Kriterienkatalog zur Zertifizierung einer IT-gestützten Verarbeitung personenbezogener Daten gem. Art. 42 DSGVO (‚DSGVO – information privacy standard') – öffentliche Version

datenschutz cert GmbH
Version 1.0 (p1)

datenschutz cert

Inhaltsverzeichnis

1. Einleitung 5
2. Der Zertifizierungsstandard ‚DSGVO – information privacy standard' 7
   2.1. Was kann zertifiziert werden? 7
   2.2. Normative Einordnung 8
   2.3. Konkretisierung des Bewertungsgegenstands 8
   2.4. Verantwortliche und / oder Auftragsverarbeiter 11
   2.5. Branchen, Bereiche, Sektoren 11
   2.6. Räumlicher Anwendungsbereich 11
   2.7. Konformitätsaussage 11
3. Anwendung des Zertifizierungsstandards ‚DSGVO – information privacy standard' 13
   3.1. Scope-Beschreibung 13
   3.2. Statement of Applicability (SOA) 19
   3.3. Realisierungsbeschreibung 23
4. Der Kriterienkatalog ‚DSGVO – information privacy standard' 25
   4.1. P.1 Zulässigkeit der Datenverarbeitung 27
   4.2. P.2 Grundsätze 40
   4.3. P.3 Pflichten des Kunden 49
   4.4. P.4 Auftragsverarbeitung 53
   4.5. P.5 Technisch-organisatorische Maßnahmen 58
   4.6. P.6 Datenschutz-Management 71
   4.7. P.7 Datenverarbeitung außerhalb der EU 82
   4.8. P.8 Betroffenenrechte 88
5. Zertifizierungsprozess 106
   5.1. Übersicht 106
   5.2. Antrag 106
   5.3. Angebot mit Kalkulation 107
   5.4. Referenzdokumentation des Kunden 109
   5.5. Evaluierungsprozess 110
   5.6. Stichprobenverfahren 111
   5.7. Bewertungsschema 111
   5.8. Evaluierungsbericht 111
   5.9. Anerkennung bestehender Zertifikate 111
   5.10. Zertifizierung 112
   5.11. Jährliche Überwachung 115
   5.12. Re-Zertifizierung 115
   5.13. Anlassbezogene Prüfungen 115
   5.14. Änderungen, die sich auf die Zertifizierung auswirken 115

5.15. Beendigung, Einschränkung, Aussetzung oder Zurückziehung der Zertifizierung 116
6. Glossar 118
7. Anhang: Übersicht über die Kriterien 123
8. Referenzen 129

Historie

Version	Datum	Grund der Änderung	Geändert durch
1.0	23.01.2025	initiale abgenommene Version	Alisha Gühr, Dr. Sönke Maseberg
1.0 (p1)	10.02.2025	Aufbereitung für öffentlich zugängliche Version	Dr. Sönke Maseberg

Dokumenten-Überwachungsverfahren

Status	Prozess- / Dokumentenbesitzer	Version
final	Dr. Sönke Maseberg	1.0 (p1)

Verteilerliste

keine (öffentlich verfügbar)

1. Einleitung

Die Europäische Datenschutzgrundverordnung (DSGVO) [DSGVO] sieht in Art. 42 Abs. 1 die Einführung von datenschutzspezifischen Zertifizierungsverfahren vor, „die dazu dienen, dass diese Verordnung bei Verarbeitungsvorgängen von Verantwortlichen oder Auftragsverarbeitern eingehalten wird." Die allgemeinen Pflichten an Verantwortliche und Auftragsverarbeiter werden in Art. 24 bzw. Art. 28 DSGVO definiert; in diesen Artikeln wird auch ausgeführt, dass ein „genehmigtes Zertifizierungsverfahren gem. Art. 42" als „Gesichtspunkt herangezogen werden [kann], um die Erfüllung der Pflichten des Verantwortlichen nachzuweisen" bzw. „als Faktor herangezogen werden [kann], um hinreichende Garantien" des Auftragsverarbeiters nachzuweisen.

Die Motivation für Verantwortliche und Auftragsverarbeiter, solch einen Nachweis vorzulegen, sind unterschiedlich:

- Nachweis zur Einhaltung der DSGVO;
- Unterstützung bei der Rechenschaftspflicht gem. Art. 5 Abs. 2 DSGVO;
- besserer Datenschutz;
- Voraussetzung bei Ausschreibungen;
- besseres Image / Marketingeffekt;
- Marktzutrittsvoraussetzung;
- Haftungsreduzierung;
- Reduktion / Rückstellung von Geldbußen;
- Vorlage bei Aufsichtsbehörden;
- Wettbewerbsvorteile durch guten Datenschutz.

Ziel des vorliegenden „Kriterienkatalogs zur Zertifizierung einer IT-gestützten Verarbeitung personenbezogener Daten gem. Art. 42 DSGVO (‚DSGVO – information privacy standard')" ist die Zertifizierung einer exakt spezifizierten Datenverarbeitung bei Verantwortlichen sowie bei Auftragsverarbeitern, die mittels IT erbracht werden. Die Kriterien sind Teil des „Konformitätsbewertungsprogramms zur Zertifizierung einer IT-gestützten Verarbeitung personenbezogener Daten gem. Art. 42 DSGVO (‚DSGVO – information privacy standard')", das die datenschutz cert GmbH in der Rolle der Programmeignerin erstellt hat.

Das vorliegende Dokument gliedert sich wie folgt auf:

- zunächst wird in Kapitel 2 der Zertifizierungsstandard ‚DSGVO – information privacy standard' vorgestellt, hier wird insbesondere erläutert, was gem. ‚DSGVO – information privacy standard' zertifiziert werden kann,
- anschließend wird in Kapitel 3 die Anwendung des Zertifizierungsstandards im Detail erläutert, bevor
- in Kapitel 4 der eigentliche Kriterienkatalog mit den Anforderungselementen folgt.
- Das Dokument schließt mit einer Beschreibung des Zertifizierungsprozesses in Abs. 5 sowie mit Glossar, einer Übersicht über die Kriterien und den Referenzen in den Kapiteln 6, 7 und 8.

Verantwortlich für den vorliegenden „Kriterienkatalog zur Zertifizierung einer IT-gestützten Verarbeitung personenbezogener Daten gem. Art. 42 DSGVO (‚DSGVO – information privacy standard')" ist die datenschutz cert GmbH.

2. Der Zertifizierungsstandard ‚DSGVO – information privacy standard'

2.1. Was kann zertifiziert werden?

Der Gesetzgeber sieht in Art. 42 DSGVO vor, dass

- Verarbeitungsvorgänge

bei

- Verantwortlichen und
- Auftragsverarbeitern

zertifiziert werden können. Zitat aus Art. 42 DSGVO: „Zertifizierungsverfahren [...], die dazu dienen, nachzuweisen, dass diese Verordnung bei Verarbeitungsvorgängen von Verantwortlichen oder Auftragsverarbeitern eingehalten wird."

Im Fokus steht daher der Verarbeitungsvorgang. Verarbeitungsvorgänge können in ihrer Gesamtheit ein Produkt oder eine Dienstleistung darstellen. Der EDSA gibt Folgendes dazu an [EDPB_Guide-1]: „ A processing operation or a set of operations within the meaning GDPR and can result in a product, process or a service in the terminology of ISO."[1]

Im Ergebnis kann damit eine Datenverarbeitung, die aus mehreren Verarbeitungsvorgängen besteht, gem. Art. 42 DSGVO zertifiziert werden. Damit können weder Unternehmen noch reine Datenschutz-Managementsysteme, reine Produkte oder Datenschutzbeauftragte durch ein Art. 42 DSGVO-konformes Zertifikat ausgezeichnet werden.

Der vorliegende Zertifizierungsstandard ‚DSGVO – information privacy standard' ist auf der einen Seite ein generischer Standard – der für eine Vielzahl von Branchen, Sektoren, Unternehmen, Organisationsformen, Datenverarbeitungen, Verarbeitungsvorgängen angewendet werden kann –, der auf der anderen Seite aber auch zwingend einen IT-Bezug einfordert. Damit sind rein manuelle Datenverarbeitungen, die ohne IT-Unterstützung auskommen, hier nicht anwendbar.

Gem. des Zertifizierungsstandards ‚DSGVO – information privacy standard' kann somit die folgende Datenverarbeitung zertifiziert werden, die damit den Scope des Zertifizierungsmechanismus' darstellt:

- „IT-gestützte Verarbeitung personenbezogener Daten"

Grundvoraussetzung für eine Zertifizierung ist, dass personenbezogene Daten gem. Art. 4 Nr. 1 DSGVO im Rahmen des materiellen und räumlichen Anwendungsbereiches der DSGVO gem. Art. 2 und 3 verarbeitet werden; erst unter dieser Voraussetzung kann das vorliegende Konformitätsbewertungsprogramm zur Anwendung kommen.

Hinweis: Dieses Schema ist kein Zertifizierungsmechanismus gemäß Art. 46 Abs. 2 (f) DSGVO.

---

[1] Übersetzung: „Ein Verarbeitungsvorgang oder eine Reihe von Vorgängen im Sinne der DSGVO, die zu einem Produkt, einem Verfahren oder einer Dienstleistung in der Terminologie der ISO führen."

2.2. Normative Einordnung

Rechtliche Grundlage ist die EU-Datenschutzgrundverordnung (DSGVO) [DSGVO].

Die Anforderungen der DSGVO werden ergänzt um einschlägige Rechtsgrundlagen aus nationalen Konkretisierungen der DSGVO auf Basis der Öffnungsklauseln. Ferner werden berücksichtigt:

- Auslegungshilfen des Europäischen Datenschutzausschusses (EDSA);
- die Rechtsprechung der Europäischen Gerichtshöfe sowie der nationalen Gerichtsbarkeiten;
- nationale Vorgaben und Auslegungshilfen der relevanten Datenschutzaufsichtsbehörden.

2.3. Konkretisierung des Bewertungsgegenstands

Die Datenverarbeitung als Bewertungsgegenstand – also das Objekt, der Scope, der Untersuchungsgegenstand oder das Target of Evaluation (ToE) der Zertifizierung – muss eindeutig festgelegt sein. Es muss eindeutig beschrieben sein, welche Verarbeitungsvorgänge exakt zum Bewertungsgegenstand gehören, an welchen Standorten diese Tätigkeiten erbracht werden, welche externen Dritte (z. B. Dienstleister, Auftragsverarbeiter, Behörden, Schwestergesellschaften oder Holding) ggf. einbezogen sind, welche IT-Komponenten erforderlich sind und auch welche Prozesse in einer Organisation etabliert sind, um die Datenverarbeitung insgesamt darstellen zu können. Diese eindeutige Festlegung ist nicht nur für die Organisation wichtig, sondern auch für die Evaluatoren und die Zertifizierungsstelle.

Aus diesem Grund muss die Datenverarbeitung (der Bewertungsgegenstand) – die „IT-gestützte Verarbeitung personenbezogener Daten“ – durch folgende Elemente (Zielobjektkategorien) charakterisiert werden:

- Verarbeitungsvorgänge (VV) zur Konkretisierung der zu zertifizierenden Datenverarbeitung;
- Datenschutz-Managementsystem (DSMS) mit den internen Prozessen zur Steuerung der Datenschutz-Konformität;
- Prozesse (PRZ) mit den Tätigkeiten, die für die konkrete Datenverarbeitung (DV) benötigt werden; Prozesse (PRZ) werden definiert als eine Reihe von in Wechselbeziehung oder Wechselwirkung miteinander stehenden Tätigkeiten, die Eingaben nutzen, um ein angestrebtes Ergebnis zu liefern, die für die zu zertifizierende Datenverarbeitung erforderlich sind;
- physische Infrastruktur (INFRA) mit Standorten und Räumen;
- IT-Infrastruktur (IT) mit allen relevanten Komponenten, z.B. Servern, Clients, Netzkomponenten, Datenbanken, Speichersystemen und Schnittstellen;
- Applikationen (APPL), über die die Datenverarbeitung realisiert wird;
- externe Dritte (DL), z. B. Dienstleister, Auftragsverarbeiter, Behörden, Schwestergesellschaften oder Holding, die für die Realisierung der Datenverarbeitung benötigt werden oder an die personenbezogene Daten übermittelt werden, sofern relevant.

Abbildung 1 illustriert den Bewertungsgegenstand mit seinen ihn charakterisierenden Elementen:

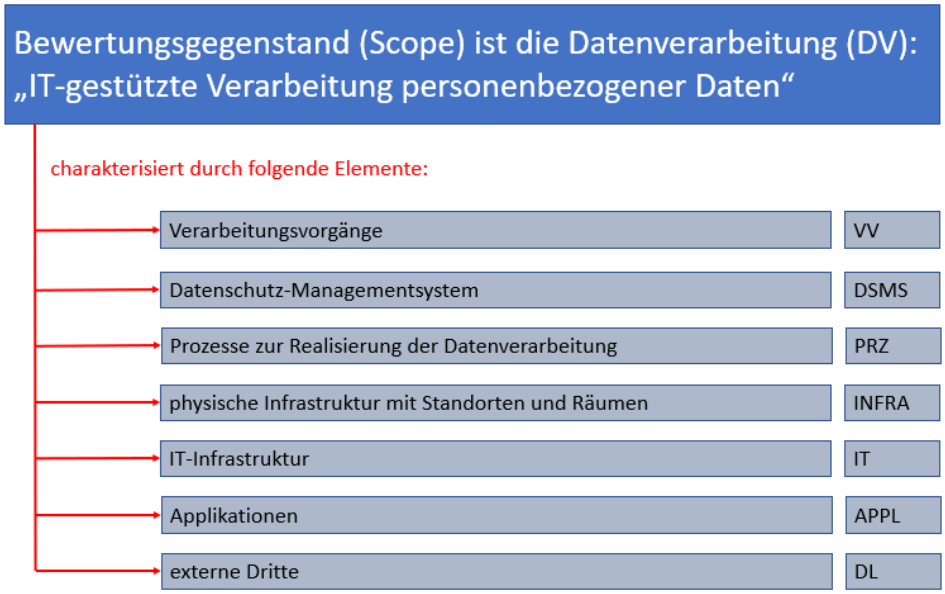


Abbildung 1: Bewertungsgegenstand (Scope)

Für eine konkrete Zertifizierung sind zunächst allgemeine Angaben erforderlich:

- Datenverarbeitung (DV):
  - Angabe der antragstellenden Organisation;
  - exakte Bezeichnung der Datenverarbeitung als „IT-gestützte Verarbeitung personenbezogener Daten“[2]; diese Bezeichnung wird abschließend im Zertifikat aufgenommen;
  - exakte Beschreibung der Datenverarbeitung;
  - Angabe der Branche/des Sektors;
  - Angabe, ob die Datenverarbeitung insgesamt als Verantwortlicher und /oder Auftragsverarbeiter erbracht wird.

Anschließend sind alle Zielobjekte aufzulisten, die für den Bewertungsgegenstand (Scope) zwingend erforderlich sind:

- Verarbeitungsvorgänge (VV):
  - exakte Bezeichnung mit Beschreibung eines jeden Verarbeitungsvorgangs;

[2] Die Beschränkung auf IT-gestützte Verarbeitung personenbezogener Daten schließt keine Scopes aus, welche nur teilweise IT-gestützt erfolgen. Lediglich Datenverarbeitungen personenbezogener Daten, die vollständig ohne IT-gestützte Verarbeitung auskommen, können nicht nach diesem Schema zertifiziert werden. Datenverarbeitungen personenbezogener Daten, die aus einer IT-gestützten Verarbeitung resultieren (z. B. Backup Kopien und ihre Löschung) sind üblicherweise Teil des Scopes.

sofern sinnvoll, können Verarbeitungsvorgänge zu einer sogenannten Vorgangsreihe gebündelt werden, um etwa einen Geschäftsprozess besser abbilden zu können;

- Angabe, ob der Verarbeitungsvorgang als Verantwortlicher und /oder Auftragsverarbeiter erbracht wird;
- Datenarten: Auflistung der personenbezogenen Daten mit Unterteilung in Primär- und Sekundärdaten (vgl. dazu Erläuterungen im Glossar in Abs. 6) und Kennzeichnung, ob "besondere Kategorie personenbezogener Daten" gem. Art. 9 DSGVO oder „personenbezogene Daten über strafrechtliche Verurteilungen und Straftaten" gem. Art. 10 DSGVO relevant sind und ob personenbezogene Daten von Kindern verarbeitet werden;

- Datenschutz-Managementsystem (DSMS):
  - Beschreibung der internen Prozesse, um eine Datenschutz-Konformität, insbesondere zur Umsetzung der Anforderungen dauerhaft sicherzustellen, vgl. Ausführungen in Kapitel 3.1.3;
- Prozesse (PRZ):
  - Beschreibung der Prozesse, die für die konkrete Datenverarbeitung benötigt werden; Prozesse (PRZ) werden definiert als eine Reihe von in Wechselbeziehung oder Wechselwirkung miteinander stehenden Tätigkeiten, die Eingaben nutzen, um ein angestrebtes Ergebnis zu liefern, die für die zu zertifizierende Datenverarbeitung erforderlich sind;
- physische Infrastruktur (INFRA):
  - exakte Angabe der Standorte und Räume, an denen die Datenverarbeitung erbracht wird;
- IT-Infrastruktur (IT):
  - exakte Angabe der IT-Systeme (Servern, Clients, Netzkomponenten, Datenbanken, Speichersystemen und Schnittstellen), die für Datenverarbeitung erforderlich sind, mit Netzstrukturplan;
- Applikationen (APPL):
  - exakte Angabe der Applikationen – sowohl interne Anwendungen als auch von Extern verfügbare Anwendungen, wie etwa Webseiten oder Apps –, die für Datenverarbeitung genutzt werden;
- externe Dritte (DL):
  - Darstellung der externen Dritten (z. B. Dienstleister, Auftragsverarbeiter, Behörden, Schwestergesellschaften oder Holding) mit Darstellung der übernommenen Zuständigkeiten und damit verbundenen Aufgaben, sofern relevant mit Bezug zu Datenschutzaspekten; hierunter fallen auch Externe, denen personenbezogene Daten im Kontext der Datenverarbeitung übermittelt werden.

In dieser Übersicht sind zunächst alle Zielobjekte aufzunehmen, auch solche, die durch externe Dritte wahrgenommen werden; diese Zielobjekte sind dann entsprechend zu kennzeichnen.

Diese exakt definierten Zielobjekte stellen damit den Bewertungsgegenstand (synonym zu: Untersuchungsgegenstand oder Scope) und somit den Geltungsbereich der Zertifizierung dar. Ein Ausschluss einzelner Zielobjekte, die für die zu zertifizierende Datenverarbeitung erforderlich ist, ist nicht zulässig.

2.4. Verantwortliche und / oder Auftragsverarbeiter

Die Datenverarbeitung „IT-gestützte Verarbeitung personenbezogener Daten“ kann durch einen Verantwortlichen und / oder Auftragsverarbeiter als Auftragsverarbeitung erbracht werden.

Kunde für ein ‚DSGVO – information privacy standard‘-Zertifikat kann damit ein Verantwortlicher und / oder ein Auftragsverarbeiter einer Datenverarbeitung sein.

Gemeinsam Verantwortliche im Sinne des Art. 26 DSGVO können nicht unter diesem Schema zertifiziert werden.

2.5. Branchen, Bereiche, Sektoren

Zertifiziert werden können Bewertungsgegenstände in verschiedenen Branchen, Bereichen oder Sektoren, beispielsweise:

- Banken und Versicherungen;
- Energie- und Wasserversorgung;
- Gesundheits- und Sozialwesen;
- Industrie und Handel;
- Marketing und Werbung;
- EDV, Informationstechnologie und Telekommunikation;
- Institute und Verbände;
- Kultureinrichtungen;
- Öffentliche Stellen und öffentliche Verwaltung;
- Transport, Verkehr und Logistik;
- Schule, Bildung und Wissenschaft;
- Ernährung.

2.6. Räumlicher Anwendungsbereich

Der räumliche Anwendungsbereich des Zertifizierungsstandards ist beschränkt auf Datenverarbeitungen innerhalb des räumlichen Anwendungsbereiches der DSGVO gem. Art. 3 DSGVO sowie auf Deutschland.

2.7. Konformitätsaussage

Mit einem ‚DSGVO – information privacy standard‘-Zertifikat wird folgende Konformitätsaussage getroffen:

Die Zertifizierungsstelle bestätigt, dass

- die in Kapitel 2.4 angegebene Organisation

- den in Kapitel 2.3 definierten Bewertungsgegenstand
- als Verantwortlicher und / oder als Auftragsverarbeiter
- konform zu folgenden Anforderungen betreibt:
  - DSGVO,
  - zusätzliche Anforderungen der Datenschutzaufsichtsbehörden,
- und dass folgende Prüfgrundlagen genutzt wurden:
  - das Konformitätsbewertungsprogramm;
  - der ‚DSGVO – information privacy standard'-Kriterienkatalog.

Mit einer Zertifizierung gemäß Art. 42 DSGVO wird ausschließlich die Organisation mit dem jeweiligen Scope zertifiziert, nicht die involvierten Subdienstleister.

Erklärung der zusätzlichen Anforderungen: Alle Kriterien müssen konform zu den Dokumenten des EDSA, der DSK und weiteren europäischen Aufsichtsbehörden für Datenschutz interpretiert werden.

3. Anwendung des Zertifizierungsstandards ‚DSGVO – information privacy standard'

Der Zertifizierungsstandard ‚DSGVO – information privacy standard' ist geeignet, eine Datenverarbeitung als „IT-gestützte Verarbeitung personenbezogener Daten" bei einem Verantwortlichen und / oder Auftragsverarbeiter gem. DSGVO so zu modellieren, dass eine anschließende Zertifizierung gem. Art. 42 DSGVO möglich ist.

In diesem Abschnitt wird die Vorgehensweise zur Beschreibung einer Datenverarbeitung gem. ‚DSGVO – information privacy standard' beschrieben.

3.1. Scope-Beschreibung

Im ersten Schritt ist der Bewertungsgegenstand – der Scope – exakt festzulegen; hierzu sind die nachfolgenden Angaben erforderlich. Wenn möglich, können Informationen gruppiert werden.

Es muss die „gesamte Kette", die zu einer Datenverarbeitung gehört, beschrieben sein (etwa in einem Datenflussdiagramm). Alle Informationen müssen klar, präzise und eindeutig sein.

3.1.1. Datenverarbeitung (DV)

Angabe des Antragstellers:

BEZEICHNUNG DER ORGANISATION
Straße, Ort, Land
Tel, Fax, E-Mail, Webseite
Ansprechpartner mit Kontaktdaten

Ferner: Darlegung der Organisationsstruktur, etwa anhand eines Organigramms, sowie eine Beschreibung der für den Datenverarbeitungsvorgang einschlägigen Rollen.

Hinweis: Gemeinsam Verantwortliche im Sinne des Art. 26 DSGVO können nicht unter diesem Schema zertifiziert werden.

Beschreibung der zu zertifizierenden Datenverarbeitung:

EXAKTE BEZEICHNUNG DER „IT-GESTÜTZTEN VERARBEITUNG PERSONENBEZOGENER DATEN“	
exakte Beschreibung der Datenverarbeitung inkl. Zweck	
Angabe der Branche	
Angabe, ob die Datenverarbeitung als Verantwortlicher und / oder Auftragsverarbeiter erbracht wird	

Hinweis: Die Bezeichnung der Datenverarbeitung der „IT-gestützten Verarbeitung personenbezogener Daten“, die abschließend in das ‚DSGVO – information privacy standard‘-Zertifikat aufgenommen wird, muss kurz und prägnant sowie korrekt sein. Ein Nutzer des Zertifikates – oftmals ein Endverbraucher – muss unmissverständlich entscheiden können, ob eine Datenverarbeitung, die ihn interessiert, vom Zertifikat abgedeckt ist. Dazu dient neben der Bezeichnung auf dem Zertifikat auch eine Zertifikatsanlage, die für jedes Zertifikat existiert, vgl. Ausführungen in Kapitel 5.10.3.

3.1.2. Verarbeitungsvorgänge (VV)

Beschreibung der Verarbeitungsvorgänge mit Angabe, ob die Datenverarbeitung als Verantwortlicher (V) und / oder Auftragsverarbeiter (AV) erbracht wird:

ID	BEZEICHNUNG	BESCHREIBUNG	V / AV	BEMERKUNG
VV-01				
VV-02				

Sofern sinnvoll, können Verarbeitungsvorgänge auch zu einer sogenannten Vorgangsreihe (VR) gebündelt werden, um etwa einen Geschäftsprozess besser abbilden zu können.

ID	BESCHREIBUNG	RELEVANTE VV'S	BEMERKUNG
VR-01			
VR-02			

Angabe aller Arten personenbezogener Daten und Kategorien betroffener Personen mit:

- Beschreibung;
- Klassifikation in Primär- und Sekundärdaten;
- Kennzeichnung,
  - ob Datenart als „besondere Kategorie personenbezogener Daten" gem. Art. 9 DSGVO klassifiziert wird;
  - ob Datenart als „personenbezogene Daten über strafrechtliche Verurteilungen und Straftaten" gem. Art. 10 DSGVO klassifiziert wird;
  - ob personenbezogene Daten von Kindern verarbeitet werden;
- Zuordnung zu den relevanten Verarbeitungsvorgängen (VV):

ID	BESCHREIBUNG	KLASSIFIKATION PRIMÄR- / SEKUNDÄR	KENNZEICHNUNG	ZUORDNUNG RELEVANTE VV	KATEGORIE BETROFFENER PERSONEN	BEMERKUNG
Dat-01						
Dat-02						

Die Datenarten sind differenziert anzugeben.

3.1.3. Datenschutz-Managementsystem (DSMS)

Beschreibung des Datenschutz-Managementsystems (DSMS) mit den internen Prozessen zur Steuerung der Datenschutz-Konformität, Anforderungen dazu finden sich u. a. im Anforderungselement P.6.1 zur fortlaufenden Datenschutz-Kontinuität.

Die Beschreibung umfasst insbesondere eine Darstellung zur Methodik und zum strukturierten Ansatz, also wie etwa ein PDCA-Zyklus („Plan-Do-Check-Act", „Planen-

Umsetzen-Überprüfen-Handeln“) umgesetzt wird. Bestandteil dieses Managementsystems sind insbesondere folgende Aspekte:

- fortlaufende Aufrechterhaltung der Angaben zur Scope-Beschreibung gem. Kapitel 3.1;
- fortlaufende Aufrechterhaltung der Angaben zum Statement of Applicability gem. Kapitel 3.2; dies umfasst insbesondere:
  - die Rechtsgrundlage der Datenverarbeitung der Kriterien P.1 (Zulässigkeit der Datenverarbeitung), vgl. Frage 1 in Kapitel 3.2.1;
  - die Anwendbarkeit der Kriterien P.4 (Auftragsverarbeitung), vgl. Frage 3 in Kapitel 3.2.2;
  - die Anwendbarkeit des Kriteriums P.6.2 (Datenschutzbeauftragter), vgl. Frage 4 in Kapitel 3.2.3;
  - die Anwendbarkeit des Kriteriums P.6.4 (Verzeichnis von Verarbeitungstätigkeiten), vgl. Frage 5 in Kapitel 3.2.4;
  - die Anwendbarkeit des Kriteriums P.6.5 (Datenschutz-Folgenabschätzung), vgl. Frage 6 in Kapitel 3.2.5;
  - die Anwendbarkeit der Kriterien P.7 (Datenverarbeitung außerhalb der EU), vgl. Frage 7 in Kapitel 3.2.6;
  - die Anwendbarkeit des Kriteriums P.8.9 (Automatisierte Entscheidungen / Profiling), vgl. Frage 8 in Kapitel3.2.7;
- regelmäßige – mindestens jährliche – sowie anlassbezogene Überprüfung von
  - Scope-Beschreibung gem. Kapitel 3.1,
  - Statement of Applicability gem. Kapitel 3.2 und
  - Realisierungsbeschreibung gem. Kapitel 3.3;
- sofern eine Datenübermittlung in Drittstaaten – unter Anwendung des Kriteriums P.7.1 – auf Grundlage eines Angemessenheitsbeschlusses der EU-Kommission erfolgt: regelmäßige Überprüfung des Vorliegens dieses Angemessenheitsbeschlusses für das betreffende Land und daraus resultierende Folgen
- sofern eine Datenübermittlung in Drittstaaten – unter Anwendung des Kriteriums P.7.1 – auf Grundlage von geeigneten Garantien erfolgt: regelmäßige Überprüfung des Vorliegens dieser geeigneten Garantien und daraus resultierende Folgen;
- kontinuierlicher Verbesserungsprozess (KVP) inkl. Ursachenanalyse bei Auftreten von Abweichungen.

Hierzu kann beispielsweise das Standard-Datenschutzmodell (SDM) der deutschen Datenschutzaufsichtsbehörden oder die ISO/IEC 27701-Norm herangezogen werden.

Die Beschreibung benennt ferner einen DSMS-Verantwortlichen – typischerweise ist dies der Datenschutzbeauftragte –, der auch als Ansprechpartner für die Zertifizierungsstelle agiert.

Die Beschreibung des Datenschutz-Managementsystems kann auf beigefügte Richtlinien, Regelungen, Prozessbeschreibungen, Handbücher etc. basieren.

3.1.4. Prozesse (PRZ)

Beschreibung der Prozesse (PRZ), die für die konkrete Datenverarbeitung (DV) benötigt werden; ggf. Verweis auf beigefügte Regelungen, Anleitungen, Prozessbeschreibungen, etc.

Prozesse (PRZ) werden definiert als eine Reihe von in Wechselbeziehung oder Wechselwirkung miteinander stehenden Tätigkeiten, die Eingaben nutzen, um ein angestrebtes Ergebnis zu liefern, die für die zu zertifizierende Datenverarbeitung erforderlich sind.

3.1.5. Applikationen (APPL)

Beschreibung aller für die zu zertifizierende Datenverarbeitung relevanten Applikationen (APPL), die in der Datenverarbeitung genutzt werden; dies sind sowohl interne Anwendungen als auch extern verfügbare Anwendungen, wie etwa Webseiten oder mobile Apps; mit Angabe der Art der Applikation und Zuordnung zu den relevanten Verarbeitungsvorgängen (VV).

ID	BESCHREIBUNG	ART DER APPLIKATION	ZUORDNUNG RELEVANTE VV	BEMERKUNG
Appl-01				
Appl-02				

3.1.6. IT-Infrastruktur (IT)

Beschreibung aller für die zu zertifizierenden Datenverarbeitung relevanten IT-Systeme (Client, Server, Netzkomponenten, Datenbanken, Speichersystemen) mit Angabe der Art der Systeme und Zuordnung zu den Applikationen.

ID	BESCHREIBUNG	ART DES IT-SYSTEMS	RELEVANTE APPLIKATION	BEMERKUNG
Client-01				
Client-02				
Serv-01				
Serv-03				

ID	BESCHREIBUNG	ART DES IT-SYSTEMS	RELEVANTE APPLIKATION	BEMERKUNG
Netz-01				
Netz-02				
DB-01				
DB-02				
Speicher-01				
Speicher-02				

Beschreibung aller für die zu zertifizierende Datenverarbeitung relevanten Schnittstellen zu anderen Systemen und Organisationen:

ID	BESCHREIBUNG	ART DER SCHNITTSTELLE	BEMERKUNG
Int-01			
Int-02			

Ferner: eine graphische Darlegung, etwa als Netzstrukturplan.

Schnittstellen zu anderen Organisationen können auch andere Organisationen innerhalb derselben Gruppe umfassen (Intra-Organisation).

3.1.7. Physische Infrastruktur (INFRA)

Beschreibung aller für die zu zertifizierende Datenverarbeitung relevanten Standorte und Räume (INFRA); mit: Zuordnung zu den dort betriebenen IT-Systemen:

ID	BESCHREIBUNG	RELEVANTE IT-SYSTEME	BEMERKUNG
Ort-01			
Ort-02			
Raum-01			
Raum-02			

3.1.8. Externe Dritte (DL)

Beschreibung aller für die zu zertifizierenden Datenverarbeitung relevanten externen Dritten (DL), z. B. Dienstleister, Auftragsverarbeiter, Dritte, Behörden, Schwestergesellschaften oder Holding, sofern relevant mit:

- Darstellung der Art des Dienstleisters / externen Dritten sowie seiner übernommenen Zuständigkeiten und Aufgaben mit Bezug zu Datenschutzaspekten;
- Klassifikation, ob Dienstleister / externer Dritter ein Auftragsverarbeiter im Sinne der DSGVO ist;
- Darstellung der rechtlichen Zulässigkeit bei Übermittlung, sofern relevant.

ID	BESCHREIBUNG	ART DES DIENSTLEISTERS	KLASSIFIKATION AV	ZULÄSSIGKEIT ÜBERMITTLUNG	BEMERKUNG
DL-01					
DL-02					

3.2. Statement of Applicability (SOA)

Der Zertifizierungsstandard ‚DSGVO – information privacy standard' gilt generisch für viele verschiedene Datenverarbeitungen; dieser generische Ansatz bedingt, dass es einige Anforderungselemente des Kriterienkatalogs gibt, die als „optional" gekennzeichnet sind. „Optional" bedeutet dazu: ein als „optional" gekennzeichnetes Anforderungselement

- muss ausgewählt werden, wenn das Kriterium für den jeweiligen Geltungsbereich relevant ist und

- kann nur ausgeschlossen werden, wenn das entsprechende Kriterium inhaltlich nicht zutrifft. Der Ausschluss eines Kriteriums muss ausführlich begründet sein.

Für diese optionalen Anforderungselemente muss zunächst für eine konkrete Datenverarbeitung die Anwendbarkeit festgelegt werden – hierüber wird der Bewertungsmaßstab für die konkrete Datenverarbeitung spezifiziert.

Wenn im SOA-Dokument ein Kriterium nicht herangezogen wird, prüft die Zertifizierungsstelle im Rahmen der Basisprüfung, ob die Begründung für den Ausschluss nachvollziehbar und plausibel ist.

Durch die nachfolgenden Fragestellungen werden die optionalen Anforderungselemente für eine konkrete Datenverarbeitung festgelegt.

3.2.1. Frage 1: Rechtsgrundlage

Auf welcher Rechtsgrundlage werden die einzelnen Verarbeitungsvorgänge der zu zertifizierenden Datenverarbeitung durchgeführt?

Der Gesetzgeber sieht in Art. 6 Abs. 1 DSGVO für den Verantwortlichen verschiedene Möglichkeiten vor:

> „Die Verarbeitung ist nur rechtmäßig, wenn mindestens eine der nachstehenden Bedingungen erfüllt ist:
>
> a. Die betroffene Person hat ihre Einwilligung zu der Verarbeitung der sie betreffenden personenbezogenen Daten für einen oder mehrere bestimmte Zwecke gegeben;
> b. die Verarbeitung ist für die Erfüllung eines Vertrags, dessen Vertragspartei die betroffene Person ist, oder zur Durchführung vorvertraglicher Maßnahmen erforderlich, die auf Anfrage der betroffenen Person erfolgen;
> c. die Verarbeitung ist zur Erfüllung einer rechtlichen Verpflichtung erforderlich, der der Kunde (als Verantwortlicher) unterliegt;
> d. die Verarbeitung ist erforderlich, um lebenswichtige Interessen der betroffenen Person oder einer anderen natürlichen Person zu schützen;
> e. die Verarbeitung ist für die Wahrnehmung einer Aufgabe erforderlich, die im öffentlichen Interesse liegt oder in Ausübung öffentlicher Gewalt erfolgt, die dem Verantwortlichen übertragen wurde;
> f. die Verarbeitung ist zur Wahrung der berechtigten Interessen des Verantwortlichen oder eines Dritten erforderlich, sofern nicht die Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person, die den Schutz personenbezogener Daten erfordern, überwiegen, insbesondere dann, wenn es sich bei der betroffenen Person um ein Kind handelt."

Dementsprechend muss der Kunde (als Verantwortlicher) für jeden Verarbeitungsvorgang (VV) eine der folgenden Anforderungselemente als rechtliche Grundlage inkl. Rechtsgültigkeit und Angemessenheit angeben:

- P.1.2 Rechtsgrundlage Vertrag
- P.1.3 Rechtsgrundlage berechtigtes Interesse

- P.1.4 Rechtsgrundlage Einwilligung
- P.1.5 Rechtsgrundlage rechtliche Verpflichtung
- P.1.6 Rechtsgrundlage lebenswichtige Interessen
- P.1.7 Rechtsgrundlage öffentliches Interesse

Demgegenüber muss der Auftragsverarbeiter für einen Verarbeitungsvorgang (VV), den er als Auftragsverarbeitung anbietet, folgendes Anforderungselement als rechtliche Grundlage angeben:

- P.1.10 Datenverarbeitung im Auftrag

Die Thematik, wenn ein Verantwortlicher Auftragsverarbeiter einsetzt, wird in Kapitel 3.2.2 erörtert.

Darüber hinaus sind die Anforderungselemente P.1.8 und P.1.9 auszuwählen, wenn folgende Daten verarbeitet werden:

- „besondere Kategorien personenbezogener Daten" gem. Art. 9 DSGVO;
- „personenbezogene Daten über strafrechtliche Verurteilungen und Straftaten“ gem. Art. 10 DSGVO.

Nähere Informationen zu den Anforderungselementen finden sich in Kapitel 4.1.

ANFORDERUNGSELEMENT LT. KRITERIENKATALOG	ANWENDBAR (JA, NEIN)	RELEVANTE VV	BEMERKUNG
P.1.2 Rechtsgrundlage Vertrag			
P.1.3 Rechtsgrundlage berechtigtes Interesse			
P.1.4 Rechtsgrundlage Einwilligung			
P.1.5 Rechtsgrundlage rechtliche Verpflichtung			
P.1.6 Rechtsgrundlage lebenswichtige Interessen			
P.1.7 Rechtsgrundlage öffentliches Interesse			
P.1.8 Verarbeitung bei besonderen Kategorien personenbezogener Daten			
P.1.9 Verarbeitung bei strafrechtlichen Verurteilungen und Straftaten			

3.2.2. Frage 2: Involvierung externer Dritter (DL) in der Datenverarbeitung

Werden externe Dritte (DL) im Geltungsbereich eingesetzt?

Wenn ja, qualifizieren sich diese womöglich als Auftragsverarbeiter, sodass dieses Anforderungselement als anwendbar zu kennzeichnen ist. Ferner sind die relevanten Verarbeitungsvorgänge (VV) und die entsprechenden Dienstleister / externen Dritten anzugeben. Nähere Informationen zu diesem Anforderungselemente finden sich in Kapitel 4.4.

ANFORDERUNGSELEMENT LT. KRITERIENKATALOG	ANWENDBAR (JA, NEIN)	RELEVANTE VV	ANGABEN ZUM DIENSTLEISTER	BEMERKUNG
P.4.1 Vertrag zur Auftragsverarbeitung (AV-Vertrag)				
P.4.3 Audit				

3.2.3. Frage 3: Datenschutzbeauftragter

Besteht für den Verantwortlichen bzw. Auftragsverarbeiter die Pflicht, einen Datenschutzbeauftragten (DSB) zu bestellen?

Wenn ja, ist dieses Anforderungselement als anwendbar zu kennzeichnen. Wenn nein, ist eine Begründung anzugeben. Nähere Informationen zu diesem Anforderungselement finden sich in Kapitel 4.6.2.

ANFORDERUNGSELEMENT LT. KRITERIENKATALOG	ANWENDBAR (JA, NEIN)	BEGRÜNDUNG
P.6.2 Datenschutzbeauftragter		

3.2.4. Frage 4: Verzeichnis von Verarbeitungstätigkeiten (VVT)

Besteht für den Verantwortlichen bzw. Auftragsverarbeiter die Pflicht, ein „Verzeichnis von Verarbeitungstätigkeiten“ (VVT) vorzuhalten?

Wenn ja, ist dieses Anforderungselement als anwendbar zu kennzeichnen. Wenn nein, ist eine Begründung anzugeben. Nähere Informationen zu diesem Anforderungselement finden sich in Kapitel 4.6.4.

ANFORDERUNGSELEMENT LT. KRITERIENKATALOG	ANWENDBAR (JA, NEIN)	BEGRÜNDUNG
P.6.4 Verzeichnis von Verarbeitungstätigkeiten		

3.2.5. Frage 5: Datenschutz-Folgenabschätzung (DSFA)

Besteht die Notwendigkeit, eine „Datenschutz-Folgenabschätzung“ (DSFA) durchzuführen?

Wenn ja, ist dieses Anforderungselement als anwendbar zu kennzeichnen und das entsprechende Zielobjekt anzugeben. Wenn nein, ist eine Begründung anzugeben. Nähere Informationen zu diesem Anforderungselement finden sich in Kapitel 4.6.5.

ANFORDERUNGSELEMENT LT. KRITERIENKATALOG	ANWENDBAR (JA, NEIN)	ZUGEORDNETE ZIELOBJEKTE	BEGRÜNDUNG
P.6.5 Datenschutz-Folgenabschätzung		(VV-1, VV-2, ...)	

3.2.6. Frage 6: Datenverarbeitung außerhalb der EU

Erfolgt eine Datenübermittlung in Drittstaaten? Ist der Antragsteller außerhalb der EU/EWR niedergelassen und hat einen Vertreter innerhalb der EU bestimmt?

Wenn ja, ist dieses Anforderungselement als anwendbar zu kennzeichnen. Nähere Informationen zu diesem Anforderungselement finden sich in Kapitel 4.7.

ANFORDERUNGSELEMENT LT. KRITERIENKATALOG	ANWENDBAR (JA, NEIN)	BEMERKUNG
P.7.1 Datenübermittlung in Drittstaaten		
P.7.2 Vertreter innerhalb der EU		

3.2.7. Frage 7: Profiling

Erfolgt eine automatisierte Entscheidung bzw. Profiling?

Wenn ja, ist dieses Anforderungselement als anwendbar zu kennzeichnen und das entsprechende Zielobjekt anzugeben. Nähere Informationen zu diesem Anforderungselement finden sich in Kapitel 4.6.5.

ANFORDERUNGSELEMENT LT. KRITERIENKATALOG	ANWENDBAR (JA, NEIN)	ZUGEORDNETE ZIELOBJEKTE	BEMERKUNG
P.8.9 Automatisierte Entscheidungen / Profiling		(APPL-1, APPL-2, ...).	

3.3. Realisierungsbeschreibung

Nachdem im vorherigen Schritt die dem generischen Ansatz des Zertifizierungsstandards ‚DSGVO – information privacy standard‘ geschuldeten „Freiheitsgrade“

eliminiert wurden, kann im nächsten Schritt die inhaltliche Auseinandersetzung des konkreten Bewertungsgegenstandes mit den Anforderungen der DSGVO erfolgen.

Dazu ist zu allen lt. SOA anwendbaren Anforderungselementen – also nicht diejenigen, die zuvor in Kapitel 3.2 ausgeschlossen wurden – anzugeben und zu beschreiben, wie diese Anforderungen umgesetzt werden.

Der Kriterienkatalog mit den Anforderungselementen findet sich in Kapitel 4. Darüber hinaus werden weiterführende Informationen und Vorgaben von der Programmeignerin vorgegeben und von den Zertifizierungsstellen zur einheitlichen Anwendbarkeit zur Verfügung gestellt.

Wichtig: Die Anforderungen beziehen sich stets auf den gesamten Bewertungsgegenstand und insbesondere auf die jeweils angegebenen Zielobjekte. Und zwar dann auf alle angegebenen Zielobjekte. Wenn also etwa zwei Gebäude relevant sind, muss sich die Umsetzungsbeschreibung zur physikalischen Sicherheit auch auf beide Gebäude beziehen. Genauso verhält es sich, wenn die zu zertifizierende Datenverarbeitung mehrere Verarbeitungsvorgänge (VV) aufweist, für die verschiedene Rechtsgrundlagen einschlägig sind; es ist dann die Rechtsgrundlage für jeden einzelnen Verarbeitungsvorgang (VV) anzugeben.

Insgesamt müssen alle Informationen klar, präzise und eindeutig sein.

4. Der Kriterienkatalog ‚DSGVO – information privacy standard'

Der vorliegende Kriterienkatalog ‚DSGVO – information privacy standard' enthält Kriterien, die im Nachfolgenden im Detail dargelegt werden:

- P.1 Zulässigkeit der Datenverarbeitung
  - P.1.1 Identifikation Grundlagen
  - P.1.2 Rechtsgrundlage Vertrag
  - P.1.3 Rechtsgrundlage berechtigtes Interesse
  - P.1.4 Rechtsgrundlage Einwilligung
  - P.1.5 Rechtsgrundlage rechtliche Verpflichtung
  - P.1.6 Rechtsgrundlage lebenswichtige Interessen
  - P.1.7 Rechtsgrundlage öffentliches Interesse
  - P.1.8 Verarbeitung bei besonderen Kategorien personenbezogener Daten
  - P.1.9 Verarbeitung bei strafrechtlichen Verurteilungen und Straftaten
  - P.1.10 Datenverarbeitung im Auftrag
- P.2 Grundsätze
  - P.2.1 Privacy-by-Design (Datenschutz durch Technikgestaltung)
  - P.2.2 Privacy-by-Default (Datenschutzfreundliche Voreinstellungen)
  - P.2.3 Zweckbindung
  - P.2.4 Datenminimierung
  - P.2.5 Richtigkeit
  - P.2.6 Speicherbegrenzung
  - P.2.7 Treu und Glauben
- P.3 Pflichten des Kunden
  - P.3.1 Informationspflichten des Kunden
- P.4 Auftragsverarbeitung
  - P.4.1 Vertrag zur Auftragsverarbeitung (AV-Vertrag)
  - P.4.2 Umsetzung der Maßnahmen gem. AV-Vertrag
  - P.4.3 Audit
- P.5 Technisch-organisatorische Maßnahmen
  - P.5.1 Festlegung geeigneter Maßnahmen
  - P.5.2 Zutrittskontrolle (Vertraulichkeit und Integrität auf Ebene der physischen Zutritte)
  - P.5.3 Zugangskontrolle (Vertraulichkeit und Integrität auf Ebene der Systemzugänge)
  - P.5.4 Zugriffskontrolle (Vertraulichkeit und Integrität auf Ebene der Anwendungszugriffe)
  - P.5.5 Transportkontrolle (Vertraulichkeit und Integrität auf Transport-Ebene)
  - P.5.6 Trennungskontrolle

    - P.5.7 Eingabekontrolle
    - P.5.8 Verfügbarkeitskontrolle
    - P.5.9 Pseudonymisierung / Anonymisierung
    - P.5.10 Überprüfung, Bewertung und Evaluierung
- P.6 Datenschutz-Management
    - P.6.1 Fortlaufende Datenschutz-Kontinuität
    - P.6.2 Datenschutzbeauftragter
    - P.6.3 Verpflichtung auf Vertraulichkeit / Schulungen
    - P.6.4 Verzeichnis von Verarbeitungstätigkeiten
    - P.6.5 Datenschutz-Folgenabschätzung
    - P.6.6 Meldung von Datenschutzverletzungen
    - P.6.7 Zusammenarbeit mit Aufsichtsbehörden
- P.7 Datenverarbeitung außerhalb der EU
    - P.7.1 Datenübermittlung in Drittstaaten
    - P.7.2 Vertreter innerhalb der EU
- P.8 Betroffenenrechte
    - P.8.1 Recht auf Auskunft
    - P.8.2 Recht auf Berichtigung
    - P.8.3 Recht auf Löschung ("Recht auf Vergessenwerden")
    - P.8.4 Recht auf Einschränkung
    - P.8.5 Mitteilungspflicht
    - P.8.6 Recht auf Datenübertragbarkeit
    - P.8.7 Recht auf Widerspruch
    - P.8.8 Recht auf Widerruf bei Einwilligung
    - P.8.9 Automatisierte Entscheidungen / Profiling
    - P.8.10 Beschwerde-Management

Alle Kriterien des vorliegenden Kriterienkatalogs sind wie folgt aufgebaut:

- eindeutige ID und Name des Anforderungselementes;
- Anforderung: hier findet sich die normative Anforderung dieses Anforderungselementes, Umsetzungshinweise finden sich in einem separaten Dokument;
- Verweis DSGVO: Verweis auf die (gesetzliche) Anforderung;
- Nachweise: hier findet sich ein Mindestsatz an Nachweisen, die der Kunde zur Verfügung stellt, um die Umsetzung nachzuweisen;
- Anwendbarkeit lt. SOA: Darstellung, ob ein Anforderungselement verpflichtend oder optional ist, vgl. Ausführungen in Kapitel 3.2;
- Zielobjektkategorie: Zuordnung zu den relevanten Zielobjekten, vgl. Ausführungen in Kapitel 3.1.

4.1. P.1 Zulässigkeit der Datenverarbeitung

4.1.1. P.1.1 Identifikation Grundlagen

Anforderung

Der Kunde (Verantwortlicher bzw. Auftragsverarbeiter) muss ein Datenschutz-Managementsystem (DSMS) aufrechterhalten, über das sichergestellt ist, dass für die Verarbeitungsvorgänge (VV) eine vollständige Übersicht der relevanten Grundlagen aktuell vorliegt.

Insbesondere sind bei der Identifikation folgende Elemente relevant:

- DSGVO;
- einschlägige Rechtsgrundlagen aus nationalen Konkretisierungen der DSGVO auf Basis der Öffnungsklauseln;
- das Konformitätsbewertungs- bzw. Zertifizierungsprogramm mit dem vorliegenden Kriterienkatalog.

Der Kunde (Verantwortlicher) muss eine begründete Analyse der Rechtsgrundlagen inklusive relevantem Recht der Mitgliedsstaaten und der Anwendbarkeit der Rechtsgrundlagen für den Zertifizierungsgegenstand vorlegen.

Der Kunde (als Auftragsverarbeiter) muss den Nachweis vorlegen, dass sich die Rechtsgrundlage aus dem Vertrag über die Auftragsverarbeitung mit dem Verantwortlichen ergibt.

Die Übersicht der relevanten Grundlagen muss dokumentiert vorliegen. Die identifizierten Grundlagen müssen jeweils exakt spezifiziert sein.

Verweis DSGVO

Art. 2 DSGVO

Art. 3 DSGVO

Art. 6 DSGVO

Art. 9 DSGVO

Art. 10 DSGVO

Nachweise

Verfahrens-, Prozessbeschreibungen

Übersicht über rechtliche Grundlagen

Verzeichnis der Verarbeitungstätigkeiten

Analyse der anwendbaren Rechtsgrundlagen

Anwendbarkeit lt. SOA

Verpflichtend für Verantwortliche und Auftragsverarbeiter

Zielobjektkategorie

DSMS

VV

4.1.2. P.1.2 Rechtsgrundlage Vertrag

Anforderung

Sofern der Kunde (als Verantwortlicher) als Rechtsgrundlage für die Durchführung des Verarbeitungsvorgangs (VV) einen Vertrag anführt, gilt Folgendes:

Die Datenverarbeitung muss erforderlich sein, um einen Vertrag mit der betroffenen Person, die Vertragspartei ist, oder um vorvertragliche Maßnahmen des Verantwortlichen, die auf Anfrage der betroffenen Person erfolgen, zu erfüllen.

Die Datenverarbeitung ist auf das zur Vertragsdurchführung Notwendige zu reduzieren. Ist eine Vertragsdurchführung ohne die Daten möglich, so liegt keine Erforderlichkeit vor.

Der Kunde (als Verantwortlicher) muss Prozesse (PRZ) zur Realisierung der Datenverarbeitung aufrechterhalten, um sicherzustellen, dass die Datenverarbeitung erst dann durchgeführt werden kann, wenn ein rechtsverbindlicher Vertrag vorliegt oder die Verarbeitung nur zum Zweck vorvertraglicher Maßnahmen erfolgt. Dies gilt entsprechend, wenn der Vertrag elektronisch über eine Applikation (APPL) abgeschlossen wird.

Erfolgt die Datenverarbeitung im Rahmen der Vertragsanbahnung, also vor Zustandekommen des Vertrags, muss der Kunde (als Verantwortlicher) Prozesse (PRZ) zur Realisierung der Datenverarbeitung aufrechterhalten, um sicherzustellen, dass die Verarbeitung mangels Rechtsgrundlage eingestellt wird, sollte der Vertrag nicht zustande kommen.

Nach Entfall dieser Rechtsgrundlage ist die Verarbeitung nur weiterhin zulässig, wenn der Kunde (als Verantwortlicher) nachweisen kann, dass die Verarbeitung für bestimmte spezifische Zwecke zur:

- Erfüllung einer rechtlichen Verpflichtung die die Verarbeitung nach dem Recht der Union oder der Mitgliedstaaten, dem der Kunde (als Verantwortlicher) unterliegt es erfordert;
- Wahrnehmung einer Aufgabe, die im öffentlichen Interesse liegt oder in Ausübung öffentlicher Gewalt erfolgt, die dem Verantwortlichen übertragen wurde;
- Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen

erforderlich ist.

Hinweis: Verträge zur Auftragsverarbeitung (AV-Verträge), die für den Kunden (als Auftragsverarbeiter) relevant sind, werden unter P.1.10 thematisiert.

Verweis DSGVO

Art. 6 Abs. 1 UAbs. 1 lit. b DSGVO

Nachweise

Muster des Vertrags (sofern vorliegend)

Abgeschlossene Verträge

Verfahrens-, Prozessbeschreibungen

Zurverfügungstellung der Applikation

Beschreibungen der Applikation zur Darlegung der Umsetzung der Anforderung (etwa Funktionsbeschreibung, Schnittstellenbeschreibungen)

Anwendbarkeit lt. SOA

Für Verantwortliche gilt für dieses optionale Anforderungselement: verpflichtend, sofern diese Rechtsgrundlage herangezogen wird

Nicht anwendbar für Auftragsverarbeiter

Zielobjektkategorie

VV

PRZ

APPL

4.1.3. P.1.3 Rechtsgrundlage berechtigtes Interesse

Anforderung

Sofern der Kunde (als Verantwortlicher) als Rechtsgrundlage für die Durchführung des Verarbeitungsvorgangs (VV) die Wahrung berechtigter Interessen anführt, gilt Folgendes:

Die Datenverarbeitung muss zur Wahrung der berechtigten Interessen des Verantwortlichen oder eines Dritten erforderlich sein. Die Erforderlichkeit ist so auszulegen, dass keine objektiv zumutbare Alternative besteht, um das Interesse zu wahren. Die Erforderlichkeit muss sich auf die gesamte Datenverarbeitung erstrecken.

Der Kunde (als Verantwortlicher) muss einerseits seine Interessen bzw. die Interessen eines Dritten sowie andererseits die Interessen der betroffenen Person identifizieren. Der Kunde (als Verantwortlicher) muss bezüglich der Auswirkungen der Datenverarbeitung seine Interessen bzw. die Interessen eines Dritten mit den Persönlichkeitsrechten der betroffenen Person und deren identifizierten Interessen sorgfältig abwägen. Der Kunde (als Verantwortlicher) muss nachweisen, dass die Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person, die den Schutz personenbezogener Daten erfordern, dabei nicht überwiegen. Bei der Durchführung der Interessenabwägung ist die besondere Schutzwürdigkeit von Kindern zu berücksichtigen, insbesondere bzgl. Risiken, Folgen und Garantien sowie das möglicherweise geringere Bewusstsein über bestehende Rechte. Die Interessen von Kindern Überwiegen grundsätzliche die kommerziellen Interessen des Kunden (als Verantwortlicher). Die Möglichkeit zur Ausübung des Widerspruchs ist den betroffenen Personen ausdrücklich in

einer verständlichen und von anderen Informationen getrennten Form zugänglich zu machen. Bei Ausübung des Widerspruchs muss der Kunde (als Verantwortlicher) die Verarbeitung beenden; dies gilt nicht, wenn er zwingende schutzwürdige Gründe nachweisen kann, die die Rechte und Freiheiten der betroffenen Personen überwiegen oder die Verarbeitung der Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen dient.

Das berechtigte Interesse ist dreistufig zu prüfen. Alle an der Datenverarbeitung beteiligten, verantwortlichen Stellen

- müssen ein berechtigtes Interesse an der jeweiligen Datenverarbeitung haben,
- die Erforderlichkeit der Datenverarbeitung zur Realisierung der berechtigten Interessen muss objektiv gegeben sein und
- es dürfen keine überwiegenden Interessen der betroffenen Personen diesen berechtigten Interessen gegenüberstehen.

Der Kunde (als Verantwortlicher) muss Prozesse (PRZ) inklusive Verantwortlichkeiten, Workflows, Zeitrahmen und/oder Fristen zur Identifikation und Abwägung des relevanten Interesses etablieren, um die Umsetzung obiger Anforderungen sicherzustellen.

Für Verarbeitungen durch Behörden darf diese Rechtsgrundlage nicht herangezogen werden, da es dem Gesetzgeber obliegt, per Rechtsvorschrift die Rechtsgrundlage für die Verarbeitung personenbezogener Daten durch die Behörden zu schaffen.

Verweis DSGVO

Art. 6 Abs. 1 UAbs. 1 lit. f DSGVO

Art. 6 Abs. 1 UAbs. 2 DSGVO

Nachweise

Darlegung des Sachverhalts mit Begründung

Verfahrens-, Prozessbeschreibungen

Dokumentierte Interessenabwägung

Richtlinien und Leitfäden zur Regulierung von Interessenabwägungen

Anwendbarkeit lt. SOA

Für Verantwortliche gilt für dieses optionale Anforderungselement: verpflichtend, sofern diese Rechtsgrundlage herangezogen wird

Nicht anwendbar für Auftragsverarbeiter

Zielobjektkategorie

VV

PRZ

4.1.4. P.1.4 Rechtsgrundlage Einwilligung

Anforderung

Sofern der Kunde (als Verantwortlicher) den Verarbeitungsvorgang (VV) auf Grundlage einer Einwilligung durchführt, gilt Folgendes:

Die Einwilligung kann nur als Rechtsgrundlage herangezogen werden, wenn die Ausübung des Widerrufs der Einwilligung einer Beendigung der Verarbeitung nicht entgegensteht, vgl. P.8.8 Recht auf Widerruf bei Einwilligung.

Die betroffene Person muss in die Verarbeitung ihrer personenbezogenen Daten für einen oder mehrere bestimmte Zwecke eingewilligt haben. Der Kunde (als Verantwortlicher) muss die Einwilligung nachweisen können.

Die Abgabe von Einwilligungen hat ausdrücklich und unabhängig voneinander für den oder die spezifischen Verarbeitungszwecke, durch ein aktives bestätigendes Handeln der betroffenen Person zu erfolgen und dokumentiert zu werden, um nachweisen zu können, dass die betroffene Person tatsächlich in die spezifischen Verarbeitungszwecke eingewilligt hat. Konkludente Einwilligungen durch Schweigen, vorangekreuzte Kästchen oder Untätigkeit der betroffenen Person stellen i.d.R. keine wirksame Einwilligung dar, sofern die ausdrückliche aktive Abgabe nicht durch den Verantwortlichen nachgewiesen werden kann.

Die Einwilligung muss freiwillig und informiert (konform zu den Anforderungen von P.3.1) durch den Betroffenen abgegeben werden und darf nicht an andere Sachverhalte gekoppelt werden. Einwilligungen können nur freiwillig gegeben werden, wenn kein ungleiches Machtverhältnis die Freiwilligkeit ausschließt.

Das Ersuchen um Einwilligung muss in verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache sowie getrennt von anderen Sachverhalten erfolgen. Die Information muss verständlich für die Zielgruppe sein.

Der Kunde (als Verantwortlicher) muss den Widerruf einer abgegebenen Einwilligung jederzeit ohne Nachteile ermöglichen sowie die betroffene Person über die Widerrufsmöglichkeit und Widerrufsfolgen informieren. Der Kunde (als Verantwortlicher) muss sicherstellen, dass Betroffene Personen müssen Ihre Einwilligung jederzeit genauso einfach ohne Nachteil widerrufen können, wie die Einwilligung abgegeben wurde.

Entfällt die Grundlage für die Datenverarbeitung, z. B. aufgrund der Ausübung des Widerrufsrechts, darf die Datenverarbeitung nicht weitergeführt werden. Des Weiteren ist zu prüfen, ob sich hieraus weiterer Handlungsbedarf ergibt, etwa Lösch- und Informationspflichten.

In Bezug auf Kinder und andere begrenzt einwilligungsfähige Personen gilt Folgendes: Die Anforderungen an eine Einwilligung für die jeweilige Datenverarbeitung durch Kinder oder andere begrenzt einwilligungsfähige Personen sind im Einzelfall durch den Verantwortlichen zu prüfen, der nachweisen muss, dass Altersverifizierungsmaßnahmen implementiert sind.

Sofern nach dem Recht der Union oder relevanter Gesetze der Mitgliedsstaaten erforderlich, muss der Kunde (als Verantwortlicher) über geeignete Prozesse verfügen, um

die Einwilligung im Einklang mit den jeweilig bestehenden nationalen Anforderungen einzuholen.

Beim direkten Anbieten von Diensten der Informationsgesellschaft i.S.d. Art. 8 DSGVO gegenüber einem Kind muss sichergestellt werden – wenn dieses Kind das sechzehnte Lebensjahr nicht vollendet hat –, dass die Einwilligung durch den Träger der elterlichen Verantwortung oder mit dessen Zustimmung erteilt wird. Je nach relevanten gesetzlichen Regelungen der Mitgliedsstaaten kann die Altersgrenze auch niedriger sein; darf jedoch niemals das dreizehnte Lebensjahr unterschreiten.

Der Kunde (als Verantwortlicher) muss Prozesse (PRZ) zur Realisierung der Datenverarbeitung aufrechterhalten, um sicherzustellen, dass die Datenverarbeitung erst dann durchgeführt werden kann, wenn eine rechtsverbindliche wirksame Einwilligung vorliegt. Dies gilt entsprechend, wenn die Einwilligung über eine Applikation (APPL) eingeholt wird.

Verweis DSGVO

Art. 6 Abs. 1 UAbs. 1 lit. a DSGVO

Art. 7 DSGVO

Art. 8 DSGVO

Art. 17 Abs. 3 DSGVO

Nachweise

Muster der Einwilligung (sofern vorliegend)

Abgeschlossene Einwilligungen

Verfahrens-, Prozessbeschreibungen

Zurverfügungstellung der Applikation

Beschreibungen zur Applikation zur Darlegung der Umsetzung der Anforderung (etwa Funktionsbeschreibung, Schnittstellenbeschreibung)

Anwendbarkeit lt. SOA

Für Verantwortliche gilt für dieses optionale Anforderungselement: verpflichtend, sofern diese Rechtsgrundlage herangezogen wird

Nicht anwendbar für Auftragsverarbeiter

Zielobjektkategorie

VV

PRZ

APPL

4.1.5. P.1.5 Rechtsgrundlage rechtliche Verpflichtung

Anforderung

Sofern der Kunde (als Verantwortlicher) als Rechtsgrundlage für die Durchführung des Verarbeitungsvorgangs (VV) eine rechtliche Verpflichtung durch oder aufgrund von Rechtsvorschriften angibt, gilt Folgendes:

Die Datenverarbeitung muss zur Erfüllung einer rechtlichen Verpflichtung erforderlich sein, der der Kunde (als Verantwortlicher) unterliegt und die eine zulässige und anwendbare gesetzliche Grundlage für die Datenverarbeitung begründet. Der Kunde (als Verantwortlicher) gibt die rechtlichen Verpflichtungen präzise an, vgl. P.1.1.

Verpflichtungen im Zusammenhang mit der Erfüllung von Verträgen sind nicht hiervon umfasst; sie fallen unter P.1.2.

Verweis DSGVO

Art. 6 Abs. 1 UAbs. 1 lit. c DSGVO

Art. 6 Abs. 2 DSGVO

Art. 6 Abs. 3 DSGVO

Nachweise

Darlegung des Sachverhalts mit Begründung

Analyse des relevanten Rechts mit Rechtsgrundlagen und ihrer Anwendbarkeit

Anwendbarkeit lt. SOA

Für Verantwortliche gilt für dieses optionale Anforderungselement: verpflichtend, sofern diese Rechtsgrundlage herangezogen wird

Nicht anwendbar für Auftragsverarbeiter

Zielobjektkategorie

VV

4.1.6. P.1.6 Rechtsgrundlage lebenswichtige Interessen

Anforderung

Sofern der Kunde (als Verantwortlicher) als Rechtsgrundlage für die Durchführung des Verarbeitungsvorgangs (VV) „lebenswichtige Interessen“ anführt, gilt Folgendes:

Die Datenverarbeitung muss erforderlich sein, um lebenswichtige Interessen der betroffenen Person oder einer anderen natürlichen Person zu schützen.

Der Kunde (als Verantwortlicher) muss darlegen, dass die Datenverarbeitung nur durch diese Rechtsgrundlage legitimiert werden kann und auf keine andere Rechtsgrundlage gestützt werden kann (Subsidiarität der Rechtsgrundlage), dement-

sprechend sind zunächst andere in Betracht kommenden Rechtsgrundlagen zu berücksichtigen.

Die Anwendbarkeit dieses Kriteriums ist nur in seltenen Fällen gegeben.

Verweis DSGVO

Art. 6 Abs. 1 UAbs. 1 lit. d DSGVO

Nachweise

Darlegung des Sachverhalts mit Begründung

Anwendbarkeit lt. SOA

Für Verantwortliche gilt für dieses optionale Anforderungselement: verpflichtend, sofern diese Rechtsgrundlage herangezogen wird

Nicht anwendbar für Auftragsverarbeiter

Zielobjektkategorie

VV

4.1.7. P.1.7 Rechtsgrundlage öffentliches Interesse

Anforderung

Sofern der Kunde (als Verantwortlicher) als Rechtsgrundlage für die Durchführung des Verarbeitungsvorgangs (VV) die Wahrnehmung von Aufgaben im öffentlichen Interesse oder die Ausübung öffentlicher Gewalt anführt, gilt Folgendes:

Der Kunde (als Verantwortlicher) darf diese Rechtsgrundlage nur heranziehen, wenn er Aufgaben wahrnimmt, die dem Verantwortlichen übertragen wurden und im öffentlichen Interesse liegen oder in Ausübung öffentlicher Gewalt erfolgen. Dies sind i.d.R. nur öffentliche Stellen.

Die Grundlage für diese Rechtsgrundlage kann sich nur aus dem Unionsrecht oder aus dem einschlägigen Recht eines Mitgliedsstaates ergeben.

Die Datenverarbeitung muss für die Wahrnehmung einer Aufgabe erforderlich sein. Um den Grundsatz der Verhältnismäßigkeit zu wahren, ist zu prüfen, ob ein milderes Mittel verfügbar ist, welches die betroffene Person weniger beeinträchtigt.

Die Möglichkeit zur Ausübung des Widerspruchs ist den betroffenen Personen ausdrücklich in einer verständlichen und von anderen Informationen getrennten Form zugänglich zu machen. Bei Ausübung des Widerspruchs muss der Kunde (als Verantwortlicher) die Verarbeitung beenden; dies gilt nicht, wenn er zwingende schutzwürdige Gründe nachweisen kann, die die Rechte und Freiheiten der betroffenen Personen überwiegen, oder die Verarbeitung der Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen dient.

Verweis DSGVO

Art. 6 Abs. 1 UAbs. 1 lit. e DSGVO

Art. 6 Abs. 2 DSGVO

Art. 6 Abs. 3 DSGVO

Nachweise

Darlegung des Sachverhalts mit Begründung

Analyse des relevanten Rechts mit Rechtsgrundlagen und ihrer Anwendbarkeit

Dokumentierte Interessenabwägung

Anwendbarkeit lt. SOA

Für Verantwortliche gilt für dieses optionale Anforderungselement: verpflichtend, sofern diese Rechtsgrundlage herangezogen wird

Nicht anwendbar für Auftragsverarbeiter

Zielobjektkategorie

VV

4.1.8. P.1.8 Verarbeitung bei besonderen Kategorien personenbezogener Daten

Anforderung

Werden durch den Kunden (als Verantwortlicher bzw. Auftragsverarbeiter) bei der Durchführung des Verarbeitungsvorgangs (VV) besondere Kategorien personenbezogener Daten verarbeitet, sind besondere Anforderungen zu beachten.

Besondere Kategorien personenbezogener Daten sind gem. Art. 9 DSGVO definiert als Daten, „aus denen

- die rassische und ethnische Herkunft,
- politische Meinungen,
- religiöse oder weltanschauliche Überzeugungen oder
- die Gewerkschaftszugehörigkeit

hervorgehen, sowie die Verarbeitung von

- genetischen Daten,
- biometrischen Daten zur eindeutigen Identifizierung einer natürlichen Person,
- Gesundheitsdaten oder
- Daten zum Sexualleben oder
- der sexuellen Orientierung einer natürlichen Person.“

Besondere Kategorien personenbezogener Daten dürfen nicht verarbeitet werden, es sei denn eine Ausnahme des Art. 9 Abs. 2 DSGVO liegt vor. Danach darf die Verarbeitung nur erfolgen, wenn eine der folgenden Rechtsgrundlagen einschlägig ist:

- die ausdrückliche Einwilligung der betroffenen Person für einen oder mehrere festgelegte Zwecke liegt vor (in Übereinstimmung mit P.1.4 Rechtsgrundlage Einwilligung). Es dürfen keine Einwilligungen in Verarbeitungen von besonderen Kategorien personenbezogener Daten eingeholt werden, die nach dem Unions-Recht oder nach dem einschlägigen Recht der Mitgliedstaaten verboten sind;
- die Verarbeitung ist zur Ausübung und Erfüllung von Rechten und Pflichten aus dem Arbeitsrecht und dem Recht der sozialen Sicherheit und des Sozialschutzes erforderlich, soweit das nach Unionsrecht, dem einschlägigen Recht der Mitgliedstaaten oder Kollektivvereinbarungen zulässig ist, die geeignete Garantien für die Grundrechte und die Interessen der betroffenen Person vorsehen; in diesem Fall gilt das Folgende:
  - der Kunde (als Verantwortlicher) muss die oben genannten zusätzlichen Maßnahmen zum Schutz der Grundrechte und Interessen der betroffenen Personen getroffen haben;
  - der Kunde (als Verantwortlicher) muss die möglicherweise anwendbaren Bestimmungen der jeweiligen spezifischen Gesetze bezüglich der Datenverarbeitung identifizieren und die Übereinstimmung der Datenverarbeitung mit diesen Gesetzen nachweisen, z.B. durch besondere Garantien;
  - wenn die Verarbeitung auf einem Tarifvertrag beruht, muss dieser Vertrag den Anforderungen der bestehenden gesetzlichen Garantien entsprechen;
- die Verarbeitung ist zum Schutz lebenswichtiger Interessen der betroffenen Person oder einer anderen natürlichen Person – im medizinischen Kontext – für eine lebensrettende Behandlung erforderlich und die betroffene Person ist aus körperlichen oder rechtlichen Gründen außerstande, ihre Einwilligung zu geben;
- die Verarbeitung erfolgt auf der Grundlage geeigneter Garantien durch eine politisch, weltanschaulich, religiös oder gewerkschaftlich ausgerichtete Stiftung, Vereinigung oder sonstige Organisation ohne Gewinnerzielungsabsicht im Rahmen ihrer rechtmäßigen Tätigkeiten und unter der Voraussetzung, dass sich die Verarbeitung ausschließlich auf die Mitglieder oder ehemalige Mitglieder der Organisation oder auf Personen, die im Zusammenhang mit deren Tätigkeitszweck regelmäßige Kontakte mit ihr unterhalten, bezieht und die personenbezogenen Daten nicht ohne Einwilligung der betroffenen Personen nach außen offengelegt werden;
- die Verarbeitung bezieht sich auf von der betroffenen Person offensichtlich öffentlich gemachte Daten;
- die Verarbeitung ist zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen oder bei Handlungen der Gerichte im Rahmen ihrer justiziellen Tätigkeit erforderlich;
- die Verarbeitung ist aus Gründen eines erheblichen öffentlichen Interesses, auf der Grundlage des Unionsrechts oder des einschlägigen Rechts eines Mitgliedstaats erforderlich;

- die Verarbeitung ist für Zwecke der Gesundheitsvorsorge oder der Arbeitsmedizin, für die Beurteilung der Arbeitsfähigkeit des Beschäftigten, für die medizinische Diagnostik, die Versorgung oder Behandlung im Gesundheits- oder Sozialbereich oder für die Verwaltung von Systemen und Diensten im Gesundheits- oder Sozialbereich auf der Grundlage des Unionsrechts oder des einschlägigen Rechts eines Mitgliedstaats oder aufgrund eines Vertrags mit einem Angehörigen eines Gesundheitsberufs erforderlich;
- die Verarbeitung ist aus Gründen des öffentlichen Interesses im Bereich der öffentlichen Gesundheit auf der Grundlage des Unionsrechts oder des einschlägigen Rechts eines Mitgliedstaats erforderlich;
- die Verarbeitung ist auf der Grundlage des Unionsrechts oder des einschlägigen Rechts eines Mitgliedstaats, das in angemessenem Verhältnis zu dem verfolgten Ziel steht, den Wesensgehalt des Rechts auf Datenschutz wahrt und angemessene und spezifische Maßnahmen zur Wahrung der Grundrechte und Interessen der betroffenen Person vorsieht, für im öffentlichen Interesse liegende Archivzwecke, für wissenschaftliche oder historische Forschungszwecke oder für statistische Zwecke gem. Art. 89 Abs. 1 DSGVO erforderlich.

Die Verarbeitung von besonderen Kategorien personenbezogener Daten für die Zwecke der präventiven oder berufsbedingten Medizin muss durch Fachpersonal oder unter dessen Verantwortung erfolgen. Das Fachpersonal muss einem Berufsgeheimnis unterliegen. Wenn die Verarbeitung durch eine andere Person unter der Verantwortung von Fachpersonal erfolgt, muss diese andere Person einer Geheimhaltungspflicht nach dem Unios-Recht oder nach dem einschlägigen Recht der Mitgliedstaaten oder Regeln der nationalen Aufsichtsbehörden unterliegen. Der Kunde muss identifizieren, ob das einschlägige, anwendbare Recht der Mitgliedstaaten die vorhergenannten Schutzmaßnahmen vorsieht und, sofern anwendbar, entsprechende Maßnahmen trifft, um die Erfüllung dieser sicherzustellen.

Der Kunde muss Prozesse (PRZ) inklusive Verantwortlichkeiten, Workflows, Zeitrahmen und/oder Fristen aufrechterhalten, um die Umsetzung obiger Grundsätze sicherzustellen.

Hinweis: Dieses Kriterium ist auch für Auftragsverarbeiter anwendbar – auch wenn die DSGVO in Art. 9 Auftragsverarbeiter nicht explizit erwähnt. Denn für einen zertifizierten Auftragsverarbeiter ist sicherzustellen, dass dieser über Prozesse (PRZ) verfügt, die den Verantwortlichen bei seinen Aufgaben entsprechend der Weisung des Verantwortlichen zu unterstützen (vgl. P.4 Auftragsverarbeitung) und die Anforderungen dieses Kriterium umgesetzt werden, sofern Art. 9 DSGVO-Daten verarbeitet werden ebenso wie die Verpflichtung des Auftragsverarbeiters, den für die Verarbeitung Verantwortlichen unverzüglich zu informieren, wenn seiner Meinung nach diese Anforderung nicht erfüllt ist.

Verweis DSGVO

Art. 9 DSGVO

Art. 4 Nr. 13, 14, 15 DSGVO

Art. 28 Abs. 3 DSGVO

Nachweise

Darlegung des Sachverhalts mit Begründung

Abgeschlossene Vereinbarungen

Verfahrens-, Prozessbeschreibungen

Anwendbarkeit lt. SOA

Für Verantwortliche und Auftragsverarbeiter gilt für dieses optionale Anforderungselement: verpflichtend, sofern Art. 9 DSGVO-Daten verarbeitet werden

Zielobjektkategorie

VV

PRZ

4.1.9. P.1.9 Verarbeitung bei strafrechtlichen Verurteilungen und Straftaten

Anforderung

Werden durch den Kunden (als Verantwortlicher) bei der Durchführung des Verarbeitungsvorgangs (VV) personenbezogene Daten über strafrechtliche Verurteilungen und Straftaten oder damit zusammenhängende Sicherungsmaßregeln verarbeitet, sind besondere Anforderungen zu beachten.

Die Verarbeitung personenbezogener Daten über strafrechtliche Verurteilungen und Straftaten oder damit zusammenhängende Sicherungsmaßregeln dürfen nur unter behördlicher Aufsicht vorgenommen werden, sofern nicht nach dem Recht der EU oder dem einschlägigen Recht der Mitgliedstaaten inklusive Schutzmaßnahmen für die Rechte und Freiheiten der betroffenen Person eine zulässige Rechtsgrundlage für die Datenverarbeitung besteht. Umfassende Register strafrechtlicher Verurteilungen müssen unter behördlicher Aufsicht geführt werden.

Der Kunde muss Prozesse (PRZ) (PRZ) inklusive Verantwortlichkeiten, Workflows, Zeitrahmen und/oder Fristen aufrechterhalten, um die Umsetzung obiger Anforderungen sicherzustellen.

Verweis DSGVO

Art. 10 DSGVO

Art. 28 Abs. 3 DSGVO

Nachweise

Darlegung des Sachverhalts mit Begründung

Verfahrens-, Prozessbeschreibungen

Vorgänge

Anwendbarkeit lt. SOA

Für Verantwortliche gilt für dieses optionale Anforderungselement: verpflichtend, sofern Art. 10 DSGVO-Daten verarbeitet werden

Nicht anwendbar für Auftragsverarbeiter

Zielobjektkategorie

VV

PRZ

4.1.10. P.1.10 Datenverarbeitung im Auftrag

Anforderung

Sofern der Kunde (als Auftragsverarbeiter) als Rechtsgrundlage für die Durchführung des Verarbeitungsvorgangs (VV) eine datenschutzrechtliche Auftragsverarbeitung anführt, gilt Folgendes:

Der Kunde (als Auftragsverarbeiter) muss nachweisen, dass die Datenverarbeitung als eine Auftragsverarbeitung zu qualifizieren ist, die den Anforderungen aus Art. 28 DSGVO genügt. Insbesondere wird darauf hingewiesen, dass sich die Rechtsgrundlage für die Datenverarbeitung selbst aus der von dem für die Verarbeitung Verantwortlichen angegebenen Rechtsgrundlage sowie aus der Umsetzung der besonderen Anforderungen für die Verarbeitung besonderer Kategorien personenbezogener Daten und von Daten über strafrechtliche Verurteilungen und Straftaten gemäß Art. 6 bis 10 GDPR, die von dem für die Verarbeitung Verantwortlichen angegeben wurden, ableitet.

Der Kunde (als Auftragsverarbeiter) muss die Auftragsverarbeitung auf Grundlage einer dokumentierten Weisung des Verantwortlichen durchführen. Der Auftragsverarbeiter darf nicht über die Zwecke und Mittel der Datenverarbeitung bestimmen.

Es muss sichergestellt sein, dass es sich um eine rechtmäßige Auftragsverarbeitung zwischen dem Verantwortlichen und dem Auftragsverarbeiter handelt und keine gemeinsame Verantwortlichkeit nach Art. 26 DSGVO vorliegt oder es sich um eine reine Übermittlung von personenbezogenen Daten handelt.

Hinweis: Die inhaltliche Ausgestaltung der Auftragsverarbeitung ist Bestandteil der Anforderung P.4.

Verweis DSGVO

Art. 28 DSGVO

Art. 29 DSGVO

Nachweise

Darlegung des Sachverhalts mit Begründung

Dokumentierte Weisung des Verantwortlichen

Vertrag über die Auftragsverarbeitung

Anwendbarkeit lt. SOA

Verpflichtend für Auftragsverarbeiter

Nicht anwendbar für Verantwortliche

Zielobjektkategorie

VV

4.2. P.2 Grundsätze

4.2.1. P.2.1 Privacy-by-Design (Datenschutz durch Technikgestaltung)

Anforderung

Der Kunde (als Verantwortlicher) muss ein Datenschutz-Managementsystem (DSMS) aufrechterhalten, um sicherzustellen, dass die Prozesse (PRZ) bzw. die Applikationen (APPL) sowie alle anderen relevanten Zielobjekte (VV, IT, INFRA, DL) so gestaltet sind, dass der Datenschutzgrundsatz „Privacy-by-Design“ (Datenschutz durch Technikgestaltung) umgesetzt wird und regelmäßig (mindestens jährlich) sowie anlassbezogen überprüft und bewertet wird.

„Privacy-by-Design“ meint, dass datenschutz-spezifische Grundsätze sowohl zu Beginn bei der Konzeption bzw. Gestaltung (Design) des Verarbeitungsvorgangs als auch über den gesamten Lebenszyklus in allen Phasen der Entstehung, der Konzeption oder des Entwurfs hinweg berücksichtigt und umgesetzt werden.

Der Kunde (als Verantwortlicher) muss zunächst für die Prozesse (PRZ) bzw. die Applikationen (APPL) festlegen, welche technischen und organisatorischen Maßnahmen geeignet sind, um die Datenschutzgrundsätze zu erfüllen.

Typische Datenschutzgrundsätze – z.T. auch „Gewährleistungsziele“ genannt – finden sich im vorliegenden Kriterienkatalog als eigene Anforderungselemente, beispielsweise:

- Zweckbindung, vgl. P.2.3;
- Nichtverkettung, vgl. P.2.3;
- Datenminimierung, vgl. P.2.4;
- Richtigkeit, vgl. P.2.5;
- Speicherbegrenzung. vgl. P.2.6;
- Intervenierbarkeit, vgl. P.8;
- Transparenz, vgl. P.8;
- Vertraulichkeit, vgl. P.5;
- Integrität, vgl. P.5;
- Verfügbarkeit, vgl. P.5.8.

Die Festlegung geeigneter technischer und organisatorischer Maßnahmen gemäß P.5.1 – um diese Datenschutzgrundsätze wirksam zu erfüllen – ist schon zum Zeitpunkt der Festlegung der Mittel für die Verarbeitung als auch während der eigentlichen Verarbeitung umzusetzen, um einen datenschutzfreundlichen Verarbeitungsvorgang (VV) in jeder Phase der Entwicklung und Durchführung zu erschaffen und soll sich am Stand der Technik und der Implementierungskosten orientieren und den konkreten Verarbeitungsvorgang sowie die unterschiedlichen Eintrittswahrscheinlichkeiten sowie die Auswirkungen (Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen) berücksichtigen ohne den Datenschutz zu kompromittieren. Hierbei ist auf den besonderen Schutz von Kindern unter 18 Jahren und anderen schutzbedürftigen Gruppen zu berücksichtigen. Selbstverständlich kann der Kunde bei der Festlegung dieser geeigneten technischen und organisatorischen Maßnahmen auf die o.g. Anforderungselemente Bezug nehmen.

Der Kunde (als Verantwortlicher) muss die Umsetzung dieses Grundsatzes bzw. dieser Anforderung nachweisen („Rechenschaftspflicht“).

Verweis DSGVO

Art. 5 Abs. 1 DSGVO

Art. 5 Abs. 2 DSGVO

Art. 25 Abs. 1 DSGVO

Nachweise

Darlegung des Sachverhalts mit Begründung

Verfahrens-, Prozessbeschreibungen

Zurverfügungstellung der Applikation

Richtlinien des Datenschutz-Managementsystems

Beschreibungen zur Applikation zur Darlegung der Umsetzung der Anforderung (etwa Funktionsbeschreibung, Schnittstellenbeschreibung)

Spezifikation einer Entwurfsstrategie

Spezifizierung aller relevanten normativen Anforderungen

Spezifikation des Entwurfs einschließlich der Schutzmaßnahmen

Dokumentation der Risikobewertung

Dokumentation der Berücksichtigung des Stands der Technik und der Implementierungskosten

Nachweise für die Wirksamkeit der Schutzmaßnahmen

Anwendbarkeit lt. SOA

Verpflichtend für Verantwortliche

Zielobjektkategorie

DSMS

PRZ

APPL

VV

IT

INFRA

DL

4.2.2. P.2.2 Privacy-by-Default (Datenschutzfreundliche Voreinstellungen)

Anforderung

Der Kunde (als Verantwortlicher) muss ein Datenschutz-Managementsystem (DSMS) aufrechterhalten, um sicherzustellen, dass die Prozesse (PRZ) bzw. die Applikationen (APPL) sowie alle anderen relevanten Zielobjekte (VV, IT, INFRA, DL) so gestaltet sind, dass der Datenschutzgrundsatz „Privacy-by-Default" (Datenschutzfreundliche Voreinstellungen) umgesetzt wird und regelmäßig (mindestens jährlich) sowie anlassbezogen überprüft und bewertet wird.

„Privacy-by-Default" meint, dass datenschutz-spezifische Grundsätze bei den Voreinstellungen (etwa Werkeinstellungen) eines Verarbeitungsvorgangs berücksichtigt werden. Hierbei ist auf den besonderen Schutz von Kindern unter 18 Jahren und anderen schutzbedürftigen Gruppen zu berücksichtigen.

Der Kunde (als Verantwortlicher) muss für die Prozesse (PRZ) bzw. die Applikationen (APPL) sicherstellen, dass durch Voreinstellung nur personenbezogene Daten verarbeitet werden, deren Verarbeitung für den jeweiligen bestimmten Verarbeitungszweck erforderlich ist; dies betrifft sowohl Umfang der Daten und ihre Speicherfrist sowie die Zugriffsrechte. Die Maßnahmen müssen sicherstellen, dass personenbezogene Daten durch Voreinstellungen nicht ohne Eingreifen der Person einer unbestimmten Zahl von natürlichen Personen zugänglich gemacht werden.

Der Kunde (als Verantwortlicher) muss die Umsetzung dieses Grundsatzes bzw. dieser Anforderung nachweisen („Rechenschaftspflicht").

Verweis DSGVO

Art. 5 Abs. 1 DSGVO

Art. 5 Abs. 2 DSGVO

Art. 25 Abs. 2 DSGVO

Nachweise

Darlegung des Sachverhalts mit Begründung

Verfahrens-, Prozessbeschreibungen

Richtlinien des Datenschutz-Managementsystems

Zurverfügungstellung der Applikation

Beschreibungen zur Applikation zur Darlegung der Umsetzung der Anforderung (etwa Funktionsbeschreibung, Schnittstellenbeschreibung)

Spezifizierung aller relevanten normativen Anforderungen

Spezifikation des Entwurfs einschließlich der Schutzmaßnahmen

Dokumentation der Risikobewertung

Dokumentation der Berücksichtigung des Standes der Technik und der Realisierungskosten

Nachweis der Wirksamkeit der Schutzmaßnahmen

Anwendbarkeit lt. SOA

Verpflichtend für Verantwortliche

Zielobjektkategorie

DSMS

PRZ

APPL

VV

IT

INFRA

DL

4.2.3. P.2.3 Zweckbindung

Anforderung

Der Kunde (als Verantwortlicher) muss für den Verarbeitungsvorgang (VV), sowie für die Prozesse (PRZ) bzw. die Applikationen (APPL) sowie alle anderen relevanten Zielobjekte (VV, IT, INFRA, DL) sicherstellen, dass die Datenverarbeitung für festgelegte, eindeutige und legitime Zwecke erfolgt und dass keine Weiterverarbeitung vorgenommen wird, die nicht mit diesen Zwecken zu vereinbaren ist. Hierüber muss insbesondere die Nichtverkettung von Daten sichergestellt werden.

Zu diesem Zweck, muss der Kunde (als Verantwortlicher) Prozesse (PRZ) implementieren, um

- die Zwecke der Verarbeitung zu identifizieren,
- die Erforderlichkeit der Daten zu diesem Zweck zu analysieren,
- die Nichtverkettbarkeit der Daten (-sets) für unterschiedliche Zwecke sicherzustellen,

- Zweckänderungen oder den „Verlust“ der Zwecke zu berücksichtigen und deren Folgen zu regeln, wie z.B. die Löschung gemäß dem auf P.8.3 basierenden Löschungskonzept.

Der Kunde (als Verantwortlicher) muss die Vereinbarkeit des anderen Zwecks mit dem Zweck, zu dem die personenbezogenen Daten ursprünglich erhoben wurden, feststellen und dabei folgende Aspekte berücksichtigen:

- jede Verbindung zwischen den Zwecken, für die die personenbezogenen Daten erhoben wurden, und den Zwecken der beabsichtigten Weiterverarbeitung;
- den Zusammenhang, in dem die personenbezogenen Daten erhoben wurden, insbesondere hinsichtlich des Verhältnisses zwischen den betroffenen Personen und dem Verantwortlichen;
- die Art der personenbezogenen Daten, insbesondere ob besondere Kategorien personenbezogener Daten oder ob personenbezogene Daten über strafrechtliche Verurteilungen und Straftaten verarbeitet werden (vgl. Anforderungen P.1.8 Verarbeitung bei besonderen Kategorien personenbezogener Daten und P.1.9 Verarbeitung bei strafrechtlichen Verurteilungen und Straftaten);
- die möglichen Folgen der beabsichtigten Weiterverarbeitung für die betroffenen Personen;
- ob geeigneter Garantien bestehen, wie Verschlüsselung oder Pseudonymisierung.

Eine Weiterverarbeitung für im öffentlichen Interesse liegende Archivzwecke, für wissenschaftliche oder historische Forschungszwecke oder für statistische Zwecke gilt gemäß Artikel 89 Absatz 1 DSGVO und den erforderlichen Schutzmaßnahmen und Ausnahmen nicht als unvereinbar mit den ursprünglichen Zwecken.

Sind die Zwecke und Mittel der Verarbeitung durch das Unionsrecht oder das einschlägige Recht der Mitgliedstaaten vorgegeben, so kann die Rolle des Verantwortlichen beziehungsweise die bestimmten Kriterien seiner Benennung nach dem Unionsrecht oder dem Recht der Mitgliedstaaten vorgesehen werden; dies ist zu berücksichtigen. Die Zweckbindung ist über die gesamte Laufzeit der Datenverarbeitung sicherzustellen. Die Prozesse zur Realisierung (PRZ) müssen auch Zweckänderung oder -wegfall und deren Folgen berücksichtigen. Die Umsetzung muss regelmäßig (mindestens jährlich) sowie anlassbezogen überprüft und bewertet werden.

Der Kunde (als Verantwortlicher) muss die Umsetzung dieses Grundsatzes bzw. dieser Anforderung nachweisen („Rechenschaftspflicht“).

Verweis DSGVO

Art. 4 Nr. 7 DSGVO

Art. 5 Abs. 1 lit. b DSGVO

Art. 5 Abs. 2 DSGVO

Art. 6 Abs. 4 DSGVO

Nachweise

Darlegung des Sachverhalts zur Umsetzung inkl. Benennung der technischen und organisatorischen Maßnahmen mit Begründung

Verfahrens-, Prozessbeschreibungen

Zurverfügungstellung der Applikation

Beschreibungen zur Applikation zur Darlegung der Umsetzung der Anforderung (etwa Funktionsbeschreibung, Schnittstellenbeschreibungen)

Verzeichnis der Verarbeitungstätigkeiten mit festgelegten Zwecken auf Grundlage der Verarbeitungsvorgänge

Anwendbarkeit lt. SOA

Verpflichtend für Verantwortliche

Zielobjektkategorie

VV

PRZ

APPL

IT

INFRA

DL

4.2.4. P.2.4 Datenminimierung

Anforderung

Der Kunde (als Verantwortlicher) muss für den Verarbeitungsvorgang (VV) sowie die Prozesse (PRZ) bzw. die Applikationen (APPL) sicherstellen, dass die Datenverarbeitung dem Zweck angemessen und erheblich sowie auf das für die Zwecke der Verarbeitung basierend auf der in P.1.1 und P.6.4 identifizierten Rechtsgrundlage notwendige Maß beschränkt ist, konform zu dem Löschkonzept gemäß P.8.3.

Der Kunde (als Verantwortlicher) muss die Kategorien personenbezogener Daten, die für die Datenverarbeitung verarbeitet werden, dokumentieren und nachweisen, dass für jede dieser Kategorien eine Erforderlichkeitsprüfung durchgeführt wurde. Hierüber muss insbesondere die Datensparsamkeit sichergestellt werden. Wenn die Zwecke nicht oder nicht mehr die Identifizierung einer betroffenen Person erfordern, ist der Kunde (als Verantwortlicher) nicht verpflichtet, zusätzliche Informationen zur Identifizierung der betroffenen Person zu erhalten, zu beschaffen oder zu verarbeiten, und zwar ausschließlich zum Zweck der Einhaltung der DSGVO.

Die Umsetzung muss regelmäßig (mindestens jährlich) sowie anlassbezogen überprüft und bewertet werden.

Der Kunde (als Verantwortlicher) muss die Umsetzung dieses Grundsatzes bzw. dieser Anforderung nachweisen („Rechenschaftspflicht“).

Verweis DSGVO

Art. 5 Abs. 1 lit. c DSGVO

Art. 5 Abs. 2 DSGVO

Art. 11 Abs. 1 DSGVO

Nachweise

Dokumentation der Erforderlichkeit im Verzeichnis der Verarbeitungstätigkeiten

Darlegung des Sachverhalts zur Umsetzung inkl. Benennung der technischen und organisatorischen Maßnahmen mit Begründung

Verfahrens-, Prozessbeschreibungen

Zurverfügungstellung der Applikation

Beschreibungen zur Applikation zur Darlegung der Umsetzung der Anforderung (etwa Funktionsbeschreibung, Schnittstellenbeschreibung)

Beschreibung des Prozesses mit allen Ein- und Ausgaben sowie den erzeugten Daten

Löschkonzept und dokumentierte Verfahren

Anwendbarkeit lt. SOA

Verpflichtend für Verantwortliche

Zielobjektkategorie

VV

PRZ

APPL

4.2.5. P.2.5 Richtigkeit

Anforderung

Der Kunde (als Verantwortlicher) muss für den Verarbeitungsvorgang (VV) sowie die Prozesse (PRZ) bzw. die datenverarbeitenden Applikationen (APPL) sicherstellen, dass die verarbeiteten Daten sachlich richtig und aktuell sind.

Der Kunde (als Verantwortlicher) muss zu diesem Zweck die Verarbeitungsvorgänge (VV) und die Umsetzung der Betroffenenrechte in P.8 so gestalten, dass die Feststellung unrichtiger Daten, die Berichtigung gemäß P.8.2 oder die Löschung gemäß P.8.3 von unrichtigen personenbezogenen Daten im Hinblick auf die Zwecke ihrer Verarbeitung unverzüglich ermöglicht. Die Umsetzung muss regelmäßig (mindestens jährlich) sowie anlassbezogen überprüft und bewertet werden.

Der Kunde (als Verantwortlicher) muss die Umsetzung dieses Grundsatzes bzw. dieser Anforderung nachweisen („Rechenschaftspflicht“).

Verweis DSGVO

Art. 5 Abs. 1 lit. d DSGVO

Art. 5 Abs. 2 DSGVO

Nachweise

Darlegung des Sachverhalts zur Umsetzung inkl. Benennung der technischen und organisatorischen Maßnahmen mit Begründung

Verfahrens-, Prozessbeschreibungen

Zurverfügungstellung der Applikation

Beschreibungen zur Applikation zur Darlegung der Umsetzung der Anforderung (etwa Funktionsbeschreibung, Schnittstellenbeschreibung)

Beschreibung zur Bestimmung des Umfangs, in dem die Datenqualität validiert werden können

Beschreibung der Implementierung der Verfahren

Anwendbarkeit lt. SOA

Verpflichtend für Verantwortliche

Zielobjektkategorie

VV

PRZ

APPL

4.2.6. P.2.6 Speicherbegrenzung

Anforderung

Der Kunde (als Verantwortlicher) muss für den Verarbeitungsvorgang (VV) sowie die Prozesse (PRZ) bzw. die Applikationen (APPL) sicherstellen, dass die Identifizierung der betroffenen Personen nur so lange möglich ist, wie es für die Zwecke, für die die personenbezogenen Daten verarbeitet werden, erforderlich ist, und die Speicherdauer auf das erforderliche Minimum begrenzen. Die Umsetzung muss regelmäßig (mindestens jährlich) sowie anlassbezogen überprüft und bewertet werden.

Eine Ausnahme gilt für personenbezogene Daten, die ausschließlich für im öffentlichen Interesse liegende Archivzwecke oder für wissenschaftliche und historische Forschungszwecke oder für statistische Zwecke gem. Art. 89 Abs. 1 DSGVO verarbeitet werden, sofern geeignete technische und organisatorische Maßnahmen getroffen wurden.

Der Verantwortliche muss die Speicherdauer und Löschverfahren unter Beachtung der rechtlichen Anforderungen, der Natur, des Kontexts und der Zwecke der Datenverarbeitung und branchenspezifischen best practice mit Relevanz für die Speicherdauer definieren. Für Auftragsverarbeiter ergibt sich die Speicherdauer aus dem Vertrag über die Auftragsverarbeitung und den Weisungen des Verantwortlichen.

Der Kunde (als Verantwortlicher) muss die Umsetzung dieses Grundsatzes bzw. dieser Anforderung nachweisen („Rechenschaftspflicht").

Verweis DSGVO

Art. 5 Abs. 1 lit. e DSGVO

Art. 5 Abs. 2 DSGVO

Nachweise

Darlegung des Sachverhalts zur Umsetzung inkl. Benennung der technischen und organisatorischen Maßnahmen mit Begründung

Verfahrens-, Prozessbeschreibungen

Zurverfügungstellung der Applikation

Beschreibungen zur Applikation zur Darlegung der Umsetzung der Anforderung (etwa Funktionsbeschreibung, Schnittstellenbeschreibung)

Löschkonzept

Verzeichnis der Verarbeitungstätigkeiten

Anwendbarkeit lt. SOA

Verpflichtend für Verantwortliche

Zielobjektkategorie

VV

PRZ

APPL

4.2.7. P.2.7 Treu und Glauben

Anforderung

Der Kunde (als Verantwortlicher) muss für den Verarbeitungsvorgang (VV) sowie die Prozesse (PRZ) bzw. die Applikationen (APPL) sicherstellen, dass personenbezogene Daten nach Treu und Glauben verarbeitet werden („Verarbeitung nach Treu und Glauben").

Treu und Glauben – in der englischen Fassung der DSGVO „fairly" oder „fairness" – meint beispielsweise ein anständiges Verhalten und eine gerechte, ehrliche Haltung anderen gegenüber. Ein Verstoß gegen „Treu und Glauben" kann als Verstoß gegen das allgemeine Gerechtigkeitsgefühl verstanden werden.

Es ist eine Interessenswertung durchzuführen und nachzuweisen, welche analysiert, ob eine Datenverarbeitung insbesondere redlich, vertrauenswürdig, rücksichtsvoll und anständig erfolgt. Die Datenverarbeitung darf entsprechend des international anerkannten Rechtsprinzips nicht rechtsmissbräuchlich sein, sie darf nicht in sich widersprüchlich sein und sie darf nicht arglistig erfolgen.

Der Kunde (als Verantwortlicher) muss die Umsetzung dieses Grundsatzes bzw. dieser Anforderung nachweisen („Rechenschaftspflicht").

Verweis DSGVO

Art. 5 Abs. 1 lit. a DSGVO

Art. 5 Abs. 2 DSGVO

Nachweise

Darlegung des Sachverhalts zur Umsetzung inkl. Benennung der technischen und organisatorischen Maßnahmen mit Begründung

Verfahrens-, Prozessbeschreibungen

Zurverfügungstellung der Applikation

Beschreibungen zur Applikation zur Darlegung der Umsetzung der Anforderung (etwa Funktionsbeschreibung, Schnittstellenbeschreibung)

Anwendbarkeit lt. SOA

Verpflichtend für Verantwortliche

Zielobjektkategorie

VV

PRZ

APPL

4.3. P.3 Pflichten des Kunden

4.3.1. P.3.1 Informationspflichten des Kunden

Anforderung

Der Kunde (als Verantwortlicher bzw. Auftragsverarbeiter) muss die Prozesse (PRZ) bzw. die Applikationen (APPL) so gestalten, dass die betroffene Person in präziser, transparenter, verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache über die Verarbeitung personenbezogener Daten informiert wird (z. B. in Kombination mit standardisierten Icons).

Sofern die Erhebung von personenbezogenen Daten bei der betroffenen Person erfolgt, muss der Kunde (als Verantwortlicher) die folgenden Informationen zum Zeitpunkt der Erhebung der Daten mitteilen:

- den Namen und die Kontaktdaten des Verantwortlichen und, wo einschlägig, der Vertreter des Verantwortlichen;
- Kontaktdaten des Datenschutzbeauftragten, sofern ein solcher bestellt wurde;
- die Zwecke der Datenverarbeitung;
- Rechtsgrundlage für die Datenverarbeitung;
- berechtigtes Interesse des Verantwortlichen, wenn die Verarbeitung auf die Rechtsgrundlage gem. P.1.5 gestützt wird;
- sofern Daten an Dritte übermittelt werden: die Empfänger oder Kategorien von Empfängern, hier zu berücksichtigen, dass Behörden keine „Empfänger" sind, wenn sie im Rahmen eines bestimmten Untersuchungsauftrags nach nationalem Recht Daten erhalten;
- Übermittlung in ein Drittland, sofern personenbezogene Daten in Drittländer übermittelt werden;
- Vorhandensein / Fehlen eines Angemessenheitsbeschlusses / geeignete Garantien und eine Möglichkeit diese einzusehen, sofern personenbezogene Daten in Drittländer übermittelt werden;
- Dauer der Datenverarbeitung oder, falls dies nicht möglich ist, die Kriterien für die Festlegung dieser Dauer;
- Bestehen eines Rechts auf Auskunft, Berichtigung oder Löschung, Einschränkung der Verarbeitung, Widerspruchsrechts, Recht auf Datenübertragbarkeit;
- Bestehen eines Rechts, Einwilligungen jederzeit zu widerrufen;
- Bestehen eines Beschwerderechts bei einer Aufsichtsbehörde;
- verpflichtende oder freiwillige Bereitstellung der personenbezogenen Daten, ob die Bereitstellung der personenbezogenen Daten gesetzlich oder vertraglich vorgeschrieben oder für einen Vertragsabschluss erforderlich ist und welche möglichen Folgen die Nichtbereitstellung hätte;
- Bestehen einer automatisierten Entscheidungsfindung einschließlich Profiling (Informationen über die involvierte Logik, Tragweite und angestrebte Auswirkungen);
- Im Falle einer Weiterverarbeitung für andere Zwecke: neben diesen anderen Zwecken alle anderen oben genannten Informationen hinsichtlich der Weiterverarbeitung der betroffenen personenbezogenen Daten für andere Zwecke.

Sofern die Erhebung von personenbezogenen Daten nicht bei der betroffenen Person erfolgt, muss der Kunde (als Verantwortlicher) die folgenden Informationen unter Berücksichtigung der spezifischen Umstände der Verarbeitung innerhalb einer angemessenen Frist nach Erlangung der personenbezogenen Daten, längstens jedoch innerhalb eines Monats zum Zeitpunkt der ersten Mitteilung an die betroffene Person erteilen, wenn die personenbezogenen Daten zu diesem Zweck verwendet werden oder wenn die Offenlegung an einen anderen Empfänger beabsichtigt ist spätestens zum Zeitpunkt der ersten Offenlegung die Information erteilen, sofern sich gem. Art. 14 Abs. 5 DSGVO nichts Abweichendes ergibt:

- Namen und der Kontaktdaten des Verantwortlichen, sowie gegebenenfalls seines Vertreters;

- Kontaktdaten des Datenschutzbeauftragten;
- Zwecke der Datenverarbeitung;
- Rechtsgrundlage der Datenverarbeitung;
- Kategorien verarbeiteter personenbezogener Daten;
- Empfänger oder Kategorien von Empfängern der personenbezogenen Daten;
- Absicht des Verantwortlichen, personenbezogene Daten an ein Drittland oder internationale Organisation zu übermitteln, sowie das Vorhandensein oder Fehlen eines Angemessenheitsbeschlusses der Kommission; einen Verweis auf die geeigneten oder angemessenen Garantien und die Möglichkeit, wie eine Kopie von ihnen zu erhalten ist, oder wo diese verfügbar sind;
- Speicherdauer;
- berechtigte Interessen, sofern die Verarbeitung auf Art. 6 Abs. 1 UAbs. 1 lit. f DSGVO beruht;
- Information über das Bestehen des Rechts auf Auskunft, Berichtigung, Einschränkung der Verarbeitung, Widerspruchs gegen die Verarbeitung und des Rechts auf Datenübertragbarkeit;
- Bestehen eines Rechts, Einwilligungen jederzeit zu widerrufen;
- Bestehen eines Beschwerderechts bei einer Aufsichtsbehörde;
- die Quelle, aus der die personenbezogenen Daten stammen, und gegebenenfalls, ob sie aus öffentlich zugänglichen Quellen stammen;
- Bestehen einer automatisierten Entscheidungsfindung einschließlich Profiling und – zumindest in diesen Fällen – aussagekräftige Informationen über die involvierte Logik, sowie die Tragweite und die angestrebten Auswirkungen einer derartigen Verarbeitung für die betroffene Person;
- Im Falle einer Weiterverarbeitung für andere Zwecke: neben diesen anderen Zwecken alle anderen oben genannten Informationen hinsichtlich der Weiterverarbeitung der betroffenen personenbezogenen Daten für andere Zwecke.

Der Kunde (als Verantwortlicher) muss die Information mittels der am meisten angemessenen Modalität und am meisten angemessenen Formats unter Beachtung des genutzten Gerätes, der Natur der Benutzeroberfläche / Interaktionen mit dem Verantwortlichen („User Journey“) übermitteln.

Der Kunde (als Verantwortlicher) muss den Betroffenen dazu eindeutig identifizieren, es sei denn:

- dies ist nicht erforderlich, da die betroffene Person bereits über die Information verfügt, oder
- die Bereitstellung dieser Information ist nicht möglich oder würde einen unverhältnismäßig hohen Aufwand erfordern, insb. für im öffentlichen Interesse liegende Archivzwecke, für wissenschaftliche oder historische Forschungszwecke oder für statistische Zwecke unter Beachtung der Voraussetzungen und Schutzmaßnahmen gem. Art. 89 Abs. 1 DSGVO, oder
- wenn die Bereitstellung der Informationen die Verwirklichung der Ziele dieser Verarbeitung wahrscheinlich unmöglich macht oder ernsthaft beeinträchtigt, soweit

der Kunde (als Verantwortlicher) geeignete Maßnahmen zum Schutz der Rechte und Freiheiten sowie der berechtigten Interessen der betroffenen Person ergreift, einschließlich der Veröffentlichung der Informationen;

- die Einholung oder Weitergabe ausdrücklich durch das Unionsrecht oder das einschlägige Recht der Mitgliedstaaten vorgesehen ist, dem der Kunde (als Verantwortlicher) unterliegt und das geeignete Maßnahmen zum Schutz der berechtigten Interessen der betroffenen Person vorsieht, oder
- wenn die personenbezogenen Daten aufgrund einer durch das Unionsrecht oder das einschlägige Recht der Mitgliedstaaten geregelten Verpflichtung zur Wahrung des Berufsgeheimnisses, einschließlich einer gesetzlichen Geheimhaltungspflicht, vertraulich bleiben müssen.

Die Informationen können individuell an den Betroffenen bereitgestellt werden, ohne diesen zu identifizieren, wenn die Information öffentlich verfügbar gemacht wird, üblicherweise in einer digitalen Umgebung, und der Verantwortliche betroffene Personen aktiv zu der Quelle der Informationen leitet.

Der Kunde (als Verantwortlicher) muss die Information schriftlich oder elektronisch bereitstellen, eine mündliche Information darf nur abgegeben werden, sofern die betroffene Person dies verlangt und die Identität der betroffenen Person in anderer Form nachgewiesen wurde.

Der Kunde (als Auftragsverarbeiter) muss den Verantwortlichen bei der Einhaltung der Informationspflicht unterstützen. Unterliegt der Auftragsverarbeiter der speziellen Weisung des Verantwortlichen zur Wahrnehmung dieser Informationspflichten oder löst eine ihm übertragene Tätigkeit eine Informationspflicht aus, so handelt es sich um eine eigene Pflicht des Auftragsverarbeiters, die Information entsprechend mitzuteilen. Bei Änderungen der Datenverarbeitung mit Relevanz für die Informationspflicht des Verantwortlichen muss der Auftragsverarbeiter diesem diese Informationen rechtzeitig zur Verfügung stellen.

Verweis DSGVO

Art. 12 Abs. 1, 5, 7 DSGVO

Art. 13 DSGVO

Art. 14 DSGVO

Nachweise

Darlegung des Sachverhalts mit Begründung

Dokumente, in denen die Informationen je nach Art des Verarbeitungsvorgangs zur Verfügung gestellt werden, z. B. Datenschutzerklärungen, Impressum, Leitfäden, Informationsblätter oder Hinweisschilder, Nachweise zur Begründung von Ausnahmen

Verfahrens-, Prozessbeschreibungen

Zurverfügungstellung der Applikation

Beschreibungen zur Applikation zur Darlegung der Umsetzung der Anforderung (etwa Funktionsbeschreibung, Schnittstellenbeschreibung)

Anwendbarkeit lt. SOA

Verpflichtend für Verantwortliche und Auftragsverarbeiter

Zielobjektkategorie

PRZ

APPL

4.4. P.4 Auftragsverarbeitung

4.4.1. P.4.1 Vertrag zur Auftragsverarbeitung (AV-Vertrag)

Anforderung

Vertrag zwischen Verantwortlichen und Auftragsverarbeitern

Der Kunde (als Verantwortlicher) muss ein Datenschutz-Managementsystem (DSMS) aufrechterhalten, um sicherzustellen, dass für jeden Dienstleister oder externen Dritten (DL), der personenbezogene Daten im Auftrag verarbeitet, ein Vertrag zur Auftragsverarbeitung (AV-Vertrag zwischen Verantwortlichen und Auftragsverarbeitern) im Sinne des Art. 28 Abs. 3 DSGVO oder ein anderes Rechtsinstrument im Zusammenhang mit der erbrachten Dienstleistung abgeschlossen wird. Dieser AV-Vertrag sollte typischerweise Bestandteil des zugrundeliegenden Vertragsverhältnisses (z. B. Dienstleistungsvertrag) sein.

Vertrag zwischen Auftragsverarbeitern und Verantwortlichen

Der Kunde (als Auftragsverarbeiter), der sich auf P.1.10 als Rechtsgrundlage stützt, muss ein Datenschutz-Managementsystem (DSMS) aufrechterhalten, um sicherzustellen, dass für jeden Verantwortlichen, für den er personenbezogene Daten im Auftrag verarbeitet, ein Vertrag zur Auftragsverarbeitung (AV-Vertrag zwischen Verantwortlichen und Auftragsverarbeitern) im Sinne des Art. 28 Abs. 3 DSGVO oder ein anderes Rechtsinstrument im Zusammenhang mit der erbrachten Dienstleistung abgeschlossen wird. Dieser AV-Vertrag sollte typischerweise Bestandteil des zugrundeliegenden Vertragsverhältnisses (z. B. Dienstleistungsvertrag) sein.

Vertrag zwischen Auftragsverarbeitern und Sub-Auftragsverarbeitern

Der Kunde (als Auftragsverarbeiter), der als Grundlage P.1.10 angeführt hat, muss ein Datenschutz-Managementsystem (DSMS) aufrechterhalten, um sicherzustellen, dass für jeden Dienstleister oder externen Dritten (DL), der personenbezogene Daten im Auftrag verarbeitet, ein Vertrag zur Auftragsverarbeitung oder ein anderes Rechtsinstrument (AV-Vertrag zwischen Auftragsverarbeitern und Sub-Auftragsverarbeitern) im Sinne des Art. 28 Abs. 4 DSGVO im Zusammenhang mit der erbrachten Dienstleistung abgeschlossen wird. Dieser AV-Vertrag sollte typischerweise Bestandteil des zugrundeliegenden Vertragsverhältnisses (z. B. Dienstleistungsvertrag) sein.

Vertrag

Der AV-Vertrag zwischen Verantwortlichen und Auftragsverarbeitern oder zwischen Auftragsverarbeitern und Sub-Auftragsverarbeitern muss in Textform oder einem

elektronischen Format als lesbare Erklärung auf einem dauerhaften Medium erfolgen und muss die folgenden Elemente beinhalten:

- Gegenstand und Dauer der Verarbeitung aller Datenverarbeitungen im Hauptvertrag, sofern bestehend;
- Art und Zweck der Verarbeitung von Daten im Auftrag;
- vollständige Aufführung aller Arten der personenbezogenen Daten;
- die Kategorien betroffener Personen;
- die Rechte und Pflichten des Verantwortlichen;
- die getroffenen erforderlichen technischen und organisatorischen Maßnahmen, um ein angemessenes Level an Sicherheit für die Rechte und Freiheiten der Betroffenen i.S.d. Art. 32 DSGVO unter Beachtung von Art, Umfang, Kontext und Zweck der Datenverarbeitung zu bewirken (siehe auch P.5.1 Festlegung geeigneter Maßnahmen);
- ob die Datenverarbeitung innerhalb der EU / des EWR erfolgt oder in welchen Drittstaaten die personenbezogenen Daten auf dokumentierte Weisung des Verantwortlichen verarbeitet werden,
  - insbesondere, wo diese gespeichert werden;
  - bei Änderung des Verarbeitungsortes, muss dieses unverzüglich der betroffenen Person mitgeteilt werden. Der betroffenen Person muss ein Kündigungsrecht eingeräumt werden, sofern der Auftragsverarbeiter von seinen Angaben abweicht.
- weitere eingesetzte Subunternehmen (Auftragsverarbeiter) inklusive Name, Adresse und ausgeführter Tätigkeit, wobei
  - der Auftragsverarbeiter sicherstellen muss, dass ein Unterauftragnehmer nur dann eingesetzt werden darf, sofern der Verantwortliche vorher gesondert oder allgemein in Schrift- oder Textform eingewilligt hat;
  - wo eine pauschale Zustimmung zu weiteren Subunternehmen im Vertrag vereinbart wird, muss der Vertrag ein Recht des Verantwortlichen oder des Auftragsverarbeiters der Einbindung weiterer Subunternehmen zu widersprechen beinhalten und Anforderungen an einen solchen Widerruf, Mitteilungsfristen sowie Folgen des Widerrufs regeln;
  - Unterauftragnehmer als Auftragsverarbeiter eingeschätzt werden, so dass damit die Anforderungen an Auftragsverarbeiter für jeden weiteren Unterauftragsnehmer gelten;
- die Pflicht des Auftragsverarbeiters, personenbezogene Daten ausschließlich auf dokumentierter Weisung des Kunden (als Verantwortlicher bzw. Auftragsverarbeiter) zu verarbeiten, inkl. hinsichtlich Übermittlungen personenbezogener Daten in Drittstaaten oder an internationale Organisationen, es sei denn, es besteht eine rechtliche Anforderung aus dem Recht der EU oder dem einschlägigen Recht der Mitgliedsstaaten, dem der Auftragsverarbeiter oder Subauftragsverarbeiter gem. Art. 28 Abs. 3 DSGVO unterliegt. In diesem Fall muss der Auftragsverarbeiter oder Subauftragsverarbeiter den Kunden (als Verantwortlicher oder

Auftragsverarbeiter) über diese gesetzliche Anforderung informieren, es sei denn, die gesetzliche Anforderung verbietet dies aus wichtigen öffentlichen Interessen;

- Pflichten des Auftragsverarbeiters zur Unterstützung des Verantwortlichen: Der Auftragsverarbeiter muss danach den Verantwortlichen wie folgt unterstützen:
  - bei der Sicherheit der Verarbeitung gem. Art. 32 DSGVO;
  - bei einer Benachrichtigung der zuständigen Aufsichtsbehörde von einer Verletzung des Schutzes personenbezogener Daten betroffenen Personen gem. Art. 33 DSGVO;
  - bei einer Meldung von Verletzungen an die betroffenen Personen gem. Art. 34 DSGVO;
  - bei einer Datenschutz-Folgenabschätzung gem. Art. 35 DSGVO;
  - bei einer vorherigen Konsultation gem. Art. 36 DSGVO;
  - der Auftragsverarbeiter muss den Verantwortlichen unverzüglich informieren, falls er der Auffassung sein sollte, dass die Datenverarbeitung gegen Vorgaben verstößt bzw. rechtswidrig ist;
- Rückgabe oder Löschung aller personenbezogenen Daten nach Beendigung der Vertragslaufzeit an den Verantwortlichen;
- Auditierung der Umsetzung durch den Auftragsverarbeiter, sowie das Recht zur Auditierung durch den Verantwortlichen;
  - dazu gewährt der Auftragsverarbeiter dem Verantwortlichen das Recht, Überprüfungen selber durchzuführen oder einen Prüfer mit der Überprüfung zu beauftragen, siehe auch P.7.1;
  - der Auftragsverarbeiter stellt dem Verantwortlichen Informationen zum Nachweis der Einhaltung der Pflichten zur Verfügung.

Verweis DSGVO

Art. 28 Abs. 2, 3, 4, 6 und 9 DSVGO

Nachweise

Verfahrens-, Prozessbeschreibungen

Vorliegende Verträge

Richtlinien (Vorgaben) für den Einsatz von anderen Mustern als das eigene Vertragsmuster

Anwendbarkeit lt. SOA

Für Verantwortliche gilt für dieses optionale Anforderungselement: verpflichtend, sofern der Verantwortliche Auftragsverarbeiter einsetzt

Verpflichtend für Auftragsverarbeiter

Zielobjektkategorie

DSMS

DL

4.4.2. P.4.2 Umsetzung der Maßnahmen gem. AV-Vertrag

Anforderung

Der Kunde (als Auftragsverarbeiter[3]) muss nachweisen, dass die getroffenen Maßnahmen konform zu den Anforderungen der DSGVO sind; insbesondere bezüglich:

- Maßnahmen zur Regelung zur Weisungsbefugnis hinsichtlich der Erteilung oder des Erhalts von Weisungen;
- der Verpflichtung zur Verschwiegenheit der mit der Verarbeitung der personenbezogenen Daten befugten Personen;
- den getroffenen erforderlichen technischen und organisatorischen Maßnahmen, um ein angemessenes Level an Sicherheit für die Rechte und Freiheiten der Betroffenen i.S.d. Art. 32 DSGVO unter Beachtung von Art, Umfang, Kontext und Zweck der Datenverarbeitung;
- dem Ort der Datenverarbeitung, s. auch P.7.1 Datenübermittlung in Drittstaaten;
- den involvierten Subunternehmen sowie Regeln zur Änderung dieser Subunternehmen;
- der Umsetzung der Unterstützungspflichten;
- der Rückgabe und Löschung;
- dem Auditrecht.

Der Kunde (als Auftragsverarbeiter) muss die Prozesse (PRZ) so gestalten, dass er für die Auftragsverarbeitung die im AV-Vertrag getroffenen Regelungen fortlaufend umsetzt.

Der Kunde (als Auftragsverarbeiter) muss über Prozesse (PRZ) zur Implementierung zusätzlicher Anforderungen, die sich aus nationalem Recht ergeben, die über die DSGVO-Regelungen hinausgehen, verfügen.

Verweis DSGVO

Art. 28 Abs. 2, 3, 4 und 5 DSGVO

Nachweise

Verfahrens-, Prozessbeschreibungen

Interne Regelungen und Vorgaben

Dokumentierte Maßnahmen (organisatorisch und technisch)

[3] Dieses Kriterium bezieht sich auf den Auftragsverarbeiter als Kunde der Zertifizierungsstelle. Dieser Kunde wird sich aus seiner Sicht immer als Auftragsverarbeiter betrachten, auch wenn er unter Umständen aus dem Blickwinkel seines Verantwortlichen einen Unterauftragsverarbeiter darstellen könnte, sofern dieser selbst als Auftragsverarbeiter agiert. Da dem Kunden die vertragliche Beziehung zum Verantwortlichen die einzige Referenz ist, hat er ggf. keine Kenntnis über seine Einordnung als Subauftragsverarbeiter. Aus diesem Grund bezieht sich der Begriff „Auftragsverarbeiter" in diesem Kriterium auf Auftragsverarbeiter, unabhängig von weiteren vertraglichen Beziehungen des für die Verarbeitung Verantwortlichen, die keine Auswirkungen auf diese Zertifizierung haben.

Anwendbarkeit lt. SOA

Verpflichtend für Auftragsverarbeiter

Nicht anwendbar für Verantwortliche

Zielobjektkategorie

PRZ

4.4.3. P.4.3 Audit

Anforderung

Der Kunde (als Verantwortlicher bzw. Auftragsverarbeiter) muss ein Datenschutz-Managementsystem (DSMS) aufrechterhalten, um sicherzustellen, dass nur Auftragsverarbeiter eingesetzt werden, die hinreichende Garantien hinsichtlich Fachwissen, Verlässlichkeit und Ressourcen mit der Auftragsverarbeitung betraut werden und jeder eingesetzte Auftragsverarbeiter vor Beginn und sodann regelmäßig – mindestens jährlich –, sowie anlassbezogen unter Beachtung eines risikobasierten Ansatzes kontrolliert wird.

Dazu muss eine Auditplanung vorliegen, aus der insbesondere hervorgeht, wann welche Auftragsverarbeiter in welchem Umfang wie geprüft werden. Die Tiefe des Audits muss unter Beachtung des Risikos durch den jeweiligen Auftragsverarbeiter oder Subauftragsverarbeiter erfolgen.

Ferner müssen anlassbezogene Kontrollen durchgeführt werden, etwa bei relevanten Änderungen der Rechtslage oder gravierenden Datenschutzverstößen beim Auftragsverarbeiter.

Es müssen dokumentierte Lieferantenkontrollen für externe Dritte (DL) vorliegen.

Verweis DSGVO

Art. 28 Abs. 3 S. 2 lit. h DSGVO

Anforderung der Programmeignerin i.V.m. Art. 32 Abs. 1 DSGVO und Art. 28 Abs. 1 DSGVO

Nachweise

Verfahrens-, Prozessbeschreibungen

Auditplanung und vorliegende Auditberichte und Zertifikate

Vorgaben zur Regelung von Audits

Anwendbarkeit lt. SOA

Für Verantwortliche gilt für dieses optionale Anforderungselement: verpflichtend, sofern der Verantwortliche Auftragsverarbeiter einsetzt

Verpflichtend für Auftragsverarbeiter

Zielobjektkategorie

DSMS

DL

4.5. P.5 Technisch-organisatorische Maßnahmen

4.5.1. P.5.1 Festlegung geeigneter Maßnahmen

Anforderung

Der Kunde (Verantwortlicher bzw. Auftragsverarbeiter) muss ein Datenschutz-Managementsystem (DSMS) aufrechterhalten, um sicherzustellen, dass zunächst geeignete technische und organisatorische Maßnahmen definiert werden, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten, und sodann diese festgelegten Maßnahmen umsetzen werden.

Zur Festlegung dieser geeigneten technisch-organisatorischen Maßnahmen muss der Kunde eine Analyse der Datenverarbeitung insgesamt mit allen Zielobjekten durchführen. Diese Analyse soll sich am Stand der Technik und der Implementierungskosten orientieren und den konkreten Verarbeitungsvorgang hinsichtlich seiner Art, Kontext und Zwecken der Verarbeitung sowie die unterschiedlichen Eintrittswahrscheinlichkeiten sowie die Auswirkungen (Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen) berücksichtigen, ohne den Datenschutz zu kompromittieren. Der Kunde (als Auftragsverarbeiter) muss die Art der Verarbeitung im Auftrag bei der Bestimmung der angemessenen Maßnahmen berücksichtigen, s. auch P.4.1 Vertrag zur Auftragsverarbeitung (AV-Vertrag). Die Analyse zur Festlegung geeigneter Maßnahmen muss insbesondere die Risiken der Vernichtung, den Verlust, die Veränderung oder die unbefugte Offenlegung von bzw. den unbefugten Zugang zu personenbezogenen Daten berücksichtigen, welche übermittelt, gespeichert oder auf andere Weise verarbeitet werden.

Die Analyse zur Festlegung geeigneter Maßnahmen muss nachvollziehbar, korrekt und dokumentiert vorliegen und regelmäßig – mindestens jährlich – sowie anlassbezogen aktualisiert werden, vgl. dazu auch die nachfolgenden Anforderungselemente:

- physische Infrastruktur (INFRA) mit Standorten und Räumen;
- IT-Infrastruktur (IT) mit Servern, Clients, Netzkomponenten, Datenbanken, Speichersystemen und Schnittstellen;
- Applikationen (APPL), über die der Datenverarbeitung realisiert wird;
- externe Dritte (DL), z. B. Dienstleister, Auftragsverarbeiter, Behörden, Schwestergesellschaften oder Holding, die für die Realisierung der Datenverarbeitung benötigt werden oder an die personenbezogene Daten übermittelt werden, sofern relevant.

Die Bewertung muss einem strukturierten Ansatz unter Nutzung einer anerkannten Bewertungsmethode folgen, mit folgenden Grundsätzen:

- Definition der Kategorien von Datenschutz-Anforderungen: mindestens drei Levels sind festzulegen:
  - „medium“;

    - „hoch“;
    - „sehr hoch“.
- Für Assets zur Verarbeitung personenbezogener Daten ist mindestens das Level „hoch“ festzulegen.
- Bestimmung der potenziellen Folgen und der realistischen Wahrscheinlichkeit des Eintretens von Ereignissen.
- Angemessene Behandlungsoptionen:
    - Durchführung von Maßnahmen zur Risikominderung oder -begrenzung
    - Eingrenzung/Änderung des Anwendungsbereichs.
- Die folgenden Optionen sind nicht akzeptabel:
    - Übertrag der Risiken (z. B. auf Versicherungen) und;
    - Akzeptanz von Restrisiken, weitere Maßnahmen sind möglich unter den vorher beschrieben Voraussetzungen.
- Ergebnisse der Bewertung, die reproduzierbar, gültig und vergleichbar sind.

Das Ergebnis der Analyse muss eine klare Aussage zu Maßnahmen für mindestens die folgenden technischen und organisatorischen Themen treffen:

- P.5.2 Zutrittskontrolle (Vertraulichkeit und Integrität auf Ebene der physischen Zutritte), vgl. P.5.2;
- P.5.3 Zugangskontrolle (Vertraulichkeit und Integrität auf Ebene der Systemzugänge), vgl. P.5.3;
- P.5.4 Zugriffskontrolle (Vertraulichkeit und Integrität auf Ebene der Anwendungszugriffe), vgl. P.5.4;
- P.5.5 Transportkontrolle (Vertraulichkeit und Integrität auf Transport-Ebene), vgl. P.5.5;
- Trennungskontrolle, vgl. P.5.6 Trennungskontrolle;
- Eingabekontrolle, vgl. P.5.7 Eingabekontrolle;
- Verfügbarkeitskontrolle, vgl. P.5.8 Verfügbarkeitskontrolle;
- Pseudonymisierungs / Anonymisierung, vgl. P.5.9 Pseudonymisierung / Anonymisierung.

Zur Klarstellung: Diese Bewertung zur Festlegung geeigneter Maßnahmen im Rahmen dieses Kriteriums geht weit über eine IT-Risikoanalyse hinaus: Der Schwerpunkt dieser Bewertung liegt auf dem Datenschutz sowie den Rechten und Freiheiten der betroffenen Personen.

Zudem ist diese Analyse zur Festlegung geeigneter Maßnahmen gem. Art. 32 DSGVO nicht die Datenschutz-Folgenabschätzung i.S.d. Art. 35 DSGVO: Für Verarbeitungen, bei denen die Datenverarbeitung ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen birgt, muss neben dieser Bewertung zusätzlich auch eine Datenschutz-Folgenabschätzung (DSFA) durchgeführt werden, siehe P.6.5.

Verweis DSGVO

Art. 24 Abs. 1 DSGVO

Art. 24 Abs. 2 DSGVO

Art. 25 Abs. 1 DSGVO

Art. 32 Abs. 1 DSGVO

Art. 32 Abs. 2 DSGVO

Art. 28 Abs. 3 lit. c) DSGVO

Nachweise

Verfahrens-, Prozessbeschreibungen zur Durchführung der Analyse

Analyse mit Beschreibung der definierten Maßnahmen

Anwendbarkeit lt. SOA

Verpflichtend für Verantwortlicher und Auftragsverarbeiter

Zielobjektkategorie

DSMS

4.5.2. P.5.2 Zutrittskontrolle (Vertraulichkeit und Integrität auf Ebene der physischen Zutritte)

Anforderung

Der Kunde (Verantwortlicher bzw. Auftragsverarbeiter) muss im Hinblick auf die physische Infrastruktur (INFRA) mit Standorten und Räumen eine geeignete Zutrittskontrolle umsetzen, um zu gewährleisten, dass sich keine unbefugten Personen Zutritt zu Datenverarbeitungsanlagen verschaffen und auf personenbezogene Daten einwirken können. Die Zutrittskontrolle verfolgt das Ziel, die Vertraulichkeit und Integrität der personenbezogenen Daten auf der Ebene der physischen Zutritte zu gewährleisten.

Die definierten Maßnahmen zur Zutrittskontrolle müssen sich aus der Analyse zur Festlegung geeigneter Maßnahmen gem. P.5.1 ergeben und dokumentiert vorliegen.

Es müssen mindestens die folgenden Maßnahmen umgesetzt sein:

- Sicherheitsbereiche müssen durch eine angemessene Zutrittssteuerung und Zutrittsstellen geschützt werden. Die physische Sicherheit von Büros, Räumen und Einrichtungen muss konzipiert und umgesetzt werden. Es ist ein Rollenkonzept zu erstellen.
- Der Schutz vor physischen und umweltbedingten Bedrohungen wie Naturkatastrophen und anderen absichtlichen oder unabsichtlichen physischen Bedrohungen der Infrastruktur muss geplant und umgesetzt werden.
- Es müssen klare Regeln für eine aufgeräumte Arbeitsumgebung hinsichtlich Unterlagen und Wechseldatenträgern und klare Regeln für Bildschirmsperren für

informationsverarbeitende Einrichtungen festgelegt und angemessen durchgesetzt werden.

- Es müssen Sicherheitsmaßnahmen ergriffen werden, wenn Mitarbeiter aus der Ferne arbeiten, um Informationen zu schützen, die außerhalb der Räumlichkeiten des Unternehmens abgerufen, verarbeitet oder gespeichert werden.

Verweis DSGVO

Art. 5 Abs. 1 lit. f DSGVO

Art. 32 Abs. 1 lit. a DSGVO

Art. 32 Abs. 1 lit. b DSGVO

Nachweise

Beschreibung der implementierten Maßnahmen

Beschreibung der internen Verfahrens-, Prozessbeschreibungen

Rechte- und Rollenkonzept

Spezifikationen und Konzepte für Zutrittssysteme

Anwendbarkeit lt. SOA

Verpflichtend für Verantwortlicher und Auftragsverarbeiter

Zielobjektkategorie

INFRA

4.5.3. P.5.3 Zugangskontrolle (Vertraulichkeit und Integrität auf Ebene der Systemzugänge)

Anforderung

Der Kunde (Verantwortlicher bzw. Auftragsverarbeiter) muss im Hinblick auf die IT-Infrastruktur (IT) eine geeignete Zugangskontrolle umsetzen, um zu gewährleisten, dass Unbefugte keinen Zugang zu (personen)datenverarbeitenden Anlagen erhalten und somit Schäden anrichten können. Die Zugangskontrolle verfolgt das Ziel, die Vertraulichkeit und Integrität der personenbezogenen Daten auf der Ebene der logischen Systemzugänge zu gewährleisten.

Die definierten Maßnahmen zur Zugangskontrolle müssen sich aus der Analyse zur Festlegung geeigneter Maßnahmen gem. P.5.1 ergeben und dokumentiert vorliegen.

Es müssen mindestens die folgenden Maßnahmen umgesetzt sein:

- Es muss ein Rollenkonzept implementiert sein.
- Regeln zur Kontrolle des logischen Zugriffs (auf Systemebene) sind auf der Grundlage von Geschäfts- und Informationssicherheitsanforderungen festzulegen und umzusetzen. Der gesamte Lebenszyklus von Identitäten ist zu verwalten.

- Zugriffsrechte (auf Systemebene) sind in Übereinstimmung mit den themenspezifischen Richtlinien und Regeln der Organisation für die Zugangskontrolle zu vergeben, überprüfen, ändern und entfernen.
- Informationen, die auf Endpunktgeräten der Benutzer gespeichert sind, von ihnen verarbeitet werden oder über sie zugänglich sind, müssen geschützt werden.
- Zuteilung und Gebrauch von privilegierten Zugangsrechten müssen eingeschränkt und verwaltet werden.
- Der Zugang und anderen damit verbundenen Werten muss in Übereinstimmung mit der festgelegten themenspezifischen Richtlinie zur Zugangssteuerung eingeschränkt werden.
- Sichere Authentisierungstechnologien und -verfahren müssen auf der Grundlage von Informationszugangsbeschränkungen und der themenspezifischen Richtlinie zur Zugangssteuerung.
- Netzwerke und Netzwerkgeräte müssen gesichert, verwaltet und kontrolliert werden, um Informationen in Systemen und Anwendungen zu schützen. Sicherheitsmechanismen, Dienstgüte und Dienstanforderungen für Netzwerkdienste müssen ermittelt, umgesetzt und überwacht werden. Informationsdienste, Benutzer und Informationssysteme müssen in Netzwerken der Organisation gruppenweise voneinander getrennt gehalten werden.

Verweis DSGVO

Art. 5 Abs. 1 lit. f DSGVO

Art. 32 Abs. 1 lit. a DSGVO

Art. 32 Abs. 1 lit. b DSGVO

Nachweise

Beschreibung der implementierten Maßnahmen

Netzwerkpläne

Rechte- und Rollenkonzept

Einsichtnahme in Konfigurationen und Berechtigungen (Rollenkonzept)

Beschreibung der Verfahrens-, Prozessbeschreibungen

Beschreibung von kryptographischen Algorithmen

Anwendbarkeit lt. SOA

Verpflichtend für Verantwortlicher und Auftragsverarbeiter

Zielobjektkategorie

IT

4.5.4. P.5.4 Zugriffskontrolle (Vertraulichkeit und Integrität auf Ebene der Anwendungszugriffe)

Anforderung

Der Kunde (Verantwortlicher bzw. Auftragsverarbeiter) muss im Hinblick auf die Applikationen (APPL) eine geeignete Zugriffskontrolle umsetzen, um zu gewährleisten, dass die zur Datenverarbeitung berechtigten Personen jeweils nur auf die Daten zugreifen können, für die sie berechtigt sind. Die Zugriffskontrolle verfolgt das Ziel, die Vertraulichkeit und Integrität der personenbezogenen Daten auf der Ebene der logischen Anwendungszugriffe zu gewährleisten.

Die definierten Maßnahmen zur Zugriffskontrolle müssen sich aus der Analyse zur Festlegung geeigneter Maßnahmen gem. P.5.1 ergeben und dokumentiert vorliegen.

Es müssen mindestens die folgenden Maßnahmen umgesetzt sein:

- Es muss ein Rollenkonzept implementiert sein.
- Regeln zur Steuerung des physischen und logischen Zugriffs (auf Anwendungsebene) auf Informationen und andere damit verbundene Werte müssen auf der Grundlage von Geschäfts- und Informationssicherheitsanforderungen aufgestellt und umgesetzt werden.
- Zugriffsrechte (auf Anwendungsebene) zu Informationen und anderen damit verbundenen Werten müssen in Übereinstimmung mit der themenspezifischen Richtlinie und den Regeln der Organisation für die Zugangssteuerung bereitgestellt, überprüft, geändert und entfernt werden.
- Zuteilung und Gebrauch von privilegierten Zugriffsrechten müssen eingeschränkt und verwaltet werden.
- Der Zugriff und anderen damit verbundenen Werten muss in Übereinstimmung mit der festgelegten themenspezifischen Richtlinie zur Zugangssteuerung eingeschränkt werden.
- Sichere Authentisierungstechnologien und -verfahren müssen auf der Grundlage von Informationszugangsbeschränkungen und der themenspezifischen Richtlinie zur Zugangssteuerung.

Verweis DSGVO

Art. 5 Abs. 1 lit. f DSGVO

Art. 32 Abs. 1 lit. a DSGVO

Art. 32 Abs. 1 lit. b DSGVO

Nachweise

Beschreibung der implementierten Maßnahmen

Rechte- und Rollenkonzept

Einsichtnahme in Konfigurationen und Berechtigungen (Rollenkonzept)

Beschreibung der Verfahrens-, Prozessbeschreibungen

Beschreibungen zur Applikation zur Darlegung der Umsetzung der Anforderung (etwa Funktionsbeschreibung, Schnittstellenbeschreibung)

Logs und Logkontrollen

Beschreibungen zu Maßnahmen zur Sanktionierung von unberechtigtem Zugriff

Beschreibung von kryptographischen Algorithmen

Anwendbarkeit lt. SOA

Verpflichtend für Verantwortlicher und Auftragsverarbeiter

Zielobjektkategorie

APPL

4.5.5. P.5.5 Transportkontrolle (Vertraulichkeit und Integrität auf Transport-Ebene)

Anforderung

Der Kunde (Verantwortlicher bzw. Auftragsverarbeiter) muss im Hinblick auf die IT-Infrastruktur (IT) und die Applikationen (APPL) eine geeignete Transportkontrolle umsetzen, um zu gewährleisten, dass bei der Übermittlung personenbezogener Daten diese nicht verändert oder eingesehen werden können. Die Transportkontrolle verfolgt das Ziel, die Vertraulichkeit und Integrität der personenbezogenen Daten auf der Transportebene zu gewährleisten.

Die definierten Maßnahmen zur Transportkontrolle müssen sich aus der Analyse zur Festlegung geeigneter Maßnahmen gem. P.5.1 ergeben und dokumentiert vorliegen.

Es müssen mindestens die folgenden Maßnahmen umgesetzt sein:

- Für alle Arten von Übermittlungseinrichtungen innerhalb der Organisation des Kunden und zwischen der Organisation des Kunden und anderen Parteien müssen Regeln, Verfahren oder Vereinbarungen zur Informationsübermittlung vorhanden sein.
- Es müssen Regeln für den wirksamen Einsatz von Kryptographie, einschließlich der Verwaltung kryptographischer Schlüssel, festgelegt und umgesetzt werden.
- Die kryptographischen Algorithmen und Parameter müssen dem aktuellen Stand der Technik entsprechen; die Eignung ist in offiziellen Listen oder Dokumenten anzugeben.

Verweis DSGVO

Art. 5 Abs. 1 lit. f DSGVO

Art. 32 Abs. 1 lit. a DSGVO

Art. 32 Abs. 1 lit. b DSGVO

Nachweise

Beschreibung der implementierten Maßnahmen

Beschreibung der Verfahrens-, Prozessbeschreibungen

Netzwerkpläne

Einsichtnahme in Konfigurationen und Berechtigungen

Zurverfügungstellung der Applikation

Beschreibungen zur Applikation zur Darlegung der Umsetzung der Anforderung (etwa Funktionsbeschreibung, Schnittstellenbeschreibung)

Beschreibung von kryptographischen Algorithmen

Anwendbarkeit lt. SOA

Verpflichtend für Verantwortlicher und Auftragsverarbeiter

Zielobjektkategorie

IT

APPL

4.5.6. P.5.6 Trennungskontrolle

Anforderung

Der Kunde (Verantwortlicher bzw. Auftragsverarbeiter) muss im Hinblick auf die IT-Infrastruktur (IT) und die Applikationen (APPL) eine geeignete Trennungskontrolle umsetzen, um zu gewährleisten, dass Daten, die zu unterschiedlichen Zwecken erhoben wurden, getrennt verarbeitet werden.

Die definierten Maßnahmen zur Trennungskontrolle müssen sich aus der Analyse zur Festlegung geeigneter Maßnahmen gem. P.5.1 ergeben und dokumentiert vorliegen.

Es müssen mindestens die folgenden Maßnahmen umgesetzt sein:

- Sich widersprechende Aufgaben und Verantwortungsbereiche müssen getrennt werden.

Verweis DSGVO

Art. 25 Abs. 1 DSGVO

Nachweise

Beschreibung der implementierten Maßnahmen

Beschreibung der Verfahrens-, Prozessbeschreibungen

Netzwerkpläne

Einsichtnahme in Konfigurationen und Berechtigungen

Zurverfügungstellung der Applikation

Beschreibungen zur Applikation zur Darlegung der Umsetzung der Anforderung (etwa Funktionsbeschreibung, Schnittstellenbeschreibung)

Anwendbarkeit lt. SOA

Verpflichtend für Verantwortlicher und Auftragsverarbeiter

Zielobjektkategorie

IT

APPL

4.5.7. P.5.7 Eingabekontrolle

Anforderung

Der Kunde (Verantwortlicher bzw. Auftragsverarbeiter) muss im Hinblick auf die IT-Infrastruktur (IT) und die Applikationen (APPL) eine geeignete Eingabekontrolle umsetzen, um zu gewährleisten, dass nachträglich überprüft und festgestellt werden kann, welche personenbezogenen Daten zu welcher Zeit von wem eingegeben oder verändert worden sind. Die Eingabekontrolle ist in Einklang mit den Rechten der Beschäftigten umzusetzen.

Die definierten Maßnahmen zur Eingabekontrolle müssen sich aus der Analyse zur Festlegung geeigneter Maßnahmen gem. P.5.1 ergeben und dokumentiert vorliegen.

Es müssen mindestens die folgenden Maßnahmen umgesetzt sein:

- Aufzeichnungen müssen vor Verlust, Zerstörung, Fälschung, unbefugtem Zugriff und unbefugter Veröffentlichung geschützt sein.
- Protokolle, die Aktivitäten, Ausnahmen, Fehler und andere relevante Ereignisse aufzeichnen, müssen erstellt, gespeichert, geschützt und analysiert werden.

Verweis DSGVO

Art. 25 Abs. 1 DSGVO

Nachweise

Beschreibung der implementierten Maßnahmen

Beschreibung der Verfahrens-, Prozessbeschreibungen

Netzwerkpläne

Einsichtnahme in Konfigurationen und Berechtigungen

Zurverfügungstellung der Applikation

Beschreibungen zur Applikation zur Darlegung der Umsetzung der Anforderung (etwa Funktionsbeschreibung, Schnittstellenbeschreibung)

Datenschutzkonzept (mit Bezug auf Beschäftigte)

Anwendbarkeit lt. SOA

Verpflichtend für Verantwortlicher und Auftragsverarbeiter

Zielobjektkategorie

IT

APPL

4.5.8. P.5.8 Verfügbarkeitskontrolle

Anforderung

Der Kunde (Verantwortlicher bzw. Auftragsverarbeiter) muss im Hinblick auf die physische Infrastruktur (INFRA) mit Standorten und Räumen, die IT-Infrastruktur (IT), sowie die Applikationen (APPL) eine geeignete Verfügbarkeitskontrolle umsetzen, um zu gewährleisten, dass alle datenverarbeitenden Systeme und sich darauf befindende personenbezogene Daten hinreichend verfügbar und belastbar sind.

Die definierten Maßnahmen zur Verfügbarkeitskontrolle müssen sich aus der Analyse zur Festlegung geeigneter Maßnahmen gem. P.5.1 ergeben und dokumentiert vorliegen.

Es müssen mindestens die folgenden Maßnahmen umgesetzt sein:

- Die Nutzung von Ressourcen muss überwacht und entsprechend den aktuellen und erwarteten Kapazitätsanforderungen angepasst werden.
- Schutz gegen Schadsoftware muss umgesetzt und durch angemessene Sensibilisierung der Benutzer unterstützt werden.
- Konfigurationen, einschließlich Sicherheitskonfigurationen, von Hardware, Software, Diensten und Netzwerken müssen festgelegt, dokumentiert, umgesetzt, überwacht und überprüft werden.
- Kabel, die Strom, Daten oder unterstützende Informationsdienste transportieren, müssen vor Abhören, Störung oder Beschädigung geschützt werden.
- Geräte und Betriebsmittel müssen ordnungsgemäß gewartet werden, um die Verfügbarkeit, Integrität und Vertraulichkeit der Informationen sicherzustellen.
- Sicherungskopien von Informationen, Software und Systemen müssen in Übereinstimmung mit der vereinbarten themenspezifischen Richtlinie zu Datensicherungen aufbewahrt und regelmäßig geprüft werden.
- Informationsverarbeitende Einrichtungen müssen mit ausreichender Redundanz für die Einhaltung der Verfügbarkeitsanforderungen.
- Netzwerke, Systeme und Anwendungen müssen auf anormales Verhalten überwacht und geeignete Maßnahmen müssen ergriffen werden, um potentielle Informationssicherheitsvorfälle zu bewerten.
- Es müssen Informationen über technische Schwachstellen verwendeter Informationssysteme eingeholt, die Gefährdung der Organisation durch derartige Schwachstellen bewertet und angemessene Maßnahmen ergriffen werden.

- Maßnahmen zur Verhinderung von Datenlecks müssen auf Systeme, Netzwerke und alle anderen Geräte angewendet werden, die sensible Informationen verarbeiten, speichern oder übermitteln.
- Die Organisation muss die Handhabung von Informationssicherheitsvorfällen planen und vorbereiten, indem sie Prozesse, Rollen und Verantwortlichkeiten für die Handhabung von Informationssicherheitsvorfällen definiert, einführt und kommuniziert.
- Die Organisation muss Informationssicherheitsereignisse beurteilen und entscheiden, ob sie als Informationssicherheitsvorfälle eingestuft werden müssen.
- Auf Informationssicherheitsvorfälle muss entsprechend den dokumentierten Verfahren reagiert werden.
- Die Organisation muss planen, wie die Informationssicherheit während einer Störung auf einem angemessenen Niveau gehalten werden kann. Die IKT-Bereitschaft muss auf der Grundlage von Business-Continuity- Zielen und IKT-Kontinuitätsanforderungen geplant, umgesetzt, aufrechterhalten und geprüft werden.

Verweis DSGVO

Art. 32 Abs. 1 lit. b DSGVO

Nachweise

Beschreibung der implementierten Maßnahmen

Beschreibung der Verfahrens-, Prozessbeschreibungen

Netzwerkpläne

Anwendbarkeit lt. SOA

Verpflichtend für Verantwortlicher und Auftragsverarbeiter

Zielobjektkategorie

INFRA

IT

APPL

4.5.9. P.5.9 Pseudonymisierung / Anonymisierung

Anforderung

Der Kunde (Verantwortlicher bzw. Auftragsverarbeiter) muss im Hinblick auf die Applikationen (APPL) eine geeignete Pseudonymisierung und / oder Anonymisierung umsetzen.

„Pseudonymisierung“ bedeutet, dass personenbezogene Daten ohne Hinzuziehung weiterer Informationen nicht mehr zugeordnet werden können. Demgegenüber zielt eine „Anonymisierung“ darauf ab, den Personenbezug aufzuheben. Die bei der

Pseudonymisierung entstehenden zusätzlichen Informationen zur Re-Identifizierung der Person müssen gesondert aufbewahrt werden.

Der Kunde (als Verantwortlicher oder Auftragsverarbeiter) muss ein Datenschutz-Managementsystem (DSMS) aufrechterhalten und ein Konzept für Pseudonymisierung und Anonymisierung vorlegen, das mindestens Folgendes beinhaltet:

- Berücksichtigung des Risikos des Wegfalls einer Pseudonymisierung / Anonymisierung durch Anreicherung;
- Prozess für die regelmäßige Überwachung der kontinuierlichen Effektivität der eingesetzten Algorithmen;
- Prozess zum Umgang mit dem Auftreten von Ineffektivität;
- Erklärung, ob Anonymisierung überhaupt möglich ist;

Hinweis: Maßnahmen der Verschlüsselung sind in den Kriterien P.5.2 Zutrittskontrolle (Vertraulichkeit und Integrität auf Ebene der physischen Zutritte), P.5.3 Zugangskontrolle (Vertraulichkeit und Integrität auf Ebene der Systemzugänge), P.5.4 Zugriffskontrolle (Vertraulichkeit und Integrität auf Ebene der Anwendungszugriffe), P.5.5 Transportkontrolle (Vertraulichkeit und Integrität auf Transport-Ebene) integriert.

Die definierten Maßnahmen zur Pseudonymisierung/Anonymisierung müssen sich aus der Analyse zur Festlegung geeigneter Maßnahmen gem. P.5.1 Festlegung geeigneter Maßnahmen ergeben und dokumentiert vorliegen.

Verweis DSGVO

Art. 32 Abs. 1 lit. a DSGVO

Nachweise

Beschreibung der implementierten Maßnahmen

Beschreibung der Verfahrens-, Prozessbeschreibungen

Darlegung Sachverhalt mit Begründung

Zurverfügungstellung der Applikation

Beschreibungen zur Applikation zur Darlegung der Umsetzung der Anforderung (etwa Funktionsbeschreibung, Schnittstellenbeschreibung)

Konzept für Pseudonymisierung und Anonymisierung

Anwendbarkeit lt. SOA

Verpflichtend für Verantwortlicher und Auftragsverarbeiter

Zielobjektkategorie

APPL

PRZ

4.5.10. P.5.10 Überprüfung, Bewertung und Evaluierung (Rechenschaftspflicht)

Anforderung

Der Kunde (Verantwortlicher bzw. Auftragsverarbeiter) muss ein Datenschutz-Managementsystem (DSMS) aufrechterhalten, über das sichergestellt ist, dass die Eignung und Wirksamkeit der umgesetzten technischen und organisatorischen Maßnahmen regelmäßig – mindestens jährlich – sowie anlassbezogen unter Anwendung eines risikobasierten Ansatzes überprüft, bewertet und evaluiert werden; dabei muss die Analyse zur Festlegung geeigneter Maßnahmen gem. P.5.1 Festlegung geeigneter Maßnahmen berücksichtigt werden. Diese Überprüfung trägt zur Erfüllung der Rechenschaftspflicht bei.

Überprüfung, Bewertung und Evaluierung erfolgen

- gem. einer strukturierten Methodik,
- geplant und dokumentiert sowie
- durch kompetente, unabhängige und unparteiliche Personen.

Die Überprüfung, Bewertung und Evaluierung, sowie der Umgang mit Abweichungen müssen dokumentiert werden. Etwaige Abweichungen müssen analysiert und korrigiert werden.

Der Auftragsverarbeiter muss dem Verantwortlichen Informationen zum Nachweis der Einhaltung der Vorgaben zur Verfügung stellen.

Verweis DSGVO

Art. 5 Abs. 2 DSGVO

Art. 24 Abs. 3 DSGVO

Art. 32 Abs. 1 lit. d DSGVO

Art. 32 Abs. 3 DSGVO

Nachweise

Verfahrens-, Prozessbeschreibungen

Vorliegende Berichte

Anwendbarkeit lt. SOA

Verpflichtend für Verantwortlicher und Auftragsverarbeiter

Zielobjektkategorie

DSMS

4.6. P.6 Datenschutz-Management

4.6.1. P.6.1 Fortlaufende Datenschutz-Kontinuität

Anforderung

Der Kunde (Verantwortlicher bzw. Auftragsverarbeiter) muss ein Datenschutz-Managementsystem (DSMS) etabliert haben und aufrechterhalten, um insbesondere die fortlaufende Datenschutz-Kontinuität und -Konformität sicherzustellen.

Das Datenschutz-Managementsystem (DSMS) folgt einer strukturierten Methodik mit PDCA-Zyklus („Plan-Do-Check-Act", „Planen-Umsetzen-Überprüfen-Handeln"). Über die etablierten Prozesse des DSMS muss sichergestellt sein, dass

- die Angaben zur Scope-Beschreibung gem. Kapitel 3.1 sowie
- die Angaben zum Statement of Applicability (SOA) gem. Kapitel 3.2

fortlaufend korrekt, aktuell zutreffend sind. Dies meint insbesondere, dass über die etablierten Prozesse des DSMS sichergestellt ist, dass die Einschätzung zur Anwendbarkeit optionaler Anforderungselemente fortlaufend zutreffend ist:

- die Rechtsgrundlage der Datenverarbeitung der Kriterien P.1 zur Zulässigkeit der Datenverarbeitung, vgl. Frage 1 in Kapitel 3.2.1;
- die Anwendbarkeit der Kriterien P.4 bei Inanspruchnahme einer Auftragsverarbeitung, vgl. Frage 3 in Kapitel 3.2.2;
- die Anwendbarkeit des Kriteriums P.6.2 zur Pflicht der Bestellung eines Datenschutzbeauftragten, vgl. Frage 4 in Kapitel 3.2.3;
- die Anwendbarkeit des Kriteriums P.6.4 zur Pflicht eines Verzeichnisses von Verarbeitungstätigkeiten, vgl. Frage 5 in Kapitel 3.2.4;
- die Anwendbarkeit des Kriteriums P.6.5 zur Pflicht der Durchführung einer Datenschutz-Folgenabschätzung, vgl. Frage 6 in Kapitel 3.2.5;
- die Anwendbarkeit der Kriterien P.7 bei einer Datenverarbeitung außerhalb der EU, vgl. Frage 7 in Kapitel 3.2.6;
- die Anwendbarkeit des Kriteriums P.8.9 zu automatisierten Entscheidungen / Profiling, vgl. Frage 8 in Kapitel 3.2.7.

Es muss eine regelmäßige – mindestens jährliche – sowie anlassbezogene Überprüfung von

- Scope-Beschreibung gem. Kapitel 3.1;
- Statement of Applicability gem. Kapitel 3.2;
- Realisierungsbeschreibung gem. Kapitel 3.3;
- Privacy-by-Design (Datenschutz durch Technikgestaltung) gem. Kapitel 4.2.1;
- Privacy-by-Default (Datenschutzfreundliche Voreinstellungen) gem. Kapitel 4.2.2;
- Festlegung geeigneter Maßnahmen gem. Kapitel 4.5.1;
- Datenschutz-Folgenabschätzung gem. Kapitel 4.6.5

durchgeführt werden.

Erfolgt eine Datenübermittlung in Drittstaaten – unter Anwendung des Kriteriums P.7.1 – auf Grundlage eines Angemessenheitsbeschlusses der EU-Kommission, muss eine regelmäßige Überprüfung des Vorliegens dieses Angemessenheitsbeschlusses für das betreffende Land und daraus resultierende Folgen erfolgen.

Es muss ein kontinuierlicher Verbesserungsprozess (KVP) inkl. Ursachenanalyse bei Auftreten von Abweichungen etabliert sein.

Verweis DSGVO

Art. 32 Abs. 1 lit. d i.V. m. Art. 5 Abs. 2 DSGVO

Art. 24 Abs. 1 und 2 DSGVO

Anforderung der Programmeignerin zur Methodik des vorliegenden Zertifizierungsstandards

Anforderungen der Datenschutzaufsichtsbehörden: „Anforderungen an datenschutzrechtliche Zertifizierungsprogramme", Kapitel 3

Nachweise

Verfahrens-, Prozessbeschreibungen

Richtlinien

Beschreibung der Organisationsstruktur

Dokumentation der Evaluation der Prozesse, z.B. Bericht des internen Audits und der Management-Bewertung

Dokumentation des kontinuierlichen Verbesserungsprozesses

Anwendbarkeit lt. SOA

Verpflichtend für Verantwortliche und Auftragsverarbeiter

Zielobjektkategorie

DSMS

4.6.2. P.6.2 Datenschutzbeauftragter

Anforderung

Der Kunde (Verantwortlicher bzw. Auftragsverarbeiter) muss im Rahmen des Datenschutz-Managementsystems (DSMS) einen Datenschutzbeauftragten (DSB) bestellen, sofern eine Pflicht dazu besteht.

In folgenden Fällen ist die Bestellung eines DSB erforderlich:

- die Datenverarbeitung wird von einer Behörde oder öffentlichen Stelle durchgeführt, mit Ausnahme von Gerichten, die im Rahmen ihrer justiziellen Tätigkeit handeln;
- die Kerntätigkeit des Verantwortlichen oder des Auftragsverarbeiters besteht in der Durchführung von Verarbeitungsvorgängen, welche aufgrund ihrer Art, ihres

Umfangs und / oder ihrer Zwecke eine umfangreiche regelmäßige und systematische Überwachung von betroffenen Personen erforderlich machen;

- die Kerntätigkeit des Verantwortlichen oder des Auftragsverarbeiters besteht in der umfangreichen Verarbeitung besonderer Kategorien von Daten gem. Art. 9 DSGVO oder von personenbezogenen Daten über strafrechtliche Verurteilungen und Straftaten gem. Art. 10 DSGVO.

Der DSB muss auf Grundlage seiner beruflichen Qualifikation und seines Fachwissens, das er auf dem Gebiet des Datenschutzrechts und der Datenschutzpraxis besitzt, sowie seiner Fähigkeit, die Aufgaben gem. Art. 39 DSGVO zu erfüllen, ausgewählt werden.

Der DSB muss formal bestellt sein; eine Bestellungsurkunde muss vorliegen.

Der DSB muss die erforderlichen Ressourcen erhalten inklusive

- materielle Ressourcen, wie Beschäftigte,
- Unterstützung und Information aus anderen Abteilungen,
- Fortbildungsmöglichkeiten, um die erforderliche Fachkunde auf Stand zu halten,
- Zugang zu Informationen hinsichtlich der Verarbeitungstätigkeiten,
- Ausrüstung, wie geeignete Räumlichkeiten, IT-Ausrüstung, Kommunikationsmedien, Software,
- finanzielle Mittel, wie Reisekosten,
- wenn erforderlich, Beratung von extern, etwa Anwälten oder IT-Experten,
- sowie Zugang zu personenbezogenen Daten und Verarbeitungstätigkeiten des Kunden.

Der Kunde (als Verantwortlicher und Auftragsverarbeiter) muss sicherstellen, dass der DSB ordentlich und zeitnah in alle Themen, die mit dem Datenschutz zusammenhängen, einbezogen wird.

Der Verantwortliche bzw. der Auftragsverarbeiter muss die Kontaktdaten des DSB veröffentlichen und diese der Aufsichtsbehörde mitteilen.

Der Kunde (als Verantwortlicher und Auftragsverarbeiter) muss sicherstellen, dass der DSB als Kontaktstelle gegenüber den folgenden Personen und Stellen agieren kann:

- Betroffene hinsichtlich aller Fragen mit Bezug zur Verarbeitung ihrer personenbezogenen Daten und der Ausübung ihrer Rechte;
- Aufsichtsbehörden zu Themen hinsichtlich der Verarbeitung, inklusive vorheriger Konsultation gem. Art. 36 DSGVO und zu beraten, wo angemessen, mit Bezug zu jedem Sachverhalt;
- Betroffene Personen, als Beschäftigte des Kunden (als Verantwortlicher oder Auftragsverarbeiter) in Bezug auf alle Fragen zur Verarbeitung ihrer personenbezogenen Daten.

Zusätzlich muss der DSB folgende Aufgaben erhalten und erfüllen können:

- den Kunden und seine Beschäftigten (als Verantwortlicher oder Auftragsverarbeiter) zu informieren;

- die Einhaltung der DSGVO und anderer anwendbarer datenschutzrechtlicher Anforderungen, sowie der Richtlinien des Kunden mit Bezug zum Datenschutz im Unternehmen zu überwachen, inkl. der Zuweisung von Verantwortlichkeiten, Sensibilisierung und Fortbildung des Personals, das mit der Verarbeitung personenbezogener Daten betraut ist sowie datenschutzbezogene Audits;
- Beratung, wo angefragt, hinsichtlich der Durchführung von Datenschutzfolgenabschätzungen und deren Durchführung gemäß Art. 35 DSGVO zu überwachen;
- Zusammenarbeit mit den Aufsichtsbehörden;
- Die Durchführung der eigenen Aufgaben unter Beachtung des Risikos durch die Datenverarbeitung unter Beachtung von Art, Kontext und Zwecke der Verarbeitung.

Der DSB darf aufgrund seiner Tätigkeit nicht benachteiligt oder aufgrund seiner Tätigkeit abberufen werden. Die besondere Schutzbedürftigkeit des DSB muss auch bei Kündigungen besonders berücksichtigt werden. Bei der Bestellung von externen und internen DSB, insbesondere im Hinblick auf deren Schutzwürdigkeit, müssen die besonderen Anforderungen aus dem relevanten nationalen Recht der Mitgliedsstaaten berücksichtigt werden.

Der DSB muss unmittelbar an die höchste Managementebene des Verantwortlichen bzw. Auftragsverarbeiters berichten, und darf bei der Erfüllung seiner Aufgaben keinen Weisungen unterliegen.

Der DSB muss auf die Wahrung der Vertraulichkeit verpflichtet sein oder nach EU- oder nationalem Recht der Mitgliedsstaaten der Geheimhaltung unterliegen.

Andere Aufgaben des DSB dürfen nicht zu Interessenskonflikten führen. Die Unabhängigkeit des DSB wird i.d.R. angenommen, wenn dieser weder ein Teil der Geschäftsführung oder der IT-Sicherheitsbeauftragte ist, noch Hinweise zu Interessenkonflikten oder Weisungen, die einer unabhängigen Ausübung der Tätigkeit widersprechen, vorliegen bzw. erkennbar sind.

Verweis DSGVO

Art. 37 DSGVO

Art. 38 DSGVO

Art. 39 DSGVO

Nachweise

Verfahrens-, Prozessbeschreibungen

Bestellungsurkunde

Nachweis für die Meldung bei der Aufsichtsbehörde

Fachkundenachweise

Darlegung der verfügbaren Ressourcen, die dem DSB zur Verfügung gestellt werden

Beschreibung der Aufgaben und Verantwortlichkeiten

Nachweis, dass kein Interessenkonflikt besteht

Nachweis für die Bekanntmachung des DSB innerhalb der Organisation

Anwendbarkeit lt. SOA

Für Verantwortliche und Auftragsverarbeiter gilt für dieses optionale Anforderungselement: verpflichtend, sofern eine gesetzliche Pflicht zur Bestellung eines DSB besteht

Zielobjektkategorie

DSMS

4.6.3. P.6.3 Verpflichtung auf Vertraulichkeit / Schulungen

Anforderung

Der Kunde (Verantwortlicher bzw. Auftragsverarbeiter) muss ein Datenschutz-Managementsystem (DSMS) aufrechterhalten, so dass insbesondere sichergestellt ist, dass die natürlichen Personen personenbezogene Daten nur auf Anweisung verarbeiten, sofern sie nicht nach dem Recht der Union oder dem relevanten Recht der Mitgliedstaaten zur Verarbeitung verpflichtet sind. Wo einschlägig müssen strengere Anforderungen beachtet werden hinsichtlich der Verarbeitung von besonderen Kategorien personenbezogener Daten, siehe P.1.8 Verarbeitung bei besonderen Kategorien personenbezogener Daten.

Mitarbeiter müssen vor Aufnahme der Tätigkeiten und sodann regelmäßig – mindestens jährlich – sowie nach Bedarf mit den für sie relevanten Bestimmungen zum Datenschutz vertraut gemacht und geschult wurden. Mitarbeiter sind zur Vertraulichkeit sowie zur Einhaltung datenschutzrechtlicher Vorgaben zu verpflichten.

Verweis DSGVO

Art. 28 Abs. 3 S. 2 lit. b DSGVO

Art. 32 Abs. 4 DSGVO

Nachweise

Verfahrens-, Prozessbeschreibungen

Nachweise zu erfolgten Schulungen

Verpflichtungserklärung bzgl. Einhaltung datenschutzrechtlicher Vorgaben

Verpflichtungserklärung bzgl. Vertraulichkeit

Schulungsunterlagen

Teilnahmebescheinigung / Zertifikate

Anwendbarkeit lt. SOA

Verpflichtend für Verantwortliche und Auftragsverarbeiter

Zielobjektkategorie

DSMS

4.6.4. P.6.4 Verzeichnis von Verarbeitungstätigkeiten

Anforderung

Der Kunde (Verantwortlicher bzw. Auftragsverarbeiter) muss für die Verarbeitungsvorgänge (VV) ein „Verzeichnis über die Verarbeitungstätigkeiten“ (VVT) führen, sofern eine Pflicht dazu besteht.

Ein solches Verzeichnis ist stets zu führen. Eine Ausnahme gilt, wenn der Verantwortliche oder Auftragsverarbeiter weniger als 250 Mitarbeiter beschäftigt, es sei denn, die Datenverarbeitung birgt ein hohes Risiko für die Rechte und Freiheiten der betroffenen Personen, die Verarbeitung erfolgt nicht nur gelegentlich oder die Verarbeitung schließt besonderer Datenkategorien ein.

Das Verzeichnis von Verarbeitungstätigkeiten (VVT) des Verantwortlichen oder Auftragsverarbeiter, bzw. seines Vertreters, muss mindestens die folgenden Informationen enthalten:

- Namen und Kontaktdaten des Verantwortlichen und seines Vertreters;
- ggf. Namen und Kontaktdaten des Datenschutzbeauftragten;
- Zwecke der Verarbeitung;
- Beschreibung der Kategorien betroffener Personen und Kategorien personenbezogener Daten;
- Kategorien von Empfängern;
- ggf. Übermittlung an Drittländer;
- wenn möglich, Löschfristen pro Datenkategorie;
- wenn möglich, allgemeine Beschreibung der technischen und organisatorischen Maßnahmen;

Das Verzeichnis von Verarbeitungstätigkeiten (VVT) des Auftragsverarbeiters oder seines Vertreters muss mindestens die folgenden Informationen enthalten:

- Namen und Kontaktdaten des Auftragsverarbeiters und seines Vertreters;
- Nennung des Verantwortlichen;
- ggf. Namen und Kontaktdaten des Datenschutzbeauftragten;
- Kategorien der Verarbeitung;
- ggf. Übermittlung an Drittländer;
- Beschreibung der technischen und organisatorischen Maßnahmen.

Das Verzeichnis der Verarbeitungstätigkeiten muss schriftlich oder elektronisch geführt und auf Anfrage der Aufsichtsbehörde zur Verfügung gestellt werden.

Der Kunde (als Verantwortlicher bzw. Auftragsverarbeiter) muss ein Datenschutz-Managementsystem (DSMS) aufrechterhalten, um sicherzustellen, dass das Verzeichnis

der Verarbeitungstätigkeiten aktuell gehalten und regelmäßig (mindestens jährlich) sowie anlassbezogen überprüft wird.

Verweis DSGVO

Art. 30 DSGVO

Nachweise

Verfahrens-, Prozessbeschreibungen

Verzeichnis der Verarbeitungstätigkeiten

Anwendbarkeit lt. SOA

Für Verantwortliche und Auftragsverarbeiter gilt für dieses optionale Anforderungselement: verpflichtend, sofern eine gesetzliche Pflicht zur Führung eines Verzeichnisses der Verarbeitungstätigkeiten besteht.

Zielobjektkategorie

VV

DSMS

4.6.5. P.6.5 Datenschutz-Folgenabschätzung

Anforderung

Der Kunde (Verantwortlicher) muss für diejenigen Verarbeitungsvorgänge (VV) eine Abschätzung der Folgen der vorgesehenen Verarbeitungsvorgänge für den Schutz personenbezogener Daten (Datenschutz-Folgenabschätzung) durchführen, sofern die Datenverarbeitung, bei denen die Art der Verarbeitung insbesondere unter Einsatz neuer Technologien und unter Beachtung von Art, Umfang, Kontext und Zwecke der Verarbeitung mit einem hohen Risiko für die Rechte und Freiheiten natürlicher Personen einhergeht. Diese Abschätzung muss vor der Aufnahme der Verarbeitung stattfinden.

Eine Datenschutz-Folgenabschätzung (DSFA) ist erforderlich, wenn die Datenverarbeitung insbesondere einen der folgenden Aspekte umfasst:

- eine systematische und umfassende Bewertung persönlicher Aspekte natürlicher Personen, mittels automatisierter Verarbeitung oder Profiling;
- besondere Kategorien personenbezogener Daten;
- Daten über strafrechtliche Verurteilungen und Straftaten;
- eine systematische umfangreiche Überwachung öffentlich zugänglicher Bereiche;
- eine Datenverarbeitung, für die eine Aufsichtsbehörde des relevanten Mitgliedsstaates eine DSFA verpflichtet (diese werden durch die Aufsichtsbehörden veröffentlicht, genauso wie eine Liste von Arten von Verarbeitungsvorgängen, für die keine DSFA erforderlich ist).

Kann der Kunde (Verantwortlicher) bei der Feststellung der Notwendigkeit nicht nachweisen, dass nach den hier festgelegten Anforderungen keine DSFA durchzuführen ist, ist eine DSFA durchzuführen.

Die DSFA muss sicherstellen, dass geeignete Maßnahmen entsprechend des Risikos der geplanten Verarbeitungstätigkeiten für den Schutz personenbezogener Daten für den Fall einer Datenschutzverletzung identifiziert und eingesetzt werden, inkl. derer zur Abwehr von Datenschutzverletzungen.

Bei der Durchführung einer DSFA muss der Verantwortliche insbesondere die Ursache, Art, Besonderheit und Schwere sowie das Risiko der Datenverarbeitung evaluieren.

Für den Nachweis, dass durch die Verarbeitung der personenbezogenen Daten das Schutzniveau der DSGVO gewahrt wird, sind beim Ergreifen der entsprechenden Maßnahmen die Ergebnisse der DSFA zu berücksichtigen.

Ergibt die DSFA, dass ein hohes Risiko besteht, wenn keine eindämmenden Maßnahmen ergriffen werden, muss der Verantwortliche vor der Verarbeitung die Aufsichtsbehörde konsultieren; zum Konsultationsverfahren werden die Vorgaben aus Art. 36 DSGVO beachtet. Wenn aufgrund anwendbaren Rechts erforderlich, muss der Kunde (als Verantwortlicher) den Rat und vorherige Zustimmung der Aufsichtsbehörde in Bezug auf die Datenverarbeitung, die der Verantwortliche im öffentlichen Interesse inkl. Sozialschutz oder Öffentliche Gesundheit durchführt, einholen.

Der Datenschutzbeauftragte muss in die Durchführung der DSFA miteinbezogen werden.

Wo angemessen, muss der Kunde (als Verantwortlicher) die Sicht der Betroffenen oder ihrer Vertreter auf die geplante Verarbeitung einholen, unbeschadet des Schutzes kommerzieller oder öffentlicher Interessen oder der Sicherheit der Verarbeitungsvorgänge.

Die DSFA muss einem strukturierten Ansatz mit folgenden Prinzipien folgen:

- eine systematische Beschreibung der geplanten Verarbeitungsvorgänge inkl. der betroffenen Personen und Akteure;
- eine systematische Beschreibung der Zwecke der Verarbeitung, ggf. einschließlich verfolgten berechtigten Interessen des Verantwortlichen;
- eine Bewertung der Notwendigkeit und Verhältnismäßigkeit der Verarbeitungsvorgänge in Bezug auf den Zweck;
- eine Identifikation der Rechtsgrundlagen;
- eine Bewertung der Risiken für die Rechte und Freiheiten der betroffenen Personen unter Bestimmung der Konsequenzen und einer realistischen Einschätzung des Eintrittsrisikos;
- angemessene Handlungsoptionen zur Reduktion oder Abschwächung der Risiken, Übernahme von Restrisiken, Änderung des Anwendungsbereichs;
- Ergebnisse, die reproduzierbar, gültig und vergleichbar sind;
- die zur Bewältigung der Risiken geplanten Abhilfemaßnahmen;

- Garantien, Sicherheitsvorkehrungen und Verfahren, durch die der Schutz personenbezogener Daten sichergestellt wird;
- Garantien, Sicherheitsvorkehrungen und Verfahren, durch die der Nachweis für die Einhaltung der DSGVO erbracht wird.

Die DSFA ist ein zusätzlicher Schritt hinsichtlich der Bewertung zur Definition geeigneter Maßnahmen, vgl. P.5.1 Festlegung geeigneter Maßnahmen.

Die Durchführung und Ergebnisse der DSFA müssen nachweisbar dokumentiert werden und sollten regelmäßig – mindestens jährlich sowie ad hoc, überprüft und erneuert werden.

Der Verantwortliche muss überprüfen und bewerten, ob die Verarbeitung gem. der DSFA und, sofern anwendbar, der Rat der Aufsichtsbehörde vor Einführung der Verarbeitungsvorgänge durchgeführt wird.

Auftragsverarbeiter müssen den Verantwortlichen bei der Durchführung einer DSFA unterstützen.

Verweis DSGVO

Art. 35 DSGVO

Art. 36 DSGVO

Art. 28 DSGVO

Nachweise

Verfahrens-, Prozessbeschreibungen

Datenschutz-Folgenabschätzung / Berichte

Anwendbarkeit lt. SOA

Für Verantwortliche und Auftragsverarbeiter gilt für dieses optionale Anforderungselement: verpflichtend, sofern eine gesetzliche Pflicht zur Durchführung einer Datenschutz-Folgenabschätzung besteht.

Zielobjektkategorie

VV

4.6.6. P.6.6 Meldung von Datenschutzverletzungen

Anforderung

Verantwortlicher

Der Kunde (als Verantwortlicher) muss sicherzustellen, dass geeignete Maßnahmen für den Fall einer Datenschutzverletzung eingesetzt werden. Um dies sicherzustellen, muss er ein Datenschutz-Managementsystem (DSMS) aufrechterhalten. Dies muss Prozesse und Maßnahmen zur Identifizierung von Datenschutzverletzungen und zur Auswertung der potentiellen Risiken für die Rechte und Freiheiten der Betroffenen

aufgrund einer Datenschutzverletzung sowie die Festlegung umfassen, wie bei Datenschutzverletzungen zu verfahren ist (Prozess und Verantwortlichkeiten).

Der Kunde (als Verantwortlicher) muss eine Datenschutzverletzung unverzüglich, spätestens aber binnen 72 Stunden nach Kenntniserhalt, an die zuständige Aufsichtsbehörde melden. Davon ausgenommen sind Verletzung des Schutzes personenbezogener Daten, wenn diese voraussichtlich nicht zu einem Risiko für die Rechte und Freiheiten natürlicher Personen führen. In dem Fall muss der Kunde (als Verantwortlicher) nachweisen, dass die Annahme eines vermutlich nicht bestehenden Risikos begründet ist. Kann die Meldung nicht in dieser Zeit erfolgen, muss die Verzögerung begründet werden. Es sollte eine Identifikation, Analyse, Bewertung der Schutzverletzung und des Risikos für die Rechte und Freiheiten natürlicher Personen vorgenommen werden.

Der Kunde (als Verantwortlicher) muss bei Datenschutzverletzungen mit einem hohen Risiko für die Rechte und Freiheiten der betroffenen Personen, oder wenn die zuständige Behörde dies verlangt, diese Personen unverzüglich benachrichtigen und den betroffenen Personen die Art der Verletzung des Schutzes personenbezogener Daten in klarer und einfacher Sprache beschreiben. Eine Benachrichtigung ist nur im Ausnahmefall entbehrlich, sofern ein in Art. 34 Abs. 3 DSGVO genannter Sachverhalt zutrifft, nämlich wenn:

- der Verantwortliche geeignete technische und organisatorische Sicherheitsvorkehrungen getroffen hat und diese Vorkehrungen auf die von der Verletzung betroffenen personenbezogenen Daten angewandt wurden, insbesondere solche, durch die die personenbezogenen Daten für alle Personen, die nicht zum Zugang zu den personenbezogenen Daten befugt sind, unzugänglich gemacht werden, etwa durch Verschlüsselung;
- der Verantwortliche durch nachfolgende Maßnahmen sichergestellt hat, dass das hohe Risiko für die Rechte und Freiheiten der betroffenen Personen aller Wahrscheinlichkeit nach nicht mehr besteht;
- die Benachrichtigung mit einem unverhältnismäßigen Aufwand verbunden wäre. In diesem Fall hat stattdessen eine öffentliche Bekanntmachung oder eine ähnliche Maßnahme zu erfolgen, durch die die betroffenen Personen vergleichbar wirksam informiert werden.

Die Aufsichtsbehörde muss unverzüglich, spätestens 72 Stunden nach Kenntniserhalt informiert werden.

Die Meldung muss inhaltlich vollständig sein und mindestens folgende Informationen enthalten:

- eine Beschreibung der Art der Verletzung des Schutzes personenbezogener Daten, soweit möglich mit Angabe der Kategorien und der ungefähren Zahl der betroffenen Personen, der betroffenen Kategorien und der ungefähren Zahl der betroffenen personenbezogenen Datensätze;
- den Namen und die Kontaktdaten des Datenschutzbeauftragten oder einer sonstigen Anlaufstelle für weitere Informationen;
- eine Beschreibung der wahrscheinlichen Folgen der Verletzung des Schutzes personenbezogener Daten;

- eine Beschreibung der von dem Verantwortlichen ergriffenen oder vorgeschlagenen Maßnahmen zur Behebung der Verletzung des Schutzes personenbezogener Daten und gegebenenfalls Maßnahmen zur Abmilderung ihrer möglichen nachteiligen Auswirkungen.

Der gesamte Vorgang, inkl. der Beurteilung der Verletzung, Benachrichtigung der zuständigen Aufsichtsbehörde und Kommunikation mit betroffenen Personen, muss dokumentiert werden.

Auftragsverarbeiter

Der Kunde (als Auftragsverarbeiter) muss sicherzustellen, dass geeignete Maßnahmen für den Fall einer Datenschutzverletzung eingesetzt werden. Um dies sicherzustellen, muss er ein Datenschutz-Managementsystem (DSMS) aufrechterhalten. Dies muss u. a. Prozesse und Maßnahmen zur Identifizierung von Datenschutzverletzungen und zur Auswertung der potentiellen Risiken für die Rechte und Freiheiten der Betroffenen aufgrund einer Datenschutzverletzung sowie die Festlegung umfassen, wie bei Datenschutzverletzungen zu verfahren ist (Prozess und Verantwortlichkeiten).

Der Kunde (als Auftragsverarbeiter) muss Datenschutzverletzungen an den Verantwortlichen unverzüglich melden, nachdem er Kenntnis davon erhalten hat.

Der Verantwortliche muss bei Datenschutzverletzungen mit einem hohen Risiko für die Rechte der Betroffenen diese Personen benachrichtigen. Eine Benachrichtigung ist nur im Ausnahmefall entbehrlich, sofern ein in Art. 34 Abs. 3 DSGVO genannter Sachverhalt zutrifft. Die Aufsichtsbehörde muss unverzüglich, spätestens 72 Stunden nach Kenntniserhalt informiert werden.

Der Kunde (als Auftragsverarbeiter) muss Prozesse etablieren, um den Verantwortlichen bei der Erfüllung dieser Pflicht zu unterstützen. Hat der Auftragsverarbeiter Kenntnis von einer Verletzung des Schutzes personenbezogener Daten, so hat er diese dem Verantwortlichen unverzüglich mitzuteilen.

Verweis DSGVO

Art. 33 DSGVO

Art. 34 DSGVO

Nachweise

Verfahrens-, Prozessbeschreibungen

Einsichtnahme in Vorgänge, sofern vorliegend

Vorgaben und Richtlinien

Muster

Anwendbarkeit lt. SOA

Verpflichtend für Verantwortliche und Auftragsverarbeiter

Zielobjektkategorie

DSMS

4.6.7. P.6.7 Zusammenarbeit mit Aufsichtsbehörden

Anforderung

Der Kunde (Verantwortlicher bzw. Auftragsverarbeiter), sofern anwendbar sein Vertreter, muss ein Datenschutz-Managementsystem (DSMS) aufrechterhalten, um insbesondere auf Anfrage mit der Datenschutzaufsichtsbehörde bei der Erfüllung ihrer Aufgaben zusammenzuarbeiten; hierfür muss ein Prozess etabliert sein.

Verweis DSGVO

Art. 31 DSGVO

Nachweise

Verfahrens-, Prozessbeschreibungen

Einsichtnahme in Vorgänge, sofern vorliegend

Anwendbarkeit lt. SOA

Verpflichtend für Verantwortliche und Auftragsverarbeiter

Zielobjektkategorie

DSMS

4.7. P.7 Datenverarbeitung außerhalb der EU

4.7.1. P.7.1 Datenübermittlung in Drittstaaten

Anforderung

Der Kunde (Verantwortlicher bzw. Auftragsverarbeiter) muss für den Verarbeitungsvorgang (VV) sicherstellen, dass die Datenübermittlung (Übermittlungen von Auftragsverarbeitern oder Subauftragsverarbeitern, Wartung und reiner Datentransit eingeschlossen) in ein Drittland zulässig ist. Der Kunde (Verantwortlicher bzw. Auftragsverarbeiter) muss seine Übermittlungen identifizieren. Zulässig ist die Datenübermittlung, wenn eine der folgenden Varianten vorliegt:

- Variante 1: Es liegt ein Angemessenheitsbeschluss der EU-Kommission gem. Art. 45 DSGVO vor, welcher ein angemessenes Schutzniveau für das betreffende Drittland feststellt.
- Variante 2: Der Verantwortliche oder der Auftragsverarbeiter hat geeignete Garantien vorgesehen, welche ein angemessenes Schutzniveau für das betroffene Drittland gewährleisten, und den betroffenen Personen stehen durchsetzbare Rechte und wirksame Rechtsbehelfe zur Verfügung (Art. 46 Abs. 1 DSGVO).

- Variante 3: Es liegt eine der Ausnahmen für bestimmte Fälle gem. Art. 49 S. 1 lit. a-g DSGVO vor:
  - die betroffene Person hat in die vorgeschlagene Datenübermittlung ausdrücklich eingewilligt, nachdem sie über die für sie bestehenden möglichen Risiken derartiger Datenübermittlungen ohne Vorliegen eines Angemessenheitsbeschlusses und ohne geeignete Garantien unterrichtet wurde;
  - die Übermittlung ist für die Erfüllung eines Vertrags zwischen der betroffenen Person und dem Verantwortlichen oder zur Durchführung von vorvertraglichen Maßnahmen auf Antrag der betroffenen Person erforderlich;
  - die Übermittlung ist zum Abschluss oder zur Erfüllung eines im Interesse der betroffenen Person von dem Verantwortlichen mit einer anderen natürlichen oder juristischen Person geschlossenen Vertrags erforderlich;
  - die Übermittlung ist aus wichtigen Gründen des öffentlichen Interesses notwendig;
  - die Übermittlung ist zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen erforderlich;
  - die Übermittlung ist zum Schutz lebenswichtiger Interessen der betroffenen Person oder anderer Personen erforderlich, sofern die betroffene Person aus physischen oder rechtlichen Gründen außerstande ist, ihre Einwilligung zu geben;
  - die Übermittlung erfolgt aus einem Register, das gemäß dem Recht der Union oder der Mitgliedstaaten zur Information der Öffentlichkeit bestimmt ist und entweder der gesamten Öffentlichkeit oder allen Personen, die ein berechtigtes Interesse nachweisen können, zur Einsichtnahme offensteht, aber nur soweit die im Recht der Union oder der Mitgliedstaaten festgelegten Voraussetzungen für die Einsichtnahme im Einzelfall gegeben sind.
- Liegen weder ein Angemessenheitsbeschluss, noch geeignete Garantien vor, ist die Übermittlung personenbezogener Daten in ein Drittland oder an eine internationale Organisation nach Art. 44 DSGVO verboten, es sei denn, der Kunde (als Verantwortlicher oder Auftragsverarbeiter) kann nachweisen, dass eine Ausnahme nach Art. 49 DSGVO vorliegt. Übermittelt der Kunde (als Verantwortlicher oder Auftragsverarbeiter) personenbezogene Daten in ein Drittland aufgrund einer Ausnahme nach Art. 49 DSGVO in ein Drittland, muss er den Ausnahmecharakter einschließlich der Beschränkung nachweisen, dass die Übermittlung nur gelegentlich und nicht wiederholt erfolgt.
- Variante 4: Liegen die Varianten 1-3 nicht vor, erfolgt eine Übermittlung in ein Drittland oder an eine internationale Organisation nur dann, wenn die Übermittlung nicht wiederholt wird und nur eine begrenzte Zahl von Betroffenen betrifft, zur Wahrung zwingender berechtigter Interessen des für die Verarbeitung Verantwortlichen (als Verantwortlicher oder Auftragsverarbeiter) erforderlich ist, sofern dieser nachweisen kann, dass die Interessen oder Rechte und Freiheiten der betroffenen Person nicht überwiegen, und der für die Verarbeitung Verantwortliche alle Umstände im Zusammenhang mit der Datenübermittlung geprüft hat und auf der Grundlage dieser Prüfung geeignete Garantien zum Schutz

personenbezogener Daten vorgesehen hat. Der Kunde (als Verantwortlicher oder Auftragsverarbeiter) unterrichtet die Aufsichtsbehörde über die Übermittlung. Der Kunde (als Verantwortlicher oder Auftragsverarbeiter) informiert zusätzlich zu den in Art. 13 und 14 DSGVO genannten Informationen die betroffene Person über die Übermittlung und die zwingenden berechtigten Interessen.

Der Kunde (Verantwortlicher bzw. Auftragsverarbeiter) muss nachweisen, dass er die Vorgaben des Europäischen Datenschutzausschusses (EDSA) beachtet hat:

- [EDPB_QA-C-311/18];
- [EDPB_01/2020];
- [EDPB _02/2018];
- [EDPB_05_2021].

Der Verantwortliche bzw. der Auftragsverarbeiter muss sicherstellen, dass den betroffenen Personen durchsetzbare Rechte und wirksame Rechtsbehelfe zur Verfügung stehen.

Bei Anwendung eines der Übermittlungsinstrumente des Art. 46 Abs. 2 DSGVO muss der Kunde (als Verantwortliche bzw. Auftragsverarbeiter), wo angemessen in Zusammenarbeit mit dem Importeur im Drittland, eine schriftliche Prüfung der Rechtslage und -Praxis im Drittland durchführen, um sicherzustellen, dass die Rechtslage oder die Praxis in dem jeweiligen Drittland, das durch die geeigneten Garantien, die der Importeur implementiert hat, gewährleistete Schutzniveau nicht beeinträchtigt. Kann eine Beeinträchtigung nicht ausgeschlossen werden, muss der Kunde (als Verantwortlicher bzw. Auftragsverarbeiter) als Exporteur vor der Datenübermittlung in das Drittland zusätzliche ergänzende Maßnahmen ergreifen, die ein gleichwertiges Schutzniveau für das betreffende Drittland gewährleisten. Die zusätzlichen ergänzenden Maßnahmen sind zu dokumentieren. Die Anwendungsfälle in den EDSA-Empfehlungen 01/2020 (Anhang 2) inkl. der dazugehörigen Maßnahmen, die durch den Importeur zu treffen sind, s. RL 07/2022 (Anhang 1), dienen als Orientierung.

Liegen offensichtliche Zweifel an einem sicheren Datentransfer in Drittstaaten vor oder sind allgemein bekannt und / oder eine höchstrichterliche Entscheidung steht in diesem Zusammenhang aus, muss der Kunde (als Verantwortlicher oder Auftragsverarbeiter) als Exporteur dies gesondert in einer Prüfung begutachten.

Erfolgt die Datenübermittlung auf Grundlage eines Angemessenheitsbeschlusses der EU-Kommission, muss der Kunde (als Verantwortlicher bzw. Auftragsverarbeiter) als Exporteur Prozesse zur regelmäßigen Überprüfung des Vorliegens des Angemessenheitsbeschlusses für das betreffende Land und die daraus resultierende Folgen, einschließlich einer Exit Strategie, falls der Angemessenheitsbeschluss zurückgezogen wird, vorhalten, vgl. P.6.2.

Erfolgt die Datenübermittlung auf Grundlage von geeigneten Garantien, die der Kunde (als Verantwortliche bzw. Auftragsverarbeiter) vorsieht, muss gem. Art. 46 Abs. 2 lit. a-f DSGVO eines der folgenden Instrumente eingesetzt werden:

- ein rechtlich bindendes und durchsetzbares Dokument zwischen den Behörden oder öffentlichen Stellen;
- verbindliche interne Datenschutzvorschriften gem. Art. 47 DSGVO;

- Standardvertragsklauseln, die von der EU-Kommission gem. Art. 93 Abs. 2 DSGVO erlassen wurden, oder Standardvertragsklauseln, die von einer Aufsichtsbehörde gem. Art. 93 Abs. 2 DSGVO genehmigt wurden;
- genehmigte Verhaltensregeln gem. Art. 40 DSGVO;
- ein genehmigter Zertifizierungsmechanismus gem. Art. 42 DSGVO;
- Vertragsklauseln oder Bestimmungen in Verwaltungsvereinbarungen zwischen Behörden oder öffentlichen Stellen gem. Art. 46 Abs. 3 DSGVO.

Erfolgt die Datenübermittlung auf Grundlage von geeigneten Garantien unter Berücksichtigung eines rechtlich bindenden und durchsetzbaren Dokuments zwischen den Behörden oder öffentlichen Stellen, so gilt:

- Der Kunde (als Verantwortlicher bzw. Auftragsverarbeiter) ist eine öffentliche Stelle und verfügt über ein rechtlich bindendes und durchsetzbares Dokument zwischen den Behörden oder öffentlichen Stellen, das von der zuständigen Aufsichtsbehörde gem. Art. 63 DSGVO genehmigt wurde.
- Dieses Dokument ist rechtlich bindend für alle betreffenden Behörden oder öffentlichen Stellen.

Erfolgt die Datenübermittlung auf Grundlage von geeigneten Garantien unter Berücksichtigung verbindlicher interner Datenschutzvorschriften, so gilt:

- Der Kunde (als Verantwortlicher bzw. Auftragsverarbeiter) verfügt über verbindliche interne Datenschutzvorschriften, die von der zuständigen Aufsichtsbehörde gem. Art. 63 DSGVO genehmigt wurden.
- Die verbindlichen internen Datenschutzvorschriften sind rechtlich bindend für alle betreffenden Mitglieder einer Unternehmensgruppe oder einer Gruppe von Unternehmen, die eine gemeinsame Wirtschaftstätigkeit ausüben, und gelten auch für deren Beschäftigten.
- Die verbindlichen internen Datenschutzvorschriften übertragen den betroffenen Personen ausdrücklich durchsetzbare Rechte in Bezug auf die Verarbeitung ihrer personenbezogenen Daten.
- Die verbindlichen internen Datenschutzvorschriften genügen den Anforderungen aus Art. 47 Abs. 2 DSGVO.

Erfolgt die Datenübermittlung auf Grundlage von geeigneten Garantien unter Berücksichtigung von Standardvertragsklauseln, so gilt:

- Der Kunde (als Verantwortlicher bzw. Auftragsverarbeiter) hat mit dem Datenimporteur, an welchen die Daten übermittelt werden sollen, die Standardvertragsklauseln abgeschlossen.
- Die Standardvertragsklauseln werden unverändert in der aktuellsten Version übernommen, die Anhänge mit der Beschreibung der Daten gefüllt.
- Andere eventuell hinzugefügte Klauseln oder zusätzliche Schutzklauseln dürfen die Verpflichtungen in den Standardvertragsklauseln nicht untergraben oder negativ beeinflussen oder die Einhaltung der in den Standardvertragsklauseln enthaltenen Verpflichtungen verhindern.

Erfolgt die Datenübermittlung auf Grundlage von geeigneten Garantien unter Berücksichtigung genehmigter Verhaltensregeln, so gilt:

- Der Verantwortliche bzw. Auftragsverarbeiter setzt genehmigte Verhaltensregeln um, die von der zuständigen Aufsichtsbehörde genehmigt wurden und den Anforderungen des Art. 40 DSGVO entsprechen.
- Zusätzlich trifft der Verantwortliche bzw. Auftragsverbeiter rechtsverbindliche und durchsetzbare Verpflichtungen in dem Drittland zur Anwendung der geeigneten Garantien.

Erfolgt die Datenübermittlung auf Grundlage von geeigneten Garantien unter Berücksichtigung genehmigter Zertifizierungsmechanismen, so gilt:

- Der Importeur in dem Drittland verfügt über ein Zertifikat gem. Art. 42 DSGVO.
- Der Kunde (als Verantwortlicher bzw. Auftragsverarbeiter) als Exporteur muss nachweisen, dass verfügt der Importeur in dem Drittland über ein Zertifikat gem. Art. 42 DSGVO verfügt.
- Zusätzlich trifft der Importeur in dem Drittland rechtsverbindliche und durchsetzbare Verpflichtungen in dem Drittland zur Anwendung der geeigneten Garantien.

Erfolgt die Datenübermittlung auf Grundlage von geeigneten Garantien unter Berücksichtigung von Vertragsklauseln oder Bestimmungen in Verwaltungsvereinbarungen zwischen Behörden oder öffentlichen Stellen, so gilt:

- Der Verantwortliche bzw. Auftragsverarbeiter hat mit dem Empfänger der personenbezogenen Daten im Drittland Vertragsklauseln oder Bestimmungen abgeschlossen, die von der zuständigen Aufsichtsbehörde gem. Art. 63 DSGVO genehmigt wurden, die wirksame Rechte für die betroffenen Personen gem. Art 46 Abs. 3 DSGVO einschließen.
- Die Vertragsklauseln oder Bestimmungen sind rechtlich bindend für alle betreffenden Mitglieder.

Geeignete Garantien sind durch den Kunden (als Verantwortlichen bzw. Auftragsverarbeiter) zu dokumentieren. Die Wahl des Übermittlungsinstruments muss im Lichte des Kapitel 5 der DSGVO gerechtfertigt und die spezielle Übermittlung davon umfasst sein.

Urteile von Gerichten oder Entscheidungen von Behörden eines Drittlands, die eine Offenlegungen oder Übermittlungen von personenbezogenen Daten erwirken, dürfen nur anerkannt oder vollstreckt werden, wenn sie auf eine internationale Übereinkunft zwischen dem ersuchenden Drittland und der Union oder dem relevanten Mitgliedstaat gestützt sind.

Der Verantwortliche oder der Auftragsverarbeiter erfasst die von ihm vorgenommene Beurteilung sowie die geeigneten Garantien gemäß Art. 30 DSGVO.

Verweis DSGVO

Art. 44-49 DSGVO

Nachweise

Darlegung Sachverhalt mit Begründung

Einsichtnahme in Vorgänge (Standardvertragsklauseln, Verträge, etc.)

Bewertung der Auswirkungen und Sicherheitsaspekte einer Übermittlung in ein Land außerhalb des EWR, für das die Kommission keine Angemessenheitsfeststellung getroffen hat, durch Verantwortlichen bzw. Auftragsverarbeiter

Nachweis über zusätzliche Maßnahmen

Anwendbarkeit lt. SOA

Für Verantwortliche und Auftragsverarbeiter gilt für dieses optionale Anforderungselement: verpflichtend, sofern eine Datenübermittlung in Drittstaaten erfolgt

Zielobjektkategorie

VV

4.7.2. P.7.2 Vertreter innerhalb der EU

Anforderung

Sofern die Verarbeitung personenbezogener Daten durch einen nicht in der Union niedergelassenen Verantwortlichen erfolgt, muss der Verantwortliche bzw. der Auftragsverarbeiter gem. Art. 27 DSGVO einen Vertreter innerhalb der EU wählen. Dieser Vertreter muss innerhalb einem der Mitgliedsstaaten der EU niedergelassen sein, in denen die Personen befinden, derer personenbezogene Daten verarbeitet werden.

Der Vertreter muss schriftlich bestellt werden.

Der Kunde (als Verantwortlicher bzw. Auftragsverarbeiter) muss sicherstellen, dass der Vertreter als Kontaktstelle für den Verantwortlichen bzw. Auftragsverarbeiter auftritt und betroffenen Personen die Ausübung Ihrer Rechte sowie den zuständigen Datenschutzaufsichtsbehörden ermöglicht Ihre Aufsichtsmaßnahmen durchzusetzen.

Verweis DSGVO

Art. 27 DSGVO

Nachweise

Darlegung Sachverhalt mit Begründung

Dokumente zur Ernennung eines Vertreters

Anwendbarkeit lt. SOA

Für Verantwortliche und Auftragsverarbeiter gilt für dieses optionale Anforderungselement: verpflichtend, sofern eine Pflicht zur Bestellung eines Vertreters innerhalb der EU im Sinne des Art. 27 DSGVO besteht.

Zielobjektkategorie

VV

4.8. P.8 Betroffenenrechte

4.8.1. P.8.1 Recht auf Auskunft

Anforderung

Der Kunde (als Verantwortlicher) muss die Prozesse (PRZ) bzw. die Applikationen (APPL) so gestalten, dass Folgendes umgesetzt wird:

Der Kunde (als Verantwortlicher) muss jede Kommunikation gem. Art. 15 DSGVO mit Betroffenen ohne Verzögerung, spätestens aber innerhalb eines Monats nach Eingang des Antrags, adressieren. Wenn der Kunde (als Verantwortlicher) dies nicht kann, muss er den Betroffenen die Gründe hierfür nennen und über die Möglichkeit, bei einer Aufsichtsbehörde Beschwerde einzulegen oder einen gerichtlichen Rechtsbehelf einzulegen, unterrichten. Stellt die betroffene Person den Antrag in elektronischer Form, müssen die Informationen nach Möglichkeit auf elektronischem Wege bereitgestellt werden, sofern die betroffene Person nicht erneut darum ersucht. Werden keine Daten verarbeitet, muss der Kunde (als Verantwortlicher) der betroffenen Person mitteilen, dass keine Daten verarbeitet werden.

Der Kunde (als Verantwortliche) muss sicherstellen, dass Betroffene zu jeder Zeit die Möglichkeit besitzen, eine Auskunft darüber einzuholen, ob – und wenn ja – welche Daten über sie verarbeitet werden.

Die betroffene Person muss Auskunft über folgende Daten erhalten können:

- welche ihrer Daten durch die Datenverarbeitung betroffen sind;
- die Zwecke der Datenverarbeitung;
- die Kategorien personenbezogener Daten, die verarbeitet werden;
- die Empfänger oder Kategorien von Empfängern, sofern die personenbezogenen Daten übermittelt oder offengelegt werden;
- ggf. Übermittlung in ein Drittland mit Beschreibung der Garantien gem. Art. 46 DSGVO;
- Dauer der Datenverarbeitung oder, wenn nicht möglich, die Kriterien zur Bestimmung der Dauer;
- Bestehen eines Rechts auf Berichtigung oder Löschung, Einschränkung der Verarbeitung, sowie eines Widerspruchsrechts;
- Bestehen eines Beschwerderechts bei einer Aufsichtsbehörde;
- sofern anwendbar, jegliche Information zur Herkunft der Daten, wenn die Daten nicht bei der betroffenen Person erhoben wurden;
- Bestehen einer automatisierten Entscheidungsfindung einschließlich Profiling (Informationen über die involvierte Logik, Tragweite und angestrebte Auswirkungen).

Der Kunde (als Verantwortliche) muss über geeignete Maßnahmen verfügen, die der betroffenen Person die Ausübung ihrer Rechte auf Auskunft erleichtern. Er darf die

Ausübung der Rechte nicht behindern. Der Kunde (als Verantwortlicher) muss alle angemessenen Mittel nutzen, um die betroffene Person, die die Information erfragt, zu identifizieren. Dennoch darf der Kunde (als Verantwortlicher) keine Informationen speichern nur zum Zweck, um mögliche Auskunftsersuchen zu beantworten.

Der Kunde (als Verantwortlicher) muss eine Kopie der vollständigen personenbezogenen Daten, die verarbeitet werden, unverzüglich oder zumindest innerhalb eines Monats, oder wo erforderlich zwei Monate, sofern die Komplexität und Menge der Anfragen dies erfordern, unentgeltlich in einem gängigen elektronischen Format zu Verfügung zur Verfügung stellen. Die Bereitstellung der Information muss in knapper, transparenter, verständlicher und leicht zugänglicher Form unter Verwendung einer klaren und einfachen Sprache in der Sprache der betroffenen Person zur Verfügung gestellt werden, insbesondere, wenn sich die Informationen speziell an ein Kind richten. Der Kunde (als Verantwortlicher) darf nur dann Gebühren dafür erheben, wenn dies aufgrund der Verwaltungskosten angemessen ist, oder im Falle offensichtlich unbegründeter oder übermäßiger Anträge einer Person. Der Kunde (als Verantwortlicher) muss den offensichtlich unbegründeten oder übermäßigen Charakter des Antrags nachweisen.

Der Kunde (als Verantwortliche) muss den Betroffenen dazu eindeutig identifizieren. Liegen beim Verantwortlichen begründete Zweifel an der Identität der natürlichen Person vor, die den Antrag gem. Art. 15 DSGVO stellt, können unter Berücksichtigung von Art. 11 DSGVO zusätzliche Informationen angefordert werden, die zur Bestätigung der Identität der betroffenen Person erforderlich sind.

Der Kunde (als Verantwortliche) muss sicherstellen, dass die Ausübung der Rechte durch betroffene Personen die Rechte und Freiheiten anderer Personen nicht beeinträchtigt.

Die Prozesse (PRZ) müssen klar festgelegt sein inkl. Zuständigkeiten / Verantwortlichkeiten, Fristen und Meldewegen.

Der Kunde (als Auftragsverarbeiter) muss Prozesse (PRZ) implementieren, um den Verantwortlichen unter Beachtung der Art der Verarbeitung und den Informationen, die ihm zur Verfügung stehen, bei der Erfüllung der Auskunftspflicht zu unterstützen. Der Kunde (als Auftragsverarbeiter) muss dem Verantwortlichen alle relevanten Informationen zur Verfügung stellen und eine Kontaktperson für den Verantwortlichen und dessen Unterstützung benennen.

Sofern der Kunde (als Verantwortlicher oder Auftragsverarbeiter) die für ihn einschlägigen oben genannten Pflichten nicht erfüllt, muss er nachweisen, dass dies einer Beschränkung aus einer Rechtsvorschrift der Union oder des relevanten Mitgliedstaats gemäß Art. 23 DSGVO, der er unterliegt, geschuldet ist.

Verweis DSGVO

Art. 15 DSGVO

Art. 12 Abs. 3 DSGVO

Art. 12 Abs. 4 DSGVO

Art. 12 Abs. 6 DSGVO

Art. 23 DSGVO

Nachweise

Darlegung Sachverhalt mit Begründung

Einsichtnahme in Vorgänge

Verfahrens-, Prozessbeschreibungen

Zurverfügungstellung der Applikation

Beschreibungen zur Applikation zur Darlegung der Umsetzung der Anforderung (etwa Funktionsbeschreibung, Schnittstellenbeschreibung)

Anwendbarkeit lt. SOA

Verpflichtend für Verantwortliche und Auftragsverarbeiter

Zielobjektkategorie

PRZ

APPL

4.8.2. P.8.2 Recht auf Berichtigung

Anforderung

Der Kunde (als Verantwortlicher) muss die Prozesse (PRZ) bzw. die Applikationen (APPL) so gestalten, dass Folgendes umgesetzt wird:

Die betroffene Person muss von dem Verantwortlichen jederzeit verlangen können, dass dieser seine gespeicherten Daten, auch mittels einer ergänzenden Erklärung, berichtigt bzw. vervollständigt.

Wenn eine betroffene Person eine Anfrage auf Berichtigung stellt, muss der Kunde (als Verantwortlicher) die Anfrage unverzüglich oder zumindest innerhalb eines Monats, oder, wo erforderlich, zwei Monate, sofern die Komplexität und Menge der Anfragen dies erfordern, adressieren. Wenn der Kunde (als Verantwortlicher) dies nicht kann, muss er den Betroffenen die Gründe hierfür nennen und über die Möglichkeit, bei einer Aufsichtsbehörde Beschwerde einzulegen oder einen gerichtlichen Rechtsbehelf einzulegen, unterrichten.

Der Kunde (als Verantwortlicher) adressiert jede Anfrage gemäß Art. 16 DSGVO über die Verarbeitung an die betroffene Person in knapper, transparenter, verständlicher und leicht zugänglicher Form unter Verwendung einer klaren und einfachen Sprache in der Sprache der betroffenen Person, insbesondere, wenn sich die Informationen speziell an ein Kind richten. Der Kunde (als Verantwortlicher) erhebt nur dann dafür Gebühren, wenn dies auf der Grundlage der Verwaltungskosten angemessen ist oder wenn es sich um offensichtlich unbegründete oder übermäßige Anträge einer Person handelt. Stellt die betroffene Person den Antrag in elektronischer Form, so werden die Informationen nach Möglichkeit auf elektronischem Wege bereitgestellt, es sei denn, die betroffene Person verlangt etwas anderes. Der Kunde (als Verantwortlicher) muss

nachweisen, dass der Antrag offensichtlich unbegründet oder übertrieben ist. Werden keine Daten verarbeitet, so teilt der Kunde (als Verantwortlicher) mit, dass keine Daten verarbeitet werden.

Der Kunde (als Verantwortlicher) trifft geeignete Maßnahmen, um das Ersuchen der betroffenen Person und die Art der Daten, die Gegenstand des Ersuchens sind, zu bewerten und die Ausübung der Rechte der betroffenen Person auf Berichtigung zu erleichtern und die Berichtigung unter Berücksichtigung aller Speicherorte rechtzeitig vorzunehmen. Er darf die Ausübung dieser Rechte nicht behindern und muss die Berichtigung bestätigen.

Die Prozesse (PRZ) sind klar festgelegt inkl. Zuständigkeiten / Verantwortlichkeiten, Fristen und Meldewegen.

Der Kunde (als Auftragsverarbeiter) muss Prozesse (PRZ) implementieren, um Verantwortlichen bei der Erfüllung dieser Verpflichtung zu unterstützen, wobei er die Art der Verarbeitung und die dem Auftragsverarbeiter zur Verfügung stehenden Informationen berücksichtigt. Der Kunde (als Auftragsverarbeiter) stellt dem Verantwortlichen alle relevanten Informationen zur Verfügung und benennt einen Ansprechpartner für den für die Verarbeitung Verantwortlichen, um diesen zu unterstützen.

Sofern der Kunde (als Verantwortlicher oder Auftragsverarbeiter) die für ihn einschlägigen oben genannten Pflichten nicht erfüllt, muss er nachweisen, dass dies einer Beschränkung aus einer Rechtsvorschrift der Union oder des relevanten Mitgliedstaats gemäß Art. 23 DSGVO, der er unterliegt, geschuldet ist.

Verweis DSGVO

Art. 16 DSGVO

Art. 23 DSGVO

Nachweise

Darlegung Sachverhalt mit Begründung

Einsichtnahme in Vorgänge

Verfahrens-, Prozessbeschreibungen

Zurverfügungstellung der Applikation

Beschreibungen zur Applikation zur Darlegung der Umsetzung der Anforderung (etwa Funktionsbeschreibung, Schnittstellenbeschreibung)

Anwendbarkeit lt. SOA

Verpflichtend für Verantwortliche und Auftragsverarbeiter

Zielobjektkategorie

PRZ

APPL

4.8.3. P.8.3 Recht auf Löschung ("Recht auf Vergessenwerden")

Anforderung

Der Kunde (als Verantwortlicher) muss die Prozesse (PRZ) bzw. die Applikationen (APPL) so gestalten, dass Folgendes umgesetzt wird:

Die betroffene Person kann grundsätzlich vom Verantwortlichen jederzeit verlangen, dass dieser seine gespeicherten Daten löscht.

Die Löschung ist in folgenden Fällen erforderlich (nicht abschließend):

- personenbezogene Daten sind für Zwecke nicht mehr erforderlich;
- Einwilligung ist widerrufen und es liegt keine sonstige Rechtsgrundlage vor;
- es fehlt eine gültige Rechtsgrundlage;
- Daten wurden unrechtmäßig verarbeitet;
- es liegt ein Widerspruch der betroffenen Person gem. Art. 21 Abs. 1 DSGVO vor und es liegen keine vorrangigen berechtigten Gründe für die Verarbeitung oder ein Widerspruch der dadurch betroffenen Person gem. Art. 21 Abs. 2 DSGVO gegen die Verarbeitung ein;
- die Löschung ist zur Erfüllung einer rechtlichen Verpflichtung nach dem Recht des relevanten Mitgliedstaats oder dem Unionsrecht erforderlich, dem der Verantwortliche unterliegt;
- die personenbezogenen Daten wurden im Zusammenhang mit einem Dienst der Informationsgesellschaft erhoben.

Die Systeme des Kunden (als Verantwortlichen bzw. des Auftragsverarbeiter) müssen diese Vorgänge auf technischer und organisatorischer Ebene zulassen, einschließlich Backups und Logs sowie andere temporäre Datensätze. Sofern die betroffene Person die Daten nicht selber löschen kann, so muss der Kunde (als Verantwortlicher bzw. der Auftragsverarbeiter) die Daten unverzüglich löschen.

Hat der Kunde (als Verantwortlicher) die Daten öffentlich gemacht, so hat er angemessene Maßnahmen zu ergreifen, um die Empfänger der Daten über die Ausübung des Rechts auf Löschung aller Kopien, Verbindungen zu oder Vervielfältigungen der Daten unter Beachtung der verfügbaren technischen Möglichkeiten und Implementierungskosten zu informieren. Der Kunde (als Verantwortlicher) muss andere Verantwortliche, die die personenbezogenen Daten ebenfalls verarbeiten, über die Anfrage zur Löschung durch die betroffene Person informieren.

Das Recht auf Löschung ist der betroffenen Person unabhängig davon zu gewähren, ob sie ihr Recht auf Datenübertragbarkeit geltend gemacht hat.

Wenn eine betroffene Person eine Anfrage auf Löschung stellt, muss der Kunde (als Verantwortlicher) die Anfrage unverzüglich oder zumindest innerhalb eines Monats, oder, wo erforderlich, zwei Monate, sofern die Komplexität und Menge der Anfragen dies erfordern, adressieren. Wenn der Kunde (als Verantwortlicher) dies nicht kann, muss er den Betroffenen die Gründe hierfür nennen und über die Möglichkeit, bei einer Aufsichtsbehörde Beschwerde einzulegen oder einen gerichtlichen Rechtsbehelf einzulegen, unterrichten.

Der Kunde (als Verantwortlicher) adressiert jede Anfrage gemäß Art. 17 DSGVO über die Verarbeitung an die betroffene Person in knapper, transparenter, verständlicher und leicht zugänglicher Form unter Verwendung einer klaren und einfachen Sprache in der Sprache der betroffenen Person, insbesondere, wenn sich die Informationen speziell an ein Kind richten. Der Kunde (als Verantwortlicher) erhebt nur dann dafür Gebühren, wenn dies auf der Grundlage der Verwaltungskosten angemessen ist oder wenn es sich um offensichtlich unbegründete oder übermäßige Anträge einer Person handelt. Stellt die betroffene Person den Antrag in elektronischer Form, so werden die Informationen nach Möglichkeit auf elektronischem Wege bereitgestellt, es sei denn, die betroffene Person verlangt etwas anderes. Der Kunde (als Verantwortlicher) muss nachweisen, dass der Antrag offensichtlich unbegründet oder übertrieben ist. Werden keine Daten verarbeitet, so teilt der Kunde (als Verantwortlicher) mit, dass keine Daten verarbeitet werden.

Der Kunde (als Verantwortlicher) muss eine formelle und detaillierte Überprüfung der Anfrage auf Löschung vornehmen und analysieren, ob ein Recht auf Löschung für die Datenverarbeitung in der spezifischen Situation anwendbar ist und ob Ausnahmen i.S.d. Art 17 Abs. 3 lit. b DSGVO greifen und, sofern erforderlich, berücksichtigen.

Der Kunde (als Verantwortlicher) muss über geeignete Maßnahmen verfügen, die der betroffenen Person die Ausübung ihrer Rechte auf Löschung erleichtern. Er darf die Ausübung der Rechte nicht behindern.

Die Prozesse (PRZ) sind klar festgelegt inkl. Zuständigkeiten / Verantwortlichkeiten, Fristen und Meldewegen.

Der Kunde (als Auftragsverarbeiter) führt Prozesse (PRZ) ein, um den Verantwortlichen bei der Erfüllung dieser Verpflichtung zu unterstützen, wobei er die Art der Verarbeitung und die dem Auftragsverarbeiter zur Verfügung stehenden Informationen berücksichtigt. Der Kunde (als Auftragsverarbeiter) stellt dem Verantwortlichen alle relevanten Informationen zur Verfügung und benennt einen Ansprechpartner für den für die Verarbeitung Verantwortlichen, um diesen zu unterstützen.

Sofern der Kunde (als Verantwortlicher oder Auftragsverarbeiter) die für ihn einschlägigen oben genannten Pflichten nicht erfüllt, muss er nachweisen, dass dies einer Beschränkung aus einer Rechtsvorschrift der Union oder des relevanten Mitgliedstaats gemäß Art. 23 DSGVO, der er unterliegt, geschuldet ist.

Verweis DSGVO

Art. 17 DSGVO

Art. 5 Abs. 1 lit. b, c, d, e, f DGSVO

Art. 23 DSGVO

Nachweise

Darlegung Sachverhalt mit Begründung

Einsichtnahme in Vorgänge

Verfahrens-, Prozessbeschreibungen

Zurverfügungstellung der Applikation

Beschreibungen zur Applikation zur Darlegung der Umsetzung der Anforderung (etwa Funktionsbeschreibung, Schnittstellenbeschreibung)

Anwendbarkeit lt. SOA

Verpflichtend für Verantwortliche und Auftragsverarbeiter

Zielobjektkategorie

PRZ

APPL

4.8.4. P.8.4 Recht auf Einschränkung

Anforderung

Der Kunde (als Verantwortlicher) muss die Prozesse (PRZ) bzw. die Applikationen (APPL) so gestalten, dass Folgendes umgesetzt wird:

Die betroffene Person kann vom Verantwortlichen grundsätzlich verlangen, dass dieser die Verarbeitung der sie betreffenden, gespeicherten Daten einschränkt, sofern

- die Richtigkeit der personenbezogenen Daten (für die Dauer der Überprüfung durch den Verantwortlichen) bestritten wird;
- die Verarbeitung unrechtmäßig ist und die betroffene Person die Löschung ablehnt und stattdessen die Einschränkung fordert;
- die Daten für die Zwecke nicht mehr benötigt werden, die betroffene Person sie jedoch noch zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen benötigt;
- die betroffene Person Widerspruch gegen die Verarbeitung eingelegt hat, der noch geprüft wird.

Der Kunde (als Verantwortlicher) muss eine formelle und detaillierte Überprüfung der Anfrage auf Löschung vornehmen und analysieren, ob ein Recht auf Einschränkung der Verarbeitung für die Datenverarbeitung in der spezifischen Situation anwendbar ist.

Der Kunde (als Verantwortlicher bzw. Auftragsverarbeiter) muss die Verarbeitung auf Verlangen der betroffenen Person einschränken, wodurch eine Weiterverarbeitung bzw. Veränderung unmöglich ist, soweit keine rechtlichen Gründe entgegenstehen. Eine weitere Verarbeitung ist nur mit einer Einwilligung der betroffenen Person, zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen oder zum Schutz der Rechte einer anderen natürlichen oder juristischen Person oder aus Gründen eines wichtigen öffentlichen Interesses der Union oder eines relevanten mitgliedstaatlichen Rechts gemäß Art. 18 Abs. 2 DSGVO zulässig.

Die Systeme des Kunden (als Verantwortlicher bzw. des Auftragsverarbeiter) müssen die Einschränkung der Bearbeitung auf technischer und organisatorischer Ebene zulassen. Sofern die betroffene Person die Daten nicht selber einschränken kann,

schränkt der Verantwortliche bzw. der Auftragsverarbeiter die Verarbeitung der Daten ein.

Wenn eine betroffene Person eine Anfrage auf Einschränkung der Verarbeitung stellt, muss der Kunde (als Verantwortlicher) die Anfrage unverzüglich oder zumindest innerhalb eines Monats, oder, wo erforderlich, zwei Monate, sofern die Komplexität und Menge der Anfragen dies erfordern, adressieren. Wenn der Kunde (als Verantwortlicher) dies nicht kann, muss er den Betroffenen die Gründe hierfür nennen und über die Möglichkeit, bei einer Aufsichtsbehörde Beschwerde einzulegen oder einen gerichtlichen Rechtsbehelf einzulegen, unterrichten.

Der Kunde (als Verantwortlicher) adressiert jede Anfrage gemäß Art. 18 DSGVO über die Verarbeitung an die betroffene Person in knapper, transparenter, verständlicher und leicht zugänglicher Form unter Verwendung einer klaren und einfachen Sprache in der Sprache der betroffenen Person, insbesondere, wenn sich die Informationen speziell an ein Kind richten. Der Kunde (als Verantwortlicher) erhebt nur dann dafür Gebühren, wenn dies auf der Grundlage der Verwaltungskosten angemessen ist oder wenn es sich um offensichtlich unbegründete oder übermäßige Anträge einer Person handelt. Stellt die betroffene Person den Antrag in elektronischer Form, so werden die Informationen nach Möglichkeit auf elektronischem Wege bereitgestellt, es sei denn, die betroffene Person verlangt etwas anderes. Der Kunde (als Verantwortlicher) muss nachweisen, dass der Antrag offensichtlich unbegründet oder übertrieben ist. Werden keine Daten verarbeitet, so teilt der Kunde (als Verantwortlicher) mit, dass keine Daten verarbeitet werden.

Der Kunde (als Verantwortlicher) muss bei einer Aufhebung der Einschränkung die betroffene Person zuvor unterrichten.

Der Kunde (als Verantwortlicher) muss über geeignete Maßnahmen verfügen, die der betroffenen Person die Ausübung ihrer Rechte auf Einschränkung der Verarbeitung erleichtern. Er darf die Ausübung der Rechte nicht behindern.

Die Prozesse (PRZ) sind klar festgelegt inkl. Zuständigkeiten / Verantwortlichkeiten, Fristen und Meldewegen.

Der Kunde (als Auftragsverarbeiter) muss Prozesse (PRZ) implementieren, um Verantwortlichen bei der Erfüllung dieser Verpflichtung zu unterstützen, wobei er die Art der Verarbeitung und die dem Auftragsverarbeiter zur Verfügung stehenden Informationen berücksichtigt. Der Kunde (als Auftragsverarbeiter) stellt dem Verantwortlichen alle relevanten Informationen zur Verfügung und benennt einen Ansprechpartner für den für die Verarbeitung Verantwortlichen, um diesen zu unterstützen.

Sofern der Kunde (als Verantwortlicher oder Auftragsverarbeiter) die für ihn einschlägigen oben genannten Pflichten nicht erfüllt, muss er nachweisen, dass dies einer Beschränkung aus einer Rechtsvorschrift der Union oder des relevanten Mitgliedstaats gemäß Art. 23 DSGVO, der er unterliegt, geschuldet ist.

Verweis DSGVO

Art. 18 DSGVO

Art. 23 DSGVO

Nachweise

Darlegung Sachverhalt mit Begründung

Einsichtnahme in Vorgänge

Verfahrens-, Prozessbeschreibungen

Zurverfügungstellung der Applikation

Beschreibungen zur Applikation zur Darlegung der Umsetzung der Anforderung (etwa Funktionsbeschreibung, Schnittstellenbeschreibung)

Anwendbarkeit lt. SOA

Verpflichtend für Verantwortliche und Auftragsverarbeiter

Zielobjektkategorie

PRZ

APPL

4.8.5. P.8.5 Mitteilungspflicht

Anforderung

Der Kunde (als Verantwortlicher) muss die Prozesse (PRZ) bzw. die Applikationen (APPL) so gestalten, dass Folgendes umgesetzt wird:

Der Kunde (als Verantwortlicher) muss Empfängern, denen Daten der betroffenen Person übermittelt oder offengelegt wurden, jede stattgegebene Berichtigung, Löschung oder Einschränkung unverzüglich mitteilen und die betroffene Person auf deren Verlangen über diese Empfänger konform zu den Anforderungen in Art. 12 DSGVO unterrichten, es sei denn, er kann nachweisen, dass dies unmöglich ist oder einen unverhältnismäßig hohen Aufwand erfordert.

Die Prozesse (PRZ) sind klar festgelegt inkl. Zuständigkeiten / Verantwortlichkeiten, Fristen und Meldewegen.

Der Kunde (als Auftragsverarbeiter) muss Prozesse (PRZ) implementieren, um Verantwortlichen bei der Erfüllung dieser Verpflichtung zu unterstützen, wobei er die Art der Verarbeitung und die dem Auftragsverarbeiter zur Verfügung stehenden Informationen berücksichtigt.

Der Kunde (als Auftragsverarbeiter) stellt dem Verantwortlichen alle relevanten Informationen zur Verfügung und benennt einen Ansprechpartner für den für die Verarbeitung Verantwortlichen, um diesen zu unterstützen.

Sofern der Kunde (als Verantwortlicher oder Auftragsverarbeiter) die für ihn einschlägigen oben genannten Pflichten nicht erfüllt, muss er nachweisen, dass dies einer Beschränkung aus einer Rechtsvorschrift der Union oder des relevanten Mitgliedstaats gemäß Art. 23 DSGVO, der er unterliegt, geschuldet ist.

Verweis DSGVO

Art. 19 DSGVO

Art. 23 DSGVO

Nachweise

Darlegung Sachverhalt mit Begründung

Einsichtnahme in Vorgänge

Verfahrens-, Prozessbeschreibungen

Zurverfügungstellung der Applikation

Beschreibungen zur Applikation zur Darlegung der Umsetzung der Anforderung (etwa Funktionsbeschreibung, Schnittstellenbeschreibung)

Anwendbarkeit lt. SOA

Verpflichtend für Verantwortliche und Auftragsverarbeiter

Zielobjektkategorie

PRZ

APPL

4.8.6. P.8.6 Recht auf Datenübertragbarkeit

Anforderung

Der Kunde (als Verantwortlicher) muss die Prozesse (PRZ) bzw. die Applikationen (APPL) so gestalten, dass Folgendes umgesetzt wird:

Wenn die Verarbeitung auf Grundlage einer Einwilligung oder eines Vertrags erfolgt muss der Kunde (als Verantwortlicher) sicherstellen, dass die Daten von betroffenen Personen in einem strukturierten maschinenlesbaren Format bereitgestellt werden können, sofern dies gewünscht wird, es sei denn die Datenverarbeitung ist erforderlich für die Durchführung einer Aufgabe im öffentlichen Interesse oder in Ausübung öffentlicher Gewalt, die dem Verantwortlichen übertragen wurde. Der Kunde (als Verantwortlicher) stellt sicher, dass die betroffene Person das Recht hat, die personenbezogenen Daten direkt von einem Verantwortlichen an einen anderen zu übermitteln, sofern dies technisch machbar ist.

Wenn eine betroffene Person eine Anfrage auf Datenübertragung stellt, muss der Kunde (als Verantwortlicher) die Anfrage unverzüglich oder zumindest innerhalb eines Monats, oder, wo erforderlich, zwei Monate, sofern die Komplexität und Menge der Anfragen dies erfordern, adressieren. Wenn der Kunde (als Verantwortlicher) dies nicht kann, muss er den Betroffenen die Gründe hierfür nennen und über die Möglichkeit, bei einer Aufsichtsbehörde Beschwerde einzulegen oder einen gerichtlichen Rechtsbehelf einzulegen, unterrichten.

Der Kunde (als Verantwortlicher) adressiert jede Anfrage gemäß Art. 20 DSGVO über die Verarbeitung an die betroffene Person in knapper, transparenter, verständlicher und leicht zugänglicher Form unter Verwendung einer klaren und einfachen Sprache in der Sprache der betroffenen Person, insbesondere, wenn sich die Informationen speziell an ein Kind richten. Der Kunde (als Verantwortlicher) erhebt nur dann hierfür Gebühren, wenn dies auf der Grundlage der Verwaltungskosten angemessen ist oder wenn es sich um offensichtlich unbegründete oder übermäßige Anträge einer Person handelt. Stellt die betroffene Person den Antrag in elektronischer Form, so werden die Informationen nach Möglichkeit auf elektronischem Wege bereitgestellt, es sei denn, die betroffene Person verlangt etwas anderes. Der Kunde (als Verantwortlicher) muss nachweisen, dass der Antrag offensichtlich unbegründet oder übertrieben ist. Werden keine Daten verarbeitet, so teilt der Kunde (als Verantwortlicher) mit, dass keine Daten verarbeitet werden.

Der Kunde (als Verantwortlicher) muss über geeignete Maßnahmen verfügen, die der betroffenen Person die Ausübung ihrer Rechte auf Datenübertragbarkeit erleichtern. Er darf die Ausübung der Rechte nicht behindern.

Der Kunde (als Verantwortlicher) muss sicherstellen, dass die Ausübung der Rechte durch betroffene Personen die Rechte und Freiheiten anderer Personen nicht beeinträchtigt.

Die Prozesse (PRZ) sind klar festgelegt inkl. Zuständigkeiten / Verantwortlichkeiten, Fristen und Meldewegen.

Der Kunde (als Auftragsverarbeiter) muss Prozesse (PRZ) implementieren, um Verantwortlichen bei der Erfüllung dieser Verpflichtung zu unterstützen, wobei er die Art der Verarbeitung und die dem Auftragsverarbeiter zur Verfügung stehenden Informationen berücksichtigt. Der Kunde (als Auftragsverarbeiter) stellt dem Verantwortlichen alle relevanten Informationen zur Verfügung und benennt einen Ansprechpartner für den für die Verarbeitung Verantwortlichen, um diesen zu unterstützen.

Sofern der Kunde (als Verantwortlicher oder Auftragsverarbeiter) die für ihn einschlägigen oben genannten Pflichten nicht erfüllt, muss er nachweisen, dass dies einer Beschränkung aus einer Rechtsvorschrift der Union oder des relevanten Mitgliedstaats gemäß Art. 23 DSGVO, der er unterliegt, geschuldet ist.

Verweis DSGVO

Art. 20 DSGVO

Art. 23 DSGVO

Nachweise

Darlegung Sachverhalt mit Begründung

Einsichtnahme in Vorgänge

Verfahrens-, Prozessbeschreibungen

Zurverfügungstellung der Applikation

Beschreibungen zur Applikation zur Darlegung der Umsetzung der Anforderung (etwa Funktionsbeschreibung, Schnittstellenbeschreibung)

Anwendbarkeit lt. SOA

Verpflichtend für Verantwortliche und Auftragsverarbeiter

Zielobjektkategorie

PRZ

APPL

4.8.7. P.8.7 Recht auf Widerspruch

Anforderung

Der Kunde (als Verantwortlicher) muss die Prozesse (PRZ) bzw. die Applikationen (APPL) so gestalten, dass Folgendes umgesetzt wird:

Der Kunde (als Verantwortlicher) muss sicherstellen, dass die betroffene Person jederzeit Widerspruch gem. Art. 21 Abs. 1 DSGVO gegen die Verarbeitung ihrer Daten einlegen kann, sofern die Datenverarbeitung aufgrund eines berechtigten Interesses (vgl. Anforderungselemente P.1.3) oder aufgrund der Wahrnehmung einer Aufgabe erforderlich ist, die im öffentlichen Interesse liegt oder in Ausübung öffentlicher Gewalt (vgl. Anforderungselement P.1.7) erfolgt.

Insbesondere müssen betroffene Personen das Recht auf Widerspruch haben:

- im Rahmen der Nutzung von Diensten der Informationsgesellschaft kann die betroffene Person ihr Widerspruchsrecht mittels automatisierter Verfahren ausüben, bei denen technische Besonderheiten zu berücksichtigen sind;
- gegen Verarbeitung personenbezogener Daten zu wissenschaftlichen oder historischen Forschungszwecken oder zu statistischen Zwecken aus Gründen, die sich aus ihrer besonderen Situation ergeben, es sei denn, die Verarbeitung ist zur Erfüllung einer Aufgabe erforderlich, die im öffentlichen Interesse liegt;
- gegen Verarbeitungen personenbezogener Daten zum Zwecke des Direktmarketings auf der Rechtsgrundlage des berechtigten Interesses.

Wenn eine betroffene Person einen Widerspruch ausübt, muss der Kunde (als Verantwortlicher) die Anfrage unverzüglich oder zumindest innerhalb eines Monats, oder, wo erforderlich, zwei Monate, sofern die Komplexität und Menge der Anfragen dies erfordern, adressieren. Wenn der Kunde (als Verantwortlicher) dies nicht kann, muss er den Betroffenen die Gründe hierfür nennen und über die Möglichkeit, bei einer Aufsichtsbehörde Beschwerde einzulegen oder einen gerichtlichen Rechtsbehelf einzulegen, unterrichten.

Der Kunde (als Verantwortlicher) muss geeignete Maßnahmen implementieren, um die Informationen gemäß Art. 13 und 14 DSGVO und jede Anfrage gemäß Art. 15-22 und 34 DSGVO über die Verarbeitung an die betroffene Person in knapper, transparenter, verständlicher und leicht zugänglicher Form unter Verwendung einer klaren und einfachen Sprache in der Sprache der betroffenen Person, insbesondere, wenn sich die

Informationen speziell an ein Kind richten. Der Kunde (als Verantwortlicher) erhebt nur dann dafür Gebühren, wenn dies auf der Grundlage der Verwaltungskosten angemessen ist oder wenn es sich um offensichtlich unbegründete oder übermäßige Anträge einer Person handelt. Stellt die betroffene Person den Antrag in elektronischer Form, so werden die Informationen nach Möglichkeit auf elektronischem Wege bereitgestellt, es sei denn, die betroffene Person verlangt etwas anderes. Der Kunde (als Verantwortlicher) muss nachweisen, dass der Antrag offensichtlich unbegründet oder übertrieben ist. Werden keine Daten verarbeitet, so teilt der Kunde (als Verantwortlicher) mit, dass keine Daten verarbeitet werden.

Der Kunde (als Verantwortlicher) darf nach Widerspruch keine Daten mehr über die betroffene Person verarbeiten, sofern er nicht zwingende schutzwürdige Gründe für die Verarbeitung oder die Erforderlichkeit der Verarbeitung zur oder für die Begründung, Ausübung oder Verteidigung von Rechtsansprüchen nachweisen kann. Der Kunde (als Verantwortlicher) muss nachweisen, dass diese zwingenden berechtigten Gründe die Interessen, Rechte und Freiheiten der betroffenen Person überwiegen. Der Verantwortliche muss über geeignete Maßnahmen verfügen, die der betroffenen Person die Ausübung ihrer Rechte auf Widerspruch erleichtern, und spätestens bei der ersten Kommunikation mit ihr klar und getrennt von allen anderen Informationen über das Bestehen dieses Rechts informieren. Er darf die Ausübung der Rechte nicht behindern.

Die Prozesse (PRZ) sind klar festgelegt inkl. Zuständigkeiten / Verantwortlichkeiten, Fristen und Meldewegen.

Der Kunde (als Auftragsverarbeiter) muss Prozesse (PRZ) implementieren, um Verantwortlichen bei der Erfüllung dieser Verpflichtung zu unterstützen, wobei er die Art der Verarbeitung und die dem Auftragsverarbeiter zur Verfügung stehenden Informationen berücksichtigt. Der Kunde (als Auftragsverarbeiter) stellt dem Verantwortlichen alle relevanten Informationen zur Verfügung und benennt einen Ansprechpartner für den für die Verarbeitung Verantwortlichen, um diesen zu unterstützen.

Sofern der Kunde (als Verantwortlicher oder Auftragsverarbeiter) die für ihn einschlägigen oben genannten Pflichten nicht erfüllt, muss er nachweisen, dass dies einer Beschränkung aus einer Rechtsvorschrift der Union oder des relevanten Mitgliedstaats gemäß Art. 23 DSGVO, der er unterliegt, geschuldet ist.

Verweis DSGVO

Art. 21 DSGVO

Art. 23 DSGVO

Nachweise

Darlegung Sachverhalt mit Begründung

Einsichtnahme in Vorgänge

Verfahrens-, Prozessbeschreibungen

Zurverfügungstellung der Applikation

Beschreibungen zur Applikation zur Darlegung der Umsetzung der Anforderung (etwa Funktionsbeschreibung, Schnittstellenbeschreibung)

Anwendbarkeit lt. SOA

Verpflichtend für Verantwortliche und Auftragsverarbeiter

Zielobjektkategorie

PRZ

APPL

4.8.8. P.8.8 Recht auf Widerruf bei Einwilligung

Anforderung

Der Kunde (als Verantwortlicher) muss die Prozesse (PRZ) bzw. die Applikationen (APPL) so gestalten, dass Folgendes umgesetzt wird: Wird die Einwilligung widerrufen, muss sie zur Beendigung der Verarbeitung führen, sofern keine alternativen Rechtsgrundlagen für die Verarbeitung bestehen. Wenn eine betroffene Person den Widerruf ausübt, muss der Kunde (als Verantwortlicher) die Anfrage unverzüglich oder zumindest innerhalb eines Monats, oder, wo erforderlich, zwei Monate, sofern die Komplexität und Menge der Anfragen dies erfordern, adressieren. Wenn der Kunde (als Verantwortlicher) dies nicht kann, muss er den Betroffenen die Gründe hierfür nennen und über die Möglichkeit, bei einer Aufsichtsbehörde Beschwerde einzulegen oder einen gerichtlichen Rechtsbehelf einzulegen, unterrichten.

Der Kunde (als Verantwortlicher) muss geeignete Maßnahmen implementieren, um die Informationen gemäß Art. 13 und 14 DSGVO und jede Anfrage gemäß Art. 15-22 und 34 DSGVO über die Verarbeitung an die betroffene Person in knapper, transparenter, verständlicher und leicht zugänglicher Form unter Verwendung einer klaren und einfachen Sprache in der Sprache der betroffenen Person, insbesondere, wenn sich die Informationen speziell an ein Kind richten. Der Kunde (als Verantwortlicher) erhebt nur dann dafür Gebühren, wenn dies auf der Grundlage der Verwaltungskosten angemessen ist oder wenn es sich um offensichtlich unbegründete oder übermäßige Anträge einer Person handelt. Stellt die betroffene Person den Antrag in elektronischer Form, so werden die Informationen nach Möglichkeit auf elektronischem Wege bereitgestellt, es sei denn, die betroffene Person verlangt etwas anderes. Der Kunde (als Verantwortlicher) muss nachweisen, dass der Antrag offensichtlich unbegründet oder übertrieben ist. Werden keine Daten verarbeitet, so teilt der Kunde (als Verantwortlicher) mit, dass keine Daten verarbeitet werden.

Der Kunde (als Verantwortlicher) muss den Widerruf bestätigen.

Die betroffene Person ist vor Abgabe ihrer Einwilligung über das Widerrufsrecht in Kenntnis zu setzen. Die Mechanismen zur Ausübung des Widerrufs müssen genauso einfach sein, wie die Abgabe der Einwilligung.

Die Prozesse (PRZ) sind klar festgelegt inkl. Zuständigkeiten / Verantwortlichkeiten, Fristen und Meldewegen.

Der Kunde (als Auftragsverarbeiter) muss Prozesse (PRZ) implementieren, um Verantwortlichen bei der Erfüllung dieser Verpflichtung zu unterstützen, wobei er die Art der Verarbeitung und die dem Auftragsverarbeiter zur Verfügung stehenden Informationen berücksichtigt. Der Kunde (als Auftragsverarbeiter) stellt dem Verantwortlichen alle relevanten Informationen zur Verfügung und benennt einen Ansprechpartner für den für die Verarbeitung Verantwortlichen, um diesen zu unterstützen.

Sofern der Kunde (als Verantwortlicher oder Auftragsverarbeiter) die für ihn einschlägigen oben genannten Pflichten nicht erfüllt, muss er nachweisen, dass dies einer Beschränkung aus einer Rechtsvorschrift der Union oder des relevanten Mitgliedstaats gemäß Art. 23 DSGVO, der er unterliegt, geschuldet ist.

Verweis DSGVO

Art. 7 Abs. 3 DSGVO

Art 17 Abs. 1 DSGVO

Art 17 Abs. 3 DSGVO

Art. 23 DSGVO

Nachweise

Darlegung Sachverhalt mit Begründung

Einsichtnahme in Vorgänge

Verfahrens-, Prozessbeschreibungen

Zurverfügungstellung der Applikation

Beschreibungen zur Applikation zur Darlegung der Umsetzung der Anforderung (etwa Funktionsbeschreibung, Schnittstellenbeschreibung)

Anwendbarkeit lt. SOA

verpflichtend für Verantwortliche und Auftragsverarbeiter

Zielobjektkategorie

PRZ

APPL

4.8.9. P.8.9 Automatisierte Entscheidungen / Profiling

Anforderung

Der Kunde (als Verantwortlicher) muss die Prozesse (PRZ) bzw. die Applikationen (APPL) so gestalten, dass Folgendes umgesetzt wird:

Betroffene Person dürfen nicht ausschließlich einer Entscheidung unterworfen werden, die auf einer automatisierten Verarbeitung – einschließlich Profiling – beruhen, es sei denn, dies ist zur Erfüllung eines Vertrags zwischen der betroffenen Person und dem Verantwortlichen erforderlich, der Kunde (als Verantwortlicher) ist gesetzlich

dazu verpflichtet oder die betroffene Person hat ausdrücklich eingewilligt. Eine gesetzliche Verpflichtung i.S.d. Art. 22 Abs. 2 lit. b DSGVO kann sich aufgrund von Rechtsvorschriften der Union oder des relevanten Mitgliedstaats, denen der Verantwortliche unterliegt, ergeben, sofern die Anforderungen des Art. 22 Abs. 2 lit. b DSGVO erfüllt sind.

Automatisierte Entscheidungen / Profiling darf nicht auf besonderen Kategorien personenbezogener Daten gem. Art. 9 Abs. 1 DSGVO beruhen, außer es gilt Art. 9 Abs. 2 a oder g DSGVO unter Nutzung angemessener technischer und organisatorischer Maßnahmen.

Bei dem Einsatz automatisierter Entscheidungen sind angemessene Maßnahmen zur Wahrung der Rechte und Freiheiten betroffener Personen zu treffen. Der betroffenen Person ist zu ermöglichen, den eigenen Standpunkt darzulegen und automatisierte Entscheidungen anzufechten. Der Kunde (als Verantwortlicher) muss menschliche Interaktion ermöglichen, um bei automatisierten Entscheidungen inkl. Profiling zu intervenieren. Der Kunde (als Verantwortlicher) muss über geeignete Maßnahmen verfügen, die der betroffenen Person die Ausübung ihrer Rechte auf automatisierte Entscheidungen im Einzelfall erleichtern. Er darf die Ausübung der Rechte nicht behindern.

Die Prozesse (PRZ) sind klar festgelegt inkl. Zuständigkeiten / Verantwortlichkeiten, Fristen und Meldewegen.

Der Kunde (als Verantwortlicher) muss die Information über getroffene Handlungen unverzüglich oder zumindest innerhalb eines Monats, oder, wo erforderlich, zwei Monate, sofern die Komplexität und Menge der Anfragen dies erfordern, adressieren. Wenn der Kunde (als Verantwortlicher) dies nicht kann, muss er den Betroffenen die Gründe hierfür nennen und über die Möglichkeit, bei einer Aufsichtsbehörde Beschwerde einzulegen oder einen gerichtlichen Rechtsbehelf einzulegen, unterrichten.

Der Kunde (als Verantwortlicher) muss jede Mitteilung gemäß Art. 22 DSGVO im Zusammenhang mit der Verarbeitung an die betroffene Person in knapper, transparenter, verständlicher und leicht zugänglicher Form unter Verwendung einer klaren und einfachen Sprache in der Sprache der betroffenen Person zu richten, insbesondere wenn sich die Informationen speziell an ein Kind richten. Der Kunde (als Verantwortlicher) erhebt nur dann Gebühren, wenn dies aufgrund der Verwaltungskosten angemessen ist oder wenn es sich um offensichtlich unbegründete oder übermäßige Anträge einer betroffenen Person handelt. Stellt die betroffene Person den Antrag in elektronischer Form, so werden die Informationen nach Möglichkeit auf elektronischem Wege bereitgestellt, es sei denn, die betroffene Person stellt erneut einen Antrag. Der Kunde (als Verantwortlicher) muss nachweisen, dass der Antrag offensichtlich unbegründet oder übertrieben ist. Werden keine Daten verarbeitet, so teilt der Kunde (als Verantwortlicher) mit, dass keine Daten verarbeitet werden.

Der Kunde (als Auftragsverarbeiter) muss Prozesse (PRZ) implementieren, um Verantwortlichen bei der Erfüllung dieser Verpflichtung zu unterstützen, wobei er die Art der Verarbeitung und die dem Auftragsverarbeiter zur Verfügung stehenden Informationen berücksichtigt. Der Kunde (als Auftragsverarbeiter) stellt dem Verantwortlichen alle relevanten Informationen zur Verfügung und benennt einen Ansprechpartner für den für die Verarbeitung Verantwortlichen, um diesen zu unterstützen.

Sofern der Kunde (als Verantwortlicher oder Auftragsverarbeiter) die für ihn einschlägigen oben genannten Pflichten nicht erfüllt, muss er nachweisen, dass dies einer Beschränkung aus einer Rechtsvorschrift der Union oder des relevanten Mitgliedstaats gemäß Art. 23 DSGVO, der er unterliegt, geschuldet ist.

Verweis DSGVO

Art. 22 DSGVO

Art. 23 DSGVO

Nachweise

Darlegung Sachverhalt mit Begründung

Einsichtnahme in Vorgänge

Verfahrens-, Prozessbeschreibungen

Zurverfügungstellung der Applikation

Beschreibungen zur Applikation zur Darlegung der Umsetzung der Anforderung (etwa Funktionsbeschreibung, Schnittstellenbeschreibung)

Anwendbarkeit lt. SOA

Für Verantwortliche und Auftragsverarbeiter gilt für dieses optionale Anforderungselement: verpflichtend, sofern, sofern automatisierte Entscheidungen inkl. Profiling im Sinne des Art. 22 DSGVO eingesetzt wird

Zielobjektkategorie

PRZ

APPL

4.8.10. P.8.10 Beschwerde-Management

Anforderung

Der Kunde (als Verantwortlicher) muss ein Datenschutz-Managementsystem (DSMS) aufrechterhalten, über das insbesondere ein Beschwerde-Management etabliert ist.

Es muss sichergestellt sein, dass die Zertifizierungsstelle über Beschwerden bezüglich des Gegenstands oder der Konformitätsaussage, inkl. Beschwerden über unrechtmäßige, unzulässige oder irreführende Nutzung des Zertifikats oder anderer Lizenzzeichen und Datenschutzverletzungen mit Relevanz für die Zertifikatsaussage informiert wird.

Das Beschwerde-Management muss hinsichtlich der Struktur (inkl. Verantwortlichkeiten, Erreichbarkeit, Fristen, Meldewege) und Verfahren dokumentiert sein.

Ferner muss die Analyse von Beschwerden Bestandteil des Beschwerde-Managements sein.

Der Beschwerdeprozess muss eine Benachrichtigung der Zertifizierungsstelle vorsehen.

Verweis DSGVO

Anforderungen der Datenschutzaufsichtsbehörden: "Anforderungen zur Akkreditierung gem. Art. 43 Abs. 3 DSGVO i.V.m. DIN EN ISO/IEC 17065", Referenz II Kapitel 2, zu 4.1.2.2 (3)

Nachweise

Verfahrens-, Prozessbeschreibungen

Einsichtnahme in Vorgänge

Anwendbarkeit lt. SOA

Verpflichtend für Verantwortliche

Zielobjektkategorie

DSMS

5. Zertifizierungsprozess

In diesem Abschnitt wird der Zertifizierungsprozess zur Erlangung eines ‚DSGVO – information privacy standard'-Zertifikates erläutert.

5.1. Übersicht

Der grundsätzliche Zertifizierungsprozess gestaltet sich wie folgt:

- Antrag: Ein Kunde bekundet Interesse an einer Zertifizierung und reicht ein Antragsformular mit den Eckdaten zum Geltungsbereich ein; antragsberechtigt für eine Zertifizierung sind der für die Datenverarbeitung Verantwortliche resp. der Auftragsverarbeiter;
- Aufwandskalkulation: Die Zertifizierungsstelle erstellt auf Grundlage des Antrags eine Aufwandschätzung und unterbreitet dem Kunden ein Angebot;
- Beauftragung durch Kunden;
- Kunde stellt Referenzdokumentation zur Verfügung;
- Zertifizierungsstelle startet die Evaluierung:
  - Beauftragung der Evaluatoren mit Prüfung der Unabhängigkeit der Evaluatoren;
  - Begleitung des Evaluierungsverfahrens mit Abnahme der Berichte;
- Zertifizierung inkl. Zertifizierungsentscheidung;
- Veröffentlichung des Zertifikates;
- Zertifikatsbegleitung über die Laufzeit mit Überwachungstätigkeiten und ggf. Beendigung, Einschränkung, Aussetzung oder Zurückziehung der Zertifizierung.

5.2. Antrag

Der Antrag umfasst insbesondere die folgenden Informationen:

- Kunde:
  - exakte Angabe der antragstellenden Organisation;
  - Ansprechpartner;
  - angestrebtes Regelwerk: ‚DSGVO – information privacy standard';
- Geltungsbereich (Scope):
  - exakte Scope-Bezeichnung der Datenverarbeitung als „IT-gestützte Verarbeitung personenbezogener Daten"; diese Bezeichnung wird abschließend im Zertifikat aufgenommen;
  - exakte Beschreibung der Datenverarbeitung;
  - Angabe der Branche;
  - Angabe, ob die Datenverarbeitung insgesamt als Verantwortlicher und / oder Auftragsverarbeiter erbracht wird.
- Details zum Geltungsbereich:
  - Verarbeitungsvorgänge (VV): Bezeichnung und Beschreibung der Verarbeitungsvorgänge; Angabe, ob ein Verarbeitungsvorgang (VV) als

Verantwortlicher und / oder Auftragsverarbeiter erbracht wird; sofern sinnvoll, können Verarbeitungsvorgänge auch zu einer sogenannten Vorgangsreihe (VR) gebündelt werden, um etwa einen Geschäftsprozess besser abbilden zu können; Angabe aller Arten personenbezogener Daten mit Beschreibung; Klassifikation in Primär- und Sekundärdaten; Kennzeichnung, ob "besondere Kategorie personenbezogener Daten" gem. Art. 9 DSGVO oder „personenbezogene Daten über strafrechtliche Verurteilungen und Straftaten" gem. Art. 10 DSGVO relevant sind und ob personenbezogene Daten von Kindern verarbeitet werden; Zuordnung der Datenarten zu den relevanten Verarbeitungsvorgängen (VV);

- Datenschutz-Managementsystem (DSMS): Beschreibung des Datenschutz-Managementsystems (DSMS) mit den internen Prozessen zur Steuerung der Datenschutz-Konformität;
- Prozesse (PRZ): Beschreibung der Aktivitäten, die für die genaue Datenverarbeitung (DP) erforderlich sind; Prozesse (PRZ) werden definiert als eine Reihe von in Wechselbeziehung oder Wechselwirkung miteinander stehenden Tätigkeiten, die Eingaben nutzen, um ein angestrebtes Ergebnis zu liefern, die für die zu zertifizierende Datenverarbeitung erforderlich sind;
- Physische Infrastruktur (INFRA): genaue Angabe der Standorte, an denen die Datenverarbeitung stattfindet;
- IT-Systeme (IT): Übersicht über eingesetzte IT-Systeme (Servern, Clients, Netzkomponenten, Datenbanken, Speichersystemen und Schnittstellen samt Netzstrukturplan), die für die IT-gestützte Verarbeitung erforderlich sind;
- Applikationen (APPL): Übersicht über eingesetzte Applikationen – sowohl interne Anwendungen als auch von Extern verfügbare Anwendungen, wie etwa Webseiten oder Apps –, die für die Dienstleistung genutzt werden;
- externe Dritte (DL): Darstellung der eingesetzten externen Dritten (z. B. Dienstleister, Auftragsverarbeiter, Behörden, Schwestergesellschaften oder Holding) mit Darstellung der übernommenen Zuständigkeiten und damit verbundenen Aufgaben, sofern relevant;
- Anzahl Mitarbeiter im Geltungsbereich;
- bereits vorliegende Zertifizierungen;
- etwaige Beratungsdienstleistungen bzgl. des Geltungsbereiches in Anspruch genommen.

5.3. Angebot mit Kalkulation

Die Zertifizierungsstelle prüft, ob eine Zertifizierung gemäß Antrag durchgeführt werden kann. Die Zertifizierungsstelle muss hierbei sicherstellen, dass der Bewertungsgegenstand angemessen ist und konkrete DSGVO-relevante Datenverarbeitungen adressiert. Ferner muss sichergestellt werden, dass die Beschreibung des Bewertungsgegenstand unmissverständlich ist.

Die Aufwandskalkulation sieht für einzelne Tätigkeiten feste Minimalwerte vor und orientiert sich ferner an folgenden Faktoren:

- Risikobasierter Ansatz, insbesondere im Hinblick auf die Arten der personenbezogenen Daten, die verarbeitet werden, kann die Zertifizierungsstelle den Umfang der Prüfung spezifizieren.[4]
- Anzahl der Mitarbeiter im Geltungsbereich, dies umfasst neben den Mitarbeitern der Datenschutzorganisation auch die Mitarbeiter, die mit der Verarbeitung von personenbezogenen Daten im Verarbeitungsvorgang betraut sind. Der Aufwand berechnet sich insbesondere mit der Kalkulationstabelle aus ISO/IEC 27006 in Abhängigkeit der Anzahl der Mitarbeiter im Geltungsbereich.
- Anzahl der Standorte.
- Bei der Aufwandskalkulation können auch gültige Zertifikate akkreditierter und anerkannter Stellen berücksichtigt werden.

Die Aufwandskalkulation orientiert sich an folgender Tabelle, wobei die nachfolgend beschriebenen Evaluierungsmethoden zum Einsatz kommen:

TÄTIGKEIT	AUFWAND	BEMERKUNG
Basisprüfung	mind. 1 Tag	Kalkulation orientiert sich am Umfang des Geltungsbereiches.
Prüfung (rechtl.)	mind. 0,15 Tage pro Verarbeitungsvorgang (VV) sowie 0,1 Tage pro Dienstleister (DL), aber mind. 1 Tag	Kalkulation orientiert sich an dem Umfang des Geltungsbereiches, der Art und dem Umfang der verwendeten Daten und den anwendbaren Anforderungen des Kriterienkatalogs.
Prüfung (techn.)	mind. 0,5 Tage pro Applikation (APPL), aber mind. 1 Tag	Kalkulation orientiert sich an dem Umfang des Geltungsbereiches, der Art und dem Umfang der verwendeten Daten und den anwendbaren Anforderungen des Kriterienkatalogs.
Auditierung Inspektion	mind. 1 Tag	Der Aufwand berechnet sich insbesondere mit der Kalkulationstabelle aus ISO/IEC 27006 in Abhängigkeit der Anzahl der Mitarbeiter im Geltungsbereich, multipliziert mit Faktor 0,2.

[4] Zur einheitlichen Zertifizierung verschiedener Verarbeitungsvorgänge sollen hierzu nähere Vorgaben in den AVVIS-Dokumenten („Anwendungshinweisen, verbindlichen Vorgaben und Interpretationen zum Schema“) gemacht werden.

TÄTIGKEIT	AUFWAND	BEMERKUNG
		Formel: Anzahl Mitarbeiter Geltungsbereich => Anzahl Tage (Basiswert); Tage = Basiswert x Faktor 0,2.
Vor- und Nachbereitung Dokumentation Projektmanagement	mind. 1,5 Tag	

Ein Multiple-Site-Verfahren (für Auditierung) muss konform zu den Vorgaben der ISO/IEC 17021-1 erfolgen.

Da bei Re-Zertifizierungsverfahren die Basisprüfung entfallen kann, reduziert sich der Aufwand hier entsprechend; ferner sind hier etwaige inhaltliche Veränderungen bei der Kalkulation einzubeziehen.

Bei der Überwachung wird grob ein Drittel des Aufwands der Erst-Zertifizierung veranschlagt.

5.4. Referenzdokumentation des Kunden

Der Kunde verpflichtet sich, der Zertifizierungsstelle eine hinreichende Referenzdokumentation zur Verfügung zu stellen. Die Referenzdokumentation des Kunden umfasst die folgenden Dokumente:

- Scope-Beschreibung: exakte Beschreibung des Geltungsbereiches mit folgenden Informationen: Datenverarbeitung (DV), Verarbeitungsvorgänge (VV), Datenschutz-Managementsystem (DSMS), Prozesse (PRZ) zur Realisierung der Datenverarbeitung, physische Infrastruktur (INFRA) mit Standorten und Räumen, IT-Infrastruktur (IT), Applikationen (APPL), externe Dritte (DL).
- SOA (Statement of Applicability, Erklärung zur Anwendbarkeit): Zusicherung, welche Anforderungen des Kriterienkatalogs umgesetzt werden sollen und Begründung für alle Anforderungen, die nicht umgesetzt werden.
- Realisierungsbeschreibung: ausführliche Umsetzungsbeschreibung für alle Anforderungen, die im SOA als anwendbar identifiziert wurden. Die Realisierungsbeschreibung ist so ausführlich, dass die Umsetzung zu den relevanten Anforderungen eindeutig hervorgeht. Die Realisierungsbeschreibung ist die verbindliche Zusicherung des Kunden, wie er die Anforderungen des vorliegenden Kriteriums konkret umsetzt. Ein Verweis auf andere Dokumente ist möglich, die Darstellung muss aber eindeutig und leicht möglich sein.

Der Kunde verpflichtet sich, die drei Dokumente Scope-Beschreibung, SOA und Realisierungsbeschreibung laufend aktuell zu halten und für die Aktualität einen entsprechenden Prozess etabliert zu haben.

Ferner verpflichtet sich der Kunde, alle weiteren, für die Evaluierung und Zertifizierung benötigten Unterlagen und Nachweise vollständig zur Verfügung zu stellen; die

erforderlichen Nachweise sind im Kriterienkatalog angegeben. Ferner verpflichtet sich der Kunde, die Evaluierung und Zertifizierung aktiv zu unterstützen und alle Zielobjekte zugänglich zu machen, die für die Prüfung erforderlich sind.

5.4.1. Scope-Beschreibung

Die Scope-Beschreibung ist in Kapitel 3.1 erläutert.

Die Scope-Beschreibung muss vom Kunden rechtsverbindlich unterschrieben werden; sie stellt damit die Grundlage für die Evaluierung und Zertifizierung dar. Es wird eine Vorlage zur Verfügung gestellt werden.

5.4.2. Statement of Applicability (SOA)

Das Statement of Applicability (SOA) ist in Kapitel 3.2 beschrieben.

Das SOA muss vom Kunden rechtsverbindlich unterschrieben werden; es stellt damit die Grundlage für die Evaluierung und Zertifizierung dar. Es wird eine Vorlage zur Verfügung gestellt werden.

5.4.3. Realisierungsbeschreibung

Die Realisierungsbeschreibung ist in Kapitel 3.3 beschrieben.

Die Realisierungsbeschreibung muss vom Kunden rechtsverbindlich unterschrieben werden; es stellt damit als Zusicherung des Kunden die Grundlage für die Evaluierung und Zertifizierung dar. Es wird eine Vorlage zur Verfügung gestellt werden.

5.5. Evaluierungsprozess

Als Konformitätsbewertungstätigkeiten werden folgende Evaluierungsmethoden angewendet:

- Basisprüfung: Analyse der Referenzdokumentation des Kunden;
- Prüfung (rechtl.): rechtliche Analyse nach geltenden rechtlichen Auslegungsmethoden;
- Prüfung (techn.): Prüfung der technisch geprägten Anforderungen des vorliegenden Kriterienkatalogs;
- Auditierung: Prüfung der Standorte;
- Inspektion: Prüfung weiterer Aspekte des Kriterienkatalogs.

Die Evaluierung insgesamt soll als ein gemeinsames Verfahren durchgeführt werden, das alle o.g. Evaluierungsmethoden „umschließt“. Selbstverständlich können dabei Einzelaspekte durch eine bestimmte Evaluierungsmethode und / oder einen bestimmten Evaluator, der beispielsweise über die erforderlichen Kompetenzen verfügt, separat evaluiert werden, beispielsweise können alle Anforderungen, die mit der Prüfung (rechtl.) evaluiert werden, in einem Block zusammengefasst evaluiert werden.

Die Evaluierung erfolgt gegen die Anforderungen des vorliegenden Kriterienkatalogs.

Es wird ein zwei-stufiger Evaluierungsprozess etabliert:

1. Basisprüfung;

2. Prüfung (rechtl.), Prüfung (techn.), Auditierung und Inspektion.

Die Basisprüfung muss abgeschlossen sein, bevor mit den weiteren Prüfschritten (bestehend aus Prüfung (rechtl.), Prüfung (techn.), Auditierung und Inspektion) fortgefahren werden kann.

5.6. Stichprobenverfahren

Grundsätzlich ist jede Evaluierung eine Stichprobe.

Die Stichprobenprüfung wird vom Evaluator risikobasiert gewählt, um eine möglichst große Repräsentanz der Stichprobe sicherzustellen. Bzgl. der Größe der Stichprobe gilt das „Prinzip der Wurzel". Beispiel: 100 Kunden haben Einwilligungen unterzeichnet, die alle dem gleichen Muster entstammen, hier werden 10 einzelne Vereinbarungen kontrolliert.

5.7. Bewertungsschema

Im vorliegenden Konformitätsbewertungsprogramm wird das folgende Bewertungsschema durchgesetzt:

- 1: Anforderung erfüllt;
- 2: Anforderung erfüllt, aber es gibt Verbesserungspotential (Empfehlung);
- 3: Anforderung nicht erfüllt (Hauptabweichung).

Zur anschließenden Zertifizierung sind keinerlei Hauptabweichungen von den Anforderungen zulässig, d.h., vor Zertifikatserteilung müssen alle Anforderungen stets erfüllt sein; es dürfen also nur die Bewertungen 1 oder 2 auftreten. Eine Hauptabweichung (Bewertung 3) kann zu keiner Zertifizierung führen.

5.8. Evaluierungsbericht

Der Evaluator dokumentiert seine Tätigkeiten.

5.9. Anerkennung bestehender Zertifikate

Es können bereits erfolgte Datenschutzzertifizierung nach Art. 42 DSGVO durch eine akkreditierte Zertifizierungsstelle, die bereits einen Teil des Zertifizierungsgegenstands abdeckt, als Teilevaluierung berücksichtigt werden. Ferner können akkreditierte oder staatliche Zertifikate als Teilevaluierung für bestimmte Teilaspekte berücksichtigt werden, etwa ISO/IEC 27001 bei Rechenzentren.

Die Gültigkeit eines Zertifikates verändert sich hierbei insoweit, als dass die Gültigkeitsdauer des Zertifikats auf das Ablaufdatum der kürzest laufenden berücksichtigten Zertifizierung reduziert wird. Bei der Rezertifizierung der Zertifizierung wird die Ablauffrist des Zertifikats auf die Laufzeit des berücksichtigten Zertifikats verlängert, jedoch maximal auf die Standardlaufzeit eines Zertifikats oder bei weiteren berücksichtigten Fremdzertifikaten auf die kürzeste Laufzeit.

Notwendig für eine solche Beachtung ist das Vorliegen eines vollständigen Zertifizierungsgutachtens oder von Informationen, die eine Bewertung der Zertifizierungstätigkeit und -ergebnisse ermöglicht. Eine Zertifizierungsurkunde oder ähnliche

Bescheinigungen über eine Zertifizierung sind hierbei nicht ausreichend. Ergeben sich bei einer solchen Prüfung Abweichungen von den Anforderungen, oder sonstige Unregelmäßigkeiten, so ist die Evaluierung im Rahmen des laufenden Zertifizierungsverfahrens zu erweitern und ggf. auf den gesamten, bereits zertifizierten Gegenstand auszudehnen.

5.10. Zertifizierung

5.10.1. Zweistufiges Verfahren

Es wird ein klassisches zwei-stufiges Verfahren eingesetzt:

- Auditierung durch Evaluatoren, die bei der Zertifizierungsstelle lizenziert sind;
- Zertifizierung.

5.10.2. Laufzeit

Das Zertifikat ist drei Jahre gültig und erfordert zur Aufrechterhaltung zwei jährliche Überwachungsaudits.

5.10.3. Zertifikat

Das Zertifikat weist alle Informationen des DAkkS-Musterzertifikates mit Anhang auf (vgl. Abbildung 2 und Abbildung 3).

Prüfstelle Logo und Anschrift

Zertifikat

Die **Zertifizierungsstelle xxxx** bestätigt hiermit als Ergebnis der Zertifizierungsentscheidung am TT.MM.JJJJ gemäß Art. 42 Abs. 5 DS-GVO, dass

[Antragsteller]: <exakter Name und Anschrift des Kunden>
[optional Niederlassungen] <Anschrift der Niederlassungen>

die Datenverarbeitung

[Bezeichnung EVG] Cloud-Mailservice AJAX 4.0 gemäß Anlage 1

als **[Datenschutzrolle g. DSGVO]** Verantwortlicher gemäß Art. 4 Nr. 7 DS-GVO / als Auftragsverarbeiter gemäß Art. 4 Nr. 8 DS-GVO innerhalb **[Geltungsbereich Regional]** D / EU / Drittland

[Optional weitere Beschränkungen Einsatzbereich] z.B. nur für B2B; unter **Beachtung der Nutzungsausschlüsse** gemäß Anlage 2

konform zu den Anforderungen der EU Verordnung 2016/679 (DS-GVO) und den zusätzlichen Anforderungen der Datenschutzaufsichtsbehörden betreibt und innerhalb der Laufzeit des Zertifikats auf Konformität überwacht wird.

Die Gründe für die Erteilung des Zertifikats wurden der Datenschutzaufsichtsbehörde (xxx) gemäß Art 43 Abs. 5 DS-GVO am TT.MM.JJJJ mitgeteilt.

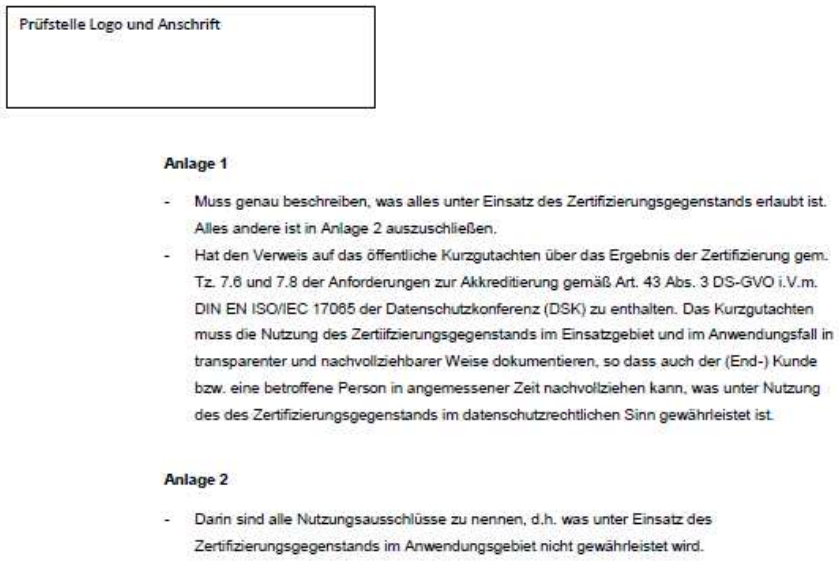
Prüfgrundlagen	[Name Programm] akkreditiertes Konformitätsbewertungsprogramm V1.2 [Name Kriterienkatalog] Von der Datenschutzaufsichtsbehörde xxx genehmigte Kriterien V 1.2.	
Zertifikats-ID/-Nummer:	XXX Zertifikatsnummer von der Prüfstelle	
letzter Audittag vor Ort:	<tt.mm.jjjj> /Berichtsnummer/Datum	
Überwachung	nächste geplante Überwachung bis spätestens <tt.mm.jjjj>	
Datum der Ausstellung	<tt.mm.jjjj>	Laufzeit bis <tt.mm.jjjj> max. 3 Jahre>

Unterschrift/Benannter Entscheider der KBS

IAF DAkkS Deutsche Akkreditierungsstelle D-XX-YYYYY-ZZ-NN

zur Verwendung gemäß SymbolVO und DAkkS-Regel 71 SD 0 011

Abbildung 2: Musterzertifikat



Prüfstelle Logo und Anschrift

Anlage 1

- Muss genau beschreiben, was alles unter Einsatz des Zertifizierungsgegenstands erlaubt ist. Alles andere ist in Anlage 2 auszuschließen.
- Hat den Verweis auf das öffentliche Kurzgutachten über das Ergebnis der Zertifizierung gem. Tz. 7.6 und 7.8 der Anforderungen zur Akkreditierung gemäß Art. 43 Abs. 3 DS-GVO i.V.m. DIN EN ISO/IEC 17065 der Datenschutzkonferenz (DSK) zu enthalten. Das Kurzgutachten muss die Nutzung des Zertifizierungsgegenstands im Einsatzgebiet und im Anwendungsfall in transparenter und nachvollziehbarer Weise dokumentieren, so dass auch der (End-) Kunde bzw. eine betroffene Person in angemessener Zeit nachvollziehen kann, was unter Nutzung des des Zertifizierungsgegenstands im datenschutzrechtlichen Sinn gewährleistet ist.

Anlage 2

- Darin sind alle Nutzungsausschlüsse zu nennen, d.h. was unter Einsatz des Zertifizierungsgegenstands im Anwendungsgebiet nicht gewährleistet wird.

Abbildung 3: Musterzertifikat Anlagen

Darüber hinaus werden als Anhang zum Zertifikat in Form eines Kurzgutachtens weitere Informationen bestätigt:

Zertifikatsdetails

Anhang zum Zertifikat mit Zertifikats-ID <ID>

zum Geltungsbereich:

- Kontaktdaten des Kunden: <xxx>
- Datenverarbeitung: <xxx>
- Branche: <xxx>
- Dienstleistungserbringung als Verantwortlicher und / oder Auftragsverarbeiter
- Verarbeitungsvorgänge: <xxx>
- zertifizierte Standorte: <exakte Angabe der Standorte mit ggf. juristischen Personen>
- SOA-Dokument: <Version 1.0, tt.mm.jjjj>

zum Audit:

- Prüfverfahren, inklusive der Zertifizierung zugrundliegender Kriterien (ggf. mit Versionsangabe): <xxx>
- Prüfergebnis: <xxx>
- eingebundene Evaluatoren: <xxx>

zur Zertifizierung:

- Informationen über die Erst-bzw. Re-Zertifizierung: <xxx>

- Angaben zu möglichen Überwachungstätigkeiten zur Aufrechterhaltung der Zertifizierung: <xxx>
- zuständige Datenschutzaufsichtsbehörde: <xxx>

5.10.4. Verzeichnis zertifizierter Verarbeitungsvorgänge

Die Zertifizierungsstelle hält eine öffentlich verfügbare Zertifikatsliste vor, aus der hervorgeht:

- Kunde, Geltungsbereich, Regelwerk, Zert-ID, Gültigkeitsdauer, Link auf Zertifikat samt Anlage (Zertifikatsdetails)

Die Webseite mit der Zertifikatsliste muss leicht erreichbar und mindestens zu Bürozeiten verfügbar sein.

Zusätzlich werden Zertifikate der zuständigen Aufsichtsbehörde übermittelt.

5.11. Jährliche Überwachung

Es sind jährliche Überwachungen vorgesehen. Überwachungen erfolgen grundsätzlich analog zur Erst-Zertifizierung, wobei jedoch nur eine Auswahl der Kriterien zu evaluieren, basierend auf dem Evaluationsplan unter Beachtung eines risikobasierten Ansatzes, ist.

5.12. Re-Zertifizierung

Nach einer Laufzeit von 3 Jahren endet der Zertifikatszyklus, der über ein Re-Zertifizierungsverfahren erneut gestartet werden kann.

Die Re-Evaluierung erfolgt analog zur Erst-Evaluierung mit dem Unterschied, dass die Basisprüfung entfallen kann, sofern Scope-Beschreibung und SOA unverändert; andernfalls wird eine Basisprüfung mit dem Schwerpunkt der Veränderungen durchgeführt.

5.13. Anlassbezogene Prüfungen

Darüber hinaus können anlassbezogene Prüfungen (Evaluierung aus besonderem Anlass) stattfinden:

- Erweiterung oder Änderung des Geltungsbereichs;
- kurzfristig angekündigte Evaluierungen.

5.14. Änderungen, die sich auf die Zertifizierung auswirken

Die Zertifizierungsstelle informiert ihre Kunden zeitnah über Änderungen am Zertifizierungsstandard.

Der Kunde ist ferner verpflichtet, signifikante tatsächliche oder rechtliche Änderungen am zertifizierten Bewertungsgegenstand unverzüglich der Zertifizierungsstelle anzuzeigen. Welche tatsächlichen oder rechtlichen Änderungen als signifikant einzustufen sind, erfolgt nach folgenden Maßgaben:

- Es liegt eine Änderung hinsichtlich der Verarbeitung personenbezogener Daten vor,

- es liegt eine Änderung der Einsatzumgebung vor,
- es liegt eine Änderung der (rechtlichen) Rahmenbedingungen vor oder
- es liegt eine Änderung am Stand der Technik vor,

die relevant für die Zertifizierungsaussage sind, dann ist die Änderung als signifikant einzustufen. Dies liegt insbesondere dann vor, wenn

- eine Änderung an verwendeten Datenarten, Applikationen, Standorten oder Dienstleistern bzw. externen Dritten macht eine Aktualisierung der Scope-Beschreibung erforderlich,
- eine Änderung macht eine Aktualisierung des SOA-Dokumentes erforderlich oder
- eine Änderung macht eine Aktualisierung an der Realisierungsbeschreibung erforderlich.

Die Zertifizierungsstelle ist bei Hinweisen über solche Änderungen, die Einfluss auf die Konformitätsbewertungsaussage haben könnten, verpflichtet, den Sachverhalt innerhalb von 4 Wochen zu ermitteln und geeignete Maßnahmen zu ergreifen.

Ziel dieser Maßnahmen ist, dass auch ein veränderter Verarbeitungsvorgang seinen zertifizierten Status behält. Damit die Zertifizierungsstelle das erteilte Zertifikat anpassen kann, sind folgende Tätigkeiten notwendig:

- Der Kunde legt eine aktualisierte Referenzdokumentation vor (Scope-Beschreibung, SOA, Referenzdokumentation), aus der insbesondere die Veränderungen deutlich erkennbar sind.
- Der Kunde legt eine Impact-Analyse vor, aus der die Konsequenzen seiner Änderungen dargestellt werden.
- Der Kunde legt aktuelle objektive Nachweise vor, sofern erforderlich.
- Die Zertifizierungsstelle überprüft die Unterlagen und entscheidet, ob eine Evaluierung aus besonderem Anlass erforderlich ist, um die Einhaltung der Anforderungen feststellen zu können.

5.15. Beendigung, Einschränkung, Aussetzung oder Zurückziehung der Zertifizierung

Es müssen alle gem. SOA anwendbaren Anforderungen des vorliegenden Kriterienkatalogs erfüllt werden; ein Umgang mit Nicht-Konformitäten ist nicht vorgesehen.

Wird bei einer Überwachung eine Hauptabweichung (Nicht-Konformität der Bewertung 3) identifiziert, ergeben sich folgende Möglichkeiten:

- Weiterführung der Zertifizierung unter Bedingungen, die von der Zertifizierungsstelle festgelegt werden (z. B. dokumentierte Ursachenanalyse, autorisierte Maßnahmenplanung mit zeitnaher Behebungsfrist, zeitnahe Behebung, fristgemäße Einreichung einer vollständigen Dokumentation des Sachverhaltes, Begutachtung durch außerordentliche Evaluierung);
- Einschränkung des Geltungsbereichs der Zertifizierung, um einen nichtkonformen Verarbeitungsvorgang zu entfernen;
- Aussetzen der Zertifizierung vorbehaltlich der Abstellmaßnahmen durch den Kunden;

- Zurückziehung der Zertifizierung.

Wird der Geltungsbereich einer Zertifizierung eingeschränkt, müssen alle zertifizierungsrelevanten Unterlagen (inkl. Zertifikat und Zertifikatsliste) angepasst werden. Außerdem muss dem Kunden der Sachverhalt und die Folgen für seine Werbung mit dem Zertifikat und Logo klar und eindeutig mitgeteilt werden.

Wird ein Zertifikat ausgesetzt, muss der Kunde darüber informiert werden, durch welche Maßnahmen er die Aussetzung beenden kann. Die Maßnahmen legt die Zertifizierungsstelle fest, die sind z. B. dokumentierte Ursachenanalyse, autorisierte Maßnahmenplanung mit zeitnaher Behebungsfrist, zeitnahe Behebung, fristgemäße Einreichung einer vollständigen Dokumentation des Sachverhaltes, Begutachtung durch außerordentliche Evaluierung.

Über jegliche Veränderungen an einem Zertifikat samt Darstellung der ergriffenen Maßnahmen wird die zuständige Aufsichtsbehörde umgehend schriftlich informiert.

Wird die Zertifizierungsstelle von der Datenschutzaufsichtsbehörde angewiesen, eine erteilte Zertifizierung gem. Art. 58 Abs. 2 lit. h DSGVO zu widerrufen, oder keine Zertifizierung zu erteilen, so muss die Zertifizierungsstelle im Rahmen ihres Managementsystems sicherstellen, dass der entsprechende Kunde hierüber und die Folgen daraus informiert wird, entsprechende Registereinträge angepasst werden und die Datenschutzaufsichtsbehörde hierüber in Kenntnis gesetzt wird.

6. Glossar

BEGRIFF	ERLÄUTERUNG
Applikationen (APPL)	Gesamtheit der Applikationen – sowohl interne Anwendungen als auch von Extern verfügbare Anwendungen, wie etwa Webseiten oder Apps –, die in der Datenverarbeitung genutzt werden
Auftragsverarbeiter	ein Auftragsverarbeiter ist eine Organisation, die personenbezogene Daten im Auftrag des Verantwortlichen verarbeitet
besonderer Kategorien personenbezogener Daten	„personenbezogene Daten, aus denen die rassische und ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen oder die Gewerkschaftszugehörigkeit hervorgehen, sowie [...] genetischen Daten, biometrischen Daten zur eindeutigen Identifizierung einer natürlichen Person, Gesundheitsdaten oder Daten zum Sexualleben oder der sexuellen Orientierung einer natürlichen Person“ (lt. Definition in Art. 9 DSGVO)
Bewertungsgegenstand	Gegenstand eines konkreten Zertifizierungsverfahrens synonym zu Untersuchungsgegenstand, Scope, Target of Evaluation (ToE)
Datenarten	Datenarten fokussieren auf personenbezogene Daten
Datenschutz-Managementsystem (DSMS)	Beschreibung der internen Prozesse, um eine Datenschutz-Konformität, insb. zur Umsetzung der Anforderungen dauerhaft sicherzustellen
Datenverarbeitung (DV)	Eine Datenverarbeitung (DV) als „IT-gestützte Verarbeitung personenbezogener Daten“ kann gem. Art. 42 DSGVO zertifiziert werden. Diese Datenverarbeitung (DV) lässt sich durch folgende Elemente charakterisieren: - Verarbeitungsvorgänge (VV); - Datenschutz-Managementsystem (DSMS); - Prozesse (PRZ); - physische Infrastruktur (INFRA); - IT-Infrastruktur (IT); - Applikationen (APPL);

BEGRIFF	ERLÄUTERUNG
	- externe Dritte (DL). Beispiele einer zertifizierbaren Datenverarbeitung: - Secure log-in5; - Online Banking5.
Evaluator	Prüfer, der eine Evaluierung durchführt
Evaluierung (engl. Evaluation)	Prüfung, durchgeführt durch: - Prüfung (rechtl.) - Prüfung (techn.) - Auditierung - Inspektion
Externe Dritte (DL)	Externe Dritte sind beispielsweise Dienstleister, Auftragsverarbeiter, Behörden, Schwestergesellschaften oder Holding, die für die Realisierung der Datenverarbeitung benötigt werden oder an die personenbezogene Daten übermittelt werden
IT-Infrastruktur (IT)	Gesamtheit der IT-Systeme (Servern, Clients, Netzkomponenten, Datenbanken, Speichersystemen und Schnittstellen), die für die IT-gestützte Verarbeitung erforderlich sind, mit Netzstrukturplan
Kunde	eine Organisation, die als Verantwortlicher und/ oder Auftragsverarbeiter ein Zertifikat anstrebt
Organisation	Person oder Personengruppe, die eigene Funktionen mit Verantwortlichkeiten, Befugnissen und Beziehungen hat, um ihre Ziele zu erreichen. Anmerkung: Der Begriff Organisation umfasst unter anderem Einzelunternehmer, Gesellschaft, Konzern, Firma, Unternehmen, Behörde, Handelsgesellschaft, Verband, Wohltätigkeitsorganisation, Institution, oder Teile oder eine Kombination der genannten, ob eingetragen oder nicht, öffentlich oder privat. (lt. Definition aus ISO 9000)

5 Vgl. [EDPB_Guide-1].

BEGRIFF	ERLÄUTERUNG
personenbezogene Daten	„alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person [...] beziehen; als identifizierbar wird eine natürliche Person angesehen, die direkt oder indirekt, insbesondere mittels Zuordnung zu einer Kennung wie einem Namen, zu einer Kennnummer, zu Standortdaten, zu einer Online-Kennung oder zu einem oder mehreren besonderen Merkmalen, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind, identifiziert werden kann“ (lt. Definition in Art. 4 DSGVO)
Primärdaten	Primärdaten sind die personenbezogenen Daten, die im Verarbeitungsvorgang (vgl. Definition unten) vornehmlich verarbeitet werden, z. B. Daten des Betroffenen; als Abgrenzung dazu vgl. Sekundärdaten
Prozesse (PRZ)	Gemäß ISO/IEC 17000 wird ein Prozess (PRZ) definiert als eine Reihe von in Wechselbeziehung oder Wechselwirkung miteinander stehenden Tätigkeiten, die Eingaben nutzen, um ein angestrebtes Ergebnis zu liefern, die für die zu zertifizierende Datenverarbeitung erforderlich sind.
physische Infrastruktur (INFRA)	Gesamtheit der Standorte und Räume, an denen Datenverarbeitung erbracht wird
Sekundärdaten	Sekundärdaten sind personenbezogenen Daten, die im Kontext des Verarbeitungsvorgangs (vgl. Definition unten) zusätzlich zu den Primärdaten anfallen, z. B. Protokolldaten, Statistikdaten, Autorisierungsdaten
Union	Synonym für Europäische Union (EU) inklusive des Europäischen Wirtschaftsraums (EWR)
Verantwortlicher	ein Verantwortlicher ist eine Organisation, die allein über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet
Verarbeitung (processing)	‚Verarbeitung‘ ist jeder mit oder ohne Hilfe automatisierter Verfahren ausgeführter Vorgang oder jede solche Vorgangsreihe im Zusammenhang mit personenbezogenen Daten wie das Erheben, das Erfassen, die Organisation, das

BEGRIFF	ERLÄUTERUNG
	Ordnen, die Speicherung, die Anpassung oder Veränderung, das Auslesen, das Abfragen, die Verwendung, die Offenlegung durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung, den Abgleich oder die Verknüpfung, die Einschränkung, das Löschen oder die Vernichtung engl. Fassung: „'processing' means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction" (lt. Definition in Art. 4 DSGVO)
Verarbeitungsvorgang (VV) (processing operation)	‚Verarbeitungsvorgänge' ist die Bündelung mehrerer Verarbeitungen (vgl. Definition oben), um ein Ziel zu erreichen. Beispiele: - Secure log-in5; - Web-Front-End5; - Besuch einer Webseite; - Anmeldung; - Registrierung; - Durchführen einer Transaktion.
Vorgangsreihe (VR) (set of processing operation)	‚Vorgangsreihen' bündeln mehrere Verarbeitungsvorgänge, um etwa einen Geschäftsprozess besser abbilden zu können Beispiele: - Registrierungsphase; - Nutzungsphase.
Zielobjektkategorien	Zielobjektkategorie charakterisiert den Scope: - Verarbeitungsvorgänge (VV) - Datenschutz-Managementsystem (DSMS) - Prozesse (PRZ) - physische Infrastruktur (INFRA) - IT-Infrastruktur (IT)

BEGRIFF	ERLÄUTERUNG
	- Applikationen (APPL) - externe Dritte (DL)
zuständige Datenschutzaufsichtsbehörde	Die Datenschutzaufsichtsbehörde, die für die Zertifizierungsstelle zuständig ist, nicht für den zertifizierten Kunden.

7. Anhang: Übersicht über die Kriterien

KRITERIEN	RELE-VANTE ZIELOB-JEKTE	ANWENDUNG FÜR VERANT-WORTLICHEN	ANWENDUNG FÜR AUF-TRAGSVERARBEI-TER
P.1 Zulässigkeit der Datenverarbeitung			
P.1.1 Identifikation Grundlagen	DSMS VV	verpflichtend	verpflichtend
P.1.2 Rechtsgrundlage Vertrag	VV PRZ APPL	anwendbar gem. SOA	nicht anwendbar
P.1.3 Rechtsgrundlage berechtigtes Interesse	VV PRZ	anwendbar gem. SOA	nicht anwendbar
P.1.4 Rechtsgrundlage Einwilligung	VV PRZ APPL	anwendbar gem. SOA	nicht anwendbar
P.1.5 Rechtsgrundlage rechtliche Verpflichtung	VV	anwendbar gem. SOA	nicht anwendbar
P.1.6 Rechtsgrundlage lebenswichtige Interessen	VV	anwendbar gem. SOA	nicht anwendbar
P.1.7 Rechtsgrundlage öffentliches Interesse	VV	anwendbar gem. SOA	nicht anwendbar
P.1.8 Verarbeitung bei besonderen Kategorien personenbezogener Daten	VV PRZ	anwendbar gem. SOA	anwendbar gem. SOA
P.1.9 Verarbeitung bei strafrechtlichen Verurteilungen und Straftaten	VV PRZ	anwendbar gem. SOA	nicht anwendbar
P.1.10 Datenverarbeitung im Auftrag	VV	nicht anwendbar	verpflichtend

KRITERIEN	RELE-VANTE ZIELOB-JEKTE	ANWENDUNG FÜR VERANT-WORTLICHEN	ANWENDUNG FÜR AUF-TRAGSVERARBEI-TER
P.2 Grundsätze			
P.2.1 Privacy-by-Design (Datenschutz durch Tech-nikgestaltung)	DSMS PRZ APPL VV IT INFRA DL	verpflichtend	
P.2.2 Privacy-by-Default (Datenschutzfreundliche Voreinstellungen)	DSMS PRZ APPL VV IT INFRA DL	verpflichtend	
P.2.3 Zweckbindung	VV PRZ APPL IT INFRA DL	verpflichtend	
P.2.4 Datenminimierung	VV PRZ APPL	verpflichtend	
P.2.5 Richtigkeit	VV PRZ APPL	verpflichtend	
P.2.6 Speicherbegrenzung	VV PRZ APPL	verpflichtend	
P.2.7 Treu und Glauben	VV PRZ APPL	verpflichtend	

KRITERIEN	RELEVANTE ZIELOBJEKTE	ANWENDUNG FÜR VERANTWORTLICHEN	ANWENDUNG FÜR AUFTRAGSVERARBEITER
P.3 Pflichten des Kunden			
P.3.1 Informationspflichten des Kunden	PRZ APPL	verpflichtend	verpflichtend
P.4 Auftragsverarbeitung			
P.4.1 Vertrag zur Auftragsverarbeitung (AV-Vertrag)	DSMS DL	anwendbar gem. SOA	verpflichtend
P.4.2 Umsetzung der Maßnahmen gem. AV-Vertrag	PRZ	nicht anwendbar	verpflichtend
P.4.3 Audit	DSMS DL	anwendbar gem. SOA	verpflichtend
P.5 Technisch-organisatorische Maßnahmen			
P.5.1 Festlegung geeigneter Maßnahmen	DSMS	verpflichtend	verpflichtend
P.5.2 Zutrittskontrolle (Vertraulichkeit und Integrität auf Ebene der physischen Zutritte)	INFRA	verpflichtend	verpflichtend
P.5.3 Zugangskontrolle (Vertraulichkeit und Integrität auf Ebene der Systemzugänge)	IT	verpflichtend	verpflichtend
P.5.4 Zugriffskontrolle (Vertraulichkeit und Integrität auf Ebene der Anwendungszugriffe)	APPL	verpflichtend	verpflichtend

KRITERIEN	RELE-VANTE ZIELOB-JEKTE	ANWENDUNG FÜR VERANT-WORTLICHEN	ANWENDUNG FÜR AUF-TRAGSVERARBEI-TER
P.5.5 Transportkontrolle (Vertraulichkeit und In-tegrität auf Transport-Ebene)	IT APPL	verpflichtend	verpflichtend
P.5.6 Trennungskontrolle	IT APPL	verpflichtend	verpflichtend
P.5.7 Eingabekontrolle	IT APPL	verpflichtend	verpflichtend
P.5.8 Verfügbarkeitskon-trolle	INFRA IT APPL	verpflichtend	verpflichtend
P.5.9 Pseudonymisierung/ Anonymisierung	PRZ APPL	verpflichtend	verpflichtend
P.5.10 Überprüfung, Be-wertung und Evaluierung	DSMS	verpflichtend	verpflichtend
P.6 Datenschutz-Management			
P.6.1 Fortlaufende Daten-schutz-Kontinuität	DSMS	verpflichtend	verpflichtend
P.6.2 Datenschutzbeauf-tragter	DSMS	anwendbar gem. SOA	anwendbar gem. SOA
P.6.3 Verpflichtung auf Vertraulichkeit/ Schulun-gen	DSMS	verpflichtend	verpflichtend
P.6.4 Verzeichnis von Ver-arbeitungstätigkeiten	VV DSMS	anwendbar gem. SOA	anwendbar gem. SOA
P.6.5 Datenschutz-Folgen-abschätzung	VV	anwendbar gem. SOA	anwendbar gem. SOA

KRITERIEN	RELE-VANTE ZIELOB-JEKTE	ANWENDUNG FÜR VERANT-WORTLICHEN	ANWENDUNG FÜR AUF-TRAGSVERARBEI-TER
P.6.6 Meldung von Daten-schutzverletzungen	DSMS	verpflichtend	verpflichtend
P.6.7 Zusammenarbeit mit Aufsichtsbehörden	DSMS	verpflichtend	verpflichtend
P.7 Datenverarbeitung außerhalb der EU			
P.7.1 Datenübermittlung in Drittstaaten	VV	anwendbar gem. SOA	anwendbar gem. SOA
P.7.2 Vertreter innerhalb der EU	VV	anwendbar gem. SOA	anwendbar gem. SOA
P.8 Betroffenenrechte			
P.8.1 Recht auf Auskunft	PRZ APPL	verpflichtend	verpflichtend
P.8.2 Recht auf Berichti-gung	PRZ APPL	verpflichtend	verpflichtend
P.8.3 Recht auf Löschung ("Recht auf Vergessenwer-den")	PRZ APPL	verpflichtend	verpflichtend
P.8.4 Recht auf Einschrän-kung	PRZ APPL	verpflichtend	verpflichtend
P.8.5 Mitteilungspflicht	PRZ APPL	verpflichtend	verpflichtend
P.8.6 Recht auf Daten-übertragbarkeit	PRZ APPL	verpflichtend	verpflichtend
P.8.7 Recht auf Wider-spruch	PRZ APPL	verpflichtend	verpflichtend

KRITERIEN	RELE-VANTE ZIELOB-JEKTE	ANWENDUNG FÜR VERANT-WORTLICHEN	ANWENDUNG FÜR AUF-TRAGSVERARBEI-TER
P.8.8 Recht auf Widerruf bei Einwilligung	PRZ APPL	verpflichtend	verpflichtend
P.8.9 Automatisierte Ent-scheidungen/Profiling	PRZ APPL	anwendbar gem. SOA	anwendbar gem. SOA
P.8.10 Beschwerde-Ma-nagement	DSMS	verpflichtend	

8. Referenzen

[DSGVO] Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung).

[EDPB_Guide-1] European Data Protection Board (EDPB), „Guidelines 1/2018 on certification and identifying certification criteria in accordance with Articles 42 and 43 of the Regulation", Version 3.0, 04.06.2019.

[EDPB_QA-C-311/18] European Data Protection Board (EDPB), „Häufig gestellte Fragen zum Urteil des Gerichtshofs der Europäischen Union in der Rechtssache C-311/18 — Data Protection Commissioner gegen Facebook Ireland Ltd und Maximillian Schrems", 23.07.2020.

[EDPB_01/2020] European Data Protection Board (EDPB), „Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data", 10.11.2020.

[EDPB _02/2018] European Data Protection Board (EDPB), „Guidelines 2/2018 on derogations of Art. 49 under Regulation 2016/679", 25.05.2018.

[EDPB_05_2021] European Data Protection Board (EDPB), „Guidelines 05/2021 on the Interplay between the application of Article 3 and the provisions on international transfers as per Chapter V of the GDPR", Version 1.0, 18.11.2021.

datenschutz cert

datenschutz cert GmbH

Konsul-Smidt-Straße 88a
28217 Bremen
Tel.: +49 421 69 66 32-550

office@datenschutz-cert.de
www.datenschutz-cert.de

datenschutz cert • ein Unternehmen der DSN GROUP