumente relevant:

- Einschlägige Zertifizierungen Dritter mit zugehörigen Prüfberichten
- Risikoanalyse des Auftragsverarbeiters
- Prozessbeschreibungen
- Backup Konzept
- Einschlägige Policies und Regelungen
- Schulungsunterlagen für Mitarbeiter

Prüftools / Anwendungshilfen:

Als Leitfaden bei Überprüfungen können die einschlägigen Prüfbausteine des BSI herangezogen werden. In diesen wird sowohl der Stand der Technik reflektiert als auch nach Maßnahmen entsprechend der Risikoklassen unterschieden. Darüber hinaus bietet ENISA einschlägige Unterstützung an und zusammen mit TeleTrusT liefert sie eine praxisbezogene Handreichung zum Stand der Technik.

Ende der Orientierungshilfe

2.1.4.4. Wiederherstellungsmechanismen (Recovery)

Anforderung in Kürze:

Der Auftragsverarbeiter MUSS sicherstellen, dass die Wiederherstellungsprozesse wie nachfolgend unter „Anforderung im Detail:“ ausgeführt ablaufen.

Orientierungshilfe

Relevante Artikel der DSGVO:

Art. 5 Abs. 1 lit. f) und Art. 32 Abs. 1 lit. b)+c) DSGVO

Einführung / Überblick:

Siehe oben (Kapitel 2.1.4)

Ende der Orientierungshilfe

Anforderung im Detail:

Der Auftragsverarbeiter MUSS nachweisen, dass:

- die Wiederherstellungsprozesse getestet worden sind,
- die Wiederherstellung einzelner Datensätze (z. B. versehentlich gelöschter Datensätze) mit Hilfe der für die Sicherung dieser Datensätze verwendeten Medien organisiert (z. B. Wiederherstellung nur nach schriftlicher Autorisierung) und dokumentiert / protokolliert wird,
- die Wiederherstellung einzelner Daten (z. B. versehentlich gelöschter Daten) mit Hilfe der für die Sicherung dieser Daten verwendeten Medien organisiert (z. B. Wiederherstellung nur nach schriftlicher Autorisierung) und dokumentiert / protokolliert wird.

Orientierungshilfe

Evaluationsmethoden:

Typischerweise kommen die folgenden Evaluationsmethoden zur Anwendung:

- Audit vor Ort zur Wirksamkeitskontrolle
- Interviews mit Vorgesetzten und Mitarbeitern
- Dokumentenprüfung
- Berücksichtigung relevanter anderer Zertifizierungen
- Testzugang

Dokumente:

Typischerweise sind insbesondere die folgenden Dokumente relevant:

- Einschlägige Zertifizierungen Dritter mit zugehörigen Prüfberichten
- Risikoanalyse des Auftragsverarbeiters
- Prozessbeschreibungen
- Backup Konzept
- Einschlägige Policies und Regelungen
- Schulungsunterlagen für Mitarbeiter

Prüftools / Anwendungshilfen:

Als Leitfaden bei Überprüfungen können die einschlägigen Prüfbausteine des BSI herangezogen werden. In diesen wird sowohl der Stand der Technik reflektiert als auch nach Maßnahmen entsprechend der Risikoklassen unterschieden. Darüber hinaus bietet ENISA einschlägige Unterstützung an und zusammen mit TeleTrusT liefert sie eine praxisbezogene Handreichung zum Stand der Technik.

Ende der Orientierungshilfe

2.1.5. Datenschutz- und IT-Sicherheitsmanagement

Anforderung in Kürze:

Der Auftragsverarbeiter MUSS sicherstellen, dass sein implementiertes Datenschutz- und IT-Sicherheitsmanagement wie erforderlich ablaufen.

Orientierungshilfe

Relevante Artikel der DSGVO:

Art. 5 Abs. 2, Art. 24 Abs. 1+2, Art. 32 Abs. 1 lit. d) und Art. 39 Abs. 1 lit. b) DSGVO

Einführung / Überblick:

Um die Nachhaltigkeit der implementierten Datenschutzmaßnahmen sicherzustellen, müssen diese Maßnahmen in ein Managementsystem eingebettet sein. Wichtige Aspekte von Datenschutz- und IT-Sicherheitsmaßnahmen sind: Gesichtspunkte der relevanten Datenschutz- und IT-Sicherheitspolitiken, die Auswahl und Begründung von Maßnahmen, eine detaillierte Dokumentation sowie eine Überprüfung der ergriffenen Maßnahmen. Des Weiteren können spezifische Maßnahmen relevant sein wie z. B. die Verpflichtung der Mitarbeiter zur Verschwiegenheit.

Im Rahmen einer Zertifizierung von Verarbeitungsvorgängen von Auftragsverarbeitern nach EuroPriSe wird allerdings nicht das gesamte Datenschutzmanagementsystem eines Auftragsverarbeiters auf den Prüfstand gestellt, sondern es werden nur Aspekte betrachtet, die einen unmittelbaren Bezug zum ToE aufweisen. Dies kann sich gegebenenfalls auch auf weitere Auftragsverarbeiter erstrecken.

Im Einzelnen müssen die nachfolgend aufgelisteten spezifischen Anforderungen eingehalten werden.

Ende der Orientierungshilfe

2.1.5.1. Risikoanalyse

Anforderung in Kürze:

Der Auftragsverarbeiter MUSS sich der möglichen Risiken und Bedrohungen für die Rechte und Freiheiten der betroffenen Personen bewusst sein.

Orientierungshilfe

Relevante Artikel der DSGVO:

Art. 24 Abs. 1, Art. 32 Abs. 1 und Art. 35 DSGVO

Einführung / Überblick:

Technische und organisatorische Datenschutzmaßnahmen müssen im Hinblick auf das Risiko einer Verletzung von Datenschutzvorschriften ausgewählt werden (vgl. Art. 32 Abs. 1 DSGVO). Dies erfordert eine Bewertung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere von Risiken für die Rechte und Freiheiten natürlicher Personen (vgl. Art. 32 Abs. 1 DSGVO).

Falls die Verarbeitung personenbezogener Daten, die aus der bestimmungsgemäßen Inanspruchnahme der zu zertifizierenden Verarbeitungsvorgänge resultiert, aufgrund der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung voraussichtlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen zur Folge hat, müssen

die Anforderungen bezüglich einer Datenschutz-Folgenabschätzung (DSFA) nicht nur in rechtlicher[99], sondern auch in technischer Hinsicht überprüft werden.

Ende der Orientierungshilfe

Anforderung im Detail:

Der Auftragsverarbeiter MUSS nachweisen, dass:

- eine schriftliche Risikoanalyse bzw. ggf. auch eine DSFA vorhanden ist,
- diese aktuell ist,
- die zu zertifizierenden Verarbeitungsvorgänge abdeckt,
- die Risikoanalyse / DSFA regelmäßig überprüft und aktualisiert wird,
- technische und organisatorische Maßnahmen auf der Grundlage der Risikoanalyse / DSFA ausgewählt werden,
- die zusammen mit den Verarbeitungsvorgängen zur Verfügung gestellte Dokumentation über Risiken, eventuelle Schwachstellen etc. informiert und hierdurch die Identifizierung und Einführung von Sicherheitsmaßnahmen durch die einsetzende Stelle der Verarbeitungsvorgänge erleichtert wird (Kapitel 1.5.3),
- Die EuroPriSe-Methodik orientiert sich bei der Klassifizierung der Risiken an der Methode des Standard-Datenschutzmodells der DSK in der jeweils gültigen Fassung.[100]

Orientierungshilfe

Evaluationsmethoden:

Typischerweise kommen die folgenden Evaluationsmethoden zur Anwendung:

- Audit vor Ort zur Wirksamkeitskontrolle
- Interviews mit Vorgesetzten und Mitarbeitern
- Dokumentenprüfung
- Berücksichtigung relevanter anderer Zertifizierungen
- Testzugang

Dokumente:

Typischerweise sind insoweit insbesondere die folgenden Dokumente relevant:

- Einschlägige Zertifizierungen Dritter mit zugehörigen Prüfberichten
- Risikoanalyse / DSFA des (weiteren) Auftragsverarbeiters
- Prozessbeschreibungen
- Einschlägige Policies und Regelungen

[99] Siehe auch Kapitel 1.2.2 dieses Kriterienkatalogs (unter Anforderung im Detail, Nr. 6).

[100] https://www.datenschutzzentrum.de/uploads/sdm/SDM-Methode_V2.0b.pdf

- Schulungsunterlagen für Mitarbeiter
- Benutzerhandbuch
- Ggf. Verträge mit weiteren Auftragsverarbeitern (insbes.: Vorgaben zu TOM)

Prüftools / Anwendungshilfen:

Als Leitfaden bei Überprüfungen können die einschlägigen Anweisungen des BSI, ENISA / TeleTrusT oder des Standarddatenschutzmodells zur Durchführung von Risikoanalysen herangezogen werden. Vgl. außerdem Kapitel 4 des Methodik-Kompendiums AV.

Ende der Orientierungshilfe

2.1.5.2. Dokumentation technischer und organisatorischer Maßnahmen zum Datenschutz

Anforderung in Kürze:

Der Auftragsverarbeiter MUSS eine Dokumentation über alle implementierten technischen und organisatorischen Maßnahmen haben und diese aktuell halten. Dies betrifft auch vertraglich festgelegte TOMs für an Subdienstleister ausgelagerte Teilprozesse.

Orientierungshilfe

Relevante Artikel der DSGVO:

Art. 5 Abs. 1 lit. a) + Abs. 2 und Art. 32 Abs. 1 DSGVO

Einführung / Überblick:

Die Grundlage für eine ordnungsgemäße Implementierung technischer und organisatorischer Maßnahmen ist eine Dokumentation der bereits implementierten oder noch zu implementierenden Maßnahmen. Eine solche Dokumentation kann verwendet werden, um die geplanten Maßnahmen mit den aktuell implementierten Maßnahmen zu vergleichen. Die Auswahl der Maßnahmen muss auf der Grundlage der Risikoanalyse erfolgen (siehe Kapitel 2.1.5.1 sowie Kapitel 4 des Kompendiums der EuroPriSe-Methodik). Da dieses Dokument als vertraulich eingestufte Informationen enthalten dürfte, wird es für gewöhnlich nicht öffentlich einsehbar sein. Deshalb sind die Aufgaben und Pflichten der Nutzer und Administratoren in einem separaten Dokument darzustellen (siehe das nachfolgende Unterkapitel 2.1.5.3).

Ende der Orientierungshilfe

Anforderung im Detail:

Der Auftragsverarbeiter MUSS nachweisen, dass:

- eine detaillierte schriftliche Dokumentation der technischen und organisatorischen Maßnahmen vorhanden ist,
- diese aktuell ist,
- eine Versionshistorie sowie eine Übersicht der Autoren und der für die Umsetzung der Maßnahmen verantwortlichen Personen zur Verfügung stehen.

Orientierungshilfe

Evaluationsmethoden:

Typischerweise kommen die folgenden Evaluationsmethoden zur Anwendung:

- Audit vor Ort zur Wirksamkeitskontrolle
- Interviews mit Vorgesetzten und Mitarbeitern
- Dokumentenprüfung
- Berücksichtigung relevanter anderer Zertifizierungen

Dokumente:

Typischerweise sind insoweit insbesondere die folgenden Dokumente relevant:

- Einschlägige Zertifizierungen Dritter mit zugehörigen Prüfberichten
- Risikoanalyse des Auftragsverarbeiters
- Prozessbeschreibungen
- Einschlägige Policies und Regelungen
- Schulungsunterlagen für Mitarbeiter
- Aktuelle Liste der technischen und organisatorischen Maßnahmen
- Ggf. Verträge mit weiteren Auftragsverarbeitern (insbes.: Vorgaben zu TOM)

Prüftools / Anwendungshilfen:

Als Leitfaden bei Überprüfungen können die einschlägigen Anweisungen des BSI, ENISA / TeleTrusT oder des Standarddatenschutzmodells herangezogen werden.

Ende der Orientierungshilfe

2.1.5.3. Dokumentation individueller Verpflichtungen

Anforderung in Kürze:

Der Auftragsverarbeiter MUSS sicherstellen, dass alle seine Mitarbeiter und in seinem Auftrag tätige weitere Auftragsverarbeiter bzw. deren Mitarbeiter ihre Aufgaben und Pflichten kennen.

Orientierungshilfe

Relevante Artikel der DSGVO:

Art. 5 Abs. 1 lit. a) + Abs. 2 und Art. 32 Abs. 1 DSGVO

Einführung / Überblick:

Damit Nutzer und Administratoren (hier sind eigene Mitarbeiter des Auftragsverarbeiters sowie weiterer Auftragsverarbeiter gemeint) ihre Aufgaben und Pflichten kennen, müssen diese dokumentiert werden (z. B. in Gestalt von Arbeitsanweisungen oder Prozessbeschreibungen - SOPs). Die entsprechende Dokumentation muss für die Nutzer und Administratoren leicht zugänglich sein.

Ende der Orientierungshilfe

Anforderung im Detail:

Der Auftragsverarbeiter MUSS nachweisen, dass:

- die Aufgaben und Pflichten einzelner Personen dokumentiert sind,
- die entsprechende Dokumentation aktuell ist,
- die Dokumentation für diese Personen jederzeit leicht zugänglich (z. B. online / im Intranet abrufbar) ist.

Orientierungshilfe

Evaluationsmethoden:

Typischerweise kommen die folgenden Evaluationsmethoden zur Anwendung:

- Audit vor Ort zur Wirksamkeitskontrolle
- Interviews mit Vorgesetzten und Mitarbeitern
- Dokumentenprüfung
- Berücksichtigung relevanter anderer Zertifizierungen

Dokumente:

Typischerweise sind insoweit insbesondere die folgenden Dokumente relevant:

- Einschlägige Zertifizierungen Dritter mit zugehörigen Prüfberichten
- Risikoanalyse des Auftragsverarbeiters
- Prozessbeschreibungen
- Einschlägige Policies und Regelungen
- Schulungsunterlagen für Mitarbeiter
- Arbeitsanweisungen
- Aktuelle Liste der technischen und organisatorischen Maßnahmen
- Ggf. Verträge mit weiteren Auftragsverarbeitern (insbes.: Vorgaben zu TOM)

Prüftools / Anwendungshilfen:

Als Leitfaden bei Überprüfungen können die einschlägigen Anweisungen des BSI, ENISA / TeleTrusT oder des Standarddatenschutzmodells herangezogen werden.

Ende der Orientierungshilfe

2.1.5.4. Inventarliste zu Hardware, Software, Daten und Medien

Anforderung in Kürze:

Der Auftragsverarbeiter MUSS sicherstellen, dass für die Verarbeitungsvorgänge eingesetzte relevante Hardware, Software, Daten und Medien in Inventarlisten erfasst sind. Bei Hardware und Software MUSS jeweils auch das aktuelle Patch-Level dokumentiert werden.

Orientierungshilfe

Relevante Artikel der DSGVO:

Art. 5 Abs. 1 lit. a) + Abs. 2 und Art. 32 Abs. 1 DSGVO

Einführung / Überblick:

Um alle Datenverarbeitungsvorgänge einschätzen und im Hinblick auf ihre Vereinbarkeit mit EU-Datenschutzrecht bewerten zu können, ist (ggf. jeweils) eine Inventarliste zu eingesetzter Hardware, Software, Daten und Medien, die zur Verarbeitung personenbezogener Daten verwendet werden, erforderlich. Da einige dieser Informationen auch für das Verzeichnis von Verarbeitungstätigkeiten (vgl. Kapitel 1.1.1) benötigt werden, kann die relevante Information in einem einzigen Dokument zusammengefasst werden.

Ende der Orientierungshilfe

Anforderung im Detail:

Der Auftragsverarbeiter MUSS nachweisen, dass:

- eine aktuelle Inventarliste aller für die Verarbeitung personenbezogener Daten verwendeten Hardware, Software, Dateien und Medien, oder mehrere getrennte, jeweils aktuelle Inventarlisten vorhanden ist/sind, die die komplette Hardware und Software sowie Kategorien von personenbezogenen Daten und Medien auflistet/n.
- die Dokumentation über die Vernetzung dieser Unternehmenswerte (Netzwerktopologie, Domänen etc.) informiert und dabei sowohl die interne Vernetzung als auch Verbindungen zu externen Netzwerken berücksichtigt.

Orientierungshilfe

Evaluationsmethoden:

Typischerweise kommen die folgenden Evaluationsmethoden zur Anwendung:

- Audit vor Ort zur Wirksamkeitskontrolle
- Interviews mit Vorgesetzten und Mitarbeitern
- Dokumentenprüfung
- Berücksichtigung relevanter anderer Zertifizierungen

Dokumente:

Typischerweise sind insoweit insbesondere die folgenden Dokumente relevant:

- Einschlägige Zertifizierungen Dritter mit zugehörigen Prüfberichten
- Risikoanalyse des Auftragsverarbeiters
- Prozessbeschreibungen
- Einschlägige Policies und Regelungen
- Schulungsunterlagen für Mitarbeiter

Prüftools / Anwendungshilfen:

Als Leitfaden bei Überprüfungen können die einschlägigen Anweisungen des BSI, und von ENISA / TeleTrusT herangezogen werden.

Ende der Orientierungshilfe

2.1.5.5. Management von Speichermedien

Anforderung in Kürze:

Der Auftragsverarbeiter muss den kontrollierten Umgang mit Speichermedien sicherstellen.

Orientierungshilfe

Relevante Artikel der DSGVO:

Art. 5 Abs. 1 lit. a) + Abs. 2 und Art. 32 Abs. 1 DSGVO

Einführung / Überblick:

Medien, auf denen personenbezogene Daten gespeichert werden können, sind beispielsweise CDs, DVDs, Bänder und USB-Datenträger.

Ende der Orientierungshilfe

Anforderung im Detail:

Der Auftragsverarbeiter muss nachweisen, dass:

- Medien, auf denen personenbezogene Daten gespeichert werden, die Identifikation der auf ihnen gespeicherten Informationen ermöglichen,
- diese Medien katalogisiert und an einem Platz aufbewahrt werden, zu dem nur die Mitarbeiter Zugang haben, die hierzu nach der Sicherheitsrichtlinie berechtigt sind,
- es ein Medieneingangsregister gibt, das – direkt oder indirekt – Informationen zu der Art des jeweiligen Mediums, zu dessen Seriennummer und zur Art der darauf gespeicherten Informationen enthält,
- das Medieneingangsregister auch Informationen zu Datum und Uhrzeit des Eingangs, zum Absender, zur Versandart und zu der Person, die für den Empfang verantwortlich ist (d. h. die Person, die den Empfang quittiert hat) enthält, falls Medien angeliefert worden sind,
- das Medieneingangsregister auch Informationen zu Datum und Uhrzeit der Erstellung, zu der Person, die das jeweilige Medium erzeugt hat (d. h. die Person, die die Daten eingegeben oder auf das Medium kopiert hat) und zu der Person, die das Medium in das Register aufgenommen hat, enthält, falls Medien organisationsintern erzeugt worden sind,
- es ein Medienausgangsregister gibt, das – direkt oder indirekt – Informationen zur Art des versendeten Mediums, zu dessen Seriennummer, zur Art der darauf gespeicherten Informationen, zu Datum und Uhrzeit der Versendung, zum Empfänger, zur Versandart und zu der Person, die für die Entgegennahme des Mediums verantwortlich ist, enthält.

Orientierungshilfe

Evaluationsmethoden:

Typischerweise kommen die folgenden Evaluationsmethoden zur Anwendung:

- Audit vor Ort zur Wirksamkeitskontrolle
- Interviews mit Vorgesetzten und Mitarbeitern

- Dokumentenprüfung
- Berücksichtigung relevanter anderer Zertifizierungen

Dokumente:

Es sind insbesondere die folgenden Dokumente relevant:

- Einschlägige Zertifizierungen Dritter mit zugehörigen Prüfberichten
- Risikoanalyse des Auftragsverarbeiters
- Prozessbeschreibungen
- Einschlägige Policies und Regelungen
- Schulungsunterlagen für Mitarbeiter
- Medienregister

Prüftools / Anwendungshilfen:

Als Leitfaden bei Überprüfungen können die einschlägigen Anweisungen des BSI und von ENISA / TeleTrusT herangezogen werden.

Ende der Orientierungshilfe

2.1.5.6. Unterweisung der Mitarbeiter; Pflicht zur Verschwiegenheit

Anforderung in Kürze:

Der Auftragsverarbeiter MUSS sicherstellen, dass Mitarbeiter hinsichtlich ihrer Aufgaben und Pflichten und damit zusammenhängender Datenschutzaspekte unterwiesen werden und Vertraulichkeits- bzw. Verschwiegenheitspflichten unterliegen.

Orientierungshilfe

Relevante Artikel der DSGVO:

Art. 28 Abs. 3 lit. b), Art. 29 und Art. 39 Abs. 1 lit. a+b DSGVO

Einführung / Überblick:

Bei Personen, die Zugriff auf personenbezogene Daten haben, handelt es sich üblicher Weise um Mitarbeiter des Auftragsverarbeiters oder um Mitarbeiter von weiteren Auftragsverarbeitern. Sie müssen sich zur Vertraulichkeit verpflichtet haben oder einer gesetzlichen Verschwiegenheitspflicht unterliegen. Solche Vertraulichkeitspflichten müssen auch über die Beendigung des jeweiligen Beschäftigungsverhältnisses hinaus Anwendung finden. Zum Thema Vertraulichkeit vgl. auch Kapitel 1.2.2.

Ende der Orientierungshilfe

Anforderung im Detail:

Der Auftragsverarbeiter MUSS nachweisen, dass:

- neue Mitarbeiter im Hinblick auf ihre Aufgaben und Pflichten eingewiesen/geschult werden,
- Mitarbeiter in regelmäßigen Abständen (z. B. einmal pro Jahr) erneut eingewiesen und geschult werden, wobei dies auf unterschiedliche Weise geschehen kann (Präsenzschulung, Selbststudium etc.),

- Datum, Uhrzeit und Teilnehmer dieser Einweisungs-/Schulungsveranstaltungen dokumentiert werden (d. h., es muss eine Liste der Personen geben, die an der jeweiligen Veranstaltung teilgenommen haben),
- die Aufgaben und Pflichten der Mitarbeiter schriftlich festgehalten werden,
- ein Verstoß gegen diese Aufgaben und Pflichten arbeitsrechtliche Konsequenzen hat, wobei dies den Mitarbeitern gegenüber deutlich gemacht werden muss (z. B. im Arbeitsvertrag oder einem Annex zu diesem).

Orientierungshilfe

Evaluationsmethoden:

Typischerweise kommen die folgenden Evaluationsmethoden zur Anwendung:

- Audit vor Ort zur Wirksamkeitskontrolle
- Interviews mit Vorgesetzten und Mitarbeitern
- Dokumentenprüfung
- Berücksichtigung relevanter anderer Zertifizierungen

Dokumente:

Typischerweise sind insbesondere die folgenden Dokumente relevant:

- Einschlägige Zertifizierungen Dritter mit zugehörigen Prüfberichten
- Risikoanalyse des Auftragsverarbeiters
- Einschlägige Policies und Regelungen
- Schulungsunterlagen für Mitarbeiter
- Ggf. Verträge mit weiteren Auftragsverarbeitern (insbes.: Vorgaben zu TOM)

Prüftools / Anwendungshilfen:

Als Leitfaden bei Überprüfungen können die einschlägigen Anweisungen des BSI und von ENISA / TeleTrusT herangezogen werden.

Orientierungshilfe

2.1.5.7. Datenschutz- und Sicherheitsaudits

Anforderung in Kürze:

Der Auftragsverarbeiter / weitere Auftragsverarbeiter MUSS die beständige Wirksamkeit der technischen und organisatorischen Maßnahmen zum Datenschutz sicherstellen.

Orientierungshilfe

Relevante Artikel der DSGVO:

Art. 28 Abs. 3 lit. h), Art. 32 Abs. 1 lit. d und Art. 35 DSGVO

Einführung / Überblick:

Um ihre (andauernde) Wirksamkeit bewerten zu können, müssen technische und organisatorische Maßnahmen zum Datenschutz regelmäßig überprüft und evaluiert

werden. Solche Audits können entweder durch Mitarbeiter der Organisation oder durch externe Prüfer durchgeführt werden.

Ende der Orientierungshilfe

Anforderung im Detail:

Der Auftragsverarbeiter MUSS nachweisen, dass:

- Maßnahmen des Datenschutzes / der Sicherheit der Verarbeitungsvorgänge regelmäßig überprüft werden,
- schriftliche Aufzeichnungen (Berichte) über die Umstände (Datum, Ort, Namen der Prüfer) und die Ergebnisse solcher Überprüfungen vorhanden sind.

Orientierungshilfe

Evaluationsmethoden:

Typischerweise kommen die folgenden Evaluationsmethoden zur Anwendung:

- Audit vor Ort zur Wirksamkeitskontrolle
- Interviews mit Vorgesetzten und Mitarbeitern
- Dokumentenprüfung
- Berücksichtigung relevanter anderer Zertifizierungen

Dokumente:

Typischerweise sind insbesondere die folgenden Dokumente relevant:

- Einschlägige Zertifizierungen Dritter mit zugehörigen Prüfberichten
- Auditjahresprogramm
- IS und/oder DS Auditberichte
- Protokolle von Managementreviews

Prüftools / Anwendungshilfen:

N/A

Ende der Orientierungshilfe

2.1.5.8. Vorfallmanagement (Incident-Management) durch Auftragsverarbeiter

Anforderung in Kürze:

Der Auftragsverarbeiter MUSS durch einen Prozess, der gegebenenfalls auch weitere Auftragsverarbeiter einbeziehen muss, sicherstellen, auf Sicherheits- oder Datenschutzvorfälle sowie auf identifizierte Schwachstellen reagieren zu können. Dies schließt Prozesse im Rahmen eines Patch / Change Managements ein.

Orientierungshilfe

Relevante Artikel der DSGVO:

Art. 32 Abs. 1 lit. d) und Art. 33 f. DSGVO

Einführung / Überblick:

Eine Organisation muss über Management-Prozesse verfügen, um auf Sicherheits- oder Datenschutzvorfälle sowie auf identifizierte Schwachstellen reagieren zu können. Dies beinhaltet eine Dokumentation solcher Vorfälle, der Abhilfe- bzw. Wiederherstellungsmaßnahmen und der Benachrichtigung der Kunden / betroffenen Personen hiervon (insoweit ist auf Art. 33 Abs. 2 DSGVO hinzuweisen, wonach der Auftragsverarbeiter dem Verantwortlichen eine Verletzung des Schutzes personenbezogener Daten unverzüglich zu melden hat, wenn ihm diese bekannt wird). Ziel eines solchen Vorfallmanagements ist die Ermöglichung eines Lernprozesses, der darauf gerichtet ist, weitere Vorfälle zu verhindern, sowie die Unterstützung der Verantwortlichen dabei, solche Vorfälle zu verhindern. Darüber hinaus müssen Verfahren vorhanden sein, die darauf abzielen, Sicherheitsschwachstellen zu adressieren, bevor diese konkrete Sicherheitsvorfälle zur Folge haben. Dieses Kapitel überschneidet sich mit dem Kapitel 1.2.2.

Ende der Orientierungshilfe

Anforderung im Detail:

Der Auftragsverarbeiter MUSS nachweisen, dass:

- schriftlich dokumentierte Vorgehensweisen vorhanden sind, welche die maßgeblichen Handlungen und Abläufe beschreiben, die im Falle eines Vorfalls vorzunehmen bzw. zu befolgen sind und dabei die verantwortlichen Mitarbeiter und ihre jeweiligen Rollen etc. benannt werden,
- in diesen Vorgehensweisen Maßnahmen benannt sind, die gewährleisten, dass der Auftragsverarbeiter den Verantwortlichen ihm bekannt gewordene Verletzungen des Schutzes personenbezogener Daten unverzüglich meldet (vgl. Art. 33 Abs. 2 DSGVO),
- die Unterstützung der Verantwortlichen durch den Auftragsverarbeiter bei der Einhaltung der in Art. 33 f. DSGVO genannten Pflichten Bestandteil dieser Vorgehensweisen ist (vgl. insoweit Art. 28 Abs. 3 S. 2 lit f) DSGVO),
- in Aufzeichnungen zu bereits eingetretenen Vorfällen der Gegenstand/die Umstände des jeweiligen Vorfalls und die insoweit getroffenen Abhilfe- bzw. Wiederherstellungsmaßnahmen benannt werden,
- Informationen über Sicherheitsschwachstellen gesammelt (z. B. über den jeweiligen Hersteller, CERT-Nachrichten etc.) und an relevante Stellen in der Organisation (z. B. ein Change Managementteam) weitergeleitet werden.

Orientierungshilfe

Evaluationsmethoden:

Typischerweise kommen die folgenden Evaluationsmethoden zur Anwendung:

- Audit vor Ort zur Wirksamkeitskontrolle
- Interviews mit Vorgesetzten und Mitarbeitern
- Dokumentenprüfung
- Berücksichtigung relevanter anderer Zertifizierungen

Dokumente:

Typischerweise sind insbesondere die folgenden Dokumente relevant:

- Einschlägige Zertifizierungen Dritter mit zugehörigen Prüfberichten
- Protokolle der Managementreviews
- Incidentliste
- Ggf. Verträge mit weiteren Auftragsverarbeitern (insbes.: Vorgaben zu TOM)

Prüftools / Anwendungshilfen:

- Art. 29 WP (vom EDSA bestätigt): Leitlinien für die Meldung von Verletzungen des Schutzes personenbezogener Daten gemäß der Verordnung (EU) 2016/679 (WP 250 rev. 01) (vgl. insbesondere Kapitel II.A.4.: „Pflichten des Auftragsverarbeiters“)
- EDSA: Guidelines 01/2021 on Examples regarding Data Breach Notification

Ende der Orientierungshilfe

2.1.5.9. Test und Freigabe

Anforderung in Kürze:

Der Auftragsverarbeiter MUSS (neue) Verarbeitungsvorgänge testen und freigeben.

Orientierungshilfe

Relevante Artikel der DSGVO:

Art. 32 Abs. 1 lit. d) DSGVO

Einführung / Überblick:

Bevor IT-Verarbeitungsvorgänge eingesetzt werden, müssen sie getestet und formal freigegeben werden. Für solche Tests dürfen grundsätzlich nur Testdaten oder anonyme Daten verwendet werden. Echtdaten dürfen hingegen nur in Ausnahmefällen hierfür genutzt werden. Durchgeführte Tests sind zu dokumentieren. Die Tests sollten sich nicht nur auf die bestimmungsgemäße Verwendung der jeweiligen IT-Komponente beziehen, sondern auch Versuche einer unberechtigten und/oder missbräuchlichen Nutzung (z. B. Verwendung unrichtiger Eingabedaten) zum Gegenstand haben. Test und Freigabe können mit einer Datenschutz-Folgenabschätzung verbunden werden (vgl. Kapitel 3 des Kompendiums der EuroPriSe-Methodik; siehe auch Kapitel 2.1.8 dieses Kriterienkatalogs - Dokumentation des Dienstes aus Kundensicht).

Ende der Orientierungshilfe

Anforderung im Detail:

Der Auftragsverarbeiter MUSS nachweisen, dass:

- es ein formales Verfahren zur Freigabe von Verfahren und Software gibt,
- Tests geplant und durchgeführt werden, bevor die Freigabe erfolgt,
- (ausschließlich) Testdaten (z. B. anonyme Daten, Dummy-Daten etc.) verwendet werden,

- Test- und Freigabeentscheidungen dokumentiert werden,
- Funktionalitäten für eine sichere Löschung von Testdaten (inklusive Protokolldaten) nach Abschluss der Tests zur Verfügung stehen.

Orientierungshilfe

Evaluationsmethoden:

Typischerweise kommen die folgenden Evaluationsmethoden zur Anwendung:

- Audit vor Ort zur Wirksamkeitskontrolle
- Interviews mit Vorgesetzten und Mitarbeitern
- Dokumentenprüfung
- Berücksichtigung relevanter anderer Zertifizierungen

Dokumente:

Typischerweise sind insbesondere die folgenden Dokumente relevant:

- Einschlägige Zertifizierungen Dritter mit zugehörigen Prüfberichten
- Prozessbeschreibungen
- Einschlägige Policies und Regelungen
- Schulungsunterlagen für Mitarbeiter

Prüftools / Anwendungshilfen:

Als Leitfaden bei Überprüfungen können die einschlägigen Prüfbausteine des BSI herangezogen werden. In diesen wird sowohl der Stand der Technik reflektiert als auch nach Maßnahmen entsprechend der Risikoklassen unterschieden.

Ende der Orientierungshilfe

2.1.6. Entsorgung und Löschung personenbezogener Daten

Anforderung in Kürze:

Der Auftragsverarbeiter MUSS die sichere Entsorgung und Löschung personenbezogener Daten nach Abschluss der Erbringung der Verarbeitungsleistungen sicherstellen. Dies auch insoweit, wie weitere Auftragsverarbeiter involviert sind.

Orientierungshilfe

Relevante Artikel der DSGVO:

Art. 5 Abs. 1 lit. e), Art. 28 Abs. 3 S. 2 lit. g) DSGVO

Einführung / Überblick:

Nach Abschluss der Verarbeitungsleistungen muss der Auftragsverarbeiter alle personenbezogenen Daten nebst angefertigter Kopien löschen und/oder zurückgeben. Er muss den Verantwortlichen außerdem dabei unterstützen, seiner Pflicht zur Beantwortung von Anträgen der betroffenen Personen auf Löschung nachzukommen. Außerdem ist das Thema Löschung auch dann relevant, wenn personenbezogene Daten für die Zwecke, für die sie verarbeitet werden, nicht mehr benötigt werden. Der Auftragsverarbeiter muss

schließlich auch die sachgerechte Entsorgung von Hardware, Software oder Medien, auf denen personenbezogene Daten gespeichert sind, sicherstellen.

Ende der Orientierungshilfe

Anforderung im Detail:

Der Auftragsverarbeiter MUSS nachweisen, dass:

- sowohl vollständige Datensätze als auch einzelne Datenelemente gelöscht werden können,
- eine solche Löschung dergestalt dokumentiert werden kann (beispielsweise in einem Logfile), dass die gelöschten Daten selbst nicht offengelegt werden,
- die Verarbeitungsvorgänge Funktionalitäten für eine automatisierte Löschung nach Ablauf bestimmter (fest definierter, relativer oder an bestimmte Bedingungen geknüpfter) Fristen zur Verfügung stellen (z. B. Funktionalitäten, die auf einen Timer oder eine Erinnerungsfunktion zurückgreifen),
- die Verarbeitungsvorgänge Daten dergestalt löschen, dass sie nicht wiederhergestellt werden können (z. B. durch das (mehrfache) Überschreiben von Daten auf einer Festplatte, CD-RW etc.),
- die verwendete Löschmethode zuverlässig und wirksam ist,
- falls erforderlich Teile der verwendeten Hardware vor der Entsorgung bzw. Wiederverwendung entfernt bzw. „gesäubert“ worden sind (Beispiele hierfür sind die Entfernung von Festplatten aus Computern oder die Entfernung von Flash-Speichern aus Routern),
- wenn Datenträger physisch zerstört werden (z. B. zwecks Beseitigung von Dokumenten, Medien, CD-ROMs, Chipkarten oder Tokens), die hierfür genutzte Methode zuverlässig und wirksam ist,
- sofern Geräte Dritter zur Verarbeitung personenbezogener Daten verwendet werden (z. B. geleaste Kopierer und die in ihnen verbauten Festplatten), Maßnahmen getroffen worden sind um sicherzustellen, dass sich keine personenbezogenen Daten mehr auf diesen Geräten befinden, wenn sie zurückgegeben / von ihren Eigentümern wieder in Besitz genommen werden,
- Medien vor ihrer Entsorgung fachgerecht „gesäubert” bzw. zerstört werden,
- falls hierfür die Dienste von Drittanbietern genutzt werden, dies rechtlich zulässig ist und nur auf zertifizierte Entsorgungsfachbetriebe zurückgegriffen wird.
- die Methoden, die für die physische Vernichtung (von Dokumenten, Medien, CD-ROMs) oder für die logische Vernichtung von Daten (z. B. durch Überschreiben) verwendet werden, zuverlässig und wirksam sind.

Orientierungshilfe

Evaluationsmethoden:

Typischerweise kommen die folgenden Evaluationsmethoden zur Anwendung:

- Audit vor Ort zur Wirksamkeitskontrolle
- Interviews mit Vorgesetzten und Mitarbeitern

- Dokumentenprüfung
- Berücksichtigung relevanter anderer Zertifizierungen

Dokumente:

Typischerweise sind insbesondere die folgenden Dokumente relevant:

- Einschlägige Zertifizierungen Dritter mit zugehörigen Prüfberichten
- Prozessbeschreibungen
- Einschlägige Policies und Regelungen
- Schulungsunterlagen für Mitarbeiter
- Ggf. Verträge mit weiteren Auftragsverarbeitern (insbes.: Vorgaben zu TOM)

Prüftools / Anwendungshilfen:

Als Leitfaden bei Überprüfungen können die einschlägigen Anweisungen des BSI, von ENISA / TeleTrusT und des SDM herangezogen werden.

Ende der Orientierungshilfe

2.1.7. Temporäre Dateien

Anforderung in Kürze:

Der Auftragsverarbeiter MUSS den sicheren Umgang auch mit temporären Dateien sicherstellen. Dies auch insoweit, wie weitere Auftragsverarbeiter involviert sind.

Orientierungshilfe

Relevante Artikel der DSGVO:

Art. 5 Abs. 1 lit. d)+f), Art. 17 und Art. 32 Abs. 1 lit. b) DSGVO

Einführung / Überblick:

Wenn temporäre Dateien oder Daten erstellt werden, muss der Zugang zu diesen genauso kontrolliert werden wie der zu anderen Arten personenbezogener Daten. Temporäre Daten sind zu löschen, wenn sie für die Zwecke, für die sie erzeugt wurden, nicht mehr benötigt werden.

Ende der Orientierungshilfe

Anforderung im Detail:

Der Auftragsverarbeiter MUSS nachweisen, dass:

- ein Überblick vorhanden ist, wo überall durch die zu zertifizierenden Verarbeitungsvorgänge temporäre Dateien erzeugt werden (z. B. temporäre Kopien von Dokumenten, die mit Hilfe eines Textverarbeitungsprogramms bearbeitet werden),
- der Zugang zu diesen Daten / Kopien im Rahmen der Verarbeitungsvorgänge kontrolliert wird (z. B. durch Dateifreigaben, die nur für die Nutzer des gerade bearbeiteten (Original)Dokuments gelten),
- temporäre Dateien oder Daten automatisiert gelöscht werden,

- dies in einer sicheren Art und Weise (siehe Kapitel 2.1.6) geschieht,
- ein automatisiertes Verfahren zur Verfügung steht, das eine Warnung ausgibt, wenn (einige) temporäre Dateien nicht gelöscht / entfernt werden konnten, und das (in der Folge) eine zuverlässige Löschung ermöglicht.

Orientierungshilfe

Evaluationsmethoden:

Typischerweise kommen die folgenden Evaluationsmethoden zur Anwendung:

- Audit vor Ort zur Wirksamkeitskontrolle
- Interviews mit Vorgesetzten und Mitarbeitern
- Dokumentenprüfung
- Berücksichtigung relevanter anderer Zertifizierungen
- Testzugang

Dokumente:

Typischerweise sind insbesondere die folgenden Dokumente relevant:

- Einschlägige Zertifizierungen Dritter mit zugehörigen Prüfberichten
- Prozessbeschreibungen
- Einschlägige Policies und Regelungen
- Schulungsunterlagen für Mitarbeiter
- Arbeitsanweisungen
- Ggf. Verträge mit weiteren Auftragsverarbeitern (insbes.: Vorgaben zu TOM)

Prüftools / Anwendungshilfen:

Als Leitfaden bei Überprüfungen können die einschlägigen Anweisungen des BSI und von ENISA / TeleTrusT herangezogen werden.

Ende der Orientierungshilfe

2.1.8. Dokumentation der Verarbeitungsvorgänge aus Kundensicht

Anforderung in Kürze:

Der Auftragsverarbeiter MUSS die Verarbeitungsvorgänge so beschreiben, dass ein Kunde (Verantwortlicher) diese im Einklang mit EU-Datenschutzrecht nutzen kann.

Orientierungshilfe

Relevante Artikel der DSGVO:

Art. 5 Abs. 1 lit. a) + Abs. 2 und Art. 32 Abs. 1 DSGVO

Einführung / Überblick:

Kunden von nach EuroPriSe zu zertifizierenden Verarbeitungsvorgängen von Auftragsverarbeitern sind üblicher Weise als Verantwortliche einzustufen und müssen

folglich die Vorgaben des EU-Datenschutzrechts einhalten. Hierfür benötigen sie Informationen, die es ihnen ermöglichen, ihre entsprechenden Rechtspflichten zu erfüllen.

Ende der Orientierungshilfe

Anforderung im Detail:

Der Auftragsverarbeiter MUSS nachweisen, dass:

- er seinen Kunden (Verantwortlichen) in Gestalt der Dokumentation (inklusive des Datenschutzmerkblatts, siehe Kapitel 1.5.3) alle Informationen sowie Hinweise und Handlungsempfehlungen zur Verfügung stellt, die die Kunden zur Erfüllung ihrer rechtlichen Verpflichtungen benötigen (z. B. Informationen zu technischen und organisatorischen Maßnahmen, das Sicherheitskonzept des Auftragsverarbeiters, Informationen über (weitere) Auftragsverarbeiter, insbesondere solche aus Drittländern),
- die Dokumentation sowohl für administratives Personal (Admins) wie auch für Nutzer leicht zu verstehen und zu verwenden ist,
- die Dokumentation Informationen, Hinweise und Handlungsempfehlungen dazu enthält, wie die Verarbeitungsvorgänge in Anspruch zu nehmen sind.

Orientierungshilfe

Evaluationsmethoden:

Typischerweise kommen die folgenden Evaluationsmethoden zur Anwendung:

- Audit vor Ort zur Wirksamkeitskontrolle
- Interviews mit Vorgesetzten und Mitarbeitern
- Dokumentenprüfung
- Berücksichtigung relevanter anderer Zertifizierungen
- Testzugang

Dokumente:

Typischerweise sind insbesondere die folgenden Dokumente relevant:

- Kundendokumentation, hier Leistungsbeschreibung der Verarbeitungsvorgänge
- Datenschutzmerkblatt
- Auftragsverarbeitungsvertrag
- TOM-Dokumente

Prüftools / Anwendungshilfen:

Als Leitfaden bei Überprüfungen können die einschlägigen Anweisungen des BSI und von ENISA / TeleTrusT herangezogen werden.

Ende der Orientierungshilfe

2.2. Technologiespezifische Anforderungen

Dieses Unterkapitel enthält technologiespezifische Anforderungen, die die Themen Verschlüsselung, Pseudonymisierung und Anonymisierung betreffen.

2.2.1. Verschlüsselung

Anforderung in Kürze:

Der Auftragsverarbeiter MUSS sichere Verschlüsselungstechniken einsetzen. Dies MUSS auch im Hinblick auf weitere Auftragsverarbeiter gewährleistet sein.

Orientierungshilfe

Relevante Artikel der DSGVO:

Art. 5 Abs. 1 lit. f) und Art. 32 Abs. 1 lit. a) DSGVO

Einführung / Überblick:

Die DSGVO benennt die Verschlüsselung ausdrücklich als eine (wichtige technische) Maßnahme zur Gewährleistung eines Sicherheitsniveaus, das im Hinblick auf die mit der Verarbeitung einhergehenden Risiken angemessen ist. Eine Verschlüsselung kann z. B. bei einer Übertragung personenbezogener Daten über ein Netzwerk oder bei deren Speicherung auf einem mobilen Gerät wie z. B. einem Notebook erforderlich sein. Außerdem kann eine Verschlüsselung auch verwendet werden, um Zugangs- bzw. Zugriffskontrollmechanismen zu implementieren (z. B. für Datenbanken und für die Speicherung von Sicherungskopien).

Ende der Orientierungshilfe

Anforderung im Detail:

Der Auftragsverarbeiter MUSS nachweisen, dass:

- für den Transport von Daten mittels Medien oder über unsichere Netzwerke Verschlüsselungsmechanismen eingesetzt werden,
- Verschlüsselungsmechanismen bei der Zugangs- / Zugriffskontrolle zum Einsatz kommen (z. B. im Hinblick auf den Zugriff auf Datenbanken oder Sicherungskopien),
- die Verschlüsselung wirksam ist, z. B. im Hinblick auf die verwendeten Schlüssellängen und Algorithmen (so MUSS es sich insbesondere um renommierte / bewährte Algorithmen handeln, zu denen bislang keine Schwachstellen bekannt geworden sind),
- die zum Einsatz kommenden Schlüssel sicher gehandhabt werden, auch für den Fall des Verlustes oder Vergessens,
- die Schlüssel auf sichere Art und Weise übertragen werden (z. B. Schlüssel für die Verschlüsselung von Festplatten gehosteter Server).

Orientierungshilfe

Evaluationsmethoden:

Typischerweise kommen die folgenden Evaluationsmethoden zur Anwendung:

- Audit vor Ort zur Wirksamkeitskontrolle
- Interviews mit Vorgesetzten und Mitarbeitern
- Dokumentenprüfung
- Berücksichtigung relevanter anderer Zertifizierungen

- Testzugang

Dokumente:

Typischerweise sind insbesondere die folgenden Dokumente relevant:

- Einschlägige Zertifizierungen Dritter mit zugehörigen Prüfberichten
- Prozessbeschreibungen
- Einschlägige Policies und Regelungen
- Schulungsunterlagen für Mitarbeiter
- Arbeitsanweisungen
- Ggf. Verträge mit weiteren Auftragsverarbeitern (insbes.: Vorgaben zu TOM)

Prüftools / Anwendungshilfen:

Als Leitfaden bei Überprüfungen können die einschlägigen Anweisungen des BSI und von ENISA / TeleTrusT herangezogen werden.

Ende der Orientierungshilfe

2.2.2. Pseudonymisierung und Anonymisierung

Anforderung in Kürze:

Grundsätzlich hat der Auftragsverarbeiter die Verarbeitungsvorgänge so zu gestalten, dass den Verantwortlichen die Einhaltung des Grundsatzes Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen so leicht wie möglich gemacht wird (vgl. Kapitel 1.5 dieses Kriterienkatalogs). Macht er in diesem Zusammenhang von den Instrumenten der Pseudonymisierung und/oder Anonymisierung Gebrauch, so MUSS er insoweit wirksame Methoden verwenden. Dies MUSS auch im Hinblick auf weitere Auftragsverarbeiter gewährleistet sein.

Orientierungshilfe

Relevante Artikel der DSGVO:

Art. 4 Nr. 5, Art. 25 Abs. 1 und Art. 32 Abs. 1 lit. a) DSGVO

Einführung / Überblick:

Zur Anonymisierung[101] und/oder Pseudonymisierung[102] personenbezogener Daten, müssen wirksame Methoden verwendet werden, die insbesondere eine Aufdeckung von Pseudonymen / anderweitige Re-Identifizierung verhindern bzw. sicherstellen, dass eine solche Re-Identifizierung einen unverhältnismäßigen Aufwand erfordert. Informationen, die zur Aufdeckung von Pseudonymen verwendet werden können (insbesondere sogenannte Zuordnungsregeln), müssen geschützt werden.

[101] Zuordnung von Daten zu einer bestimmten Person ist nach erfolgter Anonymisierung gar nicht mehr möglich, jedenfalls nicht ohne unverhältnismäßigen Aufwand.

[102] Zuordnung von Daten zu einer bestimmten Person ist nach erfolgter Pseudonymisierung nur noch unter Hinzuziehung zusätzlicher Informationen möglich (vgl. Art. 4 Nr. 5 DSGVO).

Ende der Orientierungshilfe

Anforderung im Detail:

N/A

Orientierungshilfe

Evaluationsmethoden:

Typischerweise kommen die folgenden Evaluationsmethoden zur Anwendung:

- Audit vor Ort zur Wirksamkeitskontrolle
- Interviews mit Vorgesetzten und Mitarbeitern
- Dokumentenprüfung
- Berücksichtigung relevanter anderer Zertifizierungen
- Testzugang

Dokumente:

Typischerweise befassen sich die folgenden Dokumente mit dem Sachverhalt:

- Einschlägige Zertifizierungen Dritter mit zugehörigen Prüfberichten (falls vorhanden)
- Prozessbeschreibungen
- Einschlägige Policies und Regelungen
- Schulungsunterlagen für Mitarbeiter
- Arbeitsanweisungen
- Ggf. Verträge mit weiteren Auftragsverarbeitern (insbes.: Vorgaben zu TOM)

Prüftools / Anwendungshilfen:

Als Leitfaden bei Überprüfungen können die einschlägigen Anweisungen des BSI und von ENISA / TeleTrusT herangezogen werden.

Ende der Orientierungshilfe

3. Rechte der betroffenen Personen

Aufgrund der besonderen Bedeutung der Betroffenenrechte wird dieser Aspekt in einem eigenen Kapitel des Kriterienkatalogs betrachtet. Der Zertifizierungskunde MUSS die Verantwortlichen dabei unterstützen, ihrer Pflicht zur Beantwortung von Anträgen auf Wahrnehmung der in Kapitel III der DSGVO genannten anwendbaren Rechte der betroffenen Personen nachzukommen. Hierzu MUSS er technische und organisatorische Maßnahmen treffen.

Während die Unterstützung in manchen Konstellationen einfach nur darin bestehen kann, jede erhaltene Anfrage unverzüglich weiterzuleiten und/oder den Verantwortlichen in die Lage zu versetzen, die betreffenden personenbezogenen Daten direkt zu extrahieren und zu verwalten, können dem Auftragsverarbeiter unter bestimmten Umständen spezifischere, technische Aufgaben übertragen werden. Dies insbesondere dann, wenn er dazu in der Lage ist, die personenbezogenen Daten zu extrahieren und zu verwalten.

In diesem Zusammenhang ist zu berücksichtigen, inwieweit der Verantwortliche tatsächlich auf die Unterstützung des Auftragsverarbeiters in Bezug auf die Rechte der betroffenen Person angewiesen ist. Es ist auch zu berücksichtigen, dass einige der in den verschiedenen nachstehenden Unterkapiteln behandelten Rechte der betroffenen Person immer anwendbar sind, während andere von einer weiteren rechtlichen Bewertung der Situation oder einer substanziellen Würdigung abhängen.

Bei der Bearbeitung dieses Kapitels ist zu prüfen, ob der Auftragsverarbeiter im Hinblick auf die in den Verträgen mit den einzelnen Verantwortlichen bzw. in der von ihm verwendeten Vertragsvorlage[103] vorgesehenen Unterstützungspflichten gegenüber den Verantwortlichen technische und organisatorische Maßnahmen implementiert hat.

3.1. Recht auf Information

Anforderung in Kürze:

Der Auftragsverarbeiter MUSS die Verantwortlichen bei der Erfüllung ihrer Informationspflichten gegenüber den betroffenen Personen unterstützen, indem er ihnen relevante Informationen über die zu zertifizierenden Verarbeitungstätigkeiten zur Verfügung stellt und alle sonstigen technischen und organisatorischen Maßnahmen ergreift, die in dieser Hinsicht in den Verträgen mit den einzelnen Verantwortlichen oder in der vom Auftragsverarbeiter verwendeten Vertragsvorlage vorgesehen sind.

Orientierungshilfe

Relevante Artikel der DSGVO:

Art. 28 Abs. 3 S. 2 lit. e) DSGVO i.V.m. Art. 12-14 DSGVO

Hintergrund:

Art. 28 Abs. 3 S. 2 lit. e) DSGVO verpflichtet den Auftragsverarbeiter dazu, den Verantwortlichen im Hinblick auf die Rechte der betroffenen Personen mit technischen und organisatorischen Maßnahmen zu unterstützen.

[103] Vgl. Kapitel 1.2.1 dieses Kriterienkatalogs.

Ende der Orientierungshilfe

Anforderung im Detail:

Der Auftragsverarbeiter MUSS den Verantwortlichen vor Aufnahme seiner Tätigkeit die folgenden, sich hierauf beziehenden Informationen zukommen lassen, die im Hinblick auf die Informationspflichten der Verantwortlichen gegenüber den betroffenen Personen relevant sind:

- Alle Empfänger oder Kategorien von Empfängern, an die der Auftragsverarbeiter personenbezogene Daten weitergeben wird, wenn er sie im Auftrag des Verantwortlichen verarbeitet (d. h. alle vom Auftragsverarbeiter eingesetzten Unterauftragsverarbeiter),
- Gegebenenfalls die Tatsache, dass der Auftragsverarbeiter personenbezogene Daten an ein Drittland oder eine internationale Organisation übermittelt, sowie die geeigneten oder angemessenen Garantien, die vorhanden sind.

Darüber hinaus MUSS er durch technische und organisatorische Maßnahmen sicherstellen, dass die Verantwortlichen unverzüglich über Änderungen an den zu zertifizierenden Verarbeitungsvorgängen, die im Hinblick auf die Informationspflichten der Verantwortlichen gegenüber den betroffenen Personen relevant sind, informiert werden. Dies betrifft z. B. den Fall, dass der Auftragsverarbeiter Änderungen vornehmen möchte, die zum Ergebnis haben, dass personenbezogene Daten in (weitere) Drittländer übermittelt werden.

Ggf.: Relevantes Nationales Recht:

N/A

Orientierungshilfe

Relevante Dokumente:

1. Relevante Arbeitsanweisungen und Prozessbeschreibungen
2. Liste weiterer Auftragsverarbeiter
3. TOM-Dokument

Relevante Evaluationsmethoden:

Dokumentenprüfung, Interviews

Anwendungs-/Auslegungshilfen:

- Art. 29 WP (vom EDSA bestätigt): Leitlinien für Transparenz gemäß der Verordnung 2016/679 (WP 260 rev. 01) (vgl. insbesondere Rz. 23 ff.: „Informationspflicht gegenüber der betroffenen Person – Artikel 13 & 14“)
- DE: Kurzpapier Nr. 10 der DSK

Ende der Orientierungshilfe

3.2. Auskunftsrecht

Anforderung in Kürze:

Der Auftragsverarbeiter MUSS die Verantwortlichen gemäß den einschlägigen Vertragsklauseln (vgl. Kapitel 1.2.1.2.e)) durch technische und organisatorische

Maßnahmen dabei unterstützen, ihrer Pflicht zur Beantwortung von Anträgen von betroffenen Personen auf Wahrnehmung des Auskunftsrechts nachzukommen, indem er

- alle eingegangenen Anträge unverzüglich weiterleitet,
- die Verantwortlichen in die Lage versetzt, alle personenbezogenen Daten zu extrahieren, die für die Beantwortung des Auskunftsersuchens relevant sind und/oder
- alle sonstigen technischen und organisatorischen Maßnahmen trifft, die in diesem Zusammenhang in den Verträgen mit den einzelnen Verantwortlichen oder in der vom Auftragsverarbeiter verwendeten Vertragsvorlage vorgesehen sind.

Orientierungshilfe

Relevante Artikel der DSGVO:

Art. 28 Abs. 3 S. 2 lit. e) DSGVO i.V.m. Art. 15 DSGVO

Hintergrund:

Art 28 Abs. 3 S. 2 lit. e) DSGVO verpflichtet den Auftragsverarbeiter dazu, den Verantwortlichen im Hinblick auf die Rechte der betroffenen Personen mit technischen und organisatorischen Maßnahmen zu unterstützen.

Ende der Orientierungshilfe

Anforderung im Detail:

Der Auftragsverarbeiter MUSS die Verantwortlichen durch technische und organisatorische Maßnahmen dabei unterstützen, ihrer Pflicht zur Beantwortung von Anträgen von betroffenen Personen auf Wahrnehmung des Auskunftsrechts nachzukommen. Insoweit MUSS er zumindest sicherstellen, dass Anfragen betroffener Personen, die er selbst erhalten hat, unverzüglich an den Verantwortlichen weitergeleitet werden. Wenn die Verträge mit dem/n einzelnen Verantwortlichen oder die vom Auftragsverarbeiter verwendete Vertragsvorlage weitergehende Unterstützungsleistungen vorsehen, MUSS er auch im Hinblick hierauf technische und organisatorische Maßnahmen getroffen haben.

Ggf.: Relevantes Nationales Recht:

N/A

Orientierungshilfe

Relevante Dokumente:

Relevante Arbeitsanweisungen und Prozessbeschreibungen

Relevante Evaluationsmethoden:

Dokumentenprüfung, Interviews

Anwendungs-/Auslegungshilfen:

EDPB: Guidelines 01/2022 on data subject rights - Right of access

DE: Kurzpapier Nr. 6 der DSK

Ende der Orientierungshilfe

3.3. Recht auf Berichtigung

Anforderung in Kürze:

Der Auftragsverarbeiter MUSS die Verantwortlichen gemäß den einschlägigen Vertragsklauseln (vgl. Kapitel 1.2.1.2.e) durch technische und organisatorische Maßnahmen dabei unterstützen, ihrer Pflicht zur Beantwortung von Anträgen von betroffenen Personen auf Wahrnehmung des Rechts auf Berichtigung nachzukommen, indem er

- alle eingegangenen Anträge unverzüglich weiterleitet,
- die Verantwortlichen in die Lage versetzt, die betreffenden personenbezogenen Daten zu extrahieren und zu berichtigen und/oder
- alle sonstigen technischen und organisatorischen Maßnahmen trifft, die in diesem Zusammenhang in den Verträgen mit den einzelnen Verantwortlichen oder in der vom Auftragsverarbeiter verwendeten Vertragsvorlage vorgesehen sind.

Orientierungshilfe

Relevante Artikel der DSGVO:

Art. 28 Abs. 3 S. 2 lit. e) DSGVO i.V.m. Art. 16 DSGVO

Hintergrund:

Art 28 Abs. 3 S. 2 lit. e) DSGVO verpflichtet den Auftragsverarbeiter dazu, den Verantwortlichen im Hinblick auf die Rechte der betroffenen Personen mit technischen und organisatorischen Maßnahmen zu unterstützen.

Ende der Orientierungshilfe

Anforderung im Detail:

Der Auftragsverarbeiter MUSS die Verantwortlichen durch technische und organisatorische Maßnahmen dabei unterstützen, ihrer Pflicht zur Beantwortung von Anträgen von betroffenen Personen auf Wahrnehmung des Rechts auf Berichtigung nachzukommen. Insoweit MUSS er zumindest sicherstellen, dass Anfragen betroffener Personen, die er selbst erhalten hat, unverzüglich an den Verantwortlichen weitergeleitet werden. Wenn die Verträge mit dem/n einzelnen Verantwortlichen oder die vom Auftragsverarbeiter verwendete Vertragsvorlage weitergehende Unterstützungsleistungen vorsehen, MUSS er auch im Hinblick hierauf technische und organisatorische Maßnahmen getroffen haben.

Ggf.: Relevantes Nationales Recht:

N/A

Orientierungshilfe

Relevante Dokumente:

Relevante Arbeitsanweisungen und Prozessbeschreibungen

Relevante Evaluationsmethoden:

Dokumentenprüfung, Interviews

Anwendungs-/Auslegungshilfen:

N/A

Ende der Orientierungshilfe

3.4. Recht auf Löschung

Anforderung in Kürze:

Der Auftragsverarbeiter MUSS die Verantwortlichen gemäß den einschlägigen Vertragsklauseln (vgl. Kapitel 1.2.1.2.e) durch technische und organisatorische Maßnahmen dabei unterstützen, ihrer Pflicht zur Beantwortung von Anträgen von betroffenen Personen auf Wahrnehmung des Rechts auf Löschung nachzukommen, indem er

- alle eingegangenen Anträge unverzüglich weiterleitet,
- die Verantwortlichen in die Lage versetzt, die betreffenden personenbezogenen Daten zu extrahieren und zu löschen und/oder
- alle sonstigen technischen und organisatorischen Maßnahmen trifft, die in diesem Zusammenhang in den Verträgen mit den einzelnen Verantwortlichen oder in der vom Auftragsverarbeiter verwendeten Vertragsvorlage vorgesehen sind.

Orientierungshilfe

Relevante Artikel der DSGVO:

Art. 28 Abs. 3 S. 2 lit. e) DSGVO i.V.m. Art. 17 DSGVO

Hintergrund:

Art 28 Abs. 3 S. 2 lit. e) DSGVO verpflichtet den Auftragsverarbeiter dazu, den Verantwortlichen im Hinblick auf die Rechte der betroffenen Personen mit technischen und organisatorischen Maßnahmen zu unterstützen.

Ende der Orientierungshilfe

Anforderung im Detail:

Der Auftragsverarbeiter MUSS die Verantwortlichen durch technische und organisatorische Maßnahmen dabei unterstützen, ihrer Pflicht zur Beantwortung von Anträgen von betroffenen Personen auf Wahrnehmung des Rechts auf Löschung nachzukommen. Insoweit MUSS er zumindest sicherstellen, dass Anfragen betroffener Personen, die er selbst erhalten hat, unverzüglich an den Verantwortlichen weitergeleitet werden. Wenn die Verträge mit dem/n einzelnen Verantwortlichen oder die vom Auftragsverarbeiter verwendete Vertragsvorlage weitergehende Unterstützungsleistungen vorsehen, MUSS er auch im Hinblick hierauf technische und organisatorische Maßnahmen getroffen haben.

Ggf.: Relevantes Nationales Recht:

N/A

Orientierungshilfe

Relevante Dokumente:

Relevante Arbeitsanweisungen und Prozessbeschreibungen

Relevante Evaluationsmethoden:

Dokumentenprüfung, Interviews

Anwendungs-/Auslegungshilfen:

- EDSA: Leitlinien 5/2019 zu den Kriterien des Rechts auf Vergessenwerden in Fällen in Bezug auf Suchmaschinen gemäß der DSGVO
- DE: Kurzpapier Nr. 11 der DSK

Ende der Orientierungshilfe

3.5. Recht auf Einschränkung der Verarbeitung

Anforderung in Kürze:

Der Auftragsverarbeiter MUSS die Verantwortlichen gemäß den einschlägigen Vertragsklauseln (vgl. Kapitel 1.2.1.2.e) durch technische und organisatorische Maßnahmen dabei unterstützen, ihrer Pflicht zur Beantwortung von Anträgen von betroffenen Personen auf Wahrnehmung des Rechts auf Einschränkung der Verarbeitung nachzukommen, indem er

- alle eingegangenen Anträge unverzüglich weiterleitet,
- die Verantwortlichen in die Lage versetzt, die betreffenden personenbezogenen Daten zu extrahieren und die Verarbeitung einzuschränken und/oder
- alle sonstigen technischen und organisatorischen Maßnahmen trifft, die in diesem Zusammenhang in den Verträgen mit den einzelnen Verantwortlichen oder in der vom Auftragsverarbeiter verwendeten Vertragsvorlage vorgesehen sind.

Orientierungshilfe

Relevante Artikel der DSGVO:

Art. 28 Abs. 3 S. 2 lit. e) DSGVO i.V.m. Art. 18 DSGVO

Hintergrund:

Art 28 Abs. 3 S. 2 lit. e) DSGVO verpflichtet den Auftragsverarbeiter dazu, den Verantwortlichen im Hinblick auf die Rechte der betroffenen Personen mit technischen und organisatorischen Maßnahmen zu unterstützen.

Ende der Orientierungshilfe

Anforderung im Detail:

Der Auftragsverarbeiter MUSS die Verantwortlichen durch technische und organisatorische Maßnahmen dabei unterstützen, ihrer Pflicht zur Beantwortung von Anträgen von betroffenen Personen auf Wahrnehmung des Rechts auf Einschränkung der Verarbeitung nachzukommen. Insoweit MUSS er zumindest sicherstellen, dass Anfragen betroffener Personen, die er selbst erhalten hat, unverzüglich an den Verantwortlichen weitergeleitet werden. Wenn die Verträge mit dem/n einzelnen Verantwortlichen oder die vom Auftragsverarbeiter verwendete Vertragsvorlage weitergehende Unterstützungsleistungen vorsehen, MUSS er auch im Hinblick hierauf technische und organisatorische Maßnahmen getroffen haben.

Ggf.: Relevantes Nationales Recht:

N/A

Orientierungshilfe

Relevante Dokumente:

Relevante Arbeitsanweisungen und Prozessbeschreibungen

Relevante Evaluationsmethoden:

Dokumentenprüfung, Interviews

Anwendungs-/Auslegungshilfen:

N/A

Ende der Orientierungshilfe

3.6. Recht auf Datenübertragbarkeit

Anforderung in Kürze:

Der Auftragsverarbeiter MUSS die Verantwortlichen gemäß den einschlägigen Vertragsklauseln (vgl. Kapitel 1.2.1.2.e) durch technische und organisatorische Maßnahmen dabei unterstützen, ihrer Pflicht zur Beantwortung von Anträgen von betroffenen Personen auf Wahrnehmung des Rechts auf Datenübertragbarkeit nachzukommen, indem er

- alle eingegangenen Anträge unverzüglich weiterleitet,
- die Verantwortlichen in die Lage versetzt, die betreffenden personenbezogenen Daten in einem strukturierten, gängigen und maschinenlesbaren Format zu extrahieren und diese Daten an einen anderen Verantwortlichen zu übermitteln und/oder
- alle sonstigen technischen und organisatorischen Maßnahmen trifft, die in diesem Zusammenhang in den Verträgen mit den einzelnen Verantwortlichen oder in der vom Auftragsverarbeiter verwendeten Vertragsvorlage vorgesehen sind.

Orientierungshilfe

Relevante Artikel der DSGVO:

Art. 28 Abs. 3 S. 2 lit. e) DSGVO i.V.m. Art. 20 DSGVO

Hintergrund:

Art 28 Abs. 3 S. 2 lit. e) DSGVO verpflichtet den Auftragsverarbeiter dazu, den Verantwortlichen im Hinblick auf die Rechte der betroffenen Personen mit technischen und organisatorischen Maßnahmen zu unterstützen.

Ende der Orientierungshilfe

Anforderung im Detail:

Der Auftragsverarbeiter MUSS die Verantwortlichen durch technische und organisatorische Maßnahmen dabei unterstützen, ihrer Pflicht zur Beantwortung von Anträgen von betroffenen Personen auf Wahrnehmung des Rechts auf Datenübertragbarkeit nachzukommen. Insoweit MUSS er zumindest sicherstellen, dass Anfragen betroffener Personen, die er selbst erhalten hat, unverzüglich an den Verantwortlichen weitergeleitet werden. Wenn die Verträge mit dem/n einzelnen Verantwortlichen oder die vom

Auftragsverarbeiter verwendete Vertragsvorlage weitergehende Unterstützungsleistungen vorsehen, MUSS er auch im Hinblick hierauf technische und organisatorische Maßnahmen getroffen haben.

Ggf.: Relevantes Nationales Recht:

N/A

Orientierungshilfe

Relevante Dokumente:

Relevante Arbeitsanweisungen und Prozessbeschreibungen

Relevante Evaluationsmethoden:

Dokumentenprüfung, Interviews

Anwendungs-/Auslegungshilfen:

Art. 29 WP (vom EDSA bestätigt): Leitlinien zum Recht auf Datenübertragbarkeit (WP 242 rev. 01)

Ende der Orientierungshilfe

3.7. Widerspruchsrecht

Anforderung in Kürze:

Der Auftragsverarbeiter MUSS die Verantwortlichen gemäß den einschlägigen Vertragsklauseln (vgl. Kapitel 1.2.1.2.e) durch technische und organisatorische Maßnahmen dabei unterstützen, ihrer Pflicht zur Beantwortung von Anträgen von betroffenen Personen auf Wahrnehmung des Widerspruchsrechts nachzukommen, indem er

- alle eingegangenen Anträge unverzüglich weiterleitet,
- die Verantwortlichen in die Lage versetzt, die betreffenden personenbezogenen Daten zu extrahieren und die jeweilige Verarbeitung einzustellen und/oder
- alle sonstigen technischen und organisatorischen Maßnahmen trifft, die in diesem Zusammenhang in den Verträgen mit den einzelnen Verantwortlichen oder in der vom Auftragsverarbeiter verwendeten Vertragsvorlage vorgesehen sind.

Orientierungshilfe

Relevante Artikel der DSGVO:

Art. 28 Abs. 3 S. 2 lit. e) DSGVO i.V.m. Art. 21 DSGVO

Hintergrund:

Art 28 Abs. 3 S. 2 lit. e) DSGVO verpflichtet den Auftragsverarbeiter dazu, den Verantwortlichen im Hinblick auf die Rechte der betroffenen Personen mit technischen und organisatorischen Maßnahmen zu unterstützen.

Ende der Orientierungshilfe

Anforderung im Detail:

Der Auftragsverarbeiter MUSS die Verantwortlichen durch technische und organisatorische Maßnahmen dabei unterstützen, ihrer Pflicht zur Beantwortung von Anträgen von betroffenen Personen auf Wahrnehmung des Widerspruchsrechts nachzukommen. Insoweit MUSS er zumindest sicherstellen, dass Anfragen betroffener Personen, die er selbst erhalten hat, unverzüglich an den Verantwortlichen weitergeleitet werden. Wenn die Verträge mit dem/n einzelnen Verantwortlichen oder die vom Auftragsverarbeiter verwendete Vertragsvorlage weitergehende Unterstützungsleistungen vorsehen, MUSS er auch im Hinblick hierauf technische und organisatorische Maßnahmen getroffen haben.

Ggf.: Relevantes Nationales Recht:

N/A

Orientierungshilfe

Relevante Dokumente:

Relevante Arbeitsanweisungen und Prozessbeschreibungen

Relevante Evaluationsmethoden:

Dokumentenprüfung, Interviews

Anwendungs-/Auslegungshilfen:

N/A

Ende der Orientierungshilfe