European Privacy Seal

– privacy at its best

EuroPriSe-Kriterien

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

v3.0

EuroPriSe-Kriterien

Verarbeitungsvorgänge von Auftragsverarbeitern

(v3.0 – Veröffentlichungsdatum: 15.11.2022)

©EuroPriSe Cert GmbH

EuroPriSe Cert GmbH

Joseph-Schumpeter-Allee 25 – D-53227 Bonn

Inhaltsverzeichnis

©EuroPriSe Cert GmbH

 ©EuroPriSe Cert GmbH

©EuroPriSe Cert GmbH

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.

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

 ©EuroPriSe Cert GmbH

(Art. 37 ff. DSGVO) enthalten.[1] 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.[2]

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.

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

1.1.2. Benennung eines Datenschutzbeauftragten

Anforderung in Kürze:

[1] 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.

[2] 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.

©EuroPriSe Cert GmbH

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.

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[3] 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;
   - 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;

[3] 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.

- Die geografische Ausdehnung der Verarbeitungstätigkeit ist groß.

3. Die Kerntätigkeit[4] 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.
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;

[4] Vgl. die vorangegangene Fußnote.

- 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.

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.

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:

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

 ©EuroPriSe Cert GmbH

- erfolgen nur gelegentlich[5],
- 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, dass die Zertifizierung selbst ein Übermittlungsinstrument im Sinne von Art. 46 Abs. 2 lit. f) DSGVO ist.

Ggf.: Relevantes Nationales Recht:

N/A

1.1.4. Zusammenarbeit mit der Aufsichtsbehörde

Anforderung in Kürze:

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

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

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

 ©EuroPriSe Cert GmbH

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[6] (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[7] bei der Zertifizierungsstelle vorzulegen.

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

[6] 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.

[7] 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.

©EuroPriSe Cert GmbH

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

      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[8], 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:

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

a) Der Auftragsverarbeiter verarbeitet personenbezogene Daten nur auf dokumentierte Weisung[9] 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[10], 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 dieser Kriterien zu beachten, wonach der Vertrag / die Vertragsvorlage die entsprechende Geheimhaltungspflicht adressieren MUSS. 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 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.[11] 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

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

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

[11] 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).

©EuroPriSe Cert GmbH

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 Wahrnehmung der in Kapitel III der DSGVO genannten Rechte der betroffenen Person nachzukommen. [12]

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;

[12] Die dem Auftragsverarbeiter möglichen Unterstützungsleistungen richten sich nach der Art der Verarbeitung. Vgl. insoweit auch Kapitel 3 dieser Kriterien.

- 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 niedergelegten Pflichten zur Verfügung stellt[13] und Überprüfungen[14] – 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)

[13] Vgl. hierzu auch Kapitel 1.2.2 dieser Kriterien (unter Details zum Gegenstand der Anforderung, Nr. 8).

[14] 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").

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 dieser Kriterien).

4. Einhaltung der Bedingungen für die Inanspruchnahme der Dienste eines weiteren Auftragsverarbeiters.[15]

[15] 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

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.[16]

   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).[17]

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 dieser Kriterien.
- Art. 33 f. DSGVO: Der Auftragsverarbeiter MUSS Maßnahmen getroffen haben, die gewährleisten, dass er dem Verantwortlichen ihm bekannt gewordene Verletzungen 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[18], deren Ergebnisse dokumentieren und diese den

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 dieser Kriterien.

[16] Dies ist Gegenstand von Kapitel 3 dieser Kriterien.

[17] 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).

[18] 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

©EuroPriSe Cert GmbH

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.[19]
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
      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

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.

[19] Die technischen Anforderungen, die bzgl. einer Löschung zu beachten sind, sind Gegenstand von Kapitel 2.1.6 dieser Kriterien.

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)

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,

©EuroPriSe Cert GmbH

wenn auch die weiteren Auftragsverarbeiter mit betrachtet werden, sind die nachfolgenden Anforderungen in solchen Fällen stets anwendbar.[20]

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.

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).

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).[21] Nachweisrelevant sein können

[20] 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.

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

 ©EuroPriSe Cert GmbH

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

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[22] bei der Zertifizierungsstelle vorzulegen.

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,

[22] 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.

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, 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[23], 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[24] 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[25],

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

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

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

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 dieser Kriterien 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.

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.[26] 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

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

©EuroPriSe Cert GmbH

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.[27]

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.

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.[28]

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

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

[28] Vgl. insoweit Kapitel 1.2.1.

 ©EuroPriSe Cert GmbH

niedergelegten Pflichten zur Verfügung stellt[29] und Überprüfungen[30] – 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:

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)

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.

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.

[29] 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.

©EuroPriSe Cert GmbH

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.[31]

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

[31] 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.

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)

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.[32]

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:

[32] Auch wenn die Zertifizierung auf Grundlage dieser Kriterien (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.

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[33] MÜSSEN die besondere Geheimhaltungspflicht adressieren.[34]
- 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.

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.[35]
- 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[36]

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

[33] Vgl. hierzu Kapitel 1.2.1 dieser Kriterien.

[34] 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.

[35] Vgl. hierzu die vorangegangene Fußnote sowie Kapitel 1.3.2 dieser Kriterien.

[36] - 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).

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.

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[37],

[37] 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

2. Verbindliche interne Datenschutzvorschriften gem. Art. 46 Abs. 2 lit. b) i. V. m. Art. 47 DSGVO[38],
3. Standarddatenschutzklauseln gem. Art. 46 Abs. 2 lit. c) und d) DSGVO[39],
4. Genehmigte Verhaltensregeln gem. Art. 40 DSGVO[40],
5. Ein genehmigter Zertifizierungsmechanismus gem. Art. 42 DSGVO[41],
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.[42] Ist dies der Fall,

[38] 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 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.

[39] 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.

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

[41] vgl. die vorangegangene Fußnote

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

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 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

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.

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

©EuroPriSe Cert GmbH

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.[43] 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 dieser Kriterien (technische und organisatorische Maßnahmen).

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;

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

- Transparenz;
- 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

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 dieser Kriterien (technische und organisatorische Maßnahmen).

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

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.

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.[44] 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)

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

[44] 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.

©EuroPriSe Cert GmbH

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[45], auf das auch der EDSA in seinen „Leitlinien 4/2019 zu Artikel 25 Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen“ Bezug nimmt.[46]

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):

- 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)?

[45] 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.

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

- 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.[47] 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

[47] 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.

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.

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.

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.

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.

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.

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).

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.

Anforderung im Detail:

Der Auftragsverarbeiter MUSS nachweisen, dass:

- die zu zertifizierenden Verarbeitungsvorgänge durch Identifikations- und Authentifizierungsmaßnahmen abgesichert sind,

©EuroPriSe Cert GmbH

- 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.

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.

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.

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.

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.

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.

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.

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“).

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.

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.

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:“.

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.

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.

2.1.4.1. Allgemeine Maßnahmen

Anforderung in Kürze:

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

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[48]),

2.1.4.2. Sicherungsmechanismen (Backup)

Anforderung in Kürze:

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

Der Auftragsverarbeiter MUSS sicherstellen, dass Sicherungsmechanismen wirksam sind.

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.

2.1.4.3. Speicherung von Sicherungskopien

Anforderung in Kürze:

Der Auftragsverarbeiter MUSS sicherstellen, dass Sicherungskopien sicher aufbewahrt werden.

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).

2.1.4.4. Wiederherstellungsmechanismen (Recovery)

Anforderung in Kürze:

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

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.

 ©EuroPriSe Cert GmbH

2.1.5. Datenschutz- und IT-Sicherheitsmanagement

Anforderung in Kürze:

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

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.

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.[49]

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.

Anforderung im Detail:

Der Auftragsverarbeiter MUSS nachweisen, dass:

- eine detaillierte schriftliche Dokumentation der technischen und organisatorischen Maßnahmen vorhanden ist,
- diese aktuell ist,

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

- eine Versionshistorie sowie eine Übersicht der Autoren und der für die Umsetzung der Maßnahmen verantwortlichen Personen zur Verfügung stehen.

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.

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.

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.

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.

2.1.5.5. Management von Speichermedien

Anforderung in Kürze:

Der Auftragsverarbeiter muss den kontrollierten Umgang mit Speichermedien sicherstellen.

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,

 ©EuroPriSe Cert GmbH

- 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.

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.

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).

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.

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.

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.

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.

2.1.5.9. Test und Freigabe

Anforderung in Kürze:

Der Auftragsverarbeiter MUSS (neue) Verarbeitungsvorgänge testen und freigeben.

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.

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.

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.

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.

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.

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.

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.

2.2. Technologiespezifische Anforderungen

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

 ©EuroPriSe Cert GmbH

2.2.1. Verschlüsselung

Anforderung in Kürze:

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

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).

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 dieser Kriterien). 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.

Anforderung im Detail:

N/A

©EuroPriSe Cert GmbH

3. Rechte der betroffenen Personen

Aufgrund der besonderen Bedeutung der Betroffenenrechte wird dieser Aspekt in einem eigenen Kapitel der Kriterien 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[50] 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.

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),

[50] Vgl. Kapitel 1.2.1 dieser Kriterien.

- 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

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.

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

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.

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

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.

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

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.

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

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.

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

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.

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

 ©EuroPriSe Cert GmbH