Öffentliche Version
basierend auf dem genehmigten
Kriterienkatalog 3.9(p1)

KRITERIENKATALOG FÜR ZERTIFIZIERUNGSVERFAHREN NACH ART. 42 DSGVO

Öffentliche Version zur Darstellung der genehmigten Zertifizierungskriterien

BDO

VERSIONSHISTORIE

Version	Datum	Beschreibung der Änderung
3.9	6. August 2025	Anpassung von Kriterien basierend auf Opinion 15/2025 zur Entwurfsentscheidung der österreichischen Aufsichtsbehörde (AT SA) zu den Zertifizierungskriterien
3.9 (p1)	9. September 2026	Aufbereitung der Veröffentlichungsfassung

EINLEITUNG UND ZWECK DIESER VERÖFFENTLICHUNG

Die vorliegende Veröffentlichungsfassung stellt die von der österreichischen Datenschutzbehörde genehmigten Zertifizierungskriterien der BDO Consulting GmbH für Zertifizierungsverfahren gemäß Art. 42 DSGVO in redaktionell verdichteter und lesefreundlicher Form dar. Sie dient der transparenten und hinreichend nachvollziehbaren Information darüber, welche Anforderungen im Rahmen einer Zertifizierung bewertet werden.

PRÄAMBEL

Die Datenschutz-Grundverordnung (DSGVO) bildet den verbindlichen Rechtsrahmen für Datenschutz in der Europäischen Union. Sie zielt darauf ab, unionsweit ein einheitlich hohes Datenschutzniveau zu gewährleisten sowie die Transparenz der Verarbeitung personenbezogener Daten und die Kontrolle der betroffenen Personen über ihre Daten zu stärken.

Art. 42 Abs. 1 DSGVO sieht die Förderung datenschutzspezifischer Zertifizierungsverfahren sowie von Datenschutzsiegeln und -prüfzeichen auf Unionsebene vor. Diese sollen Verantwortlichen und Auftragsverarbeiter:innen ermöglichen, die Einhaltung der auf die zertifizierten Verarbeitungsvorgänge anwendbaren datenschutzrechtlichen Anforderungen nachzuweisen. Dabei sind die besonderen Bedürfnisse von Kleinstunternehmen sowie kleinen und mittleren Unternehmen zu berücksichtigen.

Gemäß Art. 24 Abs. 3 DSGVO kann die Einhaltung eines Zertifizierungsverfahrens gemäß Art. 42 DSGVO als Gesichtspunkt herangezogen werden, um die Erfüllung der Pflichten des:der Verantwortlichen nachzuweisen. Auch Auftragsverarbeiter:innen können bei einer akkreditierten Zertifizierungsstelle eine Zertifizierung beantragen. Die Zertifizierung dient als Compliance-Instrument und schafft Transparenz hinsichtlich der zertifizierten Verarbeitungsvorgänge. Die Teilnahme ist freiwillig; die Erteilung und Aufrechterhaltung der Zertifizierung setzen jedoch regelmäßige Überprüfungen durch eine akkreditierte Zertifizierungsstelle voraus.

Die Zertifizierungskriterien der BDO Consulting GmbH wurden von der österreichischen Datenschutzbehörde genehmigt. Sie ermöglichen Verantwortlichen und Auftragsverarbeiter:innen, die Konformität der zu zertifizierenden Verarbeitungsvorgänge mit den jeweils einschlägigen Anforderungen der DSGVO nachzuweisen. Bei ihrer Ausgestaltung wurde besonderer Wert darauf gelegt, dass die Kriterien prüfbar, aussagekräftig sowie klar und verständlich formuliert sind und einen belastbaren Nachweis der DSGVO-Konformität der zertifizierten Verarbeitungsvorgänge ermöglichen.

Hinweis:

- Die Zertifizierungskriterien der BDO Consulting GmbH sind nationale Zertifizierungskriterien gemäß Art. 42 Abs. 5 DSGVO. Sie wurden nicht vom Europäischen Datenschutzausschuss als Grundlage für eine gemeinsame Zertifizierung genehmigt und begründen daher kein Europäisches Datenschutzsiegel.
- Die Zertifizierungskriterien sind kein Instrument für internationale Datenübermittlungen gemäß Art. 42 Abs. 2 i. V. m. Art. 46 Abs. 2 lit. f DSGVO. Die BDO Consulting GmbH weist ausdrücklich darauf hin, dass weder das Zertifizierungsschema noch die Zertifizierungskriterien selbst eine Zertifizierung im Sinne von Art. 46 Abs. 2 lit. f DSGVO darstellen und somit keine geeignete Garantie für die Übermittlung personenbezogener Daten in Drittländer oder an internationale Organisationen bieten.
- Übermittelt der:die Zertifizierungsantragsteller:in in der Rolle als Auftragsverarbeiter:in personenbezogene Daten an einen Datenimporteur in einem Drittland und soll diese Übermittlung zertifiziert werden, hat der:die

Zertifizierungsantragsteller:in die Wahl des konkreten Übermittlungsinstrumentes nach Kapitel V DSGVO zu begründen und zu dokumentieren (vgl. die einschlägigen Zertifizierungskriterien in Abschnitt B.11 „Übermittlung personenbezogener Daten in Drittländer oder an internationale Organisationen“). Der:die Zertifizierungsantragsteller:in hat den:die Verantwortliche:n darüber zu informieren, dass die Zertifizierungskriterien kein Übermittlungsinstrument im Sinne von Art. 42 Abs. 2 i. V. m. Art. 46 Abs. 2 lit. f DSGVO darstellen.

- Die Zertifizierungskriterien ermöglichen in ihrer aktuellen Fassung die Zertifizierung von Verantwortlichen sowie von Auftragsverarbeiter:innen, die in einem unmittelbaren Vertragsverhältnis zu Verantwortlichen stehen. Soweit einzelne Kriterien auf Unterauftragsverarbeiter:innen Bezug nehmen, regeln sie Anforderungen, die der:die Auftragsverarbeiter:in beim Einsatz von Unterauftragsverarbeiter:innen zur Einhaltung der DSGVO erfüllt. Eine eigenständige Zertifizierung von Unterauftragsverarbeiter:innen ist nach der aktuellen Fassung der Zertifizierungskriterien nicht vorgesehen.
- Eine Zertifizierung gemäß Art. 42 DSGVO entbindet Verantwortliche und Auftragsverarbeiter:innen nicht von ihrer Verantwortung für die Einhaltung der DSGVO. Die Aufgaben und Befugnisse der gemäß Art. 55 und 56 DSGVO zuständigen Aufsichtsbehörden bleiben unberührt.

ALLGEMEINE BEGRIFFSBESTIMMUNGEN

Akkreditierte Zertifizierungsstelle: Eine unabhängige Konformitätsbewertungsstelle, die gemäß der „Zertifizierungsstellen-Akkreditierungs-Verordnung – ZeStAkk-V“ akkreditiert ist.

Auftragsverarbeiter:in: Eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die personenbezogene Daten im Auftrag des Verantwortlichen verarbeitet.

Datenschutzkoordinator:in: Eine innerhalb einer Organisation benannte Person, die die operative Umsetzung von Datenschutzrichtlinien und -prozessen auf Fachbereichs- oder regionaler Ebene unterstützt. Der:die Datenschutzkoordinator:in fungiert als Schnittstelle zwischen den operativen Einheiten und der zentralen Datenschutzfunktion bzw. dem:der Datenschutzbeauftragten und unterstützt bei Sensibilisierung, Dokumentation und Compliance-Überwachung. Datenschutzkoordinator:innen sind nicht verpflichtend und können freiwillig benannt werden.

Personenbezogene Daten: Alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person (betroffene Person) beziehen; als identifizierbar wird eine Person angesehen, die direkt oder indirekt identifiziert werden kann, insbesondere mittels Zuordnung zu einer Kennung wie einem Namen, einer Kennnummer, Standortdaten, 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.

Unterauftragsverarbeiter:in: Eine juristische oder natürliche Person, die in einem Datenverarbeitungsverhältnis mit dem:der Auftragsverarbeiter:in steht, entweder direkt oder mittelbar über weitere beauftragte juristische oder natürliche Personen.

Verantwortliche:r: Die natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet; sind die Zwecke und Mittel dieser Verarbeitung durch das Unionsrecht oder das Recht der Mitgliedstaaten vorgegeben, so kann der:die Verantwortliche oder die konkreten Kriterien seiner:ihrer Benennung durch das Unionsrecht oder das Recht der Mitgliedstaaten vorgesehen werden.

Verarbeitung: Jeder Vorgang oder jede Vorgangsreihe, der/die mit oder ohne Hilfe automatisierter Verfahren im Zusammenhang mit personenbezogenen Daten ausgeführt wird, wie das Erheben, das Erfassen, die Organisation, das Ordnen, die Speicherung, die Anpassung oder Veränderung, das Auslesen, das Abfragen, die Verwendung, die Offenlegung durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung, der Abgleich oder die Verknüpfung, die Einschränkung, das Löschen oder die Vernichtung.

Zertifizierung: Bewertung und Zertifizierung durch eine akkreditierte Zertifizierungsstelle, welche bestätigt, dass die Zertifizierungskriterien erfüllt wurden.

Zertifizierungsanforderungen: Anforderungen – einschließlich der Zertifizierungskriterien –, die der:die Zertifizierungsantragsteller:in erfüllen muss, um eine Zertifizierung zu erhalten oder aufrechtzuerhalten.

Zertifizierungsantragsteller:in: Ein:e Verantwortliche:r gemäß Art. 4 Nr. 7 DSGVO oder ein:e Auftragsverarbeiter:in gemäß Art. 4 Nr. 8 DSGVO, der:die eine Zertifizierung anstrebt und für die Erfüllung der Zertifizierungsanforderungen verantwortlich ist.

Zertifizierungskriterien: Nach Art. 42 Abs. 5 DSGVO genehmigte Kriterien, anhand derer die Zertifizierung durchgeführt wird.

1. GEGENSTAND DER BEWERTUNG UND ANTRAGSTELLUNG

Gegenstand einer Zertifizierung gemäß Art. 42 DSGVO können **Verarbeitungsvorgänge von Verantwortlichen oder Auftragsverarbeiter:innen sein**. Die DSGVO enthält zwar keine eigenständige Definition des Begriffs „Verarbeitungsvorgänge“, definiert jedoch in Art. 4 Nr. 2 DSGVO den Begriff „Verarbeitung“. Darunter fällt jeder mit oder ohne Hilfe automatisierter Verfahren ausgeführte Vorgang oder jede solche Vorgangsreihe im Zusammenhang mit personenbezogenen Daten. Dazu zählen insbesondere das Erheben, Erfassen, Organisieren, Ordnen, Speichern, Anpassen oder Verändern, Auslesen, Abfragen, Verwenden, Offenlegen durch Übermittlung, Verbreiten oder eine andere Form der Bereitstellung, der Abgleich oder die Verknüpfung, die Einschränkung sowie das Löschen oder die Vernichtung personenbezogener Daten.

Ziel der Zertifizierung ist es, die Konformität der zu zertifizierenden Verarbeitungsvorgänge mit den jeweils einschlägigen Anforderungen der DSGVO festzustellen. Dazu zählen insbesondere die Einhaltung der Grundsätze gemäß Art. 5 DSGVO, die Wahrung der Rechte betroffener Personen sowie – sofern einschlägig – die Erfüllung der Anforderungen an die Übermittlung personenbezogener Daten an Drittländer oder internationale Organisationen.

Der Anwendungsbereich der Zertifizierung ist nicht auf bestimmte Verarbeitungstätigkeiten beschränkt. Die Zertifizierungskriterien folgen einem generischen Ansatz und können auf vielfältige Verarbeitungsvorgänge von Verantwortlichen und/oder Auftragsverarbeiter:innen angewendet werden – unabhängig von Branche, Geschäftstätigkeit oder Unternehmensgröße. Produkte selbst können nicht zertifiziert werden; zertifizierbar sind lediglich die mit dem Produkt oder der Dienstleistung verbundenen Verarbeitungsvorgänge.

Die Zertifizierungskriterien sind so ausgestaltet, dass sie gemäß Art. 42 Abs. 1 Satz 2 und Erwägungsgrund 100 DSGVO auch auf Verarbeitungsvorgänge von Kleinstunternehmen sowie kleinen und mittleren Unternehmen angewendet werden können. Die BDO Consulting GmbH verfolgt als akkreditierte Zertifizierungsstelle das Ziel, diese Unternehmen beim Nachweis einer DSGVO-konformen Ausgestaltung ihrer Verarbeitungsvorgänge zu unterstützen.

REIFEGRADBEWERTUNG

Es wird empfohlen, dass Zertifizierungsantragsteller:innen vor Beginn des Zertifizierungsverfahrens eine unabhängige Reifegradbewertung durchführen und prüfen, ob sie die Zertifizierungskriterien erfüllen. Eine solche Reifegradbewertung greift der Entscheidung der Zertifizierungsstelle im Zertifizierungsverfahren nicht vor.

ANTRAGSTELLUNG

Um eine Zertifizierung gemäß Art. 42 DSGVO durchzuführen, ist ein schriftlicher Antrag bei der Zertifizierungsstelle BDO Consulting GmbH einzureichen. Das Antragsformular für die Durchführung einer Datenschutz-Zertifizierung nach Art. 42 DSGVO ist auf Anfrage erhältlich. Der Zertifizierungsantrag hat sämtliche für das Zertifizierungsverfahren erforderlichen Informationen zu enthalten, und der Gegenstand der Zertifizierung ist eindeutig und unmissverständlich zu definieren.

Das Target of Evaluation (ToE) bezeichnet die Verarbeitungsvorgänge, die auf Grundlage der Zertifizierungskriterien der BDO Consulting GmbH zertifiziert werden sollen. Aus seiner Beschreibung muss klar hervorgehen, welche Verarbeitungsvorgänge vom Geltungsbereich des ToE erfasst und welche davon ausgeschlossen sind.

Zur eindeutigen Abgrenzung des ToE sind sämtliche relevanten Umstände der Verarbeitungsvorgänge festzulegen. Dazu zählen insbesondere die Verarbeitungszwecke, die Empfänger:innen sowie die Haupt- und Teilkomponenten der Verarbeitungsvorgänge. Darüber hinaus ist die unterstützende technische Infrastruktur zu beschreiben. Dies umfasst insbesondere Betriebssysteme, virtuelle Systeme, Datenbanken, Authentifizierungs- und Autorisierungssysteme, Router und Firewalls, Speichersysteme, Kommunikationsinfrastrukturen und Internetzugänge sowie die damit verbundenen technischen Maßnahmen. Sämtliche zur Spezifizierung des ToE erforderlichen Angaben sind im Antragsformular abschließend aufgeführt.

Nach Eingang des Antrags prüft die BDO Consulting GmbH die darin enthaltenen Angaben sowie die gegebenenfalls eingereichten Unterlagen auf Vollständigkeit.

2. GESTALTUNG UND STRUKTUR DER ZERTIFIZIERUNGSKRITERIEN

2.1. GESTALTUNG DER ZERTIFIZIERUNGSKRITERIEN

Die Grundlage für die Zertifizierungskriterien wurde aus den Grundsätzen und Vorschriften der DSGVO abgeleitet, um sicherzustellen, dass diese Grundsätze und Vorschriften eingehalten und die Einhaltung durch die Zertifizierungsstelle überprüft wird.

Die Zertifizierungskriterien berücksichtigen insbesondere folgende datenschutzrelevante Bereiche:

- die Grundsätze der Datenverarbeitung gemäß Art. 5 DSGVO,
- die Rechtmäßigkeit der Verarbeitung gemäß Art. 6 DSGVO,
- die Rechte der betroffenen Personen gemäß Art. 12 bis 23 DSGVO,
- die Verpflichtung zur Meldung von Datenschutzverletzungen gemäß Art. 33 DSGVO,
- die Verpflichtung zu Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen gemäß Art. 25 DSGVO,
- gegebenenfalls die Durchführung einer Datenschutz-Folgenabschätzung gemäß Art. 35 DSGVO,
- technische und organisatorische Maßnahmen gemäß Art. 32 DSGVO,
- die Übermittlung personenbezogener Daten an ein Drittland oder eine internationale Organisation gemäß Art. 44 bis 49 DSGVO (Drittlandübermittlung).

2.2. STRUKTUR DER ZERTIFIZIERUNGSKRITERIEN

Die Zertifizierungskriterien der BDO Consulting GmbH ermöglichen Verantwortlichen und Auftragsverarbeiter:innen, die Konformität ihrer Verarbeitungsvorgänge mit den jeweils einschlägigen Anforderungen der DSGVO nachzuweisen:

- Die von **Verantwortlichen zu erfüllenden Datenschutzanforderungen sind in Abschnitt 4 dargestellt (Kriterien A.01.01 bis A.11.07)**. Handelt der:die Zertifizierungsantragsteller:in als Verantwortliche:r, weist er:sie die Erfüllung der auf die zu zertifizierenden Verarbeitungsvorgänge anwendbaren Anforderungen nach.
- Die von **Auftragsverarbeiter:innen zu erfüllenden Datenschutzanforderungen sind in Abschnitt 5 dargestellt (Kriterien B.01.01 bis B.11.06)**. Handelt der:die Zertifizierungsantragsteller:in als Auftragsverarbeiter:in, weist er:sie die Erfüllung der auf die zu zertifizierenden Verarbeitungsvorgänge anwendbaren Anforderungen nach.

Ein Zertifizierungskriterium bezeichnet eine konkrete Anforderung, die für die Erteilung einer Zertifizierung gemäß Art. 42 DSGVO erfüllt sein muss. Jedem Kriterium ist eine numerische Kennung zugeordnet, die seiner eindeutigen Identifikation und Referenzierung dient.

Jedes Zertifizierungskriterium umfasst eine übergeordnete Anforderung sowie eine detaillierte Darstellung der zu erfüllenden Anforderungen. Die übergeordnete Anforderung vermittelt einen zusammenfassenden Überblick, während die detaillierten Anforderungen die erforderlichen Maßnahmen oder Vorgehensweisen konkretisieren. Die detaillierten Anforderungen haben normativen Charakter und sind zu erfüllen, sofern das jeweilige Zertifizierungskriterium auf die zu zertifizierenden Verarbeitungsvorgänge anwendbar ist.

Eine ausführliche Fassung des Kriterienkatalogs mit ergänzenden Hinweisen auf Leitlinien des Europäischen Datenschutzausschusses, frühere Leitlinien der Artikel-29-Datenschutzgruppe, einschlägige Rechtsprechung und relevante Standards ist auf Anfrage bei der BDO Consulting GmbH erhältlich. Im Bereich der technischen und organisatorischen Maßnahmen bestehen insbesondere Orientierungspunkte zu ISO/IEC 27001 und ISO/IEC 27002. Diese ergänzenden Inhalte unterstützen das Verständnis und die praktische Anwendung der Kriterien, begründen jedoch keine zusätzlichen oder von den veröffentlichten Kriterien abweichenden normativen Anforderungen.

3. NICHTANWENDBARKEIT VON ZERTIFIZIERUNGSKRITERIEN

Die Zertifizierungskriterien der BDO Consulting GmbH sind so ausgestaltet, dass sie auf Verarbeitungstätigkeiten von Verantwortlichen und/oder Auftragsverarbeiter:innen unabhängig von Branche, Geschäftstätigkeit oder Unternehmensgröße anwendbar sind. In der Praxis bedeutet dies jedoch, dass nicht alle Kriterien für jede einzelne Zertifizierung gleichermaßen relevant sind.

Für jene Kriterien, deren Anwendbarkeit von der konkreten Verarbeitungstätigkeit abhängt, ist unter „Detaillierte Anforderungen“ ein entsprechender Hinweis vorgesehen. Im Rahmen der Festlegung des Prüfgegenstands (Target of Evaluation – ToE) hat der:die Zertifizierungsantragsteller:in anzugeben, welche dieser Kriterien auf die zu zertifizierende Verarbeitungstätigkeit anwendbar sind und etwaige Ausschlüsse entsprechend zu begründen.

Beispiele für Kriterien, die nicht anwendbar sein können, umfassen:

- sofern der:die Zertifizierungsantragsteller:in in der Rolle als Verantwortliche:r keine Auftragsverarbeiter:innen einsetzt,
- sofern im Rahmen der zu zertifizierenden Verarbeitungstätigkeit keine Übermittlung personenbezogener Daten in Drittländer oder an internationale Organisationen erfolgt, oder
- sofern die in der DSGVO genannten Voraussetzungen für die Anwendung einer Anforderung nicht erfüllt sind – beispielsweise:
  - die Pflicht zur Bestellung eines:einer Datenschutzbeauftragten gemäß Art. 37 Abs. 1 und 4 DSGVO, oder
  - die Ausnahme von der Pflicht zur Führung eines Verzeichnisses von Verarbeitungstätigkeiten gemäß Art. 30 Abs. 5 DSGVO.

Dementsprechend wird die Anwendbarkeit sämtlicher Kriterien, die mit einem entsprechenden Hinweis zur Anwendbarkeit versehen sind, im Rahmen des Zertifizierungsprozesses im Einzelfall beurteilt.

4. KRITERIEN FÜR VERANTWORTLICHE

4.1. DATENSCHUTZORGANISATION

A.01.01 – EINHALTUNG VON ART. 5 DSGVO (RECHENSCHAFTSPFLICHT) DURCH IMPLEMENTIERUNG EINER DATENSCHUTZRICHTLINIE

Überblick
Der:die Zertifizierungsantragsteller:in ist für die Einhaltung der Grundsätze des Art. 5 Abs. 1 DSGVO verantwortlich und muss deren Einhaltung gemäß Art. 5 Abs. 2 DSGVO nachweisen können. Hierzu stellt der:die Zertifizierungsantragsteller:in sicher, dass geeignete Datenschutzrichtlinien festgelegt sind.
Detaillierte Anforderungen
Der:die Zertifizierungsantragsteller:in legt in einer dokumentierten Datenschutzrichtlinie den Stellenwert des Datenschutzes sowie einheitliche Prozesse und betriebliche Anweisungen fest, um die Datenschutzanforderungen und die damit verbundenen Rechenschafts- und Nachweispflichten zu erfüllen. Die Datenschutzrichtlinie kann aus einem oder mehreren Dokumenten bestehen und umfasst mindestens folgende Inhalte: ▶ Identität und Kontaktdaten des:der Verantwortlichen; ▶ Kontaktdaten des:der Datenschutzbeauftragten, sofern benannt; ▶ Kontaktdaten von Datenschutzkoordinator:innen, sofern vorhanden; ▶ Datenschutzgrundsätze (siehe Kriterien A.02.01–A.02.06); ▶ Datenschutz-Folgenabschätzung und Risikomanagement, sofern anwendbar (siehe Kriterien A.06.01 und A.09.01 ff.); ▶ „Privacy by Design“ und „Privacy by Default“, einschließlich der Integration des Datenschutzes in die Entwicklung von Produkten, Dienstleistungen und Prozessen sowie datenschutzfreundlicher Standardeinstellungen (siehe Kriterien A.04.01 und A.04.02); ▶ Umgang mit den Rechten betroffener Personen (siehe Kriterien A.03.01–A.03.11); ▶ Ablauf zum Umgang mit Datenschutzverletzungen (siehe Kriterien A.08.01–A.08.07); ▶ Prüfung der Einhaltung von Datenschutzanforderungen durch Auftragsverarbeiter:innen, sofern relevant (siehe Kriterien A.04.04–A.04.07); und ▶ Regelungen zur Datenweitergabe an Dritte und in Drittländer, sofern relevant (siehe Kriterien A.11.01–A.11.07). Sofern ein:e Datenschutzbeauftragte:r benannt wurde, wird die formale Stellungnahme zur Datenschutzrichtlinie berücksichtigt. Die Datenschutzrichtlinie wird mindestens einmal jährlich sowie anlassbezogen aktualisiert.

A.01.02 - DATENSCHUTZORGANISATION EINSCHLIEßLICH ROLLEN UND VERANTWORTLICHKEITEN

Überblick
Die Rollen und Verantwortlichkeiten innerhalb der Datenschutzorganisation werden schriftlich festgelegt. Die Gesamtheit der Rollen deckt die Anforderungen an Zuständigkeiten gemäß DSGVO sowie die Umsetzung der Datenschutzziele ab.
Detaillierte Anforderungen
Der:die Zertifizierungsantragsteller:in dokumentiert die Rollen und Verantwortlichkeiten innerhalb der Datenschutzorganisation sowie die zugrunde liegende Organisationsstruktur des Unternehmens oder der Unternehmensgruppe (z. B. in Form eines Organigramms). Die Dokumentation zur Datenschutzorganisation umfasst mindestens die Verantwortlichkeiten innerhalb der Datenschutzorganisation (z. B. Datenschutzbeauftragte:r (sofern benannt), Datenschutzkoordinator:innen (sofern benannt), Geschäftsleitung und sonstige Gremien), funktionale Schnittstellen (z. B. IT, Informationssicherheit), Aufgaben und Verantwortlichkeiten der jeweiligen Rollen, Darstellung der Zusammenarbeit zwischen den Rollen, Darstellung der Zusammenarbeit mit der Geschäftsführung. Im Falle einer Unternehmensgruppe umfasst die Datenschutzorganisation auch die datenschutzbezogenen Funktionen und deren Zusammenarbeit zwischen den Gesellschaften der Unternehmensgruppe.

A.01.03 – REGELMÄßIGE SCHULUNGS- UND SENSIBILISIERUNGSMAßNAHMEN FÜR MITARBEITENDE

Überblick
Der:die Zertifizierungsantragsteller:in informiert Mitarbeitende über die datenschutzrechtlichen Vorschriften und stellt entsprechende Datenschutzschulungen bereit.
Detaillierte Anforderungen
Der:die Zertifizierungsantragsteller:in schult jene Mitarbeitenden, die im Rahmen der zu zertifizierenden Verarbeitungstätigkeiten personenbezogene Daten verarbeiten, in regelmäßigen Abständen. Hierzu werden zielgruppenspezifische Schulungsmaßnahmen umgesetzt. Die Schulungsmaßnahmen können in unterschiedlicher Form durchgeführt werden, etwa als Präsenzschulung, Selbststudium, interaktiver Workshop, Online-Training/eLearning, Kampagnen, Broschüren, Newsletter, Informationsveranstaltungen oder E-Mails. Die Schulungsmaßnahmen sollen insbesondere das Bewusstsein in folgenden Bereichen schärfen: ▶ Grundlagen der geltenden Datenschutzgesetze (z. B. DSGVO und österreichisches Datenschutzgesetz); ▶ Grundlegende Verfahren des Datenschutzes und der Informationssicherheit (z. B. Meldung von Datenschutzverletzungen, potenzielle Datenschutzrisiken, Passwortsicherheit); ▶ Informationen zu Pflichten und Verantwortlichkeiten der Mitarbeitenden im Hinblick auf Datenschutz; ▶ Kontaktstellen für weiterführende Informationen und Beratung zum Datenschutz. Sofern ein:e Datenschutzbeauftragte:r benannt ist, bezieht der:die Zertifizierungsantragsteller:in diese:n in die Erstellung der Schulungsunterlagen ein. Die Durchführung und Teilnahme an Schulungsmaßnahmen werden nachvollziehbar dokumentiert. Bei Präsenzschulungen erfolgt der Nachweis insbesondere durch Teilnehmerlisten; bei Online-Schulungen durch geeignete elektronische Teilnahme- oder Abschlussnachweise. Soweit ein Abschlusstest vorgesehen ist, werden dessen Durchführung und Ergebnis dokumentiert.

A.01.04 - Laufende Überwachung der Einhaltung datenschutzrechtlicher Anforderungen

Überblick
Der:die Zertifizierungsantragsteller:in stellt durch eine laufende Überwachung sicher, dass die Datenschutzanforderungen wirksam umgesetzt und eingehalten werden. Die bestehenden Datenschutzmaßnahmen werden hinsichtlich Angemessenheit (Design-Kontrolle) und Wirksamkeit (Wirksamkeitskontrolle) überprüft.
Detaillierte Anforderungen
Der:die Zertifizierungsantragsteller:in richtet ein Überwachungsverfahren ein, das eine risikoorientierte Analyse der Datenschutzaktivitäten über einen definierten Zeitraum ermöglicht (z. B. Überprüfung von Richtlinien). Die Überwachung basiert auf einer Risikokarte (Monitoring-Plan). Überprüfungen sind beispielsweise bei Verarbeitungsvorgängen mit hohem Risiko, wie Profiling oder der Verarbeitung von Gesundheitsdaten, durchzuführen. Die Ergebnisse der Überwachungsaktivitäten werden dokumentiert. Werden dabei Abweichungen festgestellt, erfolgt eine zeitnahe Berichterstattung an die Geschäftsleitung. Zur Behebung der festgestellten Mängel oder Abweichungen wird ein strukturiertes und dokumentiertes Maßnahmenprogramm festgelegt und umgesetzt. Erforderliche Anpassungen bestehender Datenschutzmaßnahmen werden vor ihrer Umsetzung von der Geschäftsleitung genehmigt. Führt der:die Zertifizierungsantragsteller:in keine laufenden internen Audits auf Grundlage eines Monitoring-Plans durch, lässt er:sie die Angemessenheit (Test of Design) und Wirksamkeit (Test of Effectiveness) der bestehenden Datenschutzmaßnahmen und Datenschutzanforderungen regelmäßig durch eine unabhängige externe Stelle überprüfen (z. B. gemäß ISAE 3000, ISAE 3402 oder ISO 27001 in Verbindung mit ISO 27701).

4.2. DATENSCHUTZGRUNDSÄTZE

A.02.01 - Maßnahmen zur Umsetzung des Grundsatzes der Transparenz

Überblick
Der:die Zertifizierungsantragsteller:in stellt die Einhaltung des Grundsatzes der Transparenz gemäß Art. 5 Abs. 1 lit. a DSGVO sicher.
Detaillierte Anforderungen
Der:die Zertifizierungsantragsteller:in implementiert Verfahren, Mechanismen oder Regelungen, die gewährleisten, dass die Transparenzanforderungen der DSGVO erfüllt werden, insbesondere, dass: ▶ betroffene Personen gemäß Art. 12, 13 und 14 DSGVO informiert werden; ▶ betroffene Personen über die Ausübung ihrer Rechte gemäß Art. 15-22 DSGVO informiert werden; ▶ betroffene Personen gemäß Art. 34 DSGVO bei einer Datenschutzverletzung benachrichtigt werden. Für die zu zertifizierenden Verarbeitungstätigkeiten dokumentiert der:die Zertifizierungsantragsteller:in, auf welche Weise die erforderlichen Informationen für betroffene Personen bereitgestellt werden (z. B. durch einen Vermerk im Verzeichnis der Verarbeitungstätigkeiten, eine Verlinkung auf die Website oder einen Hinweis auf Datenschutzhinweise in Print-Unterlagen, Verweise oder Links auf übergeordnete Prozessbeschreibungen oder Datenerhebungsformulare). Die bereitgestellten Informationen erfüllen die Anforderungen des Art. 12 DSGVO. Sie sind insbesondere präzise, transparent, verständlich und leicht zugänglich sowie in klarer und einfacher Sprache formuliert. Die Informationen werden grundsätzlich schriftlich oder elektronisch und unentgeltlich bereitgestellt; auf Wunsch der betroffenen Person kann die Information auch mündlich erfolgen. Zur Umsetzung des Transparenzgrundsatzes wird ergänzend auf die Anforderungen zu Betroffenenanfragen und Betroffenenrechten gemäß A.03.01 bis A.03.11 sowie zur Mitteilung von Datenschutzverletzungen gemäß A.08.04 verwiesen.

A.02.02 – Maßnahmen zur Umsetzung des Grundsatzes der Fairness

Überblick
Der:die Zertifizierungsantragsteller:in stellt sicher, dass personenbezogene Daten gemäß dem Grundsatz der Verarbeitung nach Treu und Glauben („Fairness“) nach Art. 5 Abs. 1 lit. a DSGVO verarbeitet werden.
Detaillierte Anforderungen
Personenbezogene Daten dürfen nicht auf eine Weise verarbeitet werden, die für betroffene Personen in nicht gerechtfertigter Weise schädlich, widerrechtlich diskriminierend, unerwartet oder irreführend ist. Zu diesem Zweck bewertet der:die Zertifizierungsantragsteller:in die zu zertifizierenden Verarbeitungstätigkeiten und prüft dabei mindestens, ob ▶ betroffene Personen durch die Verarbeitung nicht irregeführt werden, ▶ deren Position oder mangelnde Kenntnisse nicht unangemessen ausgenutzt werden, ▶ betroffene Personen nicht in ungerechtfertigter Weise benachteiligt oder diskriminiert werden und ▶ die Verarbeitung nicht unangemessen von dem abweicht, was betroffene Personen vernünftigerweise erwarten können. Die Ergebnisse der Bewertung werden dokumentiert.

A.02.03 - Maßnahmen zur Umsetzung des Grundsatzes der Zweckbindung

Überblick
Der:die Zertifizierungsantragsteller:in stellt sicher, dass der Grundsatz der Zweckbindung gemäß Art. 5 Abs. 1 lit. b DSGVO eingehalten wird.
Detaillierte Anforderungen
Für die zu zertifizierenden Verarbeitungstätigkeiten dokumentiert der:die Zertifizierungsantragsteller:in ▶ die jeweiligen Verarbeitungszwecke, z. B. im Verzeichnis der Verarbeitungstätigkeiten gemäß Art. 30 DSGVO, und

Detaillierte Anforderungen

- die Information der betroffenen Personen über die Zwecke, für die ihre personenbezogenen Daten verarbeitet werden (insbesondere in den entsprechenden Datenschutzhinweisen).

Der:die Zertifizierungsantragsteller:in überprüft die Verarbeitungszwecke mindestens einmal jährlich sowie anlassbezogen bei wesentlichen Änderungen der Verarbeitungstätigkeit (z. B. aufgrund technologischer Entwicklungen). Bei beabsichtigten Änderungen einer Verarbeitung wird geprüft, ob diese auch die festgelegten Verarbeitungszwecke betreffen. Bei der Überprüfung werden relevante interne und externe Faktoren berücksichtigt, die sich auf die zertifizierten Verarbeitungstätigkeiten auswirken können.

Der:die Zertifizierungsantragsteller:in dokumentiert die Überprüfung. Ändert sich der vorgesehene Verarbeitungszweck, wird auch diese Änderung dokumentiert und ein Kompatibilitätstest gemäß Kriterium A.02.07.07 durchgeführt.

A.02.04 - Maßnahmen zur Umsetzung des Grundsatzes der Datenminimierung

Überblick

Der:die Zertifizierungsantragsteller:in stellt sicher, dass der Grundsatz der Datenminimierung gemäß Art. 5 Abs. 1 lit. c DSGVO eingehalten wird und die verarbeiteten personenbezogenen Daten auf das für die Zwecke der Verarbeitung notwendige Maß beschränkt sind.

Detaillierte Anforderungen

Für jede zu zertifizierende Verarbeitungstätigkeit dokumentiert der:die Zertifizierungsantragsteller:in die Maßnahmen zur Datenminimierung und begründet, warum die verarbeiteten personenbezogenen Daten für die vorgesehenen Zwecke angemessen, relevant und erforderlich sind.

Dies kann – muss jedoch nicht zwingend – eine vergleichende Analyse umfassen. Dabei kann insbesondere geprüft werden, ob die Zwecke mit weniger Daten erreicht, die Verarbeitung besonderer Kategorien personenbezogener Daten vermieden oder der Kreis der betroffenen Personen reduziert werden kann.

Der:die Zertifizierungsantragsteller:in überprüft die Erforderlichkeit der verarbeiteten personenbezogenen Daten mindestens einmal jährlich sowie anlassbezogen bei wesentlichen Änderungen der Verarbeitungstätigkeit, z. B. aufgrund technologischer Entwicklungen. Dabei werden sämtliche internen und externen Faktoren, die Auswirkungen auf die zertifizierten Verarbeitungstätigkeiten haben können, berücksichtigt.

Der:die Zertifizierungsantragsteller:in dokumentiert die Überprüfung sowie daraus resultierende Entscheidungen und Maßnahmen.

A.02.05 - Maßnahmen zur Umsetzung des Grundsatzes der Richtigkeit

Überblick

Der:die Zertifizierungsantragsteller:in stellt sicher, dass der Grundsatz der Richtigkeit gemäß Art. 5 Abs. 1 lit. d DSGVO eingehalten wird und die verarbeiteten personenbezogenen Daten sachlich richtig sind sowie erforderlichenfalls aktualisiert oder berichtigt werden.

Detaillierte *Anforderungen*

Für die zu zertifizierenden Verarbeitungstätigkeiten richtet der:die Zertifizierungsantragsteller:in ein Verfahren ein, mit dem die Richtigkeit und Aktualität der verarbeiteten personenbezogenen Daten sichergestellt wird. Das Verfahren umfasst mindestens:

- die Erfassung und Bewertung der relevanten Datenquellen im Hinblick auf ihre Zuverlässigkeit und Relevanz. Dabei wird insbesondere berücksichtigt,
  - ob die Daten direkt bei der betroffenen Person oder indirekt aus anderen Quellen erhoben werden,
  - ob und in welchem Umfang andere Verantwortliche vor Erhalt der Daten an deren Erhebung oder Verarbeitung beteiligt waren und
  - welche Maßnahmen bei einer indirekten Datenerhebung zur Überprüfung der Richtigkeit der Daten getroffen werden, sofern dies erforderlich ist;
- Maßnahmen zur Überprüfung der verarbeiteten personenbezogenen Daten auf Richtigkeit und Aktualität;
- Maßnahmen, die gewährleisten, dass personenbezogene Daten, die im Hinblick auf die Zwecke ihrer Verarbeitung unrichtig sind, unverzüglich berichtigt oder gelöscht werden.

Detaillierte Anforderungen
Der:die Zertifizierungsantragsteller:in überprüft das Verfahren mindestens einmal jährlich sowie anlassbezogen bei wesentlichen Änderungen der Verarbeitungstätigkeit (z. B. aufgrund technologischer Entwicklungen). Bei der Überprüfung werden relevante interne und externe Faktoren berücksichtigt, die sich auf die zertifizierten Verarbeitungstätigkeiten auswirken können.

A.02.06 - Maßnahmen zur Umsetzung des Grundsatzes der Speicherbegrenzung

Überblick
Der:die Zertifizierungsantragsteller:in stellt sicher, dass der Grundsatz der Speicherbegrenzung gemäß Art. 5 Abs. 1 lit. e DSGVO eingehalten wird und personenbezogene Daten nur so lange gespeichert werden, wie es für die festgelegten Verarbeitungszwecke erforderlich ist.
Detaillierte Anforderungen
Für die zu zertifizierenden Verarbeitungstätigkeiten legt der:die Zertifizierungsantragsteller:in Aufbewahrungsfristen für personenbezogene Daten sowie für damit verbundene Aktivitätsprotokolle im Zusammenhang mit der Nutzung von IT-Systemen fest und dokumentiert diese. Die festgelegten Aufbewahrungsfristen sind mit dem Verzeichnis der Verarbeitungstätigkeiten (A.05.01–A.05.04), den Anforderungen zum Transparenzgrundsatz (A.02.01) sowie den Vorgaben zur Festlegung von Aufbewahrungsfristen (A.07.25) konsistent.

A.02.07 - Maßnahmen zur Umsetzung des Grundsatzes der Integrität und Vertraulichkeit

Überblick
Der:die Zertifizierungsantragsteller:in stellt sicher, dass der Grundsatz der Integrität und Vertraulichkeit gemäß Art. 5 Abs. 1 lit. f DSGVO eingehalten wird. Personenbezogene Daten dürfen daher nur in einer Weise verarbeitet werden, die eine angemessene Sicherheit der personenbezogenen Daten gewährleistet.
Detaillierte Anforderungen
Für die zu zertifizierenden Verarbeitungstätigkeiten legt der:die Zertifizierungsantragsteller:in Prozesse und Maßnahmen zur Gewährleistung der Integrität und Vertraulichkeit personenbezogener Daten fest und dokumentiert diese. Dies umfasst insbesondere: ▶ die Durchführung einer Risikoanalyse (A.06.01–A.06.03); ▶ die Planung und Umsetzung risikoadäquater Maßnahmen (A.07.01–A.07.26); und ▶ die Dokumentation der getroffenen Datensicherheitsmaßnahmen zur Beseitigung oder Minderung bestehender Risiken (A.06.02).

4.3. RECHTMÄßIGKEIT DER DATENVERARBEITUNG

A.02.07.01 - Einwilligung in die Verarbeitung personenbezogener Daten

Überblick

Der:die Zertifizierungsantragsteller:in stellt sicher, dass für die zu zertifizierenden Verarbeitungsvorgänge eine Rechtsgrundlage gemäß Art. 6 DSGVO vorliegt. Stützt sich die Verarbeitung auf eine Einwilligung gemäß Art. 6 Abs. 1 lit. a DSGVO, werden zusätzlich die Anforderungen des Art. 7 und Art. 4 Nr. 11 DSGVO eingehalten.

Detaillierte Anforderungen

***Anwendbarkeit**: Dieses Kriterium gilt, wenn sich der:die Zertifizierungsantragsteller:in für die zu zertifizierende Verarbeitungstätigkeit auf die Einwilligung als Rechtsgrundlage gemäß Art. 6 Abs. 1 lit. a DSGVO stützt.*

Der:die Zertifizierungsantragsteller:in weist nach, dass für die jeweiligen Verarbeitungszwecke eine wirksame Einwilligung der betroffenen Person vorliegt. Dabei gilt Folgendes:

1. Eignung der Einwilligung als Rechtsgrundlage

Der:die Zertifizierungsantragsteller:in dokumentiert, warum die Einwilligung für die jeweilige Verarbeitungstätigkeit eine geeignete Rechtsgrundlage darstellt.

2. Einholung und Dokumentation

- Die Einwilligung wird durch eine eindeutige bestätigende Handlung eingeholt (z. B. durch Ankreuzen eines Kästchens, Wahl technischer Einstellungen oder eine mündliche Erklärung).
- Die Einwilligung ist freiwillig, spezifisch, informiert und unmissverständlich.
- Werden mehrere Zwecke verfolgt, werden getrennte Einwilligungsmöglichkeiten vorgesehen.
- Die Einwilligung wird schriftlich oder elektronisch eingeholt. Bei einer mündlichen Einwilligung dokumentiert der:die Zertifizierungsantragsteller:in Zeitpunkt, Art und Umstände ihrer Erteilung.
- Die Einwilligungsanfrage enthält einen Hinweis auf das Widerrufsrecht und darauf, dass ein Widerruf die Rechtmäßigkeit der bis dahin erfolgten Verarbeitung nicht berührt.
- Einwilligungen, Änderungen und Widerrufe werden nachvollziehbar dokumentiert (z. B. elektronisch oder durch gescannte Unterlagen).

3. Erneuerung

- Einwilligungen werden spätestens drei Jahre nach ihrer letzten Nutzung erneuert, sofern nicht der Kontext, der Umfang der ursprünglichen Einwilligung und die Erwartungen der betroffenen Person eine andere Frist rechtfertigen.

A.02.07.02 - Verarbeitung personenbezogener Daten zur Erfüllung eines Vertrags oder zur Durchführung vorvertraglicher Maßnahmen

Überblick

Der:die Zertifizierungsantragsteller:in stellt sicher, dass für die zu zertifizierenden Verarbeitungsvorgänge eine Rechtsgrundlage gemäß Art. 6 DSGVO vorliegt. Stützt sich die Verarbeitung auf Art. 6 Abs. 1 lit. b DSGVO, wird sichergestellt, dass (i) die verarbeiteten Daten für die Vertragserfüllung bzw. die vorvertraglichen Maßnahmen erforderlich sind, (ii) die betroffene Person Vertragspartei ist und — im Falle vorvertraglicher Maßnahmen — dass diese auf Anfrage der betroffenen Person erfolgen.

Detaillierte Anforderungen

***Anwendbarkeit**: Dieses Kriterium gilt, wenn sich der:die Zertifizierungsantragsteller:in für die zu zertifizierende Verarbeitungstätigkeit auf die Erfüllung eines Vertrags oder die Durchführung vorvertraglicher Maßnahmen gemäß* Art. 6 *Abs. 1 lit. b DSGVO stützt.*

Der:die Zertifizierungsantragsteller:in prüft und dokumentiert Art und konkreten Inhalt des zugrunde liegenden Vertrags. Dabei gilt Folgendes:

- Der:die Zertifizierungsantragsteller:in begründet und dokumentiert, warum die Verarbeitung personenbezogener Daten für die Vertragserfüllung oder zur Durchführung vorvertraglicher Maßnahmen auf Anfrage der betroffenen Person erforderlich ist.
- Bei der Prüfung der Erforderlichkeit wird berücksichtigt, ob der jeweilige Zweck auch durch eine weniger eingriffsintensive Verarbeitung erreicht werden kann.

A.02.07.03 - Verarbeitung personenbezogener Daten zur Erfüllung einer rechtlichen Verpflichtung

Überblick

Der:die Zertifizierungsantragsteller:in stellt sicher, dass für die zu zertifizierenden Verarbeitungsvorgänge eine Rechtsgrundlage gemäß Art. 6 DSGVO vorliegt. Stützt sich die Verarbeitung auf die Erfüllung einer rechtlichen Verpflichtung gemäß Art. 6 Abs. 1 lit. c DSGVO, wird sichergestellt, dass die jeweilige rechtliche Verpflichtung anwendbar und die Verarbeitung auf das zu ihrer Erfüllung erforderliche Maß beschränkt ist.

Detaillierte Anforderungen

***Anwendbarkeit**: Dieses Kriterium gilt, wenn sich der:die Zertifizierungsantragsteller:in für die zu zertifizierende Verarbeitungstätigkeit auf die Erfüllung einer rechtlichen Verpflichtung gemäß Art. 6 Abs. 1 lit. c DSGVO stützt.*

Der:die Zertifizierungsantragsteller:in prüft und dokumentiert die rechtliche Verpflichtung, auf die sich die Verarbeitung stützt. Dabei gilt Folgendes:

- Die anwendbare rechtliche Verpflichtung wird identifiziert und dokumentiert und ihre Relevanz für die zu zertifizierende Verarbeitungstätigkeit bewertet.
- Die zugrunde liegende Rechtsgrundlage muss hinreichend klar, präzise und vorhersehbar sein und die Zwecke bestimmen, für die die Verarbeitung erforderlich ist.
- Der:die Zertifizierungsantragsteller:in prüft und dokumentiert, dass die Verarbeitung auf das zur Erfüllung der rechtlichen Verpflichtung erforderliche Maß beschränkt ist und nicht über den hierfür notwendigen Zweck und Umfang hinausgeht.

A.02.07.04 - Verarbeitung personenbezogener Daten zum Schutz lebenswichtiger Interessen der betroffenen Person oder einer anderen natürlichen Person

Überblick

Der:die Zertifizierungsantragsteller:in stellt sicher, dass für die zu zertifizierenden Verarbeitungsvorgänge eine Rechtsgrundlage gemäß Art. 6 Abs. 1 lit. d DSGVO vorliegt. Stützt sich die Verarbeitung auf den Schutz lebenswichtiger Interessen der betroffenen Person oder einer anderen natürlichen Person, wird sichergestellt, dass zum Zeitpunkt der Verarbeitung ein entsprechendes lebenswichtiges Interesse besteht.

Detaillierte Anforderungen

***Anwendbarkeit**: Dieses Kriterium gilt, wenn der:die Zertifizierungsantragsteller:in die zu zertifizierende Verarbeitungstätigkeit auf den Schutz lebenswichtiger Interessen gemäß Art. 6 Abs. 1 lit. d DSGVO stützt.*

Der:die Zertifizierungsantragsteller:in prüft und dokumentiert:

- welches konkrete lebenswichtige Interesse der betroffenen Person oder einer anderen natürlichen Person zum Zeitpunkt der Verarbeitung besteht; und
- warum keine andere Rechtsgrundlage gemäß Art. 6 Abs. 1 DSGVO für die Verarbeitung anwendbar ist (Nachrangigkeit der Rechtsgrundlage „lebenswichtiges Interesse“).

A.02.07.05 - Verarbeitung personenbezogener Daten zur Erfüllung einer Aufgabe im öffentlichen Interesse oder in Ausübung öffentlicher Gewalt, die dem:der Zertifizierungsantragsteller:in übertragen wurde

Überblick

Der:die Zertifizierungsantragsteller:in stellt sicher, dass für die zu zertifizierenden Verarbeitungsvorgänge eine Rechtsgrundlage gemäß Art. 6 DSGVO vorliegt. Stützt sich die Verarbeitung auf Art. 6 Abs. 1 lit. e DSGVO, wird sichergestellt, dass die Verarbeitung für die Wahrnehmung einer Aufgabe erforderlich ist, die im öffentlichen Interesse liegt oder in Ausübung öffentlicher Gewalt erfolgt, die dem:der Zertifizierungsantragsteller:in übertragen wurde und auf einer anwendbaren unionsrechtlichen oder mitgliedstaatlichen Rechtsvorschrift beruht.

Detaillierte Anforderungen

***Anwendbarkeit**: Dieses Kriterium gilt, wenn der:die Zertifizierungsantragsteller:in die zu zertifizierende Verarbeitungstätigkeit auf die Wahrnehmung einer Aufgabe im öffentlichen Interesse oder in Ausübung übertragener öffentlicher Gewalt gemäß Art. 6 Abs. 1 lit. e DSGVO stützt.*

Der:die Zertifizierungsantragsteller:in prüft und dokumentiert:

- welche unionsrechtlichen oder mitgliedstaatlichen Rechtsvorschriften auf die Verarbeitung anwendbar sind und auf welcher konkreten Rechtsgrundlage die Aufgabe im öffentlichen Interesse oder die Ausübung öffentlicher Gewalt beruht;
- ob die einschlägigen Rechtsvorschriften die Verarbeitung personenbezogener Daten erlauben oder vorschreiben; und
- welche Maßnahmen vorgesehen sind, um die Verarbeitung auszusetzen, wenn betroffene Personen ihr Widerspruchsrecht gemäß Art. 21 DSGVO ausüben (siehe Kriterium A.03.09).

A.02.07.06 - Verarbeitung personenbezogener Daten zum Zweck der Wahrung berechtigter Interessen des:der Zertifizierungsantragstellers:in oder von Dritten

Überblick

Der:die Zertifizierungsantragsteller:in stellt sicher, dass für die zu zertifizierenden Verarbeitungsvorgänge eine Rechtsgrundlage gemäß Art. 6 DSGVO vorliegt. Stützt sich die Verarbeitung auf berechtigte Interessen gemäß Art. 6 Abs. 1 lit. f DSGVO, wird sichergestellt, dass ein berechtigtes Interesse von ihm:ihr oder von Dritten besteht und die Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person nicht überwiegen.

Detaillierte Anforderungen

***Anwendbarkeit**: Dieses Kriterium gilt, wenn der:die Zertifizierungsantragsteller:in die zu zertifizierende Verarbeitungstätigkeit auf die Wahrung eigener berechtigter Interessen oder der berechtigten Interessen eines:einer Dritten gemäß Art. 6 Abs. 1 lit. f DSGVO stützt.*

Der:die Zertifizierungsantragsteller:in führt für die jeweilige Verarbeitungstätigkeit eine Interessenabwägung durch und dokumentiert diese. Dabei gilt Folgendes:

- Das verfolgte berechtigte Interesse ist rechtmäßig, klar bestimmt, tatsächlich gegeben und gegenwärtig; rein hypothetische oder spekulative Interessen reichen nicht aus.
- Der:die Zertifizierungsantragsteller:in prüft und dokumentiert, ob die Verarbeitung zur Wahrung des berechtigten Interesses erforderlich ist und zur Erreichung des damit verbundenen Zwecks beiträgt.
- Der:die Zertifizierungsantragsteller:in wägt das eigene berechtigte Interesse oder das berechtigte Interesse von Dritten gegen die Interessen sowie die Grundrechte und Grundfreiheiten der betroffenen Personen ab. Dabei werden insbesondere bestehende Schutzmaßnahmen und besondere Umstände, wie das Alter der betroffenen Personen, berücksichtigt. Die Verarbeitung ist nur zulässig, wenn die Interessen oder Grundrechte und Grundfreiheiten der betroffenen Personen nicht überwiegen. Dies gilt insbesondere, wenn es sich bei der betroffenen Person um ein Kind handelt.

A.02.07.07 - Prüfung der Zweckkompatibilität

Überblick

Beabsichtigt der:die Zertifizierungsantragsteller:in, personenbezogene Daten für einen anderen Zweck weiterzuverarbeiten als denjenigen, für den sie erhoben wurden, wird sichergestellt, dass die Weiterverarbeitung mit dem ursprünglichen Zweck vereinbar ist.

Detaillierte Anforderungen

***Anwendbarkeit**: Dieses Kriterium gilt, wenn personenbezogene Daten im Rahmen der zu zertifizierenden Verarbeitungstätigkeit für einen anderen Zweck weiterverarbeitet werden sollen und die Weiterverarbeitung weder auf der Einwilligung der betroffenen Person noch auf einer unions- oder mitgliedstaatlichen Rechtsvorschrift beruht, die eine notwendige und verhältnismäßige Maßnahme zur Wahrung der in Art. 23 Abs. 1 DSGVO genannten Ziele darstellt.*

Der:die Zertifizierungsantragsteller:in führt eine Zweckkompatibilitätsprüfung durch und dokumentiert die Vereinbarkeit des ursprünglichen Zwecks mit dem Zweck der beabsichtigten Weiterverarbeitung. Dabei werden gemäß Art. 6 Abs. 4 DSGVO mindestens folgende Aspekte berücksichtigt und dokumentiert:

- die Verbindung zwischen dem ursprünglichen Erhebungszweck und dem Zweck der beabsichtigten Weiterverarbeitung;

Detaillierte Anforderungen

- der Zusammenhang, in dem die personenbezogenen Daten erhoben wurden, insbesondere die Beziehung zwischen dem:der Zertifizierungsantragsteller:in und den betroffenen Personen;
- die Art der personenbezogenen Daten, insbesondere, ob besondere Kategorien personenbezogener Daten gemäß Art. 9 DSGVO oder personenbezogene Daten über strafrechtliche Verurteilungen und Straftaten gemäß Art. 10 DSGVO verarbeitet werden;
- mögliche Folgen der beabsichtigten Weiterverarbeitung für die betroffenen Personen; und
- das Vorhandensein geeigneter Schutzmaßnahmen (z. B. Verschlüsselung oder Pseudonymisierung).

Erfolgt die Weiterverarbeitung ausschließlich durch Anonymisierung, dokumentiert der:die Zertifizierungsantragsteller:in die geplanten oder eingesetzten Anonymisierungstechniken und bewertet deren Wirksamkeit (gemäß der Stellungnahme der Art.-29-Datenschutzgruppe „Opinion 05/2014 on Anonymization Techniques, WP216, 0829/14/EN“).

Bei einer Zweckänderung werden die Verzeichnisse von Verarbeitungstätigkeiten entsprechend angepasst.

Bei einer Weiterverarbeitung zu im öffentlichen Interesse liegenden Archivzwecken, zu wissenschaftlichen oder historischen Forschungszwecken oder zu statistischen Zwecken gilt die Weiterverarbeitung nicht als unvereinbar, sofern geeignete Garantien gemäß Art. 89 Abs. 1 DSGVO umgesetzt und im Rahmen der Zweckkompatibilitätsprüfung dokumentiert werden.

A.02.07.08 - Überprüfung der Gültigkeit der Rechtsgrundlagen

Überblick

Der:die Zertifizierungsantragsteller:in stellt durch geeignete Maßnahmen sicher, dass die Anwendbarkeit und Gültigkeit der Rechtsgrundlagen für die zu zertifizierenden Verarbeitungstätigkeiten regelmäßig überprüft werden.

Detaillierte Anforderungen

Der:die Zertifizierungsantragsteller:in richtet ein schriftliches Verfahren oder einen definierten Prozess zur Überprüfung der Rechtsgrundlagen für die zu zertifizierenden Verarbeitungstätigkeiten ein.

Die Überprüfung erfolgt mindestens einmal jährlich sowie anlassbezogen bei wesentlichen Änderungen, die sich auf die Rechtsgrundlagen der zu zertifizierenden Verarbeitungstätigkeiten auswirken können.

Das Verfahren legt die einzelnen Schritte der Überprüfung, die Bewertung möglicher Auswirkungen auf die Rechtsgrundlagen, die Einbindung des:der Datenschutzbeauftragten (sofern benannt) sowie die Dokumentation der Überprüfung fest.

A.02.07.09 - Einwilligungserklärung eines Kindes bei Diensten der Informationsgesellschaft

Überblick

Werden einem Kind Dienste der Informationsgesellschaft direkt angeboten und beruht die Verarbeitung auf einer Einwilligung, stellt der:die Zertifizierungsantragsteller:in sicher, dass die Voraussetzungen für eine wirksame Einwilligung gemäß Art. 8 DSGVO und § 4 Abs. 4 DSG erfüllt sind.

Detaillierte Anforderungen

***Anwendbarkeit**: Dieses Kriterium gilt für Verarbeitungstätigkeiten, bei denen Dienste der Informationsgesellschaft direkt einem Kind angeboten werden.*

Hat das Kind das 14. Lebensjahr noch nicht vollendet, weist der:die Zertifizierungsantragsteller:in nach, dass die Einwilligung durch den Träger der elterlichen Verantwortung für das Kind oder mit dessen Zustimmung erteilt wurde. Hierzu wird dokumentiert:

- wie das Alter des Kindes überprüft wurde;
- wie die Einwilligung oder Zustimmung des Trägers der elterlichen Verantwortung eingeholt und gegebenenfalls dessen Obsorgeberechtigung überprüft wurde; die eingesetzten Überprüfungsmaßnahmen müssen dem jeweiligen Verarbeitungskontext angemessen und verhältnismäßig sein;
- die Einwilligung bzw. Zustimmung des Trägers der elterlichen Verantwortung; und
- eine gegebenenfalls vom Kind selbst abgegebene Einwilligung.

4.4. VERARBEITUNG BESONDERER KATEGORIEN PERSONENBEZOGENER DATEN

A.02.08 - Rechtsgrundlage für die Verarbeitung besonderer Kategorien personenbezogener Daten

Überblick

Vor der Verarbeitung besonderer Kategorien personenbezogener Daten prüft der:die Zertifizierungsantragsteller:in, ob neben einer Rechtsgrundlage gemäß Art. 6 DSGVO ein Rechtfertigungsgrund gemäß Art. 9 Abs. 2 und 3 DSGVO vorliegt.

Detaillierte Anforderungen

Anwendbarkeit: *Dieses Kriterium gilt für zu zertifizierende Verarbeitungstätigkeiten, in deren Rahmen besondere Kategorien personenbezogener Daten gemäß Art. 9 Abs. 1 DSGVO verarbeitet werden.*

Für die Verarbeitung besonderer Kategorien personenbezogener Daten dokumentiert der:die Zertifizierungsantragsteller:in zusätzlich zur Rechtsgrundlage gemäß Art. 6 DSGVO (siehe Kriterien A.02.07.01–A.02.07.06) den jeweils einschlägigen Rechtfertigungsgrund gemäß Art. 9 Abs. 2 DSGVO und dessen Voraussetzungen. Je nach einschlägigem Rechtfertigungsgrund gelten folgende Anforderungen:

a) Ausdrückliche Einwilligung (Art. 9 Abs. 2 lit. a DSGVO)

- Die Bereitstellung der erforderlichen Informationen und die Einholung der ausdrücklichen Einwilligung für die jeweiligen Verarbeitungszwecke werden dokumentiert.
- Es wird geprüft und dokumentiert, dass die Verarbeitung auf Grundlage einer ausdrücklichen Einwilligung nicht durch Unionsrecht oder österreichisches Recht ausgeschlossen ist. Sofern ein entsprechendes Verbot besteht, werden die einschlägige gesetzliche Bestimmung sowie die Begründung dokumentiert, weshalb diese auf die zu zertifizierenden Verarbeitungstätigkeiten nicht anwendbar ist.

b) Arbeits-, sozialversicherungs- oder sozialschutzrechtliche Pflichten (Art. 9 Abs. 2 lit. b DSGVO)

- Die einschlägigen unionsrechtlichen oder österreichischen Rechtsvorschriften, deren Anwendbarkeit und die Erforderlichkeit der Verarbeitung werden dokumentiert.
- Die zum Schutz der Grundrechte und Interessen der betroffenen Personen eingesetzten Schutzmaßnahmen, insbesondere technische und organisatorische Maßnahmen, werden dokumentiert und risikoorientiert aktuell gehalten (siehe Kriterium A.06.01).

c) Schutz lebenswichtiger Interessen (Art. 9 Abs. 2 lit. c DSGVO)

- Das konkrete lebenswichtige Interesse und die Gründe, weshalb die betroffene Person keine Einwilligung erteilen kann, werden dokumentiert.
- Es wird dokumentiert, warum die Verarbeitung zum Schutz des lebenswichtigen Interesses erforderlich ist und keine andere Rechtsgrundlage einschlägig ist.

d) Verarbeitung durch bestimmte Organisationen ohne Gewinnerzielungsabsicht (Art. 9 Abs. 2 lit. d DSGVO)

- Die Erfüllung der Voraussetzungen des Art. 9 Abs. 2 lit. d DSGVO und die Verarbeitung im Rahmen der rechtmäßigen Tätigkeiten der Organisation werden dokumentiert.
- Es wird dokumentiert, dass ausschließlich Mitglieder, ehemalige Mitglieder oder Personen betroffen sind, die im Zusammenhang mit dem Tätigkeitszweck regelmäßige Kontakte mit der Organisation unterhalten.
- Es wird sichergestellt und dokumentiert, dass die personenbezogenen Daten nicht ohne Einwilligung der betroffenen Personen nach außen offengelegt werden.
- Geeignete Schutzmaßnahmen werden dokumentiert und risikoorientiert aktuell gehalten (siehe Kriterium A.06.01).

e) Offenkundig öffentlich gemachte Daten (Art. 9 Abs. 2 lit. e DSGVO)

- Es wird dokumentiert, wo die betroffene Person die Daten offenkundig öffentlich gemacht hat und auf welcher Grundlage von einer entsprechenden Offenlegung durch die betroffene Person ausgegangen wird.

f) Rechtsansprüche und gerichtliche Tätigkeit (Art. 9 Abs. 2 lit. f DSGVO)

- Bei einer Verarbeitung zur Begründung, Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen werden die betreffenden Rechtsansprüche und die Erforderlichkeit der Verarbeitung dokumentiert.
- Soweit sich die Verarbeitung auf Rechtsansprüche stützt, wird dokumentiert, dass ein Rechtsstreit anhängig ist oder eine entsprechende rechtliche Auseinandersetzung konkret bevorsteht oder vorbereitet wird.

g) Erhebliches öffentliches Interesse (Art. 9 Abs. 2 lit. g DSGVO)

- Die einschlägigen unionsrechtlichen oder österreichischen Rechtsvorschriften, deren Anwendbarkeit und die Erforderlichkeit der Verarbeitung werden dokumentiert.

Detaillierte Anforderungen

- Die vorgesehenen Schutzmaßnahmen und gesetzlichen Garantien zum Schutz der Grundrechte und Interessen der betroffenen Personen werden dokumentiert und risikoorientiert aktuell gehalten (siehe Kriterium A.06.01).

h) Gesundheitsvorsorge, Arbeitsmedizin sowie Gesundheits- und Sozialbereich (Art. 9 Abs. 2 lit. h DSGVO)

- Die einschlägigen unionsrechtlichen oder österreichischen Rechtsvorschriften und deren Anwendbarkeit werden dokumentiert.
- Soweit erforderlich, werden die vertraglichen Vereinbarungen mit qualifiziertem Fachpersonal dokumentiert.
- Es wird nachgewiesen, dass die mit der Verarbeitung befassten Fachpersonen einer entsprechenden beruflichen Geheimhaltungspflicht unterliegen; deren Grundlage wird dokumentiert.
- Geeignete Schutzmaßnahmen zum Schutz der Grundrechte und Interessen der betroffenen Personen werden dokumentiert und risikoorientiert aktuell gehalten (siehe Kriterium A.06.01).

i) Öffentliches Interesse im Bereich der öffentlichen Gesundheit (Art. 9 Abs. 2 lit. i DSGVO)

- Die einschlägigen unionsrechtlichen oder österreichischen Rechtsvorschriften und deren Anwendbarkeit werden dokumentiert.
- Geeignete Schutzmaßnahmen zum Schutz der Grundrechte und Interessen der betroffenen Personen werden dokumentiert und risikoorientiert aktuell gehalten (siehe Kriterium A.06.01).

j) Archiv-, Forschungs- und statistische Zwecke (Art. 9 Abs. 2 lit. j DSGVO)

- Die einschlägigen unionsrechtlichen oder österreichischen Rechtsvorschriften für die Verarbeitung werden dokumentiert.
- Geeignete Schutzmaßnahmen zum Schutz der Grundrechte und Interessen der betroffenen Personen werden dokumentiert und risikoorientiert aktuell gehalten (siehe Kriterium A.06.01).

4.5. VERARBEITUNG PERSONENBEZOGENER DATEN ÜBER STRAFRECHTLICHE VERURTEILUNGEN UND STRAFTATEN

A.02.09 - Verarbeitung personenbezogener Daten über strafrechtliche Verurteilungen und Straftaten

Überblick

Werden im Rahmen der zu zertifizierenden Verarbeitungstätigkeiten personenbezogene Daten über strafrechtliche Verurteilungen und Straftaten verarbeitet, stellt der:die Zertifizierungsantragsteller:in sicher, dass die Voraussetzungen des Art. 10 DSGVO erfüllt sind. Die Verarbeitung erfolgt ausschließlich unter behördlicher Aufsicht oder auf Grundlage des Unionsrechts oder des Rechts eines Mitgliedstaates, das geeignete Garantien für die Rechte und Freiheiten der betroffenen Personen vorsieht.

Detaillierte Anforderungen

***Anwendbarkeit**: Dieses Kriterium gilt für Verarbeitungstätigkeiten, bei denen personenbezogene Daten über strafrechtliche Verurteilungen und Straftaten verarbeitet werden.*

Der:die Zertifizierungsantragsteller:in dokumentiert, welche personenbezogenen Daten über strafrechtliche Verurteilungen und Straftaten im Rahmen der zu zertifizierenden Verarbeitungstätigkeiten verarbeitet werden (z. B. im Verzeichnis der Verarbeitungstätigkeiten).

Der:die Zertifizierungsantragsteller:in dokumentiert die einschlägige unionsrechtliche oder österreichische Rechtsgrundlage für die Verarbeitung. Soweit sich die Verarbeitung auf § 4 Abs. 3 DSG stützt, gelten – abhängig davon, auf welche Bestimmung Bezug genommen wird – folgende Anforderungen:

- **§ 4 Abs. 3 Z 1 DSG:** Der:die Zertifizierungsantragsteller:in dokumentiert die Rechtsvorschriften, aus denen sich die ausdrückliche gesetzliche Ermächtigung oder Verpflichtung zur Verarbeitung ergibt, und begründet deren Anwendbarkeit.
- **§ 4 Abs. 3 Z 2 DSG:** Der:die Zertifizierungsantragsteller:in dokumentiert die gesetzlichen Sorgfaltspflichten oder die berechtigten Interessen, auf die sich die Verarbeitung stützt, sowie die Maßnahmen zum Schutz der Interessen der betroffenen Personen.

4.6. RECHTE DER BETROFFENEN PERSONEN

A.03.01 - Verfahren zur Bearbeitung von Betroffenenanfragen

Überblick
Der:die Zertifizierungsantragsteller:in richtet ein dokumentiertes Verfahren zur Umsetzung der Rechte betroffener Personen gemäß Art. 12 bis 22 DSGVO ein.
Detaillierte Anforderungen
Der:die Zertifizierungsantragsteller:in richtet für die Bearbeitung von Anträgen betroffener Personen gemäß Art. 12 bis 22 DSGVO einen dokumentierten Prozess ein und setzt diesen um. Der Prozess umfasst mindestens: ▶ die vorgesehenen Kommunikationskanäle (z. B. E-Mail, Web-Formular oder Privacy-Dashboard) und eine zentrale Kontaktstelle für den Eingang von Betroffenenanfragen; ▶ die Festlegung der für die Bearbeitung zuständigen Stelle und deren Zusammenarbeit mit anderen Abteilungen, Auftragnehmer:innen und – sofern benannt – dem:der Datenschutzbeauftragten; ▶ die einzelnen Prozessschritte und Maßnahmen zur Einhaltung der gesetzlichen Fristen, insbesondere: ○ Information der betroffenen Person unverzüglich, spätestens jedoch innerhalb eines Monats nach Eingang des Antrags (Art. 12 Abs. 3 DSGVO); ○ gegebenenfalls Verlängerung dieser Frist um bis zu zwei weitere Monate und Information der betroffenen Person innerhalb eines Monats über die Verlängerung und deren Gründe (Art. 12 Abs. 3 und 4 DSGVO); ▶ die Prüfung, welches Betroffenenrecht geltend gemacht wird; ▶ die Vorgehensweise zur Identitätsprüfung bei begründeten Zweifeln an der Identität der antragstellenden Person; ▶ Kriterien zur Beurteilung, ob ein Antrag offenkundig unbegründet oder exzessiv ist, sowie zur Feststellung, ob gegebenenfalls ein angemessenes Entgelt unter Berücksichtigung des Verwaltungsaufwands verlangt werden kann (Art. 12 Abs. 5 DSGVO); ▶ Maßnahmen, die gewährleisten, dass die Informationen für betroffene Personen präzise, transparent, verständlich und leicht zugänglich sowie in klarer und einfacher Sprache bereitgestellt werden; und ▶ die Form der Bereitstellung sowie Maßnahmen zur sicheren Übermittlung der Informationen (z. B. über einen Datenraum oder mittels verschlüsselter E-Mails bzw. Anhänge). Der:die Zertifizierungsantragsteller:in dokumentiert die Bearbeitung von Betroffenenanfragen und legt den Speicherort sowie die Aufbewahrungsfrist der Dokumentation fest.

A.03.02 - Informationspflichten bei Erhebung personenbezogener Daten direkt bei der betroffenen Person

Überblick
Werden personenbezogene Daten bei der betroffenen Person erhoben, stellt der:die Zertifizierungsantragsteller:in sicher, dass die Informationen gemäß Art. 13 Abs. 1 und 2 DSGVO zum Zeitpunkt der Erhebung und unter Berücksichtigung der Anforderungen des Art. 12 DSGVO bereitgestellt werden.
Detaillierte Anforderungen
Bei der direkten Erhebung personenbezogener Daten stellt der:die Zertifizierungsantragsteller:in den betroffenen Personen die erforderlichen Informationen über die Verarbeitung bereit. Diese werden üblicherweise in einem Datenschutzhinweis, einer Privacy Notice oder einer Datenschutzerklärung bereitgestellt und umfassen mindestens die in Art. 13 Abs. 1 und 2 DSGVO vorgesehenen Inhalte. Die Informationen können in unterschiedlicher Form bereitgestellt werden, z. B. als Datenschutzhinweis in gedruckter Form oder durch einen Verweis auf die entsprechende Seite einer Website. Erfolgt die Information mündlich, dokumentiert der:die Zertifizierungsantragsteller:in die erfolgte Information intern, z. B. durch einen Protokolleintrag. **Zulässige Ausnahme:** Verfügt die betroffene Person bereits über die erforderlichen Informationen, ist deren erneute Bereitstellung gemäß Art. 13 Abs. 4 DSGVO nicht erforderlich. Der:die Zertifizierungsantragsteller:in weist in diesem Fall nach, dass die betroffene Person bereits über die entsprechenden Informationen verfügt.

A.03.03 - Sicherstellung der ordnungsgemäßen Erfüllung der Informationspflichten bei indirekter Datenerhebung

Überblick

Werden personenbezogene Daten nicht bei der betroffenen Person erhoben, stellt der:die Zertifizierungsantragsteller:in sicher, dass die betroffene Person gemäß Art. 14 DSGVO und unter Berücksichtigung der Anforderungen des Art. 12 DSGVO informiert wird.

Detaillierte Anforderungen

Werden im Rahmen der zu zertifizierenden Verarbeitungstätigkeiten personenbezogene Daten nicht direkt bei der betroffenen Person erhoben, richtet der:die Zertifizierungsantragsteller:in ein Verfahren ein, das die rechtzeitige und vollständige Information der betroffenen Personen sicherstellt. Die erfolgte Information einschließlich Zeitpunkt und Inhalt wird dokumentiert.

Die Informationen werden gemäß Art. 14 Abs. 3 DSGVO

- innerhalb einer angemessenen Frist nach Erlangung der personenbezogenen Daten, längstens jedoch innerhalb eines Monats;
- falls die personenbezogenen Daten zur Kommunikation mit der betroffenen Person verwendet werden sollen, spätestens zum Zeitpunkt der ersten Kommunikation; oder
- falls eine Offenlegung gegenüber einem:einer anderen Empfänger:in beabsichtigt ist, spätestens zum Zeitpunkt der ersten Offenlegung bereitgestellt.

Die betroffene Person wird mindestens über die in Art. 14 Abs. 1 und 2 DSGVO vorgesehenen Inhalte informiert.

Werden die Informationen nicht bereitgestellt, dokumentiert der:die Zertifizierungsantragsteller:in die hierfür maßgeblichen Gründe und holt – sofern ein:e Datenschutzbeauftragte:r benannt ist – dessen:deren schriftliche Stellungnahme ein.

Zulässige Ausnahmen: Die Informationspflicht besteht nicht, soweit eine der Voraussetzungen des Art. 14 Abs. 5 DSGVO vorliegt. Beruft sich der:die Zertifizierungsantragsteller:in auf eine dieser Ausnahmen, wird das Vorliegen der jeweiligen Voraussetzungen und die Gründe für die Nichtbereitstellung der Informationen dokumentiert. Soweit Art. 14 Abs. 5 DSGVO geeignete Maßnahmen zum Schutz der Rechte und Freiheiten sowie der berechtigten Interessen der betroffenen Person erfordert, werden diese ebenfalls dokumentiert.

A.03.04 - Recht auf Auskunft der betroffenen Person

Überblick

Der:die Zertifizierungsantragsteller:in implementiert ein Verfahren zur Bearbeitung von Auskunftsersuchen betroffener Personen nach Art. 15 DSGVO.

Detaillierte Anforderungen

1) **Technische und organisatorische Maßnahmen zur Datenauskunft**

Der:die Zertifizierungsantragsteller:in trifft geeignete technische und organisatorische Maßnahmen, die eine vollständige Datensuche für die zu zertifizierenden Verarbeitungstätigkeiten ermöglichen. Das hierfür festgelegte systematische Vorgehen berücksichtigt personenbezogene Daten sowohl in analoger Form, soweit diese Bestandteil eines Dateisystems gemäß Art. 4 Z 6 DSGVO sind, als auch in digitaler Form.

2) Identitätsprüfung

Der:die Zertifizierungsantragsteller:in dokumentiert den Eingang des Auskunftsersuchens und – bei begründeten Zweifeln an der Identität der antragstellenden Person – die durchgeführten Maßnahmen zur Identitätsprüfung.

3) Bereitstellung der Auskunft

Der:die Zertifizierungsantragsteller:in stellt der betroffenen Person die erforderlichen Informationen unverzüglich, spätestens innerhalb eines Monats nach Eingang des Antrags bereit. Eine Verlängerung um bis zu zwei weitere Monate ist unter den Voraussetzungen des Art. 12 Abs. 3 DSGVO zulässig; die betroffene Person wird innerhalb eines Monats über die Verlängerung und deren Gründe informiert.

Die Auskunft umfasst die nach Art. 15 DSGVO erforderlichen Informationen.

Detaillierte Anforderungen

4) Bereitstellung einer Kopie

Der:die Zertifizierungsantragsteller:in stellt der betroffenen Person eine Kopie der personenbezogenen Daten gemäß Art. 15 Abs. 3 DSGVO zur Verfügung und dokumentiert deren Bereitstellung. Bei elektronischer Antragstellung werden die Informationen in einem gängigen elektronischen Format bereitgestellt, sofern die betroffene Person nichts anderes verlangt.

5) Negativauskunft

Werden keine personenbezogenen Daten der betroffenen Person verarbeitet, erteilt der:die Zertifizierungsantragsteller:in eine entsprechende Negativauskunft und dokumentiert diese.

A.03.05 - Recht auf Berichtigung

Überblick

Der:die Zertifizierungsantragsteller:in richtet ein Verfahren zur Bearbeitung von Berichtigungsanträgen betroffener Personen ein und setzt dieses um. Das Verfahren gewährleistet die Erfüllung des Rechts auf Berichtigung gemäß Art. 16 DSGVO.

Detaillierte Anforderungen

1) Technische und organisatorische Maßnahmen zur Berichtigung

Der:die Zertifizierungsantragsteller:in trifft geeignete technische und organisatorische Maßnahmen, um unrichtige personenbezogene Daten zu berichtigen und unvollständige personenbezogene Daten zu vervollständigen. Die Berichtigung erfolgt in allen relevanten Systemen und Speicherorten innerhalb der gemäß Art. 12 Abs. 3 DSGVO geltenden Fristen.

2) Identitätsprüfung und Durchführung der Berichtigung

Der:die Zertifizierungsantragsteller:in dokumentiert den Eingang des Berichtigungsantrags und – bei begründeten Zweifeln an der Identität der antragstellenden Person – die durchgeführten Maßnahmen zur Identitätsprüfung. Die erforderliche Berichtigung wird in allen relevanten Systemen vorgenommen.

3) Benachrichtigung der Empfänger:innen

Der:die Zertifizierungsantragsteller:in informiert die Empfänger:innen, denen die betreffenden personenbezogenen Daten offengelegt wurden, gemäß Art. 19 DSGVO über die Berichtigung und dokumentiert die erfolgte Benachrichtigung.

Ist die Benachrichtigung unmöglich oder mit einem unverhältnismäßigen Aufwand verbunden, werden die hierfür maßgeblichen Gründe dokumentiert.

4) Empfänger:innenliste und regelmäßige Überprüfung

Der:die Zertifizierungsantragsteller:in führt eine aktuelle Liste der Empfänger:innen, an die personenbezogene Daten übermittelt werden, und überprüft deren Vollständigkeit und Richtigkeit mindestens einmal jährlich.

Sofern ein:e Datenschutzbeauftragte:r benannt ist, wird eine Stellungnahme zur Richtigkeit der Liste eingeholt. Die Durchführung der jährlichen Überprüfung wird dokumentiert.

A.03.06 - Recht auf Löschung

Überblick

Der:die Zertifizierungsantragsteller:in richtet ein Verfahren zur Bearbeitung von Löschungsersuchen betroffener Personen ein und setzt dieses um. Das Verfahren gewährleistet die Erfüllung des Rechts auf Löschung gemäß Art. 17 DSGVO.

Detaillierte Anforderungen

1) Technische und organisatorische Maßnahmen zur Löschung

Der:die Zertifizierungsantragsteller:in trifft geeignete technische und organisatorische Maßnahmen, um sicherzustellen, dass personenbezogene Daten in allen relevanten Systemen und Speicherorten unverzüglich und ohne unangemessene Verzögerung, jedenfalls innerhalb eines Monats nach Eingang des Löschungsersuchens, gelöscht werden.

2) Identitätsprüfung und Durchführung der Löschung

Der:die Zertifizierungsantragsteller:in dokumentiert den Eingang des Löschungsersuchens und – bei begründeten Zweifeln an der Identität der antragstellenden Person – die durchgeführten Maßnahmen zur Identitätsprüfung.

Der:die Zertifizierungsantragsteller:in prüft und dokumentiert, ob mindestens einer der folgenden Löschungsgründe gemäß Art. 17 Abs. 1 DSGVO vorliegt:

- Die personenbezogenen Daten sind für die Zwecke, für die sie erhoben oder verarbeitet wurden, nicht mehr notwendig.
- Die betroffene Person widerruft ihre Einwilligung gemäß Art. 6 Abs. 1 lit. a oder Art. 9 Abs. 2 lit. a DSGVO und es besteht keine andere Rechtsgrundlage für die Verarbeitung.
- Die betroffene Person legt gemäß Art. 21 Abs. 1 DSGVO Widerspruch ein und es liegen keine vorrangigen berechtigten Gründe für die Verarbeitung vor oder sie legt gemäß Art. 21 Abs. 2 DSGVO Widerspruch ein.
- Die personenbezogenen Daten wurden unrechtmäßig verarbeitet.
- Die Löschung ist zur Erfüllung einer rechtlichen Verpflichtung nach dem Unionsrecht oder dem Recht eines Mitgliedstaates erforderlich, dem der:die Zertifizierungsantragsteller:in unterliegt;
- Die personenbezogenen Daten wurden in Bezug auf angebotene Dienste der Informationsgesellschaft gemäß Art. 8 Abs. 1 DSGVO erhoben.

Ist das Löschungsersuchen aufgrund der Voraussetzungen des Art. 17 Abs. 3 DSGVO unbegründet, hat der:die Zertifizierungsantragsteller:in diese Gründe schriftlich zu dokumentieren und die betroffene Person unter Angabe der Gründe über die Nichtumsetzung der Löschung zu informieren:

- Die Verarbeitung ist zur Ausübung des Rechts auf freie Meinungsäußerung und Information erforderlich.
- Die Verarbeitung ist zur Erfüllung einer rechtlichen Verpflichtung nach dem Unionsrecht oder dem Recht eines Mitgliedstaats oder zur Wahrnehmung einer Aufgabe erforderlich, die im öffentlichen Interesse liegt oder in Ausübung übertragener öffentlicher Gewalt erfolgt.
- Die Verarbeitung ist aus Gründen des öffentlichen Interesses im Bereich der öffentlichen Gesundheit gemäß Art. 9 Abs. 2 lit. h und i sowie Art. 9 Abs. 3 DSGVO erforderlich.
- Die Verarbeitung ist für im öffentlichen Interesse liegende Archivzwecke, wissenschaftliche oder historische Forschungszwecke oder statistische Zwecke gemäß Art. 89 Abs. 1 DSGVO erforderlich und die Verwirklichung dieser Zwecke würde durch die Ausübung des Rechts auf Löschung voraussichtlich unmöglich gemacht oder ernsthaft beeinträchtigt.
- Die Verarbeitung ist zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen erforderlich.

Sofern ein:e Datenschutzbeauftragte:r benannt ist, wird diese:r in die Prüfung einbezogen.

Besteht ein Anspruch auf Löschung, werden die betreffenden personenbezogenen Daten in allen relevanten Systemen gelöscht und die Durchführung der Löschung dokumentiert.

3) Benachrichtigung der Empfänger:innen

Der:die Zertifizierungsantragsteller:in informiert die Empfänger:innen, denen die betreffenden personenbezogenen Daten offengelegt wurden, gemäß Art. 19 DSGVO über die Löschung und dokumentiert die erfolgte Benachrichtigung.

Ist die Benachrichtigung unmöglich oder mit einem unverhältnismäßigen Aufwand verbunden, werden die hierfür maßgeblichen Gründe dokumentiert.

4) Empfänger:innenliste und regelmäßige Überprüfung

Der:die Zertifizierungsantragsteller:in führt eine aktuelle Liste der Empfänger:innen, an die personenbezogene Daten übermittelt werden, und überprüft deren Vollständigkeit und Richtigkeit mindestens einmal jährlich.

Sofern ein:e Datenschutzbeauftragte:r benannt ist, wird eine Stellungnahme zur Richtigkeit der Liste eingeholt. Die Durchführung der jährlichen Überprüfung wird dokumentiert.

A.03.07 - Recht auf Einschränkung der Verarbeitung

Überblick

Der:die Zertifizierungsantragsteller:in richtet ein Verfahren zur Bearbeitung von Anträgen auf Einschränkung der Verarbeitung ein und setzt dieses um. Das Verfahren gewährleistet die Erfüllung des Rechts auf Einschränkung der Verarbeitung gemäß Art. 18 DSGVO.

Detaillierte Anforderungen

1) Technische und organisatorische Maßnahmen zur Einschränkung

Der:die Zertifizierungsantragsteller:in trifft geeignete technische und organisatorische Maßnahmen, die eine Einschränkung der Verarbeitung in allen relevanten Systemen und Speicherorten ermöglichen. Die betroffenen personenbezogenen Daten werden entsprechend gesperrt oder gekennzeichnet und nicht mehr für andere als die gemäß Art. 18 Abs. 2 DSGVO zulässigen Verarbeitungsvorgänge verwendet.

2) Identitätsprüfung und Durchführung der Einschränkung

Der:die Zertifizierungsantragsteller:in dokumentiert den Eingang des Antrags und – bei begründeten Zweifeln an der Identität der antragstellenden Person – die durchgeführten Maßnahmen zur Identitätsprüfung.

Der:die Zertifizierungsantragsteller:in prüft und dokumentiert, ob mindestens eine der folgenden Voraussetzungen gemäß Art. 18 Abs. 1 DSGVO vorliegt:

- Die Richtigkeit der personenbezogenen Daten wird von der betroffenen Person bestritten; die Einschränkung erfolgt für die Dauer der Überprüfung der Richtigkeit.
- Die Verarbeitung ist unrechtmäßig und die betroffene Person verlangt anstelle der Löschung die Einschränkung der Nutzung.
- Die personenbezogenen Daten werden für die Zwecke der Verarbeitung nicht mehr benötigt, die betroffene Person benötigt sie jedoch zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen.
- Die betroffene Person hat gemäß Art. 21 Abs. 1 DSGVO Widerspruch eingelegt und es steht noch nicht fest, ob die berechtigten Gründe des:der Verantwortlichen gegenüber den Gründen der betroffenen Person überwiegen.

Sofern ein:e Datenschutzbeauftragte:r benannt ist, wird diese:r in die Prüfung einbezogen.

Liegen die Voraussetzungen vor, wird die Einschränkung der Verarbeitung in allen relevanten Systemen vorgenommen und die betroffene Person unverzüglich und in jedem Fall innerhalb eines Monats nach Eingang des Antrags über die Umsetzung informiert.

3) Benachrichtigung der Empfänger:innen

Der:die Zertifizierungsantragsteller:in informiert die Empfänger:innen, denen die betreffenden personenbezogenen Daten offengelegt wurden, gemäß Art. 19 DSGVO über die Einschränkung und dokumentiert die erfolgte Benachrichtigung.

Ist die Benachrichtigung unmöglich oder mit einem unverhältnismäßigen Aufwand verbunden, werden die hierfür maßgeblichen Gründe dokumentiert. Auf Verlangen der betroffenen Person informiert der:die Zertifizierungsantragsteller:in diese über die betreffenden Empfänger:innen.

4) Empfänger:innenliste und regelmäßige Überprüfung

Der:die Zertifizierungsantragsteller:in führt eine aktuelle Liste der Empfänger:innen, an die personenbezogene Daten übermittelt werden, und überprüft deren Vollständigkeit und Richtigkeit mindestens einmal jährlich.

Sofern ein:e Datenschutzbeauftragte:r benannt ist, wird dessen:deren Stellungnahme eingeholt. Die Durchführung der jährlichen Überprüfung wird dokumentiert.

1) Aufhebung der Einschränkung der Verarbeitung (falls zutreffend)

Bei Aufhebung einer Einschränkung informiert der:die Zertifizierungsantragsteller:in die betroffene Person vor der Wiederaufnahme der Verarbeitung und dokumentiert die Gründe, warum die personenbezogenen Daten wieder verarbeitet werden, insbesondere wenn:

- die betroffene Person eingewilligt hat,
- die Daten zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen erforderlich sind,
- die Verarbeitung zum Schutz der Rechte einer anderen natürlichen oder juristischen Person erforderlich ist,
- die Verarbeitung aus wichtigen Gründen des öffentlichen Interesses der Union oder der Republik Österreich erforderlich ist.

A.03.08 - Recht auf Datenübertragbarkeit

Überblick
Der:die Zertifizierungsantragsteller:in richtet ein Verfahren zur Bearbeitung von Anträgen auf Datenübertragbarkeit ein und setzt dieses um. Das Verfahren gewährleistet die Erfüllung des Rechts auf Datenübertragbarkeit gemäß Art. 20 DSGVO.
Detaillierte Anforderungen
1) Technische und organisatorische Maßnahmen zur Datenübertragbarkeit Der:die Zertifizierungsantragsteller:in trifft geeignete technische und organisatorische Maßnahmen, die gewährleisten, dass die betroffene Person die sie betreffenden personenbezogenen Daten, die sie dem:der Zertifizierungsantragsteller:in bereitgestellt hat, in einem strukturierten, gängigen und maschinenlesbaren Format erhält. Dabei wird sichergestellt, dass der Export ausschließlich personenbezogene Daten der betroffenen Person enthält. **2) Identitätsprüfung und Prüfung der Anwendbarkeit** Der:die Zertifizierungsantragsteller:in dokumentiert den Eingang des Antrags und – bei begründeten Zweifeln an der Identität der antragstellenden Person – die durchgeführten Maßnahmen zur Identitätsprüfung. Der:die Zertifizierungsantragsteller:in prüft und dokumentiert, ob die Voraussetzungen des Art. 20 DSGVO erfüllt sind. Das Recht auf Datenübertragbarkeit besteht insbesondere, wenn ▶ die Verarbeitung auf Einwilligung gemäß Art. 6 Abs. 1 lit. a oder Art. 9 Abs. 2 lit. a DSGVO beruht oder ▶ die Verarbeitung auf einem Vertrag gemäß Art. 6 Abs. 1 lit. b DSGVO beruht; und ▶ die Verarbeitung automatisiert erfolgt. Sofern ein:e Datenschutzbeauftragte:r benannt ist, wird diese:r in die Prüfung einbezogen. **3) Durchführung der Datenübertragung** Liegen die Voraussetzungen vor, prüft der:die Zertifizierungsantragsteller:in die zu übertragenden Daten vor der Bereitstellung auf Vollständigkeit und stellt sie in einem strukturierten, gängigen und maschinenlesbaren Format bereit. Hierfür können geeignete Prüfmethoden eingesetzt werden, z. B. der Abgleich der Anzahl der Datensätze oder Dateien vor und nach dem Export, Abgleich der Anzahl exportierter Datensätze, Berechnung und Abgleich von Checksums (Hashwerten) vor bzw. nach dem Export. Auf Verlangen der betroffenen Person werden die personenbezogenen Daten – soweit technisch machbar – direkt an eine:n andere:n Verantwortliche:n übermittelt. Die Daten werden unverzüglich und in jedem Fall innerhalb eines Monats nach Eingang des Antrags bereitgestellt. **4) Dokumentation** Der:die Zertifizierungsantragsteller:in dokumentiert die Bearbeitung des Antrags nachvollziehbar. Die Dokumentation umfasst insbesondere ▶ den Eingang des Antrags; ▶ das Ergebnis der Prüfung der Voraussetzungen des Art. 20 DSGVO; ▶ die Datenbereitstellung bzw. -übertragung einschließlich der durchgeführten Vollständigkeitsprüfung; ▶ den Zeitpunkt der Bereitstellung bzw. Übermittlung; und ▶ die Information der betroffenen Person.

4.7. WIDERSPRUCHSRECHT UND AUTOMATISIERTE ENTSCHEIDUNGEN IM EINZELFALL

A.03.09 - Recht auf Widerspruch

Überblick
Der:die Zertifizierungsantragsteller:in richtet ein Verfahren zur Bearbeitung von Widersprüchen betroffener Personen ein und setzt dieses um. Das Verfahren gewährleistet die Erfüllung des Widerspruchsrechts gemäß Art. 21 DSGVO.
Detaillierte Anforderungen
Der:die Zertifizierungsantragsteller:in trifft geeignete Maßnahmen, um die Umsetzung des Widerspruchsrechts für die jeweils betroffenen Verarbeitungstätigkeiten in allen relevanten Systemen sicherzustellen. **1) Allgemeines Widerspruchsrecht gemäß Art. 21 Abs. 1 DSGVO** Legt eine betroffene Person aus Gründen, die sich aus ihrer besonderen Situation ergeben, Widerspruch gegen eine Verarbeitung gemäß Art. 6 Abs. 1 lit. e oder f DSGVO einschließlich eines darauf gestützten Profilings ein, wird der Widerspruch geprüft und dokumentiert. Die Verarbeitung wird nicht fortgeführt, es sei denn, ▶ es bestehen zwingende schutzwürdige Gründe für die Verarbeitung, die die Interessen, Rechte und Freiheiten der betroffenen Person überwiegen; oder ▶ die Verarbeitung dient der Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen. Die Gründe für die Entscheidung werden dokumentiert. **2) Widerspruch gegen Direktwerbung gemäß Art. 21 Abs. 2 und 3 DSGVO** Widerspricht die betroffene Person der Verarbeitung ihrer personenbezogenen Daten für Zwecke der Direktwerbung einschließlich eines damit zusammenhängenden Profilings, stellt der:die Zertifizierungsantragsteller:in sicher, dass die personenbezogenen Daten nicht mehr für diese Zwecke verarbeitet werden. **3) Information über das Widerspruchsrecht gemäß Art. 21 Abs. 4 DSGVO** Der:die Zertifizierungsantragsteller:in weist nach, dass die betroffene Person spätestens zum Zeitpunkt der ersten Kommunikation ausdrücklich, in verständlicher und von anderen Informationen getrennter Form auf das Widerspruchsrecht hingewiesen wurde. **4) Dienste der Informationsgesellschaft gemäß Art. 21 Abs. 5 DSGVO** Im Zusammenhang mit der Nutzung von Diensten der Informationsgesellschaft stellt der:die Zertifizierungsantragsteller:in sicher, dass die betroffene Person ihr Widerspruchsrecht mittels automatisierter Verfahren ausüben kann, bei denen technische Spezifikationen verwendet werden. **5) Wissenschaftliche oder historische Forschungszwecke und statistische Zwecke gemäß Art. 21 Abs. 6 DSGVO** Bei Verarbeitungen zu wissenschaftlichen oder historischen Forschungszwecken oder zu statistischen Zwecken gemäß Art. 89 Abs. 1 DSGVO stellt der:die Zertifizierungsantragsteller:in sicher, dass ein Widerspruch aus Gründen der besonderen Situation der betroffenen Person berücksichtigt wird, es sei denn, die Verarbeitung ist zur Erfüllung einer im öffentlichen Interesse liegenden Aufgabe erforderlich. **6) Dokumentation** Der:die Zertifizierungsantragsteller:in dokumentiert die Bearbeitung des Widerspruchs, die Entscheidung und die zur Umsetzung des Widerspruchs ergriffenen Maßnahmen.

A.03.10 - Automatisierte Entscheidungen im Einzelfall einschließlich Profiling

Überblick

Werden Entscheidungen getroffen, die ausschließlich auf einer automatisierten Verarbeitung einschließlich Profiling beruhen und gegenüber betroffenen Personen rechtliche Wirkung entfalten oder sie in ähnlicher Weise erheblich beeinträchtigen, beurteilt der:die Zertifizierungsantragsteller:in im Vorhinein im Rahmen einer Datenschutz-Folgenabschätzung die zugrunde liegende Logik sowie die Folgen und beabsichtigten Wirkungen der Verarbeitung für die betroffenen Personen (zur Datenschutz-Folgenabschätzung siehe Kriterium A.09.01 ff.).

Detaillierte Anforderungen

***Anwendbarkeit**: Dieses Kriterium gilt in Fällen automatisierter Entscheidungen im Einzelfall und Profiling, bei denen Entscheidungen ausschließlich automatisiert getroffen werden („vollständig automatisierte Entscheidungen"). Dies liegt vor, wenn die Entscheidung ohne jegliche menschliche Mitwirkung erfolgt (Erwägungsgrund 71 DSGVO). Kann die Entscheidung einer natürlichen Person zugerechnet werden (anstelle einer Maschine), findet dieses Kriterium keine Anwendung.*

1) Information der betroffenen Person

Der:die Zertifizierungsantragsteller:in stellt der betroffenen Person im Rahmen der Informationspflichten und bei Auskunftsersuchen aussagekräftige Informationen über die involvierte Logik sowie die Tragweite und die angestrebten Auswirkungen der automatisierten Verarbeitung bereit (siehe Kriterien A.03.02–A.03.04).

2) Zulässigkeit automatisierter Entscheidungen

Entfaltet die automatisierte Entscheidung rechtliche Wirkung gegenüber der betroffenen Person (z. B. Ablehnung eines Kredits) oder beeinträchtigt sie die betroffene Person in vergleichbar erheblicher Weise (z. B. automatische Ablehnung eines Online-Kreditantrags), prüft und dokumentiert der:die Zertifizierungsantragsteller:in, ob mindestens eine der Voraussetzungen des Art. 22 Abs. 2 DSGVO vorliegt:

- Die Entscheidung ist für den Abschluss oder die Erfüllung eines Vertrags zwischen der betroffenen Person und dem:der Zertifizierungsantragsteller:in erforderlich.
- Die Entscheidung ist aufgrund von Unionsrecht oder dem Recht eines Mitgliedstaates zulässig und die einschlägigen Rechtsvorschriften sehen angemessene Maßnahmen zur Wahrung der Rechte und Freiheiten sowie der berechtigten Interessen der betroffenen Person vor.
- Die Entscheidung erfolgt mit ausdrücklicher Einwilligung der betroffenen Person.

3) Maßnahmen zum Schutz der betroffenen Person

Beruht die automatisierte Entscheidung auf der Erforderlichkeit für einen Vertragsabschluss bzw. eine Vertragserfüllung oder auf einer ausdrücklichen Einwilligung, setzt der:die Zertifizierungsantragsteller:in angemessene Maßnahmen zur Wahrung der Rechte und Freiheiten sowie der berechtigten Interessen der betroffenen Person um und dokumentiert diese. Mindestens werden gewährleistet:

- das Recht auf Erwirkung des Eingreifens einer Person seitens des:der Verantwortlichen;
- das Recht auf Darlegung des eigenen Standpunkts; und
- das Recht auf Anfechtung der Entscheidung.

Beruht die automatisierte Entscheidung auf Unionsrecht oder dem Recht eines Mitgliedstaates, dokumentiert der:die Zertifizierungsantragsteller:in die einschlägige Rechtsgrundlage und setzt die darin vorgesehenen Schutzmaßnahmen um.

4) Besondere Kategorien personenbezogener Daten

Werden besondere Kategorien personenbezogener Daten für eine ausschließlich automatisierte Entscheidung verarbeitet, prüft und dokumentiert der:die Zertifizierungsantragsteller:in, dass die Voraussetzungen des Art. 22 Abs. 4 i. V. m. Art. 9 Abs. 2 lit. a oder g DSGVO erfüllt und geeignete Maßnahmen zum Schutz der Rechte und Freiheiten sowie der berechtigten Interessen der betroffenen Person umgesetzt sind (siehe Kriterium A.02.04).

5) Dokumentation

Der:die Zertifizierungsantragsteller:in dokumentiert insbesondere:

- den Prozess der automatisierten Entscheidungsfindung einschließlich der vorgesehenen menschlichen Intervention und der Möglichkeiten zur Darlegung des eigenen Standpunkts und zur Anfechtung der Entscheidung;
- die involvierte Logik, die Tragweite und die beabsichtigten Auswirkungen der automatisierten Entscheidungsfindung;
- die Rechtsgrundlage und die Voraussetzungen für die Zulässigkeit der automatisierten Entscheidung (sofern die Verarbeitung für den Abschluss oder die Erfüllung eines Vertrags zwischen der betroffenen Person und dem:der Zertifizierungsantragsteller:in erforderlich ist, die Begründung dieser Erforderlichkeit; sofern die Verarbeitung auf einer Einwilligung beruht, das Vorliegen einer ausdrücklichen Einwilligung);
- die möglichen Auswirkungen auf die betroffene Person sowie die umgesetzten Maßnahmen zum Schutz der Rechte und Freiheiten sowie der berechtigten Interessen der betroffenen Personen; und
- Anträge betroffener Personen im Zusammenhang mit automatisierten Entscheidungen sowie deren Bearbeitung.

4.8. EINSCHRÄNKUNGEN

A.03.11 - Einschränkungen der Rechte betroffener Personen nach Unions- oder nationalem Recht

Überblick
Stützt sich der:die Zertifizierungsantragsteller:in auf eine gesetzliche Einschränkung von Rechten und Pflichten gemäß Art. 23 DSGVO, wird geprüft und dokumentiert, ob die Voraussetzungen der Einschränkung im konkreten Fall erfüllt sind.
Detaillierte Anforderungen
***Anwendbarkeit**: Dieses Kriterium gilt, wenn sich der:die Zertifizierungsantragsteller:in auf eine Einschränkung von Rechten oder Pflichten gemäß Art. 23 DSGVO beruft.* Bestehen unionsrechtliche Vorschriften oder Vorschriften des Rechts der Republik Österreich, denen der:die Zertifizierungsantragsteller:in unterliegt und die Einschränkungen der in Art. 12 bis 22 und Art. 34 DSGVO sowie in Art. 5 DSGVO vorgesehenen Rechte und Pflichten vorsehen, soweit dessen Bestimmungen den Rechten und Pflichten gemäß Art. 12 bis 22 DSGVO entsprechen, prüft und dokumentiert der:die Zertifizierungsantragsteller:in deren Anwendbarkeit im konkreten Fall. Die beschränkende gesetzliche Maßnahme muss erforderlich und verhältnismäßig sein. Dabei prüft und dokumentiert der:die Zertifizierungsantragsteller:in insbesondere, ob: ▶ die Einschränkung auf einer einschlägigen unionsrechtlichen oder österreichischen Rechtsvorschrift beruht; ▶ die Einschränkung einem der in Art. 23 Abs. 1 DSGVO genannten Zwecke dient; ▶ der Wesensgehalt der Grundrechte und Grundfreiheiten gewahrt bleibt; ▶ die Einschränkung in einer demokratischen Gesellschaft notwendig und verhältnismäßig ist; ▶ die Einschränkung auf das erforderliche Maß begrenzt ist; und ▶ die zugrunde liegende Rechtsvorschrift die Anforderungen des Art. 23 Abs. 2 DSGVO erfüllt. Bei der Bearbeitung von Anträgen betroffener Personen dokumentiert der:die Zertifizierungsantragsteller:in, ob und in welchem Umfang das jeweils geltend gemachte Recht aufgrund einer solchen Rechtsvorschrift eingeschränkt ist.

4.9. DATENSCHUTZ DURCH TECHNIKGESTALTUNG UND DURCH DATENSCHUTZFREUNDLICHE VOREINSTELLUNGEN

A.04.01 - Datenschutz durch Technikgestaltung

Überblick
Der:die Zertifizierungsantragsteller:in setzt die Datenschutzgrundsätze gemäß Art. 5 DSGVO durch geeignete technische und organisatorische Maßnahmen im Sinne des Art. 25 Abs. 1 DSGVO um.
Detaillierte Anforderungen
Der:die Zertifizierungsantragsteller:in legt für die zu zertifizierenden Verarbeitungstätigkeiten geeignete technische und organisatorische Maßnahmen zur Umsetzung der Datenschutzgrundsätze fest und dokumentiert diese. Dabei wird gemäß Art. 25 Abs. 1 DSGVO insbesondere berücksichtigt: ▶ der Stand der Technik; ▶ die Implementierungskosten; ▶ Art, Umfang, Umstände und Zwecke der Verarbeitung; sowie ▶ die unterschiedliche Eintrittswahrscheinlichkeit und Schwere der mit der Verarbeitung verbundenen Risiken für die Rechte und Freiheiten natürlicher Personen. Die technischen und organisatorischen Maßnahmen werden in Abhängigkeit von den zu zertifizierenden Verarbeitungstätigkeiten festgelegt. Konkrete technische und organisatorische Maßnahmen sind in Abschnitt 4.13 „Technische und organisatorische Maßnahmen zur Gewährleistung eines dem Risiko angemessenen Schutzniveaus" beschrieben. Die Anforderungen des Datenschutzes durch Technikgestaltung werden bereits bei der Planung und Konzeption neuer oder geänderter Datenverarbeitungsverfahren und -technologien sowie bei deren Entwicklung, Beschaffung und im laufenden Betrieb berücksichtigt.

Detaillierte Anforderungen

Ist der:die Zertifizierungsantragsteller:in für die Implementierung oder Anpassung von Systemen verantwortlich, die für die zu zertifizierenden Verarbeitungstätigkeiten eingesetzt werden, werden die Datenschutzgrundsätze in den entsprechenden technischen Konzepten und Entwicklungs- bzw. Programmierungsrichtlinien berücksichtigt (dies kann beispielsweise durch eine Beschreibung der Phasen des Entwicklungsprozesses erfolgen, in denen der Datenschutz berücksichtigt wird. Dazu zählen insbesondere die Planungs-, Design-, Implementierungs- und Testphase sowie Risikobewertungen zur Identifikation und Behandlung möglicher Datenschutzrisiken).

A.04.02 – Datenschutz durch Voreinstellungen

Überblick

Der:die Zertifizierungsantragsteller:in stellt sicher, dass die zu zertifizierenden Verarbeitungstätigkeiten dem Grundsatz des Datenschutzes durch datenschutzfreundliche Voreinstellungen gemäß Art. 25 Abs. 2 DSGVO entsprechen.

Detaillierte Anforderungen

Der:die Zertifizierungsantragsteller:in setzt technische und organisatorische Maßnahmen um, die sicherstellen, dass standardmäßig nur personenbezogene Daten verarbeitet werden, deren Verarbeitung für den jeweiligen bestimmten Verarbeitungszweck erforderlich ist. Dies betrifft insbesondere:

- die Menge der erhobenen personenbezogenen Daten;
- den Umfang ihrer Verarbeitung;
- ihre Speicherfrist; und
- ihre Zugänglichkeit.

Personenbezogene Daten werden insbesondere nicht ohne Eingreifen der betroffenen Person einer unbestimmten Zahl natürlicher Personen zugänglich gemacht.

Der:die Zertifizierungsantragsteller:in dokumentiert die der Auswahl der technischen und organisatorischen Maßnahmen zugrunde liegenden Überlegungen und Gründe.

4.10. GEMEINSAME VERANTWORTLICHE

A.04.03 - Vereinbarung zwischen gemeinsam Verantwortlichen

Überblick

Bei einer gemeinsamen Verarbeitung mit anderen Unternehmen schließt der:die Zertifizierungsantragsteller:in mit den weiteren Verantwortlichen eine Vereinbarung gemäß Art. 26 Abs. 1 und 2 DSGVO.

Detaillierte Anforderungen

***Anwendbarkeit**: Dieses Kriterium gilt für Verarbeitungstätigkeiten, bei denen der:die Zertifizierungsantragsteller:in eine gemeinsame Verantwortlichkeit angibt.*

Der:die Zertifizierungsantragsteller:in dokumentiert, in welchem Umfang die beteiligten Parteien die Zwecke („Warum“) und die Mittel der Verarbeitung („Wie“) festlegen und Kontrolle über die Verarbeitung ausüben. Dies bildet die Grundlage für die Beurteilung, ob eine gemeinsame Verantwortlichkeit gemäß Art. 26 DSGVO vorliegt.

Im Falle einer gemeinsamen Verantwortlichkeit mit anderen Verantwortlichen schließt der:die Zertifizierungsantragsteller:in eine Vereinbarung gemäß Art. 26 Abs. 1 und 2 DSGVO ab. Die Vereinbarung definiert die jeweiligen Verantwortlichkeiten gemäß DSGVO klar und eindeutig und berücksichtigt die tatsächlichen Funktionen und Beziehungen der gemeinsam Verantwortlichen im Hinblick auf die betroffenen Personen. Sie regelt insbesondere die Aufteilung der Aufgaben hinsichtlich:

- der Einhaltung der Grundsätze der Datenverarbeitung gemäß Art. 5 DSGVO;
- der Erfüllung der Informationspflichten gemäß Art. 13 und 14 DSGVO;
- der Bereitstellung der wesentlichen Inhalte der Vereinbarung gemäß Art. 26 Abs. 2 DSGVO;
- des Umgangs mit den Rechten betroffener Personen gemäß Art. 12–22 DSGVO einschließlich der damit verbundenen Mitteilungs- und Kommunikationspflichten;

Detaillierte Anforderungen

- der Erfüllung der Melde- und Benachrichtigungspflichten bei Datenschutzverletzungen gemäß Art. 33 und 34 DSGVO; und
- der Festlegung einer Anlaufstelle für betroffene Personen.

Die wesentlichen Inhalte der Vereinbarung werden den betroffenen Personen elektronisch über die Website der Organisation zur Verfügung gestellt. Dies umfasst insbesondere:

- die klare Zuordnung der jeweiligen Pflichten zu den gemeinsam Verantwortlichen;
- die Verantwortlichkeit für die Informationspflichten gemäß Art. 13 und 14 DSGVO; und
- die Zuständigkeiten für die Umsetzung der Rechte betroffener Personen.

4.11. ANFORDERUNGEN GEMÄß ART. 28 DSGVO (VERHÄLTNIS ZWISCHEN VERANTWORTLICHEN UND AUFTRAGSVERARBEITER:INNEN)

A.04.04 - Richtlinie zum Umgang mit Auftragsverarbeiter:innen und Dienstleister:innen

Überblick

Der:die Zertifizierungsantragsteller:in trifft Regelungen für den Umgang mit Auftragsverarbeiter:innen und sonstigen Dienstleister:innen, um die Einhaltung der datenschutz- und sicherheitsrechtlichen Anforderungen sicherzustellen. Es werden nur Auftragsverarbeiter:innen eingesetzt, die hinreichende Garantien dafür bieten, dass geeignete technische und organisatorische Maßnahmen so durchgeführt werden, dass die Verarbeitung im Einklang mit der DSGVO erfolgt und der Schutz der Rechte der betroffenen Personen gewährleistet ist.

Detaillierte Anforderungen

***Anwendbarkeit**: Dieses Zertifizierungskriterium gilt, wenn der:die Zertifizierungsantragsteller:in für die zu zertifizierende Verarbeitungstätigkeit Auftragsverarbeiter:innen einsetzt oder beabsichtigt, die Verarbeitung oder Teile davon an eine:n oder mehrere Auftragsverarbeiter:innen auszulagern.*

Der:die Zertifizierungsantragsteller:in erstellt und pflegt Richtlinien für den Umgang mit Auftragsverarbeiter:innen und sonstigen Dritten, die Dienstleistungen erbringen. Die Richtlinien enthalten mindestens:

- Vorgaben für die Auswahl und Beauftragung externer Lieferant:innen, Dienstleister:innen und Auftragsverarbeiter:innen (z. B. Auswahlverfahren inkl. Lieferant:innenbewertung, die auch Datenschutz- und Sicherheitsaspekte berücksichtigt, Standort der Auftragsverarbeiter:innen, angemessene technische und organisatorische Maßnahmen, Fachkunde der Auftragsverarbeiter:innen, Zuverlässigkeit der Auftragsverarbeiter:innen, Ressourcen der Auftragsverarbeiter:innen, anerkannte internationale Zertifizierungen (z. B. ISO/IEC 27001) sowie etwaige Zertifizierungen gemäß DSGVO oder Teilnahme an datenschutzrechtlichen Verhaltensregeln);
- Vorgaben für den Umgang mit Dritten mit Sitz außerhalb der EU unter Berücksichtigung der Anforderungen an internationale Datenübermittlungen gemäß Art. 44 ff. DSGVO (z. B. Berücksichtigung in der Risikobewertung); und
- Festlegungen zu Verantwortlichkeiten, Rechten und Pflichten sowie vertraglichen Regelungen für Dritte gemäß den Anforderungen der DSGVO (z. B. Verpflichtung zum Abschluss von Vertraulichkeitsvereinbarungen, Durchführung eines Impact-Assessments, allgemeine Sicherheitsanforderungen für die Auftragsverarbeiter:innen, Verfahren zur Änderung von Aufträgen oder zur Vertragsbeendigung (z. B. Rückgabe von Daten oder Geräten), Umgang mit Dritten während des laufenden Betriebs (z. B. regelmäßige Überprüfung des Vertrags, Überprüfung der Servicequalität)).

A.04.05 - Vereinbarungen zur Datenverarbeitung mit Auftragsverarbeiter:innen, die alle Anforderungen des Art. 28 DSGVO erfüllen

Überblick

Der:die Zertifizierungsantragsteller:in trifft Regelungen für den Umgang mit Auftragsverarbeiter:innen und sonstigen Dienstleister:innen, um die Einhaltung der datenschutz- und sicherheitsrechtlichen Anforderungen sicherzustellen. Es werden nur Auftragsverarbeiter:innen eingesetzt, die hinreichende Garantien dafür bieten, dass geeignete technische und organisatorische Maßnahmen so durchgeführt werden, dass die Verarbeitung im Einklang mit der DSGVO erfolgt und der Schutz der Rechte der betroffenen Personen gewährleistet ist.

Detaillierte Anforderungen

***Anwendbarkeit**: Dieses Zertifizierungskriterium gilt, wenn der:die Zertifizierungsantragsteller:in für die zu zertifizierende Verarbeitungstätigkeit Auftragsverarbeiter:innen einsetzt oder beabsichtigt, die Verarbeitung oder Teile davon an eine:n oder mehrere Auftragsverarbeiter:innen auszulagern.*

Der:die Zertifizierungsantragsteller:in schließt mit allen Auftragsverarbeiter:innen vor Beginn der Verarbeitung einen schriftlichen Vertrag gemäß Art. 28 DSGVO ab. Alternativ wird sichergestellt, dass die Verarbeitung durch ein unionsrechtliches oder mitgliedstaatliches Rechtsinstrument geregelt wird, das den Anforderungen des Art. 28 DSGVO entspricht.

Der Vertrag bzw. das Rechtsinstrument legt insbesondere Gegenstand und Dauer, Art und Zweck der Verarbeitung, die Art der personenbezogenen Daten und die Kategorien betroffener Personen sowie die Rechte und Pflichten des:der Zertifizierungsantragstellers:in fest. Darüber hinaus werden die Auftragsverarbeiter:innen gemäß Art. 28 Abs. 3 DSGVO insbesondere verpflichtet:

- personenbezogene Daten nur auf dokumentierte Weisung des:der Zertifizierungsantragstellers:in zu verarbeiten, einschließlich bei Übermittlungen an Drittländer oder internationale Organisationen, soweit keine gesetzliche Verpflichtung zur Verarbeitung besteht; besteht eine solche Verpflichtung, informiert der:die Auftragsverarbeiter:in den:die Zertifizierungsantragsteller:in vorab darüber, sofern das betreffende Recht eine solche Information nicht aus wichtigen Gründen des öffentlichen Interesses untersagt;
- sicherzustellen, dass die zur Verarbeitung befugten Personen zur Vertraulichkeit verpflichtet wurden oder einer gesetzlichen Verschwiegenheitspflicht unterliegen;
- die erforderlichen Maßnahmen gemäß Art. 32 DSGVO zu ergreifen;
- weitere Auftragsverarbeiter:innen nur nach vorheriger gesonderter oder allgemeiner schriftlicher Genehmigung einzusetzen (siehe Kriterium A.04.06);
- bei der Erfüllung der Rechte betroffener Personen sowie der Pflichten gemäß Art. 32–36 DSGVO zu unterstützen;
- nach Abschluss der Leistungserbringung personenbezogene Daten nach Wahl des:der Zertifizierungsantragstellers:in zu löschen oder zurückzugeben und vorhandene Kopien zu löschen, soweit keine gesetzliche Aufbewahrungspflicht besteht;
- die für den Nachweis der Einhaltung der Anforderungen des Art. 28 DSGVO erforderlichen Informationen bereitzustellen und Audits einschließlich Inspektionen zu ermöglichen und zu unterstützen; und
- den:die Zertifizierungsantragsteller:in unverzüglich zu informieren, wenn eine Weisung nach eigener Auffassung gegen die DSGVO oder andere Datenschutzvorschriften verstößt.

Der:die Zertifizierungsantragsteller:in bewahrt die Vereinbarungen strukturiert und leicht zugänglich auf.

A.04.06 - Widerspruchsrecht gegen weitere Unterauftragsverarbeiter:innen

Überblick

Der:die Zertifizierungsantragsteller:in stellt sicher, dass beauftragte Auftragsverarbeiter:innen Unterauftragsverarbeiter:innen nur mit vorheriger gesonderter oder allgemeiner schriftlicher Genehmigung des:der Verantwortlichen einsetzen.

Detaillierte Anforderungen

***Anwendbarkeit**: Dieses Zertifizierungskriterium gilt, wenn der:die Zertifizierungsantragsteller:in für die zu zertifizierende Verarbeitungstätigkeit Auftragsverarbeiter:innen einsetzt oder beabsichtigt, die Verarbeitung oder Teile davon an eine:n oder mehrere Auftragsverarbeiter:innen auszulagern.*

Detaillierte Anforderungen

Der:die Zertifizierungsantragsteller:in vereinbart mit Auftragsverarbeiter:innen, dass Unterauftragsverarbeiter:innen nur nach vorheriger gesonderter oder allgemeiner schriftlicher Genehmigung eingesetzt werden dürfen.

Bei einer allgemeinen schriftlichen Genehmigung werden insbesondere folgende Regelungen getroffen:

- Kriterien für die Auswahl von Unterauftragsverarbeiter:innen, einschließlich der Garantien hinsichtlich technischer und organisatorischer Maßnahmen, Fachkunde und Zuverlässigkeit;
- ein Widerspruchsrecht des:der Zertifizierungsantragstellers:in gegen beabsichtigte Änderungen hinsichtlich der Hinzuziehung oder Ersetzung von Unterauftragsverarbeiter:innen;
- eine Frist, innerhalb derer der:die Auftragsverarbeiter:in den:die Zertifizierungsantragsteller:in vor der beabsichtigten Änderung informiert;
- eine Frist für die Ausübung des Widerspruchsrechts; und
- die Festlegung der internen Ansprechpartner:innen sowie der Ansprechpartner:innen bei den Auftragsverarbeiter:innen.

A.04.07 - Überprüfung der Sicherheit der Datenverarbeitung

Überblick

Der:die Zertifizierungsantragsteller:in stellt sicher, dass ausschließlich Auftragsverarbeiter:innen eingesetzt werden, die hinreichende Garantien dafür bieten, dass geeignete technische und organisatorische Maßnahmen umgesetzt werden, sodass die Verarbeitung gemäß den Anforderungen der DSGVO erfolgt und die Rechte der betroffenen Personen gewahrt werden.

Detaillierte Anforderungen

***Anwendbarkeit**: Dieses Zertifizierungskriterium gilt, wenn der:die Zertifizierungsantragsteller:in für die zu zertifizierende Verarbeitungstätigkeit Auftragsverarbeiter:innen einsetzt oder beabsichtigt, die Verarbeitung oder Teile davon an eine:n oder mehrere Auftragsverarbeiter:innen auszulagern.*

Der:die Zertifizierungsantragsteller:in verfügt über ein dokumentiertes Verfahren zur Überprüfung der eingesetzten Auftragsverarbeiter:innen und legt auf Grundlage einer Risikobewertung Art und Häufigkeit der durchzuführenden Prüfungen fest.

Die Art der Prüfung richtet sich nach dem mit der Verarbeitung verbundenen Risiko und kann insbesondere anhand von Fragebögen und Dokumentennachweisen oder durch Vor-Ort-Audits erfolgen. Ein Fragebogen kann bei weniger komplexen Verfahren und geringeren Risiken ausreichend sein, sofern der:die Auftragsverarbeiter:in die erforderlichen Informationen und Nachweise liefern kann. Bei komplexeren Verarbeitungen oder höheren Risiken kann ein Vor-Ort-Audit erforderlich sein, um die Umsetzung der Maßnahmen vor Ort zu prüfen und zusätzliche Nachweise zu erlangen. Bei der Festlegung der Prüfungsmaßnahmen und -häufigkeit werden insbesondere die Sensitivität der verarbeiteten Daten, die Risiken für die Rechte und Freiheiten betroffener Personen, die Komplexität der technischen und organisatorischen Maßnahmen und die Bedeutung der Verarbeitung für die Geschäftsfortführung berücksichtigt. Anlassbezogene Prüfungen können insbesondere bei Datenschutzverletzungen oder wesentlichen Änderungen bei Auftragsverarbeiter:innen erforderlich sein. Als Nachweise können insbesondere einschlägige Zertifizierungen (z. B. ISO/IEC 27001, ISO/IEC 27701 etc.), Prüfberichte (z. B. nach ISAE 3402 und ISAE 3000) sowie die Einhaltung genehmigter Verhaltensregeln gemäß Art. 40 DSGVO oder Zertifizierungen gemäß Art. 42 DSGVO berücksichtigt werden.

Der:die Zertifizierungsantragsteller:in prüft die Nachweise der Auftragsverarbeiter:innen entsprechend dem festgelegten Verfahren und dokumentiert die Ergebnisse. Bei Vor-Ort-Audits werden insbesondere Umfang, angewandte Methoden, Auditnachweise, Ergebnisse und Feststellungen sowie gegebenenfalls daraus resultierende Maßnahmen dokumentiert.

Die Häufigkeit der Audits richtet sich nach dem Risikoprofil der Auftragsverarbeiter:innen und der Sensitivität der verarbeiteten Daten. Bei kritischen Auftragsverarbeiter:innen oder Verarbeitung sensibler Daten kann eine jährliche Prüfung erforderlich sein. Bei geringeren Risiken kann ein Intervall von zwei oder drei Jahren ausreichen.

A.04.08 - Liste der Auftragsverarbeiter:innen, die personenbezogene Daten verarbeiten

Überblick
Der:die Zertifizierungsantragsteller:in führt eine Übersicht über alle Auftragsverarbeiter:innen, die zur Verarbeitung personenbezogener Daten eingesetzt werden.
Detaillierte Anforderungen
***Anwendbarkeit**: Dieses Zertifizierungskriterium gilt, wenn der:die Zertifizierungsantragsteller:in für die zu zertifizierende Verarbeitungstätigkeit Auftragsverarbeiter:innen einsetzt oder beabsichtigt, die Verarbeitung oder Teile davon an eine:n oder mehrere Auftragsverarbeiter:innen auszulagern.* Der:die Zertifizierungsantragsteller:in führt eine vollständige und aktuelle Liste der eingesetzten Auftragsverarbeiter:innen. Diese enthält mindestens: ▶ Name bzw. Firma, Anschrift und Kontaktdaten der Auftragsverarbeiter:innen; ▶ Zweck und allgemeine Beschreibung der Verarbeitung; ▶ Kategorien der an die Auftragsverarbeiter:innen übermittelten personenbezogenen Daten; ▶ Datum des Abschlusses des Auftragsverarbeitungsvertrags; und ▶ Angaben dazu, ob die Auftragsverarbeiter:innen in einem Drittland ansässig sind, sowie gegebenenfalls zu den geeigneten Garantien gemäß Art. 46 DSGVO.

4.12. VERZEICHNIS VON VERARBEITUNGSTÄTIGKEITEN

A.05.01 - Inventar der an den Verarbeitungstätigkeiten beteiligten Systeme (Asset Register)

Überblick
Der:die Zertifizierungsantragsteller:in dokumentiert die Systeme, in denen personenbezogene Daten verarbeitet werden, um die relevanten Verarbeitungstätigkeiten zu identifizieren.
Detaillierte Anforderungen
Der:die Zertifizierungsantragsteller:in führt ein Inventar der eingesetzten Systeme, Hardware und Software, das einen Überblick über die für die Verarbeitungstätigkeiten verwendete Infrastruktur ermöglicht. Darüber hinaus werden die Datenflüsse und die Vernetzung der eingesetzten Systeme und Komponenten einschließlich interner Verbindungen und Verbindungen zu externen Netzwerken dokumentiert. Die Dokumentation kann insbesondere in Form eines Datenflussdiagramms erfolgen. Das Inventar und die Dokumentation der Datenflüsse werden mindestens einmal jährlich sowie bei wesentlichen Änderungen überprüft und erforderlichenfalls aktualisiert.

A.05.02 - Verzeichnis der Verarbeitungstätigkeiten

Überblick
Der:die Zertifizierungsantragsteller:in führt ein Verzeichnis der Verarbeitungstätigkeiten.
Detaillierte Anforderungen
***Anwendbarkeit**: Dieses Kriterium findet bei Zertifizierungsantragsteller:innen mit weniger als 250 Mitarbeitenden keine Anwendung, sofern die Verarbeitung nicht ein Risiko für die Rechte und Freiheiten betroffener Personen birgt, nur gelegentlich erfolgt und weder besondere Kategorien personenbezogener Daten gemäß Art. 9 Abs. 1 DSGVO noch personenbezogene Daten über strafrechtliche Verurteilungen und Straftaten gemäß Art. 10 DSGVO umfasst (Art. 30 Abs. 5 DSGVO).* Der:die Verantwortliche führt ein Verzeichnis der Verarbeitungstätigkeiten, das die Verarbeitungstätigkeiten im Geltungsbereich der Zertifizierung umfasst. Das Verzeichnis enthält gemäß Art. 30 Abs. 1 DSGVO mindestens:

Detaillierte Anforderungen

- Name und Kontaktdaten des:der Zertifizierungsantragstellers:in und gegebenenfalls des:der gemeinsam Verantwortlichen, eines Vertreters sowie des:der Datenschutzbeauftragten;
- die Zwecke der Verarbeitung;
- eine Beschreibung der Kategorien betroffener Personen und der Kategorien personenbezogener Daten;
- die Kategorien von Empfänger:innen, gegenüber denen personenbezogene Daten offengelegt wurden oder werden, einschließlich Empfänger:innen in Drittländern oder internationalen Organisationen;
- gegebenenfalls Angaben zu Datenübermittlungen an ein Drittland oder eine internationale Organisation, einschließlich deren Bezeichnung, sowie – im Fall von Übermittlungen gemäß Art. 49 Abs. 1 Unterabs. 2 DSGVO – Dokumentation geeigneter Garantien;
- soweit möglich, die vorgesehenen Löschfristen für die verschiedenen Datenkategorien;
- soweit möglich, eine allgemeine Beschreibung der gemäß Art. 32 Abs. 1 DSGVO getroffenen technischen und organisatorischen Maßnahmen.

Das Verzeichnis wird in schriftlicher (elektronischer) Form geführt.

A.05.03 - Pflege und regelmäßige Aktualisierung des Verzeichnisses von Verarbeitungstätigkeiten

Überblick

Der:die Zertifizierungsantragsteller:in hält das Verzeichnis der Verarbeitungstätigkeiten aktuell.

Detaillierte Anforderungen

***Anwendbarkeit**: Dieses Kriterium findet bei Zertifizierungsantragsteller:innen mit weniger als 250 Mitarbeitenden keine Anwendung, sofern die Verarbeitung nicht ein Risiko für die Rechte und Freiheiten betroffener Personen birgt, nur gelegentlich erfolgt und weder besondere Kategorien personenbezogener Daten gemäß Art. 9 Abs. 1 DSGVO noch personenbezogene Daten über strafrechtliche Verurteilungen und Straftaten gemäß Art. 10 DSGVO umfasst (Art. 30 Abs. 5 DSGVO).*

Der:die Zertifizierungsantragsteller:in überprüft das Verzeichnis der Verarbeitungstätigkeiten mindestens einmal jährlich und aktualisiert es erforderlichenfalls. Die Verantwortlichkeiten für die Erfassung und Pflege der Einträge werden festgelegt (z. B. in einer Richtlinie oder als Bestandteil des Verzeichnisses der Verarbeitungstätigkeiten).

Der:die Zertifizierungsantragsteller:in dokumentiert die durchgeführte Überprüfung schriftlich.

Änderungen des Verzeichnisses werden versioniert, sodass neue Einträge, inhaltliche Änderungen und die Löschung von Verarbeitungstätigkeiten nachvollziehbar bleiben.

A.05.04 - Vorlage des Verzeichnisses der Verarbeitungstätigkeiten an die Aufsichtsbehörde

Überblick

Der:die Zertifizierungsantragsteller:in stellt das Verzeichnis der Verarbeitungstätigkeiten der Aufsichtsbehörde auf Anfrage zur Verfügung.

Detaillierte Anforderungen

***Anwendbarkeit**: Dieses Kriterium findet bei Zertifizierungsantragsteller:innen mit weniger als 250 Mitarbeitenden keine Anwendung, sofern die Verarbeitung nicht ein Risiko für die Rechte und Freiheiten betroffener Personen birgt, nur gelegentlich erfolgt und weder besondere Kategorien personenbezogener Daten gemäß Art. 9 Abs. 1 DSGVO noch personenbezogene Daten über strafrechtliche Verurteilungen und Straftaten gemäß Art. 10 DSGVO umfasst (Art. 30 Abs. 5 DSGVO).*

Der:die Zertifizierungsantragsteller:in stellt das Verzeichnis der Verarbeitungstätigkeiten gemäß Art. 30 Abs. 4 DSGVO auf Anfrage der Aufsichtsbehörde zur Verfügung. Hierzu werden Ansprechpersonen bzw. klare Verantwortlichkeiten für die Übermittlung des Verzeichnisses an die Aufsichtsbehörde festgelegt.

4.13. TECHNISCHE UND ORGANISATORISCHE MAßNAHMEN ZUR GEWÄHRLEISTUNG EINES DEM RISIKO ANGEMESSENEN SCHUTZNIVEAUS

A.06.01 - Dokumentation eines Risikomanagementprozesses

Überblick
Der:die Zertifizierungsantragsteller:in entwickelt einen geeigneten Risikomanagementprozess für den Umgang mit IT-Risiken.
Detaillierte Anforderungen
Der:die Zertifizierungsantragsteller:in implementiert einen dokumentierten Prozess zur Identifizierung, Analyse und Kategorisierung von Risiken für die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit personenbezogener Daten im Rahmen der zu zertifizierenden Verarbeitungstätigkeiten. Der Risikomanagementprozess umfasst mindestens: **a) Identifizierung potenzieller Risiken** Der:die Zertifizierungsantragsteller:in berücksichtigt insbesondere Risiken aus Projekten und dem laufenden Betrieb, im Zusammenhang mit Datenschutzvorfällen, aus Prozessen zum Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen sowie aus Datenschutz-Folgenabschätzungen. **b) Bewertung der identifizierten Risiken** Der:die Zertifizierungsantragsteller:in bewertet und dokumentiert die identifizierten Risiken hinsichtlich ihrer Auswirkungen auf die Rechte und Freiheiten betroffener Personen (z. B. körperliche, materielle oder immaterielle Schäden, Verlust der Kontrolle über personenbezogene Daten, Diskriminierung, Identitätsdiebstahl etc.) und ihrer Eintrittswahrscheinlichkeit. Die Bewertung erfolgt anhand einer festgelegten Bewertungsmethodik. **c) Umsetzung und Überwachung von Maßnahmen** Für die identifizierten Risiken legt der:die Zertifizierungsantragsteller:in geeignete technische und organisatorische Maßnahmen fest und setzt diese um (siehe Kriterium A.06.02). Der Risikomanagementprozess wird mindestens einmal jährlich sowie bei wesentlichen Änderungen überprüft.

A.06.02 - Risikoorientierte technische und organisatorische Maßnahmen zur Gewährleistung der Sicherheit der Datenverarbeitung

Überblick
Der:die Zertifizierungsantragsteller:in legt Maßnahmen für die im Rahmen der Risikoanalyse identifizierten Risiken für die Rechte und Freiheiten betroffener Personen fest, plant deren Umsetzung, bestimmt die Risikoverantwortlichen und verfolgt den Umsetzungsstatus.
Detaillierte Anforderungen
Auf Grundlage der Risikobewertung gemäß Kriterium A.06.01 dokumentiert der:die Zertifizierungsantragsteller:in die technischen und organisatorischen Maßnahmen, die zur Gewährleistung eines dem jeweiligen Risiko angemessenen Schutzniveaus umgesetzt werden. Der Umsetzungsstatus der Maßnahmen und die jeweils zugeordneten Risikoverantwortlichen werden dokumentiert. Wird ein Restrisiko akzeptiert, werden die Gründe hierfür im Risikomanagementplan dokumentiert. Gemäß Art. 32 Abs. 1 DSGVO umfassen die Maßnahmen gegebenenfalls: ▶ die Pseudonymisierung und Verschlüsselung personenbezogener Daten; ▶ die Fähigkeit, die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung auf Dauer sicherzustellen; ▶ die Fähigkeit, die Verfügbarkeit personenbezogener Daten und den Zugang zu ihnen bei einem physischen oder technischen Zwischenfall rasch wiederherzustellen; und ▶ ein Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung. Die Kriterien A.07.01–A.07.25 beschreiben technische und organisatorische Maßnahmen zur Erfüllung der Anforderungen des Art. 32 DSGVO, die grundsätzlich umzusetzen sind. Die Auswahl und Umsetzung der Maßnahmen erfolgt auf Grundlage der Risikobewertung gemäß Kriterium A.06.01. Werden einzelne Maßnahmen nicht umgesetzt, dokumentiert der:die Zertifizierungsantragsteller:in nachvollziehbar, weshalb diese im konkreten Fall nicht erforderlich oder nicht verhältnismäßig sind.

A.06.03 - Regelmäßige Überprüfung der Risikoanalyse

Überblick
Der:die Zertifizierungsantragsteller:in überprüft die durchgeführten Risikobewertungen mindestens einmal jährlich sowie bei wesentlichen Änderungen.
Detaillierte Anforderungen
Der:die Zertifizierungsantragsteller:in überprüft die Risikobewertung mindestens einmal jährlich sowie bei wesentlichen Änderungen, die sich auf die Verarbeitungstätigkeiten oder deren Risikolage auswirken können (z. B. Einsatz neuer IT-Systeme, Änderung/Erweiterung der verarbeiteten personenbezogenen Daten, Änderungen in der Art und Weise der Verarbeitung personenbezogener Daten – z. B. Einsatz neuer Analysetools). Die Überprüfung erfolgt anhand einer dokumentierten Methodik und berücksichtigt interne und externe Faktoren, die die Risikobewertung beeinflussen können. Dazu zählen insbesondere Änderungen der Rechtslage, Unternehmensumstrukturierungen (z. B. Outsourcing, Fusionen oder Übernahmen), Anpassungen in den Datenschutzpraktiken, Einsatz neuer Technologien, Änderungen in der Dienstleistungserbringung sowie organisatorische oder technische Veränderungen. Im Rahmen der Überprüfung bewertet der:die Zertifizierungsantragsteller:in auch, ob die umgesetzten technischen und organisatorischen Maßnahmen unter Berücksichtigung der aktuellen Risikolage weiterhin angemessen und wirksam sind, und passt diese erforderlichenfalls an. Ist ein:e Datenschutzbeauftragte:r benannt, holt der:die Zertifizierungsantragsteller:in eine Stellungnahme ein und dokumentiert die Gründe, wenn von dieser abgewichen wird. Die Überprüfung und deren Ergebnis werden dokumentiert und durch die Geschäftsleitung bestätigt.

A.07.01 - Performanceparameter zur Sicherstellung der Belastbarkeit gegenüber Störungen und deren Überwachung

Überblick
Der:die Zertifizierungsantragsteller:in legt Performance- und Kapazitätsanforderungen fest, um die Belastbarkeit der für die zu zertifizierenden Verarbeitungstätigkeiten relevanten IT-Systeme sicherzustellen.
Detaillierte Anforderungen
Der:die Zertifizierungsantragsteller:in legt für die relevanten IT-Systeme geeignete Performanceparameter fest. Diese können insbesondere zulässige Ausfallzeiten, Reaktionszeiten bei Störungen, Verarbeitungsgeschwindigkeiten oder Verfügbarkeitszeiten umfassen. Die Einhaltung der festgelegten Performanceparameter wird durch geeignete Überwachungsmaßnahmen erfasst (z. B. Monitoring- oder Protokollierungs-Tools).

A.07.02 - Schutz vor Malware

Überblick
Der:die Zertifizierungsantragsteller:in implementiert Schutzmaßnahmen gegen Malware, um personenbezogene Daten vor Malware zu schützen.
Detaillierte Anforderungen
Der:die Zertifizierungsantragsteller:in richtet auf Grundlage des Risikomanagements Richtlinien und Verfahren zum Schutz der für die Verarbeitung personenbezogener Daten eingesetzten Systeme und Geräte vor Malware und bekannten Schwachstellen ein. Die eingesetzten Malware-Schutzmaßnahmen werden regelmäßig aktualisiert, um aktuellen Bedrohungen entgegenzuwirken.

A.07.03 - Netzwerksegmentierung

Überblick
Der:die Zertifizierungsantragsteller:in unterteilt Netzwerke in Sicherheitszonen und trennt diese vom öffentlichen Netzwerk.
Detaillierte Anforderungen
Der:die Zertifizierungsantragsteller:in setzt auf Grundlage der Risikobewertung gemäß den Kriterien A.06.01 und A.06.02 geeignete Maßnahmen zur Netzwerksegmentierung um. Netzwerke werden logisch getrennt, um unbefugte Zugriffe auf personenbezogene Daten zu verhindern. Dabei werden insbesondere Systeme mit unterschiedlichen Anforderungen an Vertraulichkeit und Verfügbarkeit voneinander isoliert (z. B. Trennung medizinischer Netzwerke in Krankenhäusern oder Personalverwaltungsnetzwerke von administrativen Netzwerken) und relevante Netzwerkbereiche vom öffentlichen Netzwerk getrennt.

A.07.04 - Netzwerküberwachung

Überblick
Der:die Zertifizierungsantragsteller:in implementiert eine Netzwerküberwachung, um potenzielle Sicherheitsverletzungen und Datenschutzverstöße zu erkennen.
Detaillierte Anforderungen
Der:die Zertifizierungsantragsteller:in setzt auf Grundlage der Risikobewertung gemäß den Kriterien A.06.01 und A.06.02 geeignete Maßnahmen zur Netzwerküberwachung um. Die Überwachung ermöglicht die frühzeitige Erkennung potenzieller Sicherheitsverletzungen und Datenschutzverstöße sowie eine zeitnahe Reaktion. Umfang und Häufigkeit der Überwachungsmaßnahmen werden an die identifizierten Risiken angepasst und berücksichtigen geschäftliche sowie datenschutzrechtliche Anforderungen. Überwachungsprotokolle werden für einen festgelegten Zeitraum entsprechend den rechtlichen, regulatorischen und betrieblichen Anforderungen aufbewahrt.

A.07.05 - Remote-Working

Überblick
Der:die Zertifizierungsantragsteller:in implementiert Sicherheitsmaßnahmen für Remote-Zugriffe, um die Vertraulichkeit, Integrität und Verfügbarkeit personenbezogener Daten sicherzustellen.
Detaillierte Anforderungen
Der:die Zertifizierungsantragsteller:in setzt auf Grundlage der Risikobewertung gemäß den Kriterien A.06.01 und A.06.02 geeignete Sicherheitsmaßnahmen für Remote-Zugriffe auf das Unternehmensnetzwerk um. Diese umfassen sichere Authentifizierungsmechanismen und definierte Regeln für Remote-Zugriffe.

A.07.06 - Zugriffsregelung für sensible Bereiche

Überblick
Der:die Zertifizierungsantragsteller:in stellt sicher, dass der Zugang zu sensiblen Bereichen geregelt ist.
Detaillierte Anforderungen
Der:die Zertifizierungsantragsteller:in setzt auf Grundlage der Risikobewertung gemäß den Kriterien A.06.01 und A.06.02 geeignete Sicherheitsmaßnahmen für Räumlichkeiten und Bereiche um, in denen personenbezogene Daten verarbeitet werden oder auf diese zugegriffen werden kann (z. B. IT-Abteilung, HR-Abteilung). Der Zugang zu unterschiedlichen Sicherheitszonen wird entsprechend den Sicherheitsanforderungen der verarbeiteten Daten geregelt.

A.07.07 - Zugangsfreigabeprozess für sensible Bereiche

Überblick
Der:die Zertifizierungsantragsteller:in stellt sicher, dass der Zugang zu sensiblen Bereichen geregelt ist.
Detaillierte Anforderungen
Der:die Zertifizierungsantragsteller:in richtet auf Grundlage der Risikobewertung gemäß den Kriterien A.06.01 und A.06.02 ein Verfahren zur Zugangskontrolle für sensible Bereiche ein, in denen personenbezogene Daten verarbeitet werden. Das Verfahren stellt sicher, dass nur autorisierte Personen Zugang erhalten und das Niveau der Zugangskontrolle der Sensibilität der verarbeiteten Daten und den identifizierten Risiken entspricht.

A.07.08 - Schutz vor externen und umweltbedingten Bedrohungen

Überblick
Der:die Zertifizierungsantragsteller:in mindert oder beseitigt potenzielle nachteilige Auswirkungen externer und umweltbedingter Bedrohungen durch geeignete Maßnahmen.
Detaillierte Anforderungen
Der:die Zertifizierungsantragsteller:in setzt auf Grundlage der Risikobewertung gemäß den Kriterien A.06.01 und A.06.02 geeignete Sicherheitsmaßnahmen zum Schutz personenbezogener Daten vor externen und umweltbedingten Bedrohungen um (z. B. Einbrüche, Diebstahl von Hardware oder Datenträgern, Feuer, Überschwemmungen, Stromausfälle).

A.07.09 - Verfahren zur Datenpseudonymisierung oder -anonymisierung

Überblick
Der:die Zertifizierungsantragsteller:in setzt Verfahren zur Pseudonymisierung und Anonymisierung personenbezogener Daten ein, die dem Stand der Technik entsprechen und praktikabel sind.
Detaillierte Anforderungen
Sofern im Rahmen der zu zertifizierenden Verarbeitungstätigkeiten Pseudonymisierungs- oder Anonymisierungstechniken eingesetzt werden, stellt der:die Zertifizierungsantragsteller:in sicher, dass diese dem Stand der Technik entsprechen und geeignet sind, die gemäß den Kriterien A.06.01 und A.06.02 identifizierten Risiken zu mindern. Der:die Zertifizierungsantragsteller:in dokumentiert die eingesetzten Verfahren zur Pseudonymisierung und Anonymisierung nachvollziehbar. Die Dokumentation beschreibt das jeweilige Verfahren und enthält – soweit möglich – auch eine Demonstration/Begründung der Wirksamkeit des Verfahrens.

A.07.10 - Protokollierungsfunktionen für toolgestützte Verarbeitung

Überblick
Der:die Zertifizierungsantragsteller:in stellt sicher, dass beim Einsatz von Tools oder Software zur Unterstützung von Verarbeitungstätigkeiten geeignete Protokollierungsfunktionen implementiert sind.
Detaillierte Anforderungen
Der:die Zertifizierungsantragsteller:in implementiert geeignete Protokollierungsmechanismen, um Zugriffe auf personenbezogene Daten, relevante Verarbeitungsvorgänge sowie Änderungen an personenbezogenen Daten nachvollziehbar zu erfassen. Protokolldaten werden sicher gespeichert und vor unbefugtem Zugriff geschützt. Umfang und technische Umsetzung der Protokollierung richten sich nach der Risikobewertung gemäß den Kriterien A.06.01 und A.06.02.

A.07.11 - Kontinuitätspläne und Wiederherstellungsmaßnahmen

Überblick
Der:die Zertifizierungsantragsteller:in legt Kontinuitätspläne sowie Reaktions- und Wiederherstellungsverfahren fest.
Detaillierte Anforderungen
Der:die Zertifizierungsantragsteller:in setzt auf Grundlage der Risikobewertung gemäß den Kriterien A.06.01 und A.06.02 geeignete Kontinuitäts-, Reaktions- und Wiederherstellungsmaßnahmen um, um die Verfügbarkeit personenbezogener Daten bei Störungen, Notfällen oder Datenverlust rasch wiederherzustellen. Die festgelegten Maßnahmen werden regelmäßig auf ihre Angemessenheit und Wirksamkeit überprüft.

A.07.12 - Festlegungen und Maßnahmen zur Datensicherung (Datensicherungskonzept)

Überblick
Der:die Zertifizierungsantragsteller:in legt ein Sicherungskonzept fest, das den Anforderungen der Organisation an Datenaufbewahrung und Informationssicherheit entspricht.
Detaillierte Anforderungen
Der:die Zertifizierungsantragsteller:in legt eine Backup-Richtlinie fest, die auf die Geschäfts- und Sicherheitsanforderungen der Organisation sowie die Kritikalität der personenbezogenen Daten abgestimmt ist. Die Richtlinie legt insbesondere Umfang und Häufigkeit der Backups fest. Der:die Zertifizierungsantragsteller:in testet die Backups und den Wiederherstellungsprozess regelmäßig, um deren Zuverlässigkeit im Notfall sicherzustellen und Datenverluste zu vermeiden.

A.07.13 - Überwachung der Verfügbarkeit

Überblick
Der:die Zertifizierungsantragsteller:in legt unter Berücksichtigung der geschäftlichen Anforderungen die Verfügbarkeitsanforderungen für IT-Systeme und Anwendungen fest, die zur Verarbeitung personenbezogener Daten eingesetzt werden, und stellt diese durch geeignete technische oder organisatorische Maßnahmen sicher.
Detaillierte Anforderungen
Der:die Zertifizierungsantragsteller:in überwacht die Verfügbarkeit der IT-Systeme und Anwendungen, die im Rahmen der zu zertifizierenden Verarbeitungstätigkeiten personenbezogene Daten verarbeiten. Die Überwachung stellt sicher, dass die festgelegten Verfügbarkeitsanforderungen eingehalten und mögliche Störungen frühzeitig erkannt und behoben werden.

A.07.14 - Verschlüsselungsmaßnahmen

Überblick
Der:die Zertifizierungsantragsteller:in legt Maßnahmen zur Verschlüsselung fest, um gespeicherte und übertragene personenbezogene Daten zu schützen.
Detaillierte Anforderungen
Der:die Zertifizierungsantragsteller:in legt auf Grundlage der Risikobewertung gemäß den Kriterien A.06.01 und A.06.02 geeignete Verschlüsselungsverfahren für die Speicherung und Übertragung personenbezogener Daten fest. Bei der Auswahl geeigneter Verschlüsselungsmethoden können folgende Kriterien berücksichtigt werden: ▶ Verschlüsselungsmethoden und eingesetzte Sicherheitsprotokolle entsprechen dem Stand der Technik; ▶ verwendete Schlüssel entsprechen hinsichtlich ihrer Länge und Komplexität aktuellen Empfehlungen und Standards; ▶ ein sicheres Schlüsselmanagement einschließlich sicherer Speicherung, regelmäßiger Aktualisierung und angemessener Zugriffskontrollen ist gewährleistet; und

Detaillierte Anforderungen

- bei der Übertragung werden geeignete Protokolle und Mechanismen eingesetzt, welche die Vertraulichkeit der Daten sicherstellen.

Der:die Zertifizierungsantragsteller:in weist nach, dass die eingesetzten Sicherheitsprotokolle und deren Konfiguration dem Stand der Technik entsprechen (z. B. kann eine veraltete TLS-Version Sicherheitslücken aufweisen). Verschlüsselungsmethoden, die nicht mehr aktuellen technischen Empfehlungen entsprechen, werden durch geeignete Verfahren ersetzt.

A.07.15 - Umgang mit Passwörtern

Überblick

Der:die Zertifizierungsantragsteller:in stellt sicher, dass für Systeme und Benutzerkonten sichere Passwortverfahren eingesetzt werden.

Detaillierte Anforderungen

Der:die Zertifizierungsantragsteller:in regelt auf Grundlage der Risikobewertung gemäß den Kriterien A.06.01 und A.06.02 die Vergabe, Nutzung und Verwaltung von Passwörtern und legt hierzu eine Passwort-Richtlinie fest. Diese berücksichtigt insbesondere:

- Anforderungen an Passwortlänge und -komplexität, Passwortänderungen sowie, soweit zutreffend, den Einsatz von Mehrfaktor-Authentifizierung;
- Anforderungen an Passwortzurücksetzungen; und
- Vorgaben für die sichere Verwaltung und den Schutz von Passwörtern (z. B. durch die Nutzung sicherer Passwortspeicher, Verschlüsselungstechniken oder andere Maßnahmen zur Gewährleistung der Vertraulichkeit von Passwörtern).

Der:die Zertifizierungsantragsteller:in informiert und schult Mitarbeitende zum sicheren Umgang mit Passwörtern und Authentifizierungsverfahren.

A.07.16 – Zuweisung, Entzug oder Anpassung von Benutzerberechtigungen

Überblick

Der:die Zertifizierungsantragsteller:in stellt sicher, dass die Vergabe, Anpassung und der Entzug von Benutzerzugriffsrechten auf einem definierten Prozess basieren.

Detaillierte Anforderungen

Der:die Zertifizierungsantragsteller:in richtet einen Prozess zur Vergabe, Anpassung und zum Entzug von Benutzerberechtigungen für Verarbeitungstätigkeiten und Systeme ein. Dabei gilt insbesondere:

- Zugriffsrechte werden auf Grundlage von Rollenkonzepten vergeben; bei sensiblen personenbezogenen Daten erfolgt die Vergabe auf Grundlage eines Genehmigungsprozesses.
- Zugriffe auf personenbezogene Daten erfolgen ausschließlich über eindeutig zugeordnete Benutzerkonten.
- Gemeinsam genutzte Benutzerkonten sind nur zulässig, wenn sie aus geschäftlichen oder betrieblichen Gründen erforderlich, genehmigt und dokumentiert sind.

Der Umfang der Zugriffskontrollmechanismen richtet sich nach der Risikobewertung gemäß den Kriterien A.06.01 und A.06.02.

A.07.17 - Zuweisung von privilegierten Zugriffsrechten

Überblick
Der:die Zertifizierungsantragsteller:in stellt sicher, dass die Vergabe und Nutzung privilegierter Zugriffsrechte beschränkt und kontrolliert erfolgt.
Detaillierte Anforderungen
Der:die Zertifizierungsantragsteller:in stellt sicher, dass privilegierte Zugriffs- oder Sonderrechte für personenbezogene Daten (z. B. Administratorrechte, System- oder Datenbankadministratorrechte) nur einem begrenzten Personenkreis gewährt werden. Vergabe und Umfang der privilegierten Zugriffsrechte werden auf Grundlage der Risikobewertung gemäß den Kriterien A.06.01 und A.06.02 festgelegt.

A.07.18 - Authentifizierungsmethoden

Überblick
Der:die Zertifizierungsantragsteller:in stellt sicher, dass sichere Authentifizierungstechnologien und -verfahren eingesetzt werden.
Detaillierte Anforderungen
Der:die Zertifizierungsantragsteller:in setzt für die zu zertifizierenden Verarbeitungstätigkeiten geeignete Authentifizierungsverfahren ein, um die Identität der Nutzer:innen zu überprüfen und einen legitimen Zugriff sicherzustellen. Wiederholte Identifikations- und Authentifizierungsversuche werden nach einer festgelegten Anzahl fehlgeschlagener Versuche beschränkt. Bei der Auswahl der Authentifizierungsverfahren berücksichtigt der:die Zertifizierungsantragsteller:in insbesondere: ▶ die gemäß den Kriterien A.06.01 und A.06.02 identifizierten Risiken und Bedrohungen; ▶ die Art und Sensibilität der verarbeiteten Daten (sensible oder vertrauliche Daten erfordern in der Regel strengere und sicherere Authentifizierungsmethoden); und ▶ die Nutzer:innen, deren Rollen und Berechtigungen (z. B. können Administrator:innen oder privilegierte Nutzer:innen strengere Authentifizierungsmethoden benötigen als reguläre Nutzer:innen).

A.07.19 - Automatische Beendigung der Verbindung zu IT-Systemen aufgrund von Inaktivität

Überblick
Der:die Zertifizierungsantragsteller:in legt ein Verfahren für die Abmeldung an Systemen und Anwendungen fest, um das Risiko unbefugter Zugriffe zu minimieren.
Detaillierte Anforderungen
Der:die Zertifizierungsantragsteller:in setzt Maßnahmen um, durch die Verbindungen zu IT-Systemen nach einem festgelegten Zeitraum der Benutzerinaktivität automatisch beendet werden. Dauer und Bedingungen der automatischen Beendigung werden auf Grundlage der Risikobewertung gemäß den Kriterien A.06.01 und A.06.02 unter Berücksichtigung der Sensibilität der Daten und der Risiken unbefugter Zugriffe festgelegt.

A.07.20 - Regelmäßige Überprüfung von Benutzerkonten, Benutzergruppen und Zugriffsberechtigungen

Überblick
Der:die Zertifizierungsantragsteller:in überprüft die Zugriffsrechte auf personenbezogene Daten gemäß den unternehmensinternen Zugriffsregelungen.

Detaillierte Anforderungen
Der:die Zertifizierungsantragsteller:in überprüft regelmäßig die Benutzerkonten und Benutzergruppen mit Zugang zu personenbezogenen Daten sowie die eingeräumten Zugriffsberechtigungen auf ihre Angemessenheit und Erforderlichkeit. Die Zugriffsberechtigungen müssen den aktuellen geschäftlichen Anforderungen sowie den Tätigkeiten entsprechen, für die das jeweilige Benutzerkonto eingerichtet wurde. Umfang und Häufigkeit der Überprüfungen werden auf Grundlage der Risikobewertung gemäß den Kriterien A.06.01 und A.06.02 festgelegt. Der:die Zertifizierungsantragsteller:in dokumentiert die Überprüfungen. Die Dokumentation umfasst mindestens: ▶ die überprüften Benutzerkonten und Benutzergruppen; ▶ Zeitpunkt und Verantwortliche der Überprüfung; ▶ die Kriterien zur Bewertung der Angemessenheit und Erforderlichkeit der Zugriffsberechtigungen; und ▶ Änderungen der Zugriffsberechtigungen, die sich aus der Überprüfung ergeben. ▶ sonstige relevante Hinweise oder Beobachtungen zum Überprüfungsprozess.

A.07.21 - Richtlinien für Mitarbeitende zum Umgang mit tragbaren Speichermedien

Überblick
Der:die Zertifizierungsantragsteller:in legt eine Richtlinie zum sicheren Umgang mit tragbaren Speichermedien fest.
Detaillierte Anforderungen
Der:die Zertifizierungsantragsteller:in legt für Mitarbeitende eine Richtlinie zum sicheren Umgang mit tragbaren Speichermedien fest (z. B. externe Festplatten, Speicherkarten, USB-Sticks), die auf dem unternehmensweiten Risikomanagementverfahren basiert und mit diesem im Einklang steht. Die Richtlinie wird allen Mitarbeitenden in geeigneter Weise (über das Intranet, per E-Mail oder ein anderes Kommunikationsmittel) bekannt gemacht.

A.07.22 - Funktionstrennung

Überblick
Der:die Zertifizierungsantragsteller:in trennt Aufgaben und Verantwortungsbereiche, um zu verhindern, dass eine einzelne Person potenziell konfligierende Aufgaben allein ausführt.
Detaillierte Anforderungen
Der:die Zertifizierungsantragsteller:in setzt geeignete Mechanismen zur Funktionstrennung innerhalb der Verarbeitungstätigkeiten und Systeme um. Dies umfasst die funktionale Trennung von Aufgaben und Verantwortlichkeiten sowie die Trennung von Entwicklungs-, Test- und Produktionsumgebungen. Umfang und Ausgestaltung der Maßnahmen werden auf Grundlage der Risikobewertung gemäß den Kriterien A.06.01 und A.06.02 unter Berücksichtigung der potenziellen Auswirkungen auf personenbezogene Daten und der identifizierten Risiken festgelegt.

A.07.23 - Verpflichtung zur Wahrung der Vertraulichkeit

Überblick
Der:die Zertifizierungsantragsteller:in stellt sicher, dass Mitarbeitende vor Beginn der Verarbeitung personenbezogener Daten zur Vertraulichkeit verpflichtet werden, sofern sie nicht bereits einer gesetzlichen Verschwiegenheitspflicht unterliegen.
Detaillierte Anforderungen
Der:die Zertifizierungsantragsteller:in stellt sicher, dass alle Mitarbeitenden, die im Rahmen der zu zertifizierenden Verarbeitungstätigkeiten personenbezogene Daten verarbeiten, durch geeignete Geheimhaltungs- oder Vertraulichkeitsvereinbarungen bzw. betriebliche oder dienstliche Regelungen zur Wahrung der Vertraulichkeit verpflichtet sind. Dies gilt unabhängig davon, ob personenbezogene Daten in automatisierten oder nicht automatisierten Prozessen verarbeitet werden.

A.07.24 - Prüfung der Wirksamkeit technischer und organisatorischer Maßnahmen

Überblick
Der:die Zertifizierungsantragsteller:in führt regelmäßige Prüfungen durch, um die Wirksamkeit der implementierten technischen und organisatorischen Maßnahmen zu überprüfen.
Detaillierte Anforderungen
Der:die Zertifizierungsantragsteller:in überprüft die Wirksamkeit der implementierten technischen und organisatorischen Maßnahmen regelmäßig (z. B. alle 12 bis 24 Monate). Die Prüfintervalle werden unter Berücksichtigung der Auswirkungen der jeweiligen Maßnahmen auf den Datenschutz und die organisatorische Sicherheit festgelegt. Hierzu richtet der:die Zertifizierungsantragsteller:in einen Prozess ein, der mindestens: ▶ festlegt, welche Maßnahmen jährlich und welche aufgrund geringerer Risiken in längeren Intervallen überprüft werden; ▶ die Verantwortlichkeiten für die jeweiligen Prüfbereiche festlegt; ▶ die Prüfanforderungen einschließlich Methodik, Dokumentation und Umgang mit Nachweisen definiert; ▶ die Kommunikation der Prüfungsergebnisse regelt; und ▶ den Umgang mit Feststellungen sowie die Umsetzung von Verbesserungsmaßnahmen festlegt. Der:die Zertifizierungsantragsteller:in dokumentiert die durchgeführten Prüfungen einschließlich der Feststellungen, identifizierten Verbesserungspotenziale und festgelegten Verbesserungsmaßnahmen.

A.07.25 – Festlegung von Aufbewahrungsfristen / Löschung von Daten

Überblick
Der:die Zertifizierungsantragsteller:in stellt sicher, dass für die zu zertifizierenden Verarbeitungstätigkeiten Löschmechanismen und -prozesse entsprechend den festgelegten Aufbewahrungsfristen implementiert sind. Diese ermöglichen die vollständige Löschung personenbezogener Daten und stellen sicher, dass die festgelegten Aufbewahrungsfristen nicht überschritten werden.
Detaillierte Anforderungen
Der:die Zertifizierungsantragsteller:in legt Richtlinien, Verfahren und/oder Mechanismen für die Löschung personenbezogener Daten fest und dokumentiert diese. Diese umfassen mindestens: ▶ die Aufbewahrungsfristen und die jeweiligen Auslöser für deren Beginn (z. B. Beendigung eines Vertragsverhältnisses, Ende des Geschäftsjahres); ▶ die anzuwendenden Löschmethoden (z. B. automatisierte (z. B. Batch-Verarbeitung) oder nicht-automatisierte Löschmechanismen/-prozesse); ▶ die vollständige Löschung personenbezogener Daten in vor- und nachgelagerten Systemen sowie in Datenextrakten, einschließlich der Festlegung von Löschintervallen und der Protokollierung durchgeführter Löschungen;

Detaillierte Anforderungen

- soweit zutreffend, die Begründung von Löschfristen, die für bestimmte Datenarten von gesetzlichen Aufbewahrungsfristen abweichen;
- die Verantwortlichkeiten für die Implementierung, Durchführung und Überwachung der Löschung; und
- regelmäßige Tests sowie Verfahren für den Umgang mit festgestellten Unregelmäßigkeiten.

Der:die Verantwortliche testet mindestens einmal jährlich die Funktionsfähigkeit der Verfahren zur Anonymisierung oder Löschung personenbezogener Daten einschließlich Backups und Protokollen. Zeitpunkt und Umfang der Tests sowie festgestellte Abweichungen und deren Behebung werden dokumentiert.

A.07.26 - Entsorgungskonzept für das Löschen oder Vernichten von Datenträgern

Überblick

Der:die Zertifizierungsantragsteller:in legt eine dokumentierte Entsorgungsrichtlinie fest, um sicherzustellen, dass nicht mehr benötigte personenbezogene Daten nach dem Stand der Technik sicher gelöscht oder die betreffenden Datenträger physisch vernichtet werden.

Detaillierte Anforderungen

Der:die Zertifizierungsantragsteller:in legt in einer schriftlichen Entsorgungsrichtlinie fest, welche Datenträger unter welchen Bedingungen sicher zu löschen oder zu vernichten sind. Dabei werden insbesondere folgende Anforderungen berücksichtigt:

- Für die Entsorgung sensibler Datenträger stehen geeignete sichere Entsorgungsmöglichkeiten zur Verfügung.
- Vor der Weitergabe oder Wiederverwendung von Datenträgern werden darauf gespeicherte personenbezogene Daten sicher gelöscht.
- Für die Löschung oder Vernichtung werden geeignete Werkzeuge und Verfahren eingesetzt, die dem jeweiligen Datenträger, der Art der Datenspeicherung und dem Schutzbedarf der Informationen entsprechen und eine sichere Löschung oder Vernichtung gewährleisten (Hinweis: Die Auswahl geeigneter Werkzeuge und Verfahren hängt von der Art der Datenspeicherung, den Datenträgern und dem Schutzbedarf der Informationen ab), z. B.:
  - sichere physische Vernichtung von Datenträgern,
  - Zerstörung von Backup-Bändern durch Schreddern,
  - physische Zerstörung von Festplatten (z. B. durch Demontage und Zerstörung einzelner Magnetscheiben),
  - Schreddern von Papierdokumenten mindestens auf Sicherheitsstufe P-3 gemäß ISO/IEC 21964-2,
  - Zurücksetzen von Smartphones auf Werkseinstellungen inkl. vollständigem Löschabschluss durch vollständigen Setup-Durchlauf,
  - Zurücksetzen von IoT-Geräten auf Werkseinstellungen und Änderung sämtlicher gespeicherter Zugangsdaten.

Der:die Zertifizierungsantragsteller:in informiert die Mitarbeitenden über die Entsorgungsrichtlinie und die Vorgaben zur sicheren Entsorgung von Dokumenten und Datenträgern.

Die Entsorgungsrichtlinie wird mindestens einmal jährlich sowie bei wesentlichen Änderungen überprüft.

Erfolgt die Vernichtung durch ein externes Entsorgungsunternehmen, bewahrt der:die Zertifizierungsantragsteller:in für jede Vernichtung eine Vernichtungsbestätigung auf und schließt mit dem Entsorgungsunternehmen einen Auftragsverarbeitungsvertrag gemäß Art. 28 Abs. 3 DSGVO ab (siehe Kriterium A.04.04).

4.14. VERLETZUNG DES SCHUTZES PERSONENBEZOGENER DATEN

A.08.01 - Incident-Response-Plan

Überblick
Der:die Zertifizierungsantragsteller:in legt einen formellen und strukturierten Ansatz für den Umgang mit Datenschutzverletzungen fest.
Detaillierte Anforderungen
Der:die Zertifizierungsantragsteller:in legt einen „Incident-Response-Plan“ für den Umgang mit potenziellen und eingetretenen Datenschutzverletzungen fest und setzt diesen um. Der Plan umfasst insbesondere: ▶ Aufgaben und Verantwortlichkeiten; ▶ die Schritte zur Behandlung von Datenschutzverletzungen; ▶ Vorgaben zur Meldung an die Aufsichtsbehörde und zur Benachrichtigung betroffener Personen; ▶ Eskalationsmaßnahmen außerhalb der Geschäftszeiten; ▶ Vorgaben zur Dokumentation für die weitere Analyse und Bewertung; und ▶ Verfahren für unterschiedliche Notfallszenarien.

A.08.02 - Bewertung einer Datenschutzverletzung

Überblick
Der:die Zertifizierungsantragsteller:in legt Kriterien für die Klassifizierung von Datenschutzverletzungen und die Bewertung der daraus resultierenden Risiken für die Rechte und Freiheiten betroffener Personen fest.
Detaillierte Anforderungen
Der:die Zertifizierungsantragsteller:in dokumentiert Kriterien für die Bewertung von Datenschutzverletzungen (z. B. Bewertung der Eintrittswahrscheinlichkeit und der möglichen Auswirkungen auf die Rechte und Freiheiten betroffener Personen anhand einer definierten Risikoskala, z. B. von 1 (niedriges Risiko) bis 5 (hohes Risiko)). Diese berücksichtigen insbesondere die Eintrittswahrscheinlichkeit und die möglichen Auswirkungen auf die Rechte und Freiheiten betroffener Personen. Auf Grundlage dieser Kriterien bewertet der:die Zertifizierungsantragsteller:in Datenschutzverletzungen objektiv und dokumentiert die Ergebnisse der Bewertung.

A.08.03 - Meldung einer Datenschutzverletzung an die Aufsichtsbehörde

Überblick
Besteht im Falle einer Datenschutzverletzung ein vorhersehbares Risiko für die Rechte und Freiheiten natürlicher Personen, meldet der:die Zertifizierungsantragsteller:in die Datenschutzverletzung der zuständigen Aufsichtsbehörde innerhalb von 72 Stunden nach Bekanntwerden. Die Meldung erfüllt die Anforderungen des Art. 33 Abs. 3 DSGVO.
Detaillierte Anforderungen
Ergibt die Risikobewertung gemäß Kriterium A.08.02 voraussichtlich ein Risiko für die Rechte und Freiheiten natürlicher Personen, weist der:die Zertifizierungsantragsteller:in die fristgerechte Meldung an die Aufsichtsbehörde nach und bewahrt die entsprechende Dokumentation auf. Die Meldung hat gemäß Art. 33 Abs. 3 DSGVO mindestens folgende Angaben zu enthalten: a) Beschreibung der Art der Datenschutzverletzung einschließlich – soweit möglich – der Kategorien und der ungefähren Zahl der betroffenen Personen sowie der Kategorien und der ungefähren Zahl der betroffenen personenbezogenen Datensätze; b) Name und Kontaktdaten des:der Datenschutzbeauftragten oder sonstiger Ansprechpartner:innen für weitere Informationen; c) Beschreibung der wahrscheinlichen Folgen der Datenschutzverletzung;

Detaillierte Anforderungen

d) Beschreibung der ergriffenen oder vorgeschlagenen Maßnahmen zur Behebung der Datenschutzverletzung sowie gegebenenfalls zur Abmilderung ihrer möglichen nachteiligen Auswirkungen.

Der:die Zertifizierungsantragsteller:in hält hierfür Vorlagen vor, die eine einheitliche Dokumentation und Meldung an die Aufsichtsbehörde unterstützen.

Können die erforderlichen Informationen nicht gleichzeitig bereitgestellt werden, dokumentiert der:die Zertifizierungsantragsteller:in die Gründe hierfür und weist die schrittweise Nachreichung der fehlenden Informationen gemäß Art. 33 Abs. 4 DSGVO nach.

A.08.04 - Mitteilung einer Datenschutzverletzung an die betroffene Person

Überblick

Besteht bei einer Datenschutzverletzung voraussichtlich ein hohes Risiko für die Rechte und Freiheiten betroffener Personen, informiert der:die Zertifizierungsantragsteller:in die betroffenen Personen unverzüglich über die Datenschutzverletzung. Die Mitteilung erfüllt die Anforderungen des Art. 34 DSGVO.

Detaillierte Anforderungen

Ergibt die Risikobewertung gemäß Kriterium A.08.02 ein voraussichtlich hohes Risiko für die Rechte und Freiheiten natürlicher Personen, benachrichtigt der:die Zertifizierungsantragsteller:in die betroffenen Personen unverzüglich über die Datenschutzverletzung.

Die Mitteilung wird schriftlich dokumentiert, erfolgt in klarer und verständlicher Sprache und enthält mindestens:

- Name und Kontaktdaten des:der Datenschutzbeauftragten oder einer sonstigen Anlaufstelle;
- eine Beschreibung der wahrscheinlichen Folgen der Datenschutzverletzung;
- eine Beschreibung der ergriffenen oder vorgeschlagenen Maßnahmen zur Behebung der Datenschutzverletzung; und
- gegebenenfalls Maßnahmen zur Abmilderung möglicher nachteiliger Auswirkungen.

Der:die Zertifizierungsantragsteller:in weist den Zeitpunkt der Mitteilung nach (z. B. Zeitstempel bei Versand einer E-Mail; Zeitpunkt der Veröffentlichung einer Pressemitteilung oder auf der Website).

Unterbleibt die Mitteilung aufgrund einer Ausnahme gemäß Art. 34 Abs. 3 DSGVO, dokumentiert der:die Zertifizierungsantragsteller:in nachvollziehbar das Vorliegen der jeweiligen Voraussetzungen und die Gründe für die unterbliebene Mitteilung.

A.08.05 - Umgesetzte Maßnahmen

Überblick

Der:die Zertifizierungsantragsteller:in dokumentiert die für jede Datenschutzverletzung ergriffenen und geplanten Maßnahmen (Maßnahmenübersicht).

Detaillierte Anforderungen

Der:die Zertifizierungsantragsteller:in dokumentiert die ergriffenen oder geplanten Maßnahmen zur Behebung der Datenschutzverletzung sowie gegebenenfalls Maßnahmen zur Abmilderung möglicher nachteiliger Auswirkungen.

Für vorgeschlagene oder festgelegte Folgemaßnahmen richtet der:die Zertifizierungsantragsteller:in ein Verfahren zur Nachverfolgung ihrer Umsetzung ein. Das Verfahren legt insbesondere fest:

- die Verantwortlichkeiten für die erforderlichen Folgeaktivitäten;
- die Verantwortlichkeiten für die Nachverfolgung des Umsetzungsstatus; und
- die zu dokumentierenden Informationen (z. B. Umsetzungsfristen, Priorität, Beschreibung der einzelnen Aktivitäten, formaler Abschluss einer Maßnahme, wie z. B. E-Mail mit „Maßnahme X abgeschlossen“ oder Abschluss des entsprechenden Workflow-Schritts).

A.08.06 - Dokumentation von Datenschutzverletzungen

Überblick
Der:die Zertifizierungsantragsteller:in stellt zur Erfüllung der Rechenschaftspflicht eine ordnungsgemäße und umfassende interne Dokumentation sämtlicher eingetretener Datenschutzverletzungen sicher.
Detaillierte Anforderungen
Der:die Zertifizierungsantragsteller:in dokumentiert Datenschutzverletzungen so, dass deren Feststellung, Bewertung, Behandlung und gegebenenfalls Meldung bzw. Benachrichtigung nachvollziehbar sind. Die Dokumentation umfasst für jede Datenschutzverletzung mindestens: ▶ den Zeitpunkt der Feststellung; ▶ betroffene Auftragsverarbeiter:innen, IT-Systeme und Datenkategorien; ▶ das Ergebnis der Risikoanalyse; ▶ ergriffene oder geplante Maßnahmen zur Behebung der Datenschutzverletzung sowie gegebenenfalls zur Abmilderung möglicher nachteiliger Auswirkungen; und ▶ die Angabe, ob die Datenschutzverletzung der Aufsichtsbehörde gemeldet wurde. Ergibt sich aus der Datenschutzverletzung ein Risiko für die Rechte und Freiheiten betroffener Personen, werden zusätzlich dokumentiert: ▶ Art der Datenschutzverletzung sowie Kategorien und Umfang der betroffenen personenbezogenen Datensätze und Kategorien und Anzahl der betroffenen Personen; ▶ die wahrscheinlichen Folgen bzw. Auswirkungen der Datenschutzverletzung; ▶ Maßnahmen zur Behebung der Datenschutzverletzung und zur Verhinderung einer Wiederholung; ▶ Zeitpunkt und Inhalt der Kommunikation mit der Aufsichtsbehörde; und ▶ Zeitpunkt und Inhalt der Benachrichtigung der betroffenen Personen.

A.08.07 - Vertraglich festgelegte Meldepflicht bei einer Datenschutzverletzung durch Auftragsverarbeiter:innen

Überblick
Der:die Zertifizierungsantragsteller:in legt Vorgaben fest, um Datenschutzverletzungen bei Auftragsverarbeiter:innen zu identifizieren, zu bewerten und nachvollziehbar zu dokumentieren sowie erforderlichenfalls die Aufsichtsbehörde oder betroffene Personen zu informieren.
Detaillierte Anforderungen
Der:die Zertifizierungsantragsteller:in stellt durch vertragliche Regelungen mit sämtlichen Auftragsverarbeiter:innen sicher, dass Datenschutzverletzungen bei Auftragsverarbeiter:innen unverzüglich gemeldet und die für deren Bewertung und weitere Behandlung erforderlichen Informationen übermittelt werden. Die vertraglichen Regelungen können zusätzlich Vorgaben zu Methoden zur Erkennung von Datenschutzverletzungen bei Auftragsverarbeiter:innen enthalten.

4.15. DATENSCHUTZ-FOLGENABSCHÄTZUNG

A.09.01 - Bewertung und Dokumentation einer Datenschutz-Folgenabschätzung (DSFA)

Überblick

Der:die Zertifizierungsantragsteller:in prüft, ob für die zu zertifizierenden Verarbeitungsvorgänge eine Datenschutz-Folgenabschätzung erforderlich ist. Eine Datenschutz-Folgenabschätzung wird durchgeführt, wenn die Verarbeitung aufgrund ihrer Art, ihres Umfangs, ihres Kontexts und ihrer Zwecke voraussichtlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen zur Folge hat oder einer der in Art. 35 Abs. 3 lit. a–c DSGVO genannten Fälle vorliegt:

- systematische und umfangreiche Bewertung persönlicher Aspekte natürlicher Personen auf Grundlage automatisierter Verarbeitung einschließlich Profiling, die zu Entscheidungen mit rechtlicher oder ähnlich erheblicher Wirkung führt;
- umfangreiche Verarbeitung besonderer Kategorien personenbezogener Daten gemäß Art. 9 Abs. 1 DSGVO oder personenbezogener Daten über strafrechtliche Verurteilungen und Straftaten gemäß Art. 10 DSGVO; oder
- systematische umfangreiche Überwachung öffentlich zugänglicher Bereiche.

Bei der Risikobewertung berücksichtigt der:die Zertifizierungsantragsteller:in die Eintrittswahrscheinlichkeit und Schwere möglicher Auswirkungen auf die Rechte und Freiheiten betroffener Personen (Erwägungsgrund 90 DSGVO).

Detaillierte Anforderungen

Der:die Zertifizierungsantragsteller:in führt eine Bewertung der Erforderlichkeit zur Durchführung einer Datenschutz-Folgenabschätzung (DSFA) für die zu zertifizierenden Verarbeitungstätigkeiten durch und dokumentiert die Ergebnisse dieser Bewertung sowie die dabei berücksichtigten Aspekte (z. B. Einsatz neuer Technologien (gemäß dem aktuellen Stand der Technik); Verarbeitung besonderer Kategorien personenbezogener Daten; die „Verordnung über Verarbeitungsvorgänge, für die eine Datenschutz-Folgenabschätzung durchzuführen ist (DSFA-V)“ – sogenannte „Blacklist“ – sowie die „Datenschutz-Folgenabschätzung-Ausnahmenverordnung (DSFA-AV)“ – sogenannte „Whitelist“ – der österreichischen Datenschutzbehörde (vgl. Art. 35 Abs. 4 und 5 DSGVO)).

Ergibt die Bewertung die Notwendigkeit einer Datenschutz-Folgenabschätzung, legt der:die Zertifizierungsantragsteller:in eine Methode für deren Durchführung fest. Diese umfasst mindestens:

- Kriterien zur Bewertung der Eintrittswahrscheinlichkeit von Bedrohungen (z. B. niedrig, mittel, hoch);
- Kriterien zur Bewertung des Schadensausmaßes und des daraus resultierenden Risikos (z. B. niedrig, mittel, hoch); und
- Vorgaben zum Umgang mit identifizierten Risiken.

Die Datenschutz-Folgenabschätzung dokumentiert mindestens:

- eine systematische Beschreibung der geplanten Verarbeitungsvorgänge und ihrer Zwecke einschließlich gegebenenfalls verfolgter berechtigter Interessen;
- die Bewertung der Notwendigkeit und Verhältnismäßigkeit der Verarbeitung;
- die Bewertung der Risiken für die Rechte und Freiheiten betroffener Personen;
- die geplanten Maßnahmen zur Risikobehandlung, einschließlich Schutzmaßnahmen, Sicherheitsmaßnahmen und Mechanismen zur Sicherstellung des Schutzes personenbezogener Daten und des Nachweises der DSGVO-Konformität unter Berücksichtigung der Rechte und berechtigten Interessen betroffener Personen;
- die Einbindung des:der Datenschutzbeauftragten, sofern benannt;
- gegebenenfalls eingeholte Stellungnahmen betroffener Personen oder ihrer Vertreter:innen;
- gegebenenfalls berücksichtigte Verhaltensregeln gemäß Art. 40 DSGVO; und
- gegebenenfalls eine vorherige Konsultation der Aufsichtsbehörde und deren Rückmeldungen.

Soweit im Rahmen der Datenschutz-Folgenabschätzung risikomindernde Maßnahmen festgelegt werden, stellt der:die Zertifizierungsantragsteller:in deren Umsetzung vor Beginn der Verarbeitung sicher. Es werden hierfür Verantwortlichkeiten und Verfahren zur Nachverfolgung und Dokumentation des Umsetzungsstatus festgelegt (z. B. Umsetzungsfristen, Priorität, Beschreibung der einzelnen Aktivitäten, Abschluss einer Maßnahme durch einen formellen Vorgang, wie etwa eine E-Mail mit „Maßnahme X abgeschlossen“ oder das Abschließen eines entsprechenden Workflow-Schritts).

Der:die Zertifizierungsantragsteller:in überprüft die Datenschutz-Folgenabschätzung mindestens einmal jährlich sowie bei wesentlichen Änderungen mit Auswirkungen auf die Datenschutz-Folgenabschätzung und passt erforderlichenfalls die Risikomaßnahmen an. Die Überprüfung und deren Ergebnisse werden dokumentiert.

A.09.02 - Vorherige Konsultation der Aufsichtsbehörde

Überblick
Stellt der:die Zertifizierungsantragsteller:in im Rahmen einer Datenschutz-Folgenabschätzung fest, dass die Verarbeitung ein hohes Risiko für die Rechte und Freiheiten betroffener Personen zur Folge hat und dieses Risiko unter Berücksichtigung der verfügbaren Technologien und der Implementierungskosten nicht gemindert werden kann, wird eine vorherige Konsultation gemäß Art. 36 DSGVO eingeleitet.
Detaillierte Anforderungen
***Anwendbarkeit**: Dieses Kriterium gilt, wenn die Datenschutz-Folgenabschätzung gemäß Kriterium A.09.01 ergibt, dass die Verarbeitung ein hohes Risiko für die Rechte und Freiheiten betroffener Personen zur Folge hat und dieses Risiko nicht durch geeignete Maßnahmen gemindert werden kann.* Ist eine Konsultation erforderlich, stellt der:die Zertifizierungsantragsteller:in der Aufsichtsbehörde gemäß Art. 36 Abs. 3 DSGVO folgende Informationen bereit: ▶ soweit zutreffend, Angaben zu den jeweiligen Verantwortlichkeiten, der gemeinsam Verantwortlichen und der Auftragsverarbeiter:innen, insbesondere bei einer Verarbeitung innerhalb einer Unternehmensgruppe; ▶ die Zwecke und Mittel der beabsichtigten Verarbeitung; ▶ die vorgesehenen Maßnahmen und Garantien zum Schutz der Rechte und Freiheiten betroffener Personen; ▶ die Kontaktdaten des:der Datenschutzbeauftragten, sofern benannt; ▶ die Datenschutz-Folgenabschätzung gemäß Art. 35 DSGVO; und ▶ sonstige von der Aufsichtsbehörde angeforderte Informationen.

4.16. DATENSCHUTZBEAUFTRAGTE:R

A.10.01 - Bestellung eines:einer Datenschutzbeauftragten

Überblick
Der:die Zertifizierungsantragsteller:in prüft, ob die Voraussetzungen für die Bestellung eines:einer Datenschutzbeauftragten gemäß Art. 37 Abs. 1 DSGVO erfüllt sind.
Detaillierte Anforderungen
***Anwendbarkeit**: Dieses Kriterium gilt, wenn die Voraussetzungen für die Bestellung eines:einer Datenschutzbeauftragten erfüllt sind oder eine freiwillige Bestellung erfolgt.* Eine Bestellung ist gemäß Art. 37 Abs. 1 DSGVO erforderlich, wenn: ▶ die Verarbeitung von einer Behörde oder öffentlichen Stelle durchgeführt wird, mit Ausnahme von Gerichten, die im Rahmen ihrer justiziellen Tätigkeit handeln; ▶ die Kerntätigkeiten in Verarbeitungsvorgängen bestehen, die aufgrund ihrer Art, ihres Umfangs und/oder ihrer Zwecke eine umfangreiche regelmäßige und systematische Überwachung betroffener Personen erfordern; oder ▶ die Kerntätigkeiten in der umfangreichen Verarbeitung besonderer Kategorien personenbezogener Daten gemäß Art. 9 DSGVO sowie personenbezogener Daten über strafrechtliche Verurteilungen und Straftaten gemäß Art. 10 DSGVO bestehen. Die Begründung für die Bestellung oder Nichtbestellung wird dokumentiert. Ist eine Bestellung erforderlich oder erfolgt diese freiwillig, stellt der:die Zertifizierungsantragsteller:in sicher, dass: ▶ die Bestellung formell und schriftlich erfolgt; ▶ die Dokumentation über die Bestellung oder Benennung aufbewahrt wird; ▶ die Kontaktdaten des:der Datenschutzbeauftragten innerhalb der Organisation zugänglich sind (z. B. Intranet, Onboarding-Unterlagen oder interne Verzeichnisse); und ▶ die Kontaktdaten des:der Datenschutzbeauftragten gemäß Art. 37 Abs. 7 DSGVO veröffentlicht (z. B. auf der Unternehmenswebsite oder in Datenschutzhinweisen) und der zuständigen Aufsichtsbehörde mitgeteilt werden.

A.10.02 - Aufgaben- bzw. Tätigkeitsbeschreibung

Überblick

Der:die Zertifizierungsantragsteller:in dokumentiert die Aufgaben des:der Datenschutzbeauftragten in einer Aufgaben- bzw. Tätigkeitsbeschreibung oder – im Fall eines:einer externen Datenschutzbeauftragten – in der Beauftragung.

Detaillierte Anforderungen

***Anwendbarkeit**: Dieses Kriterium gilt, wenn die Voraussetzungen für die Bestellung eines:einer Datenschutzbeauftragten erfüllt sind oder eine freiwillige Bestellung erfolgt.*

Die Aufgaben- bzw. Tätigkeitsbeschreibung oder die Beauftragung bei externer Bestellung berücksichtigt die Anforderungen des Art. 39 Abs. 1 und 2 DSGVO. Sie umfasst insbesondere:

- die Unterrichtung und Beratung des:der Verantwortlichen sowie der mit der Verarbeitung betrauten Mitarbeitenden über ihre datenschutzrechtlichen Pflichten;
- die Überwachung der Einhaltung der DSGVO, anderer anwendbarer Datenschutzvorschriften und der Datenschutzrichtlinien des:der Verantwortlichen einschließlich der Zuweisung von Verantwortlichkeiten, Sensibilisierung und Schulung der Mitarbeitenden sowie diesbezüglicher Prüfungen;
- die Beratung hinsichtlich der Datenschutz-Folgenabschätzung auf Anfrage und die Überwachung ihrer Durchführung gemäß Art. 35 DSGVO;
- die Zusammenarbeit mit der Aufsichtsbehörde; und
- die Tätigkeit als Anlaufstelle für die Aufsichtsbehörde in Fragen im Zusammenhang mit der Verarbeitung einschließlich der vorherigen Konsultation gemäß Art. 36 DSGVO sowie Beratung in sonstigen Angelegenheiten nach Bedarf.

Werden dem:der Datenschutzbeauftragten zusätzliche Aufgaben im Zusammenhang mit der Datenschutzorganisation übertragen (z. B. die Führung des Verzeichnisses von Verarbeitungstätigkeiten oder die Koordinierung von Betroffenenanfragen), dokumentiert der:die Zertifizierungsantragsteller:in auch diese in der Aufgaben- bzw. Tätigkeitsbeschreibung bzw. Beauftragung.

A.10.03 - Aufgaben und Befugnisse

Überblick

Der:die Zertifizierungsantragsteller:in ergreift Maßnahmen, um sicherzustellen, dass der:die Datenschutzbeauftragte die Position und Aufgaben innerhalb der Organisation ordnungsgemäß wahrnehmen kann.

Detaillierte Anforderungen

***Anwendbarkeit**: Dieses Kriterium gilt, wenn die Voraussetzungen für die Bestellung eines:einer Datenschutzbeauftragten erfüllt sind oder eine freiwillige Bestellung erfolgt.*

Der:die Zertifizierungsantragsteller:in stellt die ordnungsgemäße und unabhängige Wahrnehmung der Aufgaben des:der Datenschutzbeauftragten durch geeignete organisatorische Maßnahmen sicher und weist insbesondere nach, dass:

- schriftliche Qualifikationsanforderungen festgelegt sowie deren Erfüllung überprüft und dokumentiert werden;
- spätestens mit der Benennung eine Vertraulichkeitsverpflichtung abgeschlossen wird, soweit eine solche nicht bereits gesetzlich oder aufgrund anderer Regelungen besteht.
- eine unabhängige und weisungsfreie Aufgabenwahrnehmung gewährleistet ist und keine Tätigkeiten ausgeübt werden, die zu Interessenkonflikten führen; Maßnahmen zur Vermeidung von Interessenkonflikten werden dokumentiert (z. B. schriftliche Erklärung zur Interessenkonfliktfreiheit oder Stellenbeschreibung ohne operative Verantwortlichkeiten);
- angemessene zeitliche, organisatorische und finanzielle Ressourcen für die Wahrnehmung der Aufgaben bereitgestellt werden;
- die Aufrechterhaltung und Weiterentwicklung der fachlichen Expertise unterstützt wird;
- eine ordnungsgemäße und frühzeitige Einbindung in Angelegenheiten und Entscheidungen mit Datenschutzbezug erfolgt und diese dokumentiert wird;
- die erfolgte Unterrichtung und Beratung der Organisation nachvollziehbar dokumentiert wird (z. B. anhand von Berichten, Schulungsunterlagen oder vergleichbaren Nachweisen); und
- regelmäßig über den Status des Datenschutzmanagements an die oberste Leitungsebene berichtet und diese Berichterstattung dokumentiert wird.

4.17. ÜBERMITTLUNG PERSONENBEZOGENER DATEN IN DRITTLÄNDER ODER AN INTERNATIONALE ORGANISATIONEN

***Hinweis**: Die Kriterien in Abschnitt A.11 stellen keinen Zertifizierungsmechanismus gemäß Art. 42 Abs. 2 i. V. m. Art. 46 Abs. 2 lit. f DSGVO dar. Die Zertifizierung bestätigt ausschließlich, dass ein Transferinstrument für die zu zertifizierenden Verarbeitungsvorgänge ausgewählt wurde und dass die damit verbundenen Dokumentationsanforderungen erfüllt wurden.*

A.11.01 - Allgemeine Grundsätze der Datenübermittlung gemäß Art. 44 ff. DSGVO

Überblick
Beinhalten die zu zertifizierenden Verarbeitungstätigkeiten eine Übermittlung personenbezogener Daten in Drittländer oder an internationale Organisationen, stellt der:die Zertifizierungsantragsteller:in sicher, dass das eingesetzte Übermittlungsinstrument die Anforderungen des Kapitels V DSGVO (Art. 44–49 DSGVO) erfüllt und das durch die DSGVO gewährleistete Schutzniveau gewahrt wird.
Detaillierte Anforderungen
***Anwendbarkeit**: Dieses Kriterium gilt ausschließlich, wenn personenbezogene Daten im Rahmen der zu zertifizierenden Verarbeitungstätigkeiten in Drittländer oder an internationale Organisationen übermittelt werden.* Der:die Zertifizierungsantragsteller:in erstellt eine Standardarbeitsanweisung (SOP), die das Verfahren zur Analyse sämtlicher möglicher Übermittlungsmechanismen, deren Eignung für die jeweilige Verarbeitungstätigkeit gemäß Kapitel V DSGVO sowie die Bewertung der Übermittlungsinstrumente im Hinblick auf die Anforderungen der DSGVO beschreibt. Die SOP umfasst mindestens: ▶ Methoden zur Überprüfung des Bestehens und der Anwendbarkeit von Angemessenheitsbeschlüssen, verbindlichen internen Datenschutzvorschriften (BCR), Standard-Datenschutzklauseln, genehmigten Verhaltensregeln und Zertifizierungsmechanismen; und ▶ Verfahren zur fortlaufenden Überwachung und Überprüfung der Wirksamkeit und Konformität des jeweiligen Übermittlungsinstruments. Je nach eingesetztem Übermittlungsinstrument dokumentiert der:die Zertifizierungsantragsteller:in gemäß Art. 45 ff. DSGVO mindestens: • **Angemessenheitsbeschluss:** die Anwendbarkeit des Angemessenheitsbeschlusses auf das betreffende Drittland, relevante Gebiete innerhalb des Drittlands oder die internationale Organisation; • **verbindliche interne Datenschutzvorschriften (BCR) gemäß Art. 47 DSGVO:** die Anwendbarkeit der verbindlichen internen Datenschutzvorschriften auf die zu zertifizierenden Verarbeitungsvorgänge und ein Transfer Impact Assessment gemäß Kriterium A.11.07; • **Standard-Datenschutzklauseln:** die Anwendbarkeit der Standard-Datenschutzklauseln auf die vorgesehene Drittlandsübermittlung und ein Transfer Impact Assessment gemäß Kriterium A.11.07; • **genehmigte Verhaltensregeln gemäß Art. 40 DSGVO:** die Anwendbarkeit des Verhaltenskodex auf die zu zertifizierenden Verarbeitungstätigkeiten und die betreffenden Drittlandsübermittlungen und ein Transfer Impact Assessment gemäß Kriterium A.11.07; • **genehmigter Zertifizierungsmechanismus:** das Bestehen einer gültigen Zertifizierung des:der Zertifizierungsantragstellers:in gemäß Art. 42 Abs. 2 i. V. m. Art. 46 Abs. 2 lit. f DSGVO und ein Transfer Impact Assessment gemäß Kriterium A.11.07; • **vertragliche Klauseln gemäß Art. 46 Abs. 3 lit. a DSGVO:** die Anwendbarkeit der vertraglichen Regelungen auf die zu zertifizierenden Verarbeitungstätigkeiten und die betreffenden Drittlandsübermittlungen und ein Transfer Impact Assessment gemäß Kriterium A.11.07; und • **Verwaltungsvereinbarungen zwischen Behörden oder öffentlichen Stellen gemäß Art. 46 Abs. 3 lit. b DSGVO:** die Anwendbarkeit der Vereinbarungen auf die zu zertifizierenden Verarbeitungstätigkeiten und die betreffenden Drittlandsübermittlungen und ein Transfer Impact Assessment gemäß Kriterium A.11.07.

A.11.02 - Ausnahmen für bestimmte Fälle

Überblick

Der:die Zertifizierungsantragsteller:in stellt sicher, dass in Abwesenheit eines Angemessenheitsbeschlusses gemäß Art. 45 Abs. 3 DSGVO oder geeigneter Garantien gemäß Art. 46 DSGVO eine Übermittlung personenbezogener Daten in ein Drittland oder an eine internationale Organisation nur erfolgt, wenn die Voraussetzungen einer Ausnahme gemäß Art. 49 DSGVO erfüllt sind.

Detaillierte Anforderungen

***Anwendbarkeit**: Dieses Kriterium gilt ausschließlich, wenn personenbezogene Daten im Rahmen der zu zertifizierenden Verarbeitungstätigkeiten in Drittländer oder an internationale Organisationen übermittelt werden.*

Ausnahmen gemäß Art. 49 Abs. 1 Unterabs. 1 DSGVO

Stützt sich der:die Zertifizierungsantragsteller:in gemäß Art. 49 Abs. 1 lit. a DSGVO auf eine ausdrückliche Einwilligung, wird die betroffene Person nachweislich über die möglichen Risiken der Datenübermittlung informiert und die ausdrückliche Einwilligung in die vorgesehene Übermittlung eingeholt.

Bei einer Übermittlung gemäß Art. 49 Abs. 1 lit. b–g DSGVO werden die Voraussetzungen der jeweils herangezogenen Ausnahme geprüft und dokumentiert:

lit. b: Bei einer zur Erfüllung eines Vertrags zwischen der betroffenen Person und dem:der Zertifizierungsantragsteller:in oder zur Durchführung vorvertraglicher Maßnahmen erforderlichen Übermittlung werden die Notwendigkeit der Übermittlung sowie – bei vorvertraglichen Maßnahmen – die Anfrage der betroffenen Person dokumentiert.

lit. c: Bei einer für den Abschluss oder die Erfüllung eines im Interesse der betroffenen Person geschlossenen Vertrags erforderlichen Übermittlung werden die Notwendigkeit der Übermittlung, das Interesse der betroffenen Person sowie der unmittelbare und objektive Zusammenhang zwischen der betroffenen Person und dem Vertragszweck dokumentiert.

lit. d: Bei einer aus wichtigen Gründen des öffentlichen Interesses erforderlichen Übermittlung werden das öffentliche Interesse und dessen Anerkennung im Unionsrecht oder im österreichischen Recht dokumentiert.

lit. e: Bei einer für die Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen erforderlichen Übermittlung wird deren Notwendigkeit dokumentiert.

lit. f: Bei einer zum Schutz lebenswichtiger Interessen erforderlichen Übermittlung werden das lebenswichtige Interesse der betroffenen Person oder einer anderen Person sowie die rechtliche oder physische Unfähigkeit der betroffenen Person, ihre Einwilligung zu erteilen, dokumentiert.

lit. g: Bei einer Übermittlung aus einem Register werden die Rechtsgrundlage für die Führung des Registers, dessen Zugangsbedingungen sowie die Voraussetzungen für die Datenübermittlung geprüft und dokumentiert. Es wird sichergestellt, dass die gesetzlichen Voraussetzungen für die Einsichtnahme im konkreten Fall erfüllt sind und weder das gesamte Register noch ganze Kategorien personenbezogener Daten übermittelt werden. Ist die Einsichtnahme an ein berechtigtes Interesse geknüpft, wird dieses nachgewiesen und die Übermittlung erfolgt ausschließlich an die anfragende Person.

Ausnahme gemäß Art. 49 Abs. 1 Unterabs. 2 DSGVO

Stützt sich der:die Zertifizierungsantragsteller:in in einem Einzelfall auf Art. 49 Abs. 1 Unterabs. 2 DSGVO, wird geprüft und dokumentiert, dass:

- die Übermittlung nicht wiederholt erfolgt;
- nur eine begrenzte Anzahl betroffener Personen betroffen ist;
- die Übermittlung für zwingende berechtigte Interessen des:der Zertifizierungsantragstellers:in erforderlich ist, die nicht von den Interessen oder Rechten und Freiheiten der betroffenen Personen überwogen werden; und
- alle Umstände der Datenübermittlung geprüft und auf dieser Grundlage geeignete Garantien zum Schutz personenbezogener Daten vorgesehen wurden.

Die Prüfung und die vorgesehenen geeigneten Garantien werden gemäß Art. 49 Abs. 6 DSGVO im Verzeichnis von Verarbeitungstätigkeiten dokumentiert.

A.11.03 - Information der Aufsichtsbehörde über eine Datenübermittlung

Überblick
Der:die Zertifizierungsantragsteller:in informiert die Aufsichtsbehörde über eine Datenübermittlung gemäß Art. 49 Abs. 1 Unterabs. 2 DSGVO.
Detaillierte Anforderungen
***Anwendbarkeit**: Dieses Kriterium gilt ausschließlich, wenn personenbezogene Daten im Rahmen der zu zertifizierenden Verarbeitungstätigkeiten auf Grundlage des Art. 49 Abs. 1 Unterabs. 2 DSGVO in ein Drittland oder an eine internationale Organisation übermittelt werden.* Der:die Zertifizierungsantragsteller:in weist die Mitteilung an die Aufsichtsbehörde nach und dokumentiert sowohl die Kommunikation mit der Aufsichtsbehörde als auch deren Antwort.

A.11.04 – Information der betroffenen Person über die Datenübermittlung

Überblick
Der:die Zertifizierungsantragsteller:in informiert die betroffene Person nachweislich über eine Datenübermittlung gemäß Art. 49 Abs. 1 Unterabs. 2 DSGVO.
Detaillierte Anforderungen
***Anwendbarkeit**: Dieses Kriterium gilt ausschließlich, wenn personenbezogene Daten im Rahmen der zu zertifizierenden Verarbeitungstätigkeiten auf Grundlage des Art. 49 Abs. 1 Unterabs. 2 DSGVO in ein Drittland oder an eine internationale Organisation übermittelt werden.* Der:die Zertifizierungsantragsteller:in informiert die betroffene Person nachweislich über die Übermittlung und die damit verfolgten zwingenden berechtigten Interessen.

A.11.05 - Dokumentation der Datenübermittlungen

Überblick
Der:die Zertifizierungsantragsteller:in dokumentiert die im Rahmen der zu zertifizierenden Verarbeitungstätigkeiten vorgenommenen Übermittlungen personenbezogener Daten in Drittländer oder an internationale Organisationen.
Detaillierte Anforderungen
***Anwendbarkeit**: Dieses Kriterium gilt ausschließlich, wenn personenbezogene Daten im Rahmen der zu zertifizierenden Verarbeitungstätigkeiten in Drittländer oder an internationale Organisationen übermittelt werden.* Der:die Zertifizierungsantragsteller:in dokumentiert die zu zertifizierenden Verarbeitungstätigkeiten, in deren Rahmen personenbezogene Daten in Drittländer oder an internationale Organisationen übermittelt werden, sodass Auskunftsersuchen betroffener Personen erfüllt werden können. Die Dokumentation enthält folgende Informationen: die Arten der betreffenden Daten, die betroffenen Drittländer (einschließlich Transitländer), ob die Übermittlung auf einem Angemessenheitsbeschluss beruht oder — andernfalls — auf welchen geeigneten Garantien gemäß Art. 46 DSGVO, und die verwendeten Technologien.

A.11.06 – Regelmäßige Überprüfung der Zulässigkeit der Datenübermittlung

Überblick
Der:die Zertifizierungsantragsteller:in überprüft und bewertet regelmäßig das angemessene Schutzniveau sowie die Zulässigkeit von Datenübermittlungen gemäß Art. 44–49 DSGVO.
Detaillierte Anforderungen
***Anwendbarkeit**: Dieses Kriterium gilt ausschließlich, wenn personenbezogene Daten im Rahmen der zu zertifizierenden Verarbeitungstätigkeiten in Drittländer oder an internationale Organisationen übermittelt werden.* Der:die Zertifizierungsantragsteller:in überprüft und bewertet mindestens einmal jährlich das angemessene Schutzniveau bzw. die Zulässigkeit der Datenübermittlungen gemäß Art. 44–49 DSGVO für die zu zertifizierenden Verarbeitungstätigkeiten. Dabei werden interne und externe Faktoren berücksichtigt, die die Gültigkeit der gewählten Übermittlungsinstrumente beeinflussen können. Hierzu zählen insbesondere Änderungen des einschlägigen Rechtsrahmens, unternehmerische Veränderungen wie Outsourcing, Fusionen oder Übernahmen, Änderungen der Datenschutzpraktiken, der Einsatz neuer Technologien sowie sonstige organisatorische oder technische Änderungen. Die Bewertung umfasst mindestens: ▶ die Aktualität der Angemessenheitsbeschlüsse der Europäischen Kommission in Bezug auf Drittländer und internationale Organisationen; ▶ das Vorliegen und die Angemessenheit geeigneter Garantien gemäß Art. 46 DSGVO für die jeweilige Datenübermittlung; ▶ die fortbestehende Wirksamkeit, Durchsetzbarkeit und Angemessenheit der implementierten Garantien; ▶ die Prüfung und Genehmigung der Anwendung von Ausnahmen gemäß Art. 49 DSGVO einschließlich der Dokumentation der Begründung; und ▶ vertragliche Vereinbarungen mit Auftragsverarbeiter:innen und sonstigen Empfänger:innen, die diese zur Einhaltung der vorgenannten Anforderungen verpflichten. Sofern ein:e Datenschutzbeauftragte:r benannt ist, wird die Stellungnahme in die Bewertung einbezogen. Die Ergebnisse der Überprüfung werden dokumentiert.

A.11.07 – Bewertung der Wirksamkeit des gewählten Übermittlungsinstruments gemäß Art. 46 DSGVO

Überblick
Der:die Zertifizierungsantragsteller:in stellt durch ein „Transfer Impact Assessment“ sicher, dass das durch die DSGVO gewährleistete Schutzniveau durch die Übermittlung personenbezogener Daten in Drittländer oder an internationale Organisationen nicht untergraben wird.
Detaillierte Anforderungen
***Anwendbarkeit**: Dieses Kriterium gilt ausschließlich, wenn der:die Zertifizierungsantragsteller:in im Rahmen der zu zertifizierenden Verarbeitungstätigkeiten personenbezogene Daten in ein Drittland oder an eine internationale Organisation übermittelt und die Übermittlung auf geeignete Garantien gemäß Art. 46 DSGVO gestützt wird.* Der:die Zertifizierungsantragsteller:in prüft, ob die Wirksamkeit der geeigneten Garantien des gemäß Art. 46 DSGVO gewählten Übermittlungsinstruments im Kontext der beabsichtigten Übermittlung durch die im Drittland geltenden Gesetze oder Praktiken beeinträchtigt werden kann. Erfolgt die Datenübermittlung aufgrund eines Angemessenheitsbeschlusses der Europäischen Kommission oder einer Ausnahme gemäß Art. 49 DSGVO, ist kein Transfer Impact Assessment erforderlich. Im Rahmen des Transfer Impact Assessments werden mindestens folgende Aspekte in strukturierter Form (z. B. anhand eines Fragebogens) berücksichtigt und dokumentiert: ▶ konkrete Umstände der Datenübermittlung: Identifikation des Datenexporteurs und Datenimporteurs sowie Rechtsgrundlage der Datenübermittlung gemäß Art. 44 ff. DSGVO; ▶ Übermittlungsumstände: Kategorien personenbezogener Daten (z. B. Arbeitnehmer:innen, Kund:innen), Arten der übermittelten Daten (z. B. E-Mail-Adressen, IP-Adressen), Häufigkeit der Übermittlung (z. B. einmalig, gelegentlich), Übermittlungsmethode (z. B. E-Mail, Secure File Transfer Protocol, Remote-Zugriff); ▶ Anwendbares Recht des Bestimmungslandes: Beschreibung der relevanten Gesetze für die Verarbeitung im Drittland, einschließlich Übersicht über Gesetze, die staatliche Stellen betreffen;

Detaillierte Anforderungen

- Bewertung der Rechtslage im Drittland: Bewertung, inwieweit die Rechtsvorschriften im Drittland den Schutz der personenbezogenen Daten und der Rechte betroffener Personen gewährleisten;
- Risiken für betroffene Personen: Bewertung der inhärenten Risiken, die sich aus der geplanten Verarbeitung im Drittland für betroffene Personen ergeben;
- Risiko behördlicher Zugriffe, soweit zutreffend: Bewertung der Rechtslage im Drittland hinsichtlich der Wahrscheinlichkeit eines Zugriffs staatlicher Stellen (z. B. im Fall der USA Prüfung, ob Datenempfänger:innen als Anbieter:innen elektronischer Kommunikationsdienste einzustufen sind und ob sie personenbezogene Daten im Klartext einsehen können); und
- Schlussfolgerung: abschließende Bewertung, ob die Verarbeitung im Drittland den Anforderungen der DSGVO und der Rechtsprechung des EuGH entspricht (für die abschließende Bewertung kann ein Scoring-Modell oder eine Risikomatrix verwendet werden, um den Entscheidungsprozess für Dritte nachvollziehbar zu machen);

Ergibt die Bewertung, dass das gewählte Übermittlungsinstrument kein ausreichendes Schutzniveau gewährleistet, werden ergänzende technische, organisatorische oder vertragliche Maßnahmen umgesetzt und dokumentiert.

Der:die Zertifizierungsantragsteller:in überprüft die dem Transfer Impact Assessment zugrunde liegende Bewertung in angemessenen Abständen sowie anlassbezogen, wenn Entwicklungen im Drittland oder Änderungen der Übermittlung die ursprüngliche Bewertung oder die Wirksamkeit der getroffenen Maßnahmen beeinflussen können.

Der:die Zertifizierungsantragsteller:in stellt sicher, dass die Übermittlung ausgesetzt oder beendet wird, wenn der Datenimporteur seine Verpflichtungen aus dem Übermittlungsinstrument gemäß Art. 46 DSGVO nicht mehr erfüllen kann oder die getroffenen ergänzenden Maßnahmen nicht mehr wirksam sind.

5. KRITERIEN FÜR AUFTRAGSVERARBEITER:INNEN

5.1. DATENSCHUTZORGANISATION

B.01.01 - Datenschutzorganisation einschließlich Rollen und Verantwortlichkeiten

Überblick
Die Rollen und Verantwortlichkeiten innerhalb der Datenschutzorganisation werden schriftlich festgelegt. Die Gesamtheit der Rollen deckt die Anforderungen an Zuständigkeiten gemäß DSGVO sowie die Umsetzung der Datenschutzziele ab.
Detaillierte Anforderungen
Der:die Zertifizierungsantragsteller:in dokumentiert die Rollen und Verantwortlichkeiten innerhalb der Datenschutzorganisation sowie die zugrunde liegende Organisationsstruktur des Unternehmens oder der Unternehmensgruppe (z. B. in Form eines Organigramms). Die Dokumentation zur Datenschutzorganisation umfasst mindestens die Verantwortlichkeiten innerhalb der Datenschutzorganisation (z. B. Datenschutzbeauftragte:r (sofern benannt), Datenschutzkoordinator:innen (sofern benannt), Geschäftsleitung und sonstige Gremien), funktionale Schnittstellen (z. B. IT, Informationssicherheit), Aufgaben und Verantwortlichkeiten der jeweiligen Rollen, Darstellung der Zusammenarbeit zwischen den Rollen, Darstellung der Zusammenarbeit mit der Geschäftsführung. Im Falle einer Unternehmensgruppe umfasst die Datenschutzorganisation auch die datenschutzbezogenen Funktionen und deren Zusammenarbeit zwischen den Gesellschaften der Unternehmensgruppe.

B.01.02 - Regelmäßige Schulungs- und Sensibilisierungsmaßnahmen für Mitarbeitende

Überblick
Der:die Zertifizierungsantragsteller:in informiert Mitarbeitende über die datenschutzrechtlichen Vorschriften und stellt entsprechende Datenschutzschulungen bereit.
Detaillierte Anforderungen
Der:die Zertifizierungsantragsteller:in schult jene Mitarbeitenden, die im Rahmen der zu zertifizierenden Verarbeitungstätigkeiten personenbezogene Daten verarbeiten, in regelmäßigen Abständen. Hierzu werden zielgruppenspezifische Schulungsmaßnahmen umgesetzt. Die Schulungsmaßnahmen können in unterschiedlicher Form durchgeführt werden, etwa als Präsenzschulung, Selbststudium, interaktiver Workshop, Online-Training/eLearning, Kampagnen, Broschüren, Newsletter, Informationsveranstaltungen oder E-Mails. Die Schulungsmaßnahmen sollen insbesondere das Bewusstsein in folgenden Bereichen schärfen: ▶ Grundlagen der geltenden Datenschutzgesetze (z. B. DSGVO und österreichisches Datenschutzgesetz); ▶ Grundlegende Verfahren des Datenschutzes und der Informationssicherheit (z. B. Meldung von Datenschutzverletzungen, potenzielle Datenschutzrisiken, Passwortsicherheit); ▶ Informationen zu Pflichten und Verantwortlichkeiten der Mitarbeitenden im Hinblick auf Datenschutz; ▶ Kontaktstellen für weiterführende Informationen und Beratung zum Datenschutz. Sofern ein:e Datenschutzbeauftragte:r benannt ist, bezieht der:die Zertifizierungsantragsteller:in diese:n in die Erstellung der Schulungsunterlagen ein. Die Durchführung und Teilnahme an Schulungsmaßnahmen werden nachvollziehbar dokumentiert. Bei Präsenzschulungen erfolgt der Nachweis insbesondere durch Teilnehmerlisten; bei Online-Schulungen durch geeignete elektronische Teilnahme- oder Abschlussnachweise. Soweit ein Abschlusstest vorgesehen ist, werden dessen Durchführung und Ergebnis dokumentiert.

5.2. RECHTE DER BETROFFENEN PERSONEN

B.02.01 – Unterstützung bei der Erfüllung der Informationspflichten

Überblick
Der:die Zertifizierungsantragsteller:in unterstützt den:die Verantwortliche:n bei der Erfüllung der Informationspflichten gemäß Art. 13 und 14 DSGVO, indem er:sie relevante Informationen bereitstellt und unverzüglich über hierfür maßgebliche Änderungen der zu zertifizierenden Verarbeitungstätigkeiten informiert.
Detaillierte Anforderungen
Der:die Zertifizierungsantragsteller:in legt offen, welche Unterauftragsverarbeiter:innen zur Verarbeitung personenbezogener Daten im Auftrag des:der Verantwortlichen eingesetzt werden sowie sämtliche geeigneten bzw. angemessenen Garantien, die bei einer Übermittlung personenbezogener Daten in ein Drittland oder an eine internationale Organisation bestehen. Darüber hinaus trifft der:die Zertifizierungsantragsteller:in technische und organisatorische Maßnahmen, um den:die Verantwortliche:n unverzüglich über wesentliche Änderungen der Verarbeitungstätigkeiten zu informieren, die Auswirkungen auf die Informationspflichten des:der Verantwortlichen gegenüber betroffenen Personen haben, wie etwa die Übermittlung personenbezogener Daten in weitere Drittländer oder an zusätzliche Empfänger:innen.

B.02.02 - Unterstützung bei Auskunftsersuchen betroffener Personen

Überblick
Der:die Zertifizierungsantragsteller:in stellt durch geeignete technische und organisatorische Maßnahmen sicher, dass der:die Verantwortliche bei der Bearbeitung von Auskunftsersuchen betroffener Personen gemäß Art. 15 DSGVO unterstützt werden kann.
Detaillierte Anforderungen
Die Unterstützungspflichten des:der Zertifizierungsantragstellers:in richten sich nach den vertraglichen Vereinbarungen mit dem:der Verantwortlichen. Sieht die vertragliche Vereinbarung ausschließlich die Weiterleitung von Betroffenenanfragen vor, bewahrt der:die Zertifizierungsantragsteller:in Nachweise über den Zeitpunkt des Eingangs der Betroffenenanfrage, den Zeitpunkt der Weiterleitung an den:die Verantwortliche:n sowie den Inhalt der Weiterleitung auf (z. B. E-Mails, Gesprächsprotokolle). Sehen die vertraglichen Vereinbarungen umfassende Unterstützungsleistungen vor, weil der:die Zertifizierungsantragsteller:in personenbezogene Daten im Auftrag des:der Verantwortlichen in eigenen Systemen verarbeitet, stellt der:die Zertifizierungsantragsteller:in Folgendes sicher: ▶ Festlegung einer zentralen Anlaufstelle (z. B. Abteilung) für die Bearbeitung von Betroffenenanfragen und Anfragen von Verantwortlichen; ▶ Umsetzung technischer Maßnahmen, die eine Zuordnung der betroffenen Person zu den Verantwortlichen ermöglichen (z. B. Mandantentrennung in Systemen, logische Trennung gespeicherter personenbezogener Daten), sofern personenbezogene Daten für mehrere Verantwortliche verarbeitet werden; und ▶ Festlegung eines Verfahrens für Fälle, in denen Verantwortliche nicht eindeutig identifiziert werden können. Etwaige zusätzliche vertraglich vereinbarte Unterstützungsleistungen werden in die internen Richtlinien aufgenommen. Bei unmittelbar eingehenden Auskunftsersuchen dokumentiert der:die Zertifizierungsantragsteller:in den Eingang und die Weiterleitung der Anfrage an den:die Verantwortliche:n einschließlich ihres Inhalts sowie gegebenenfalls Zeitpunkt und Inhalt der Information an die betroffene Person.

B.02.03 - Unterstützung bei der Bearbeitung von Berichtigungsersuchen

Überblick
Der:die Zertifizierungsantragsteller:in stellt durch geeignete technische und organisatorische Maßnahmen sicher, dass der:die Verantwortliche bei der Bearbeitung von Berichtigungsersuchen betroffener Personen gemäß Art. 16 DSGVO unterstützt werden kann.
Detaillierte Anforderungen
Die Unterstützungspflichten des:der Zertifizierungsantragstellers:in richten sich nach den vertraglichen Vereinbarungen mit dem:der Verantwortlichen. Sieht die vertragliche Vereinbarung ausschließlich die Weiterleitung von Betroffenenanfragen vor, bewahrt der:die Zertifizierungsantragsteller:in Nachweise über den Zeitpunkt des Eingangs der Betroffenenanfrage, den Zeitpunkt der Weiterleitung an den:die Verantwortliche:n sowie den Inhalt der Weiterleitung auf (z. B. E-Mails, Gesprächsprotokolle). Sehen die vertraglichen Vereinbarungen umfassende Unterstützungsleistungen vor, weil der:die Zertifizierungsantragsteller:in personenbezogene Daten im Auftrag des:der Verantwortlichen in eigenen Systemen verarbeitet, stellt der:die Zertifizierungsantragsteller:in Folgendes sicher: ▶ Festlegung einer zentralen Anlaufstelle (z. B. Abteilung) für die Bearbeitung von Betroffenenanfragen und Anfragen von Verantwortlichen; ▶ Umsetzung technischer Maßnahmen, die eine Zuordnung der betroffenen Person zu den Verantwortlichen ermöglichen (z. B. Mandantentrennung in Systemen, logische Trennung gespeicherter personenbezogener Daten), sofern personenbezogene Daten für mehrere Verantwortliche verarbeitet werden; ▶ Implementierung geeigneter technischer und organisatorischer Maßnahmen, die es ermöglichen, personenbezogene Daten, die im Auftrag von Verantwortlichen verarbeitet werden, unverzüglich zu berichtigen; und ▶ Festlegung eines Verfahrens für Fälle, in denen Verantwortliche nicht eindeutig identifiziert werden können. Etwaige zusätzliche vertraglich vereinbarte Unterstützungsleistungen werden in die internen Richtlinien aufgenommen. Bei unmittelbar eingehenden Berichtigungsersuchen dokumentiert der:die Zertifizierungsantragsteller:in den Eingang und die Weiterleitung der Anfrage an den:die Verantwortliche:n einschließlich ihres Inhalts sowie gegebenenfalls Zeitpunkt und Inhalt der Information an die betroffene Person.

B.02.04 - Unterstützung bei Löschungsersuchen

Überblick
Der:die Zertifizierungsantragsteller:in stellt durch geeignete technische und organisatorische Maßnahmen sicher, dass der:die Verantwortliche bei der Bearbeitung von Löschungsersuchen betroffener Personen gemäß Art. 17 DSGVO unterstützt werden kann.
Detaillierte Anforderungen
Die Unterstützungspflichten des:der Zertifizierungsantragstellers:in richten sich nach den vertraglichen Vereinbarungen mit dem:der Verantwortlichen. Sieht die vertragliche Vereinbarung ausschließlich die Weiterleitung von Betroffenenanfragen vor, bewahrt der:die Zertifizierungsantragsteller:in Nachweise über den Zeitpunkt des Eingangs der Betroffenenanfrage, den Zeitpunkt der Weiterleitung an den:die Verantwortliche:n sowie den Inhalt der Weiterleitung auf (z. B. E-Mails, Gesprächsprotokolle). Sehen die vertraglichen Vereinbarungen umfassende Unterstützungsleistungen vor, weil der:die Zertifizierungsantragsteller:in personenbezogene Daten im Auftrag des:der Verantwortlichen in eigenen Systemen verarbeitet, stellt der:die Zertifizierungsantragsteller:in Folgendes sicher: ▶ Festlegung einer zentralen Anlaufstelle (z. B. Abteilung) für die Bearbeitung von Betroffenenanfragen und Anfragen von Verantwortlichen; ▶ Umsetzung technischer Maßnahmen, die eine Zuordnung der betroffenen Person zu den Verantwortlichen ermöglichen (z. B. Mandantentrennung in Systemen, logische Trennung gespeicherter personenbezogener Daten), sofern personenbezogene Daten für mehrere Verantwortliche verarbeitet werden; ▶ Implementierung geeigneter technischer und organisatorischer Maßnahmen, die es ermöglichen, personenbezogene Daten, die im Auftrag von Verantwortlichen verarbeitet werden, zu löschen; und ▶ Festlegung eines Verfahrens für Fälle, in denen Verantwortliche nicht eindeutig identifiziert werden können. Etwaige zusätzliche vertraglich vereinbarte Unterstützungsleistungen werden in die internen Richtlinien aufgenommen. Bei unmittelbar eingehenden Löschungsersuchen dokumentiert der:die Zertifizierungsantragsteller:in den Eingang und die Weiterleitung der Anfrage an den:die Verantwortliche:n einschließlich ihres Inhalts sowie gegebenenfalls Zeitpunkt und Inhalt der Information an die betroffene Person.

B.02.05 - Unterstützung bei der Einschränkung der Verarbeitung

Überblick
Der:die Zertifizierungsantragsteller:in stellt durch geeignete technische und organisatorische Maßnahmen sicher, dass der:die Verantwortliche bei der Bearbeitung von Anträgen betroffener Personen auf Einschränkung der Verarbeitung gemäß Art. 18 DSGVO unterstützt werden kann.
Detaillierte Anforderungen
Die Unterstützungspflichten des:der Zertifizierungsantragstellers:in richten sich nach den vertraglichen Vereinbarungen mit dem:der Verantwortlichen. Sieht die vertragliche Vereinbarung ausschließlich die Weiterleitung von Betroffenenanfragen vor, bewahrt der:die Zertifizierungsantragsteller:in Nachweise über den Zeitpunkt des Eingangs der Betroffenenanfrage, den Zeitpunkt der Weiterleitung an den:die Verantwortliche:n sowie den Inhalt der Weiterleitung auf (z. B. E-Mails, Gesprächsprotokolle). Sehen die vertraglichen Vereinbarungen umfassende Unterstützungsleistungen vor, weil der:die Zertifizierungsantragsteller:in personenbezogene Daten im Auftrag des:der Verantwortlichen in eigenen Systemen verarbeitet, stellt der:die Zertifizierungsantragsteller:in Folgendes sicher: ▶ Festlegung einer zentralen Anlaufstelle (z. B. Abteilung), die für die Bearbeitung von Betroffenenanfragen sowie Anfragen von Verantwortlichen zuständig ist; ▶ Umsetzung technischer Maßnahmen, die eine Zuordnung der betroffenen Person zum jeweiligen Verantwortlichen ermöglichen (z. B. Mandantentrennung in Systemen, logische Trennung gespeicherter personenbezogener Daten), sofern der:die Zertifizierungsantragsteller:in Daten für mehr als einen Verantwortlichen verarbeitet; ▶ Implementierung geeigneter technischer und organisatorischer Maßnahmen, die es ermöglichen, personenbezogene Daten, die im Auftrag eines Verantwortlichen verarbeitet werden, einzuschränken; ▶ Festlegung eines Verfahrens für Fälle, in denen Verantwortliche nicht eindeutig identifiziert werden können. Etwaige zusätzliche vertraglich vereinbarte Unterstützungsleistungen werden in die internen Richtlinien aufgenommen. Wendet sich eine betroffene Person unmittelbar an den:die Zertifizierungsantragsteller:in, werden der Eingang und die Weiterleitung der Anfrage an den:die Verantwortliche:n einschließlich ihres Inhalts sowie Zeitpunkt und Inhalt der Information an die betroffene Person dokumentiert.

B.02.06 - Unterstützung bei der Datenübertragbarkeit

Überblick
Der:die Zertifizierungsantragsteller:in stellt durch geeignete technische und organisatorische Maßnahmen sicher, dass der:die Verantwortliche bei der Bearbeitung von Anträgen betroffener Personen auf Datenübertragbarkeit gemäß Art. 20 DSGVO unterstützt werden kann.
Detaillierte Anforderungen
Die Unterstützungspflichten des:der Zertifizierungsantragstellers:in richten sich nach den vertraglichen Vereinbarungen mit dem:der Verantwortlichen. Sieht die vertragliche Vereinbarung ausschließlich die Weiterleitung von Betroffenenanfragen vor, bewahrt der:die Zertifizierungsantragsteller:in Nachweise über den Zeitpunkt des Eingangs der Betroffenenanfrage, den Zeitpunkt der Weiterleitung an den:die Verantwortliche:n sowie den Inhalt der Weiterleitung auf (z. B. E-Mails, Gesprächsprotokolle). Sehen die vertraglichen Vereinbarungen umfassende Unterstützungsleistungen vor, weil der:die Zertifizierungsantragsteller:in personenbezogene Daten im Auftrag des:der Verantwortlichen in eigenen Systemen verarbeitet, stellt der:die Zertifizierungsantragsteller:in Folgendes sicher: ▶ Festlegung einer zentralen Anlaufstelle (z. B. Abteilung), die für die Bearbeitung von Betroffenenanfragen sowie Anfragen von Verantwortlichen zuständig ist; ▶ Umsetzung technischer Maßnahmen, die eine Zuordnung der betroffenen Person zum jeweiligen Verantwortlichen ermöglichen (z. B. Mandantentrennung in Systemen, logische Trennung gespeicherter personenbezogener Daten), sofern der:die Zertifizierungsantragsteller:in Daten für mehr als einen Verantwortlichen verarbeitet; ▶ Implementierung geeigneter technischer und organisatorischer Maßnahmen zur Unterstützung des:der Verantwortlichen bei der Bereitstellung der personenbezogenen Daten in einem gängigen, strukturierten und maschinenlesbaren Format; ▶ Festlegung eines Verfahrens für Fälle, in denen Verantwortliche nicht eindeutig identifiziert werden können. Etwaige zusätzliche vertraglich vereinbarte Unterstützungsleistungen werden in die internen Richtlinien aufgenommen.

Detaillierte Anforderungen

Wendet sich eine betroffene Person unmittelbar an den:die Zertifizierungsantragsteller:in, werden der Eingang und die Weiterleitung der Anfrage an den:die Verantwortliche:n einschließlich ihres Inhalts sowie Zeitpunkt und Inhalt der Information an die betroffene Person dokumentiert.

B.02.07 - Unterstützung bei der Bearbeitung von Widersprüchen betroffener Personen

Überblick

Der:die Zertifizierungsantragsteller:in stellt durch geeignete technische und organisatorische Maßnahmen sicher, dass der:die Verantwortliche bei der Bearbeitung von Widersprüchen gemäß Art. 21 DSGVO unterstützt werden kann.

Detaillierte Anforderungen

Die Unterstützungspflichten des:der Zertifizierungsantragstellers:in richten sich nach den vertraglichen Vereinbarungen mit dem:der Verantwortlichen.

Sieht die vertragliche Vereinbarung ausschließlich die Weiterleitung von Betroffenenanfragen vor, bewahrt der:die Zertifizierungsantragsteller:in Nachweise über den Zeitpunkt des Eingangs der Betroffenenanfrage, den Zeitpunkt der Weiterleitung an den:die Verantwortliche:n sowie den Inhalt der Weiterleitung auf (z. B. E-Mails, Gesprächsprotokolle).

Sehen die vertraglichen Vereinbarungen umfassende Unterstützungsleistungen vor, weil der:die Zertifizierungsantragsteller:in personenbezogene Daten im Auftrag des:der Verantwortlichen in eigenen Systemen verarbeitet, stellt der:die Zertifizierungsantragsteller:in Folgendes sicher:

- Festlegung einer zentralen Anlaufstelle (z. B. Abteilung), die für die Bearbeitung von Betroffenenanfragen sowie Anfragen von Verantwortlichen zuständig ist;
- Umsetzung technischer Maßnahmen, die eine Zuordnung der betroffenen Person zum jeweiligen Verantwortlichen ermöglichen (z. B. Mandantentrennung in Systemen, logische Trennung gespeicherter personenbezogener Daten), sofern der:die Zertifizierungsantragsteller:in Daten für mehrere Verantwortliche verarbeitet;
- Implementierung geeigneter technischer und organisatorischer Maßnahmen zur Unterstützung des:der Verantwortlichen bei der Identifikation der betroffenen Daten und zur Einstellung der entsprechenden Verarbeitung;
- Festlegung eines Verfahrens für Fälle, in denen Verantwortliche nicht eindeutig identifiziert werden können.

Etwaige zusätzliche vertraglich vereinbarte Unterstützungsleistungen werden in die internen Richtlinien aufgenommen.

Wendet sich eine betroffene Person unmittelbar an den:die Zertifizierungsantragsteller:in, werden der Eingang und die Weiterleitung der Anfrage an den:die Verantwortliche:n einschließlich ihres Inhalts sowie Zeitpunkt und Inhalt der Information an die betroffene Person dokumentiert.

5.3. DATENSCHUTZ DURCH TECHNIKGESTALTUNG UND DURCH DATENSCHUTZFREUNDLICHE VOREINSTELLUNGEN

B.03.01 - Unterstützung bei der Umsetzung von Datenschutz durch Technikgestaltung

Überblick

Der:die Zertifizierungsantragsteller:in unterstützt durch geeignete technische und organisatorische Maßnahmen dabei, die Datenschutzgrundsätze gemäß Art. 5 DSGVO wirksam umzusetzen.

Detaillierte Anforderungen

Der:die Zertifizierungsantragsteller:in stellt durch geeignete technische und organisatorische Maßnahmen sicher, dass Verantwortliche die Grundsätze des Art. 5 DSGVO (Rechtmäßigkeit, Verarbeitung nach Treu und Glauben, Transparenz, Zweckbindung, Datenminimierung, Richtigkeit, Speicherbegrenzung, Integrität und Vertraulichkeit sowie Rechenschaftspflicht) wirksam umsetzen können.

Bei der Festlegung der Maßnahmen berücksichtigt der:die Zertifizierungsantragsteller:in den Stand der Technik, die Implementierungskosten sowie Art, Umfang, Kontext und Zwecke der Verarbeitung und die unterschiedlichen Eintrittswahrscheinlichkeiten und Schweregrade der Risiken für die Rechte und Freiheiten natürlicher Personen.

Detaillierte Anforderungen
Der:die Zertifizierungsantragsteller:in dokumentiert bereits in einer frühen Phase der Planung sowie während der Verarbeitung die Festlegung technischer und/oder organisatorischer Maßnahmen zur Umsetzung des Datenschutzes durch Technikgestaltung (Data Protection by Design). Konkrete technische und organisatorische Maßnahmen sind in den Kriterien B.06.01 bis B.07.25 beschrieben.

B.03.02 - Unterstützung bei der Umsetzung von Datenschutz durch Voreinstellungen

Überblick
Der:die Zertifizierungsantragsteller:in stellt durch datenschutzfreundliche Voreinstellungen sicher, dass nur jene personenbezogenen Daten verarbeitet werden, die zur Erbringung der vertraglichen Leistungen erforderlich sind.
Detaillierte Anforderungen
Der:die Zertifizierungsantragsteller:in stellt durch geeignete technische und organisatorische Maßnahmen sicher, dass bei Produkten, Dienstleistungen und Anwendungen eine datenminimierende Verarbeitung erreicht wird. Dies umfasst insbesondere: ▶ die Menge der erhobenen personenbezogenen Daten; ▶ den Umfang ihrer Verarbeitung; ▶ die Dauer ihrer Speicherung; und ▶ ihre Zugänglichkeit, insbesondere dahingehend, dass personenbezogene Daten standardmäßig nicht ohne Zutun der betroffenen Person einer unbestimmten Anzahl natürlicher Personen zugänglich gemacht werden. Der:die Zertifizierungsantragsteller:in dokumentiert sowohl in der Planungsphase der Datenverarbeitung als auch während der tatsächlichen Verarbeitung die Festlegung technischer und/oder organisatorischer Maßnahmen zur Umsetzung datenschutzfreundlicher Voreinstellungen.

5.4. ANFORDERUNGEN GEMÄß ART. 28 DSGVO (VERHÄLTNIS ZWISCHEN VERANTWORTLICHE:R UND ZERTIFIZIERUNGSANTRAGSTELLER:IN)

B.04.01 - Information über neue Unterauftragsverarbeiter:innen und Ermöglichung eines Widerspruchs

Überblick
Der:die Zertifizierungsantragsteller:in stellt sicher, dass weitere Unterauftragsverarbeiter:innen nur mit vorheriger gesonderter oder allgemeiner schriftlicher Genehmigung der Verantwortlichen eingesetzt werden.
Detaillierte Anforderungen
Bei einer beabsichtigten Änderung oder Einbindung neuer Unterauftragsverarbeiter:innen stellt der:die Zertifizierungsantragsteller:in sicher, dass: ▶ alle betroffenen Verantwortlichen unter Einhaltung der vertraglich vereinbarten Informationsfrist rechtzeitig informiert werden; ▶ bei fehlender allgemeiner Genehmigung die schriftliche Genehmigung von Verantwortlichen vor Umsetzung der Änderung bzw. Beauftragung der neuen Unterauftragsverarbeiter:innen eingeholt wird; und ▶ bei Vorliegen einer allgemeinen Genehmigung den Verantwortlichen die Möglichkeit eingeräumt wird, der Änderung oder Einbindung neuer Unterauftragsverarbeiter:innen zu widersprechen. Die Information erfolgt elektronisch oder in Textform. Für die Erhebung eines Widerspruchs wird dem:der Verantwortlichen vertraglich eine Frist von mindestens sieben Tagen eingeräumt. Der:die Zertifizierungsantragsteller:in dokumentiert mindestens: ▶ den Ablauf für die Information des:der Verantwortlichen, die Einholung von Genehmigungen und die Ermöglichung von Widersprüchen;

Detaillierte Anforderungen

- das Vorgehen bei nicht erteilter Genehmigung oder bei einem Widerspruch;
- Nachweise über die erfolgte Information der Verantwortlichen einschließlich der jeweils eingeräumten Widerspruchsfrist;
- die schriftlichen Genehmigungen der Verantwortlichen; und
- eingegangene Widersprüche sowie deren Bearbeitung.

B.04.02 - Rückgabe oder Löschung von Daten

Überblick

Der:die Zertifizierungsantragsteller:in stellt sicher, dass Datenträger und personenbezogene Daten nach Abschluss der Verarbeitungstätigkeiten entweder zurückgegeben oder endgültig gelöscht werden.

Detaillierte Anforderungen

Der:die Zertifizierungsantragsteller:in stellt sicher, dass nach Beendigung der vertraglich vereinbarten Verarbeitung alle personenbezogenen Daten gemäß der Weisung der Verantwortlichen entweder vollständig zurückgegeben oder unwiderruflich gelöscht werden, sofern keine gesetzliche Aufbewahrungspflicht nach Unionsrecht oder österreichischem Recht besteht.

Die Umsetzung erfolgt im Einklang mit den Anforderungen des Kriteriums B.07.25.

B.04.03 - Abschluss von Vereinbarungen zur Auftragsverarbeitung

Überblick

Der:die Zertifizierungsantragsteller:in schließt mit allen Verantwortlichen eine Vereinbarung über die Auftragsverarbeitung personenbezogener Daten ab, die den Anforderungen des Art. 28 DSGVO entspricht.

Detaillierte Anforderungen

Der:die Zertifizierungsantragsteller:in schließt mit allen Verantwortlichen einen Vertrag über die Auftragsverarbeitung ab. Der Auftragsverarbeitungsvertrag kann individuell, auf Basis von Vorlagen oder auf Grundlage der Standardvertragsklauseln gemäß Art. 28 Abs. 7 DSGVO erstellt werden, sofern die Anforderungen des Art. 28 Abs. 3 und 4 DSGVO erfüllt sind.

Der Mindestinhalt des Auftragsverarbeitungsvertrags gemäß Art. 28 Abs. 3 DSGVO umfasst insbesondere:

- Gegenstand und Dauer der Verarbeitung;
- Art und Zweck der Verarbeitung;
- Kategorien personenbezogener Daten;
- Kategorien betroffener Personen;
- Rechte und Pflichten des:der Verantwortlichen;
- Eigene Pflichten, insbesondere:
  - Verarbeitung personenbezogener Daten ausschließlich auf dokumentierte Weisung von Verantwortlichen, einschließlich hinsichtlich etwaiger Übermittlungen in ein Drittland oder an eine internationale Organisation, sofern keine gesetzliche Verpflichtung besteht; in diesem Fall wird der:die Verantwortliche vorab informiert, soweit dies nicht aus wichtigen Gründen des öffentlichen Interesses gesetzlich untersagt ist (siehe Kriterium B.04.04);
  - Sicherstellung, dass zur Verarbeitung befugte Personen zur Vertraulichkeit verpflichtet oder einer entsprechenden gesetzlichen Verschwiegenheitspflicht unterliegen (siehe Kriterium B.07.23);
  - Umsetzung der Maßnahmen gemäß Art. 32 DSGVO (siehe Kriterien B.07.01–B.07.25);
  - Einsatz weiterer Auftragsverarbeiter:innen nur mit vorheriger gesonderter oder allgemeiner schriftlicher Genehmigung der Verantwortlichen;
  - Unterstützung der Verantwortlichen durch geeignete technische und organisatorische Maßnahmen bei der Erfüllung der Betroffenenrechte gemäß Kapitel III DSGVO, soweit möglich (vgl. Kriterien B.02.01–B.02.07);

Detaillierte Anforderungen

- Unterstützung der Verantwortlichen bei der Einhaltung der Pflichten gemäß Art. 32–36 DSGVO unter Berücksichtigung der Art der Verarbeitung und der vorliegenden Informationen (siehe Kriterien B.08.01 und B.09.01);
- Löschung oder Rückgabe sämtlicher personenbezogener Daten nach Abschluss der Verarbeitungstätigkeiten nach Wahl der Verantwortlichen sowie Löschung verbleibender Kopien, sofern keine gesetzliche Aufbewahrungspflicht besteht; und
- Bereitstellung aller erforderlichen Informationen zum Nachweis der Einhaltung der Pflichten aus Art. 28 DSGVO sowie Ermöglichung und Unterstützung von Prüfungen einschließlich Inspektionen durch die Verantwortlichen oder von diesen beauftragten Prüfer:innen.

Beim Einsatz von Unterauftragsverarbeiter:innen stellt der:die Zertifizierungsantragsteller:in sicher, dass mit diesen entsprechende Vereinbarungen abgeschlossen werden, die die vorstehenden Anforderungen erfüllen.

Der:die Zertifizierungsantragsteller:in legt schriftlich fest, welche Personen oder Abteilungen berechtigt sind, Weisungen gegenüber Unterauftragsverarbeiter:innen zu erteilen. Die Vereinbarungen mit Unterauftragsverarbeiter:innen enthalten zudem eine Vertraulichkeitsverpflichtung.

B.04.04 - Verarbeitung personenbezogener Daten nur auf Grundlage dokumentierter Weisung von Verantwortlichen

Überblick

Der:die Zertifizierungsantragsteller:in verarbeitet personenbezogene Daten ausschließlich auf dokumentierte Weisung von Verantwortlichen.

Detaillierte Anforderungen

Der:die Zertifizierungsantragsteller:in legt schriftlich fest, welche Personen oder Abteilungen berechtigt sind, Weisungen der jeweiligen Verantwortlichen für die zu zertifizierenden Verarbeitungstätigkeiten entgegenzunehmen. Zudem legt der:die Zertifizierungsantragsteller:in einen Ablauf für den Umgang mit mündlichen und schriftlichen Weisungen der jeweiligen Verantwortlichen fest.

B.04.05 - Abschluss von Vertraulichkeitsvereinbarungen / Vertraulichkeitserklärungen mit an der Verarbeitung beteiligten Personen

Überblick

Der:die Zertifizierungsantragsteller:in stellt sicher, dass ausschließlich Personen in die Verarbeitung eingebunden werden, die sich zur Vertraulichkeit bzw. Verschwiegenheit verpflichtet haben oder einer gesetzlichen Verschwiegenheitspflicht unterliegen.

Detaillierte Anforderungen

Der:die Zertifizierungsantragsteller:in stellt eine Vorlage für eine Vertraulichkeitsvereinbarung bereit (z. B. als Bestandteil des Dienstleistungsvertrags), die insbesondere folgende Inhalte umfasst:

- Definition vertraulicher Informationen;
- Umfang der Vertraulichkeitspflichten; und
- gegebenenfalls Sanktionen bei Verstößen.

Sofern Personen einer einschlägigen gesetzlichen Verschwiegenheitspflicht unterliegen, wird die entsprechende Rechtsgrundlage dokumentiert.

Der:die Zertifizierungsantragsteller:in stellt sicher, dass die Vertraulichkeitsvereinbarungen von allen relevanten Personen unterzeichnet werden.

5.5. ANFORDERUNGEN GEMÄß ART. 28 DSGVO (VERHÄLTNIS ZWISCHEN ZERTIFIZIERUNGSANTRAGSTELLER:IN UND UNTERAUFTRAGSVERARBEITER:IN)

Hinweis: Die Zertifizierungskriterien in ihrer aktuellen Fassung konzentrieren sich auf die Zertifizierung von Zertifizierungsantragsteller:innen in einem direkten Verhältnis zu Verantwortlichen. Soweit einzelne Zertifizierungskriterien auf Unterauftragsverarbeiter:innen Bezug nehmen, handelt es sich um Anforderungen, die Zertifizierungsantragsteller:innen bei der Einbindung von Unterauftragsverarbeiter:innen zur Einhaltung der DSGVO erfüllen müssen. Eine Zertifizierung von Unterauftragsverarbeiter:innen ist anhand dieser Kriterien nicht möglich.

B.04.06 – Auftragsverarbeitungsverträge mit Unterauftragsverarbeiter:innen

Überblick
Der:die Zertifizierungsantragsteller:in trifft Vorkehrungen für den Einsatz von Unterauftragsverarbeiter:innen und setzt nur solche ein, die Garantien dafür bieten, dass geeignete technische und organisatorische Maßnahmen umgesetzt werden, um eine Verarbeitung gemäß den Anforderungen der DSGVO und den Schutz der Rechte betroffener Personen sicherzustellen.
Detaillierte Anforderungen
***Anwendbarkeit**: Dieses Kriterium gilt, wenn Zertifizierungsantragsteller:innen für die zu zertifizierende Verarbeitungstätigkeit Unterauftragsverarbeiter:innen einsetzen oder beabsichtigen, die Verarbeitung oder Teile davon an Unterauftragsverarbeiter:innen auszulagern.* Vor der Beauftragung von Unterauftragsverarbeiter:innen stellt der:die Zertifizierungsantragsteller:in sicher, dass die erforderliche vorherige schriftliche gesonderte oder allgemeine Genehmigung von Verantwortlichen gemäß Kriterium B.04.01 vorliegt. Der:die Zertifizierungsantragsteller:in schließt mit allen eingesetzten Unterauftragsverarbeiter:innen einen Auftragsverarbeitungsvertrag, der: ▶ Unterauftragsverarbeiter:innen dieselben Pflichten auferlegt, denen der:die Zertifizierungsantragsteller:in gegenüber den Verantwortlichen unterliegt; und ▶ Unterauftragsverarbeiter:innen verpflichtet, ausreichende Garantien zu bieten oder geeignete technische und organisatorische Maßnahmen umzusetzen, um ein dem jeweiligen Verarbeitungsvorgang angemessenes Sicherheitsniveau zu gewährleisten. Dabei kann sich der:die Zertifizierungsantragsteller:in an den Anforderungen des Kriteriums B.04.07 orientieren. Die vorstehenden Anforderungen werden durch geeignete vertragliche Regelungen umgesetzt. Sofern ein:e Datenschutzbeauftragte:r benannt ist, wird diese:r in diesem Zusammenhang konsultiert und die entsprechende Beratung dokumentiert. Der:die Zertifizierungsantragsteller:in bewahrt die abgeschlossenen Auftragsverarbeitungsverträge strukturiert und leicht zugänglich auf und hält sie so vor, dass sie den Verantwortlichen auf Anfrage vorgelegt werden können. Beruht die Auftragsverarbeitung anstelle eines Vertrags auf einem anderen Rechtsinstrument nach dem Unionsrecht oder dem österreichischen Recht, dokumentiert der:die Zertifizierungsantragsteller:in das maßgebliche Rechtsinstrument und dessen Anwendbarkeit auf die betreffende Verarbeitung.

B.04.07 - Überprüfung der Sicherheit der Unterauftragsverarbeitung

Überblick
Der:die Zertifizierungsantragsteller:in stellt sicher, dass ausschließlich Unterauftragsverarbeiter:innen eingesetzt werden, die hinreichende Garantien dafür bieten, dass geeignete technische und organisatorische Maßnahmen umgesetzt werden, sodass die Verarbeitung gemäß den Anforderungen der DSGVO erfolgt und die Rechte der betroffenen Personen gewahrt werden.
Detaillierte Anforderungen
***Anwendbarkeit**: Dieses Kriterium gilt, wenn der:die Zertifizierungsantragsteller:in für die zu zertifizierende Verarbeitungstätigkeit Unterauftragsverarbeiter:innen einsetzt oder beabsichtigt, die Verarbeitung oder Teile davon an Unterauftragsverarbeiter:innen auszulagern.*

Detaillierte Anforderungen

Der:die Zertifizierungsantragsteller:in verfügt über ein dokumentiertes Verfahren zur Überprüfung der eingesetzten Unterauftragsverarbeiter:innen und legt auf Grundlage einer Risikobewertung Art und Häufigkeit der durchzuführenden Prüfungen fest.

Die Art der Prüfung richtet sich nach dem mit der Verarbeitung verbundenen Risiko und kann insbesondere anhand von Fragebögen und Dokumentennachweisen oder durch Vor-Ort-Audits erfolgen. Ein Fragebogen kann bei weniger komplexen Verfahren und geringeren Risiken ausreichend sein, sofern der:die Unterauftragsverarbeiter:in die erforderlichen Informationen und Nachweise liefern kann. Bei komplexeren Verarbeitungen oder höheren Risiken kann ein Vor-Ort-Audit erforderlich sein, um die Umsetzung der Maßnahmen vor Ort zu prüfen und zusätzliche Nachweise zu erlangen. Bei der Festlegung der Prüfungsmaßnahmen und -häufigkeit werden insbesondere die Sensitivität der verarbeiteten Daten, die Risiken für die Rechte und Freiheiten betroffener Personen, die Komplexität der technischen und organisatorischen Maßnahmen und die Bedeutung der Verarbeitung für die Geschäftsfortführung berücksichtigt. Anlassbezogene Prüfungen können insbesondere bei Datenschutzverletzungen oder wesentlichen Änderungen bei dem:der Unterauftragsverarbeiter:in erforderlich sein.

Als Nachweise können insbesondere einschlägige Zertifizierungen (z. B. ISO/IEC 27001, ISO/IEC 27701 etc.), Prüfberichte (z. B. nach ISAE 3402 und ISAE 3000) sowie die Einhaltung genehmigter Verhaltensregeln gemäß Art. 40 DSGVO oder Zertifizierungen gemäß Art. 42 DSGVO berücksichtigt werden.

Der:die Zertifizierungsantragsteller:in prüft die Nachweise der Unterauftragsverarbeiter:innen entsprechend dem festgelegten Verfahren und dokumentiert die Ergebnisse. Bei Vor-Ort-Audits werden insbesondere Umfang, angewandte Methoden, Auditnachweise, Ergebnisse und Feststellungen sowie gegebenenfalls daraus resultierende Maßnahmen dokumentiert.

Die Häufigkeit der Audits richtet sich nach dem Risikoprofil der Unterauftragsverarbeiter:innen und der Sensitivität der verarbeiteten Daten. Bei kritischen Unterauftragsverarbeiter:innen oder Verarbeitung sensibler Daten kann eine jährliche Prüfung erforderlich sein. Bei geringeren Risiken kann ein Intervall von zwei oder drei Jahren ausreichen.

B.04.08 - Einhaltung der im Auftragsverarbeitungsvertrag festgelegten Pflichten

Überblick

Der:die Zertifizierungsantragsteller:in stellt sicher, dass die Verarbeitung personenbezogener Daten durch Unterauftragsverarbeiter:innen ausschließlich auf dokumentierte Weisung des:der Verantwortlichen erfolgt.

Detaillierte Anforderungen

***Anwendbarkeit**: Dieses Kriterium gilt, wenn der:die Zertifizierungsantragsteller:in für die zu zertifizierende Verarbeitungstätigkeit Unterauftragsverarbeiter:innen einsetzen oder beabsichtigen, die Verarbeitung oder Teile davon an Unterauftragsverarbeiter:innen auszulagern.*

Beim Einsatz von Unterauftragsverarbeiter:innen stellt der:die Zertifizierungsantragsteller:in sicher, dass diese die im Auftragsverarbeitungsvertrag festgelegten Verpflichtungen einhalten. Hierzu wird mindestens Folgendes schriftlich festgelegt:

- welche Personen oder Abteilungen berechtigt sind, Weisungen gegenüber Unterauftragsverarbeiter:innen zu erteilen, sowie der Ablauf für mündliche und schriftliche Weisungen;
- welche Personen oder Abteilungen berechtigt sind, hinsichtlich des Einsatzes weiterer Auftragsverarbeiter:innen durch Unterauftragsverarbeiter:innen eine Zustimmung zu erteilen oder einen Widerspruch zu erheben;
- welche Personen oder Abteilungen als Ansprechpartner:innen gegenüber Unterauftragsverarbeiter:innen im Zusammenhang mit den Unterstützungspflichten gemäß Art. 32–36 DSGVO fungieren; und
- an welche Personen oder Abteilungen Unterauftragsverarbeiter:innen Datenschutzverletzungen zu melden haben und wie der Ablauf zur Information des:der Verantwortlichen über die Datenschutzverletzung ausgestaltet ist.

B.04.09 - Liste der Unterauftragsverarbeiter:innen

Überblick
Der:die Zertifizierungsantragsteller:in führt eine Übersicht über alle Unterauftragsverarbeiter:innen, die zur Verarbeitung personenbezogener Daten eingesetzt werden.
Detaillierte Anforderungen
***Anwendbarkeit**: Dieses Kriterium gilt, wenn der:die Zertifizierungsantragsteller:in für die zu zertifizierende Verarbeitungstätigkeit Unterauftragsverarbeiter:innen einsetzt oder beabsichtigt, die Verarbeitung oder Teile davon an Unterauftragsverarbeiter:innen auszulagern.* Der:die Zertifizierungsantragsteller:in führt eine vollständige und aktuelle Liste aller Unterauftragsverarbeiter:innen. Die Liste enthält mindestens folgende Informationen: ▶ Name bzw. Firma der Unterauftragsverarbeiter:innen; ▶ Adresse und Kontaktdaten der Unterauftragsverarbeiter:innen; ▶ Zweck der Unterauftragsverarbeitung und allgemeine Beschreibung der Verarbeitung; ▶ Kategorien personenbezogener Daten, die an die Unterauftragsverarbeiter:innen übermittelt werden; ▶ Datum des Auftragsverarbeitungsvertrags; und ▶ Information, ob sich die Unterauftragsverarbeiter:innen in einem Drittland befinden, und gegebenenfalls Angaben zu den geeigneten Garantien gemäß Art. 46 DSGVO.

5.6. VERZEICHNIS VON VERARBEITUNGSTÄTIGKEITEN

B.05.01 - Verzeichnis von Verarbeitungstätigkeiten

Überblick
Der:die Zertifizierungsantragsteller:in dokumentiert alle Kategorien von Verarbeitungstätigkeiten, die für Verantwortliche durchgeführt werden.
Detaillierte Anforderungen
***Anwendbarkeit**: Dieses Kriterium ist nicht relevant, wenn der:die Zertifizierungsantragsteller:in weniger als 250 Personen beschäftigt, es sei denn, die Verarbeitung ist wahrscheinlich mit einem Risiko für die Rechte und Freiheiten betroffener Personen verbunden, erfolgt nicht nur gelegentlich oder umfasst besondere Kategorien personenbezogener Daten gemäß Art. 9 Abs. 1 DSGVO oder personenbezogene Daten über strafrechtliche Verurteilungen und Straftaten gemäß Art. 10 DSGVO (Art. 30 Abs. 5 DSGVO).* Das Verzeichnis von Verarbeitungstätigkeiten umfasst die im Geltungsbereich der Zertifizierung liegenden Verarbeitungstätigkeiten und enthält gemäß Art. 30 Abs. 2 DSGVO: ▶ Name und Kontaktdaten des:der Zertifizierungsantragsteller:in sowie der Verantwortlichen, in deren Auftrag die Verarbeitung erfolgt, und gegebenenfalls der jeweiligen Vertreter:innen und Datenschutzbeauftragten; ▶ die Kategorien der im Auftrag der jeweiligen Verantwortlichen durchgeführten Verarbeitungen; ▶ gegebenenfalls Übermittlungen personenbezogener Daten an ein Drittland oder eine internationale Organisation einschließlich der Identifizierung des betreffenden Drittlands oder der internationalen Organisation und – im Fall von Übermittlungen gemäß Art. 49 Abs. 1 Unterabs. 2 DSGVO – die Dokumentation geeigneter Garantien; und ▶ soweit möglich, eine allgemeine Beschreibung der technischen und organisatorischen Sicherheitsmaßnahmen gemäß Art. 32 Abs. 1 DSGVO. Das Verzeichnis wird schriftlich bzw. in elektronischer Form geführt.

B.05.02 - Pflege und regelmäßige Aktualisierung des Verzeichnisses von Verarbeitungstätigkeiten

Überblick
Der:die Zertifizierungsantragsteller:in stellt sicher, dass das Verzeichnis von Verarbeitungstätigkeiten regelmäßig überprüft, gepflegt und aktualisiert wird.
Detaillierte Anforderungen
***Anwendbarkeit**: Dieses Kriterium ist nicht relevant, wenn der:die Zertifizierungsantragsteller:in weniger als 250 Personen beschäftigt, es sei denn, die Verarbeitung ist wahrscheinlich mit einem Risiko für die Rechte und Freiheiten betroffener Personen verbunden, erfolgt nicht nur gelegentlich oder umfasst besondere Kategorien personenbezogener Daten gemäß Art. 9 Abs. 1 DSGVO oder personenbezogene Daten über strafrechtliche Verurteilungen und Straftaten gemäß Art. 10 DSGVO (Art. 30 Abs. 5 DSGVO).* Der:die Zertifizierungsantragsteller:in überprüft das Verzeichnis von Verarbeitungstätigkeiten mindestens einmal jährlich. Die Verantwortlichkeiten für die Erfassung und Pflege der Verzeichniseinträge werden eindeutig festgelegt (z. B. in einer Richtlinie oder im Verzeichnis von Verarbeitungstätigkeiten). Die Überprüfung wird schriftlich dokumentiert. Änderungen des Verzeichnisses werden versioniert, sodass neue Einträge, inhaltliche Änderungen und die Löschung einzelner Verarbeitungstätigkeiten nachvollziehbar sind.

B.05.03 - Übermittlung des Verzeichnisses von Verarbeitungstätigkeiten an die Aufsichtsbehörde

Überblick
Der:die Zertifizierungsantragsteller:in stellt der Aufsichtsbehörde das Verzeichnis von Verarbeitungstätigkeiten auf Anfrage zur Verfügung.
Detaillierte Anforderungen
***Anwendbarkeit**: Dieses Kriterium ist nicht relevant, wenn der:die Zertifizierungsantragsteller:in weniger als 250 Personen beschäftigt, es sei denn, die Verarbeitung ist wahrscheinlich mit einem Risiko für die Rechte und Freiheiten betroffener Personen verbunden, erfolgt nicht nur gelegentlich oder umfasst besondere Kategorien personenbezogener Daten gemäß Art. 9 Abs. 1 DSGVO oder personenbezogene Daten über strafrechtliche Verurteilungen und Straftaten gemäß Art. 10 DSGVO (Art. 30 Abs. 5 DSGVO).* Der:die Zertifizierungsantragsteller:in legt Ansprechpartner:innen oder klare Zuständigkeiten für die Übermittlung des Verzeichnisses von Verarbeitungstätigkeiten an die Aufsichtsbehörde fest.

5.7. TECHNISCHE UND ORGANISATORISCHE MAßNAHMEN ZUR GEWÄHRLEISTUNG EINES DEM RISIKO ANGEMESSENEN SCHUTZNIVEAUS

B.06.01 - Dokumentation eines Risikomanagementprozesses

Überblick
Der:die Zertifizierungsantragsteller:in entwickelt einen geeigneten Risikomanagementprozess für den Umgang mit IT-Risiken.
Detaillierte Anforderungen
Der:die Zertifizierungsantragsteller:in implementiert einen dokumentierten Prozess zur Identifizierung, Analyse und Kategorisierung von Risiken für die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit personenbezogener Daten im Rahmen der zu zertifizierenden Verarbeitungstätigkeiten. Der Risikomanagementprozess umfasst mindestens: **a) Identifizierung potenzieller Risiken** Der:die Zertifizierungsantragsteller:in berücksichtigt insbesondere Risiken aus Projekten und dem laufenden Betrieb, im Zusammenhang mit Datenschutzvorfällen, aus Prozessen zum Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen sowie aus Datenschutz-Folgenabschätzungen.

Detaillierte Anforderungen

b) Bewertung der identifizierten Risiken

Der:die Zertifizierungsantragsteller:in bewertet und dokumentiert die identifizierten Risiken hinsichtlich ihrer Auswirkungen auf die Rechte und Freiheiten betroffener Personen (z. B. körperliche, materielle oder immaterielle Schäden, Verlust der Kontrolle über personenbezogene Daten, Diskriminierung, Identitätsdiebstahl etc.) und ihrer Eintrittswahrscheinlichkeit. Die Bewertung erfolgt anhand einer festgelegten Bewertungsmethodik.

c) Umsetzung und Überwachung von Maßnahmen

Für die identifizierten Risiken legt der:die Zertifizierungsantragsteller:in geeignete technische und organisatorische Maßnahmen fest und setzt diese um (siehe Kriterium B.06.02).

Der Risikomanagementprozess wird mindestens einmal jährlich sowie bei wesentlichen Änderungen überprüft.

B.06.02 - Risikoorientierte technische und organisatorische Maßnahmen zur Gewährleistung der Sicherheit der Datenverarbeitung

Überblick

Der:die Zertifizierungsantragsteller:in legt Maßnahmen für die im Rahmen der Risikoanalyse identifizierten Risiken für die Rechte und Freiheiten betroffener Personen fest, plant deren Umsetzung, bestimmt die Risikoverantwortlichen und verfolgt den Umsetzungsstatus.

Detaillierte Anforderungen

Auf Grundlage der Risikobewertung gemäß Kriterium B.06.01 dokumentiert der:die Zertifizierungsantragsteller:in die technischen und organisatorischen Maßnahmen, die zur Gewährleistung eines dem jeweiligen Risiko angemessenen Schutzniveaus umgesetzt werden. Der Umsetzungsstatus der Maßnahmen und die jeweils zugeordneten Risikoverantwortlichen werden dokumentiert. Wird ein Restrisiko akzeptiert, werden die Gründe hierfür im Risikomanagementplan dokumentiert.

Gemäß Art. 32 Abs. 1 DSGVO umfassen die Maßnahmen gegebenenfalls:

- die Pseudonymisierung und Verschlüsselung personenbezogener Daten;
- die Fähigkeit, die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung auf Dauer sicherzustellen;
- die Fähigkeit, die Verfügbarkeit personenbezogener Daten und den Zugang zu ihnen bei einem physischen oder technischen Zwischenfall rasch wiederherzustellen; und
- ein Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung.

Die Kriterien B.07.01–B.07.25 beschreiben technische und organisatorische Maßnahmen zur Erfüllung der Anforderungen des Art. 32 DSGVO, die grundsätzlich umzusetzen sind. Die Auswahl und Umsetzung der Maßnahmen erfolgt auf Grundlage der Risikobewertung gemäß Kriterium B.06.01. Werden einzelne Maßnahmen nicht umgesetzt, dokumentiert der:die Zertifizierungsantragsteller:in nachvollziehbar, weshalb diese im konkreten Fall nicht erforderlich oder nicht verhältnismäßig sind.

B.06.03 - Regelmäßige Überprüfung der Risikoanalyse

Überblick

Der:die Zertifizierungsantragsteller:in überprüft die durchgeführten Risikobewertungen mindestens einmal jährlich sowie bei wesentlichen Änderungen.

Detaillierte Anforderungen

Der:die Zertifizierungsantragsteller:in überprüft die Risikobewertung mindestens einmal jährlich sowie bei wesentlichen Änderungen, die sich auf die Verarbeitungstätigkeiten oder deren Risikolage auswirken können (z. B. Einsatz neuer IT-Systeme, Änderung/Erweiterung der verarbeiteten personenbezogenen Daten, Änderungen in der Art und Weise der Verarbeitung personenbezogener Daten – z. B. Einsatz neuer Analysetools).

Die Überprüfung erfolgt anhand einer dokumentierten Methodik und berücksichtigt interne und externe Faktoren, die die Risikobewertung beeinflussen können. Dazu zählen insbesondere Änderungen der Rechtslage, Unternehmensumstrukturierungen (z. B. Outsourcing, Fusionen oder Übernahmen), Anpassungen in den

Detaillierte Anforderungen
Datenschutzpraktiken, Einsatz neuer Technologien, Änderungen in der Dienstleistungserbringung sowie organisatorische oder technische Veränderungen. Im Rahmen der Überprüfung bewertet der:die Zertifizierungsantragsteller:in auch, ob die umgesetzten technischen und organisatorischen Maßnahmen unter Berücksichtigung der aktuellen Risikolage weiterhin angemessen und wirksam sind, und passt diese erforderlichenfalls an. Ist ein:e Datenschutzbeauftragte:r benannt, holt der:die Zertifizierungsantragsteller:in eine Stellungnahme ein und dokumentiert die Gründe, wenn von dieser abgewichen wird. Die Überprüfung und deren Ergebnis werden dokumentiert und durch die Geschäftsleitung bestätigt.

B.07.01 - Performanceparameter zur Sicherstellung der Belastbarkeit gegenüber Störungen und deren Überwachung

Überblick
Der:die Zertifizierungsantragsteller:in legt Performance- und Kapazitätsanforderungen fest, um die Belastbarkeit der für die zu zertifizierenden Verarbeitungstätigkeiten relevanten IT-Systeme sicherzustellen.
Detaillierte Anforderungen
Der:die Zertifizierungsantragsteller:in legt für die relevanten IT-Systeme geeignete Performanceparameter fest. Diese können insbesondere zulässige Ausfallzeiten, Reaktionszeiten bei Störungen, Verarbeitungsgeschwindigkeiten oder Verfügbarkeitszeiten umfassen. Die Einhaltung der festgelegten Performanceparameter wird durch geeignete Überwachungsmaßnahmen erfasst (z. B. Monitoring- oder Protokollierungs-Tools).

B.07.02 - Schutz vor Malware

Überblick
Der:die Zertifizierungsantragsteller:in implementiert Schutzmaßnahmen gegen Malware, um personenbezogene Daten vor Malware zu schützen.
Detaillierte Anforderungen
Der:die Zertifizierungsantragsteller:in richtet auf Grundlage des Risikomanagements Richtlinien und Verfahren zum Schutz der für die Verarbeitung personenbezogener Daten eingesetzten Systeme und Geräte vor Malware und bekannten Schwachstellen ein. Die eingesetzten Malware-Schutzmaßnahmen werden regelmäßig aktualisiert, um aktuellen Bedrohungen entgegenzuwirken.

B.07.03 - Netzwerksegmentierung

Überblick
Der:die Zertifizierungsantragsteller:in unterteilt Netzwerke in Sicherheitszonen und trennt diese vom öffentlichen Netzwerk.
Detaillierte Anforderungen
Der:die Zertifizierungsantragsteller:in setzt auf Grundlage der Risikobewertung gemäß den Kriterien B.06.01 und B.06.02 geeignete Maßnahmen zur Netzwerksegmentierung um. Netzwerke werden logisch getrennt, um unbefugte Zugriffe auf personenbezogene Daten zu verhindern. Dabei werden insbesondere Systeme mit unterschiedlichen Anforderungen an Vertraulichkeit und Verfügbarkeit voneinander isoliert (z. B. Trennung medizinischer Netzwerke in Krankenhäusern oder Personalverwaltungsnetzwerke von administrativen Netzwerken) und relevante Netzwerkbereiche vom öffentlichen Netzwerk getrennt.

B.07.04 - Netzwerküberwachung

Überblick
Der:die Zertifizierungsantragsteller:in implementiert eine Netzwerküberwachung, um potenzielle Sicherheitsverletzungen und Datenschutzverstöße zu erkennen.
Detaillierte Anforderungen
Der:die Zertifizierungsantragsteller:in setzt auf Grundlage der Risikobewertung gemäß den Kriterien B.06.01 und B.06.02 geeignete Maßnahmen zur Netzwerküberwachung um. Die Überwachung ermöglicht die frühzeitige Erkennung potenzieller Sicherheitsverletzungen und Datenschutzverstöße sowie eine zeitnahe Reaktion. Umfang und Häufigkeit der Überwachungsmaßnahmen werden an die identifizierten Risiken angepasst und berücksichtigen geschäftliche sowie datenschutzrechtliche Anforderungen. Überwachungsprotokolle werden für einen festgelegten Zeitraum entsprechend den rechtlichen, regulatorischen und betrieblichen Anforderungen aufbewahrt.

B.07.05 - Remote-Working

Überblick
Der:die Zertifizierungsantragsteller:in implementiert Sicherheitsmaßnahmen für Remote-Zugriffe, um die Vertraulichkeit, Integrität und Verfügbarkeit personenbezogener Daten sicherzustellen.
Detaillierte Anforderungen
Der:die Zertifizierungsantragsteller:in setzt auf Grundlage der Risikobewertung gemäß den Kriterien B.06.01 und B.06.02 geeignete Sicherheitsmaßnahmen für Remote-Zugriffe auf das Unternehmensnetzwerk um. Diese umfassen sichere Authentifizierungsmechanismen und definierte Regeln für Remote-Zugriffe.

B.07.06 - Zugriffsregelung für sensible Bereiche

Überblick
Der:die Zertifizierungsantragsteller:in stellt sicher, dass der Zugang zu sensiblen Bereichen geregelt ist.
Detaillierte Anforderungen
Der:die Zertifizierungsantragsteller:in setzt auf Grundlage der Risikobewertung gemäß den Kriterien B.06.01 und B.06.02 geeignete Sicherheitsmaßnahmen für Räumlichkeiten und Bereiche um, in denen personenbezogene Daten verarbeitet werden oder auf diese zugegriffen werden kann (z. B. IT-Abteilung, HR-Abteilung). Der Zugang zu unterschiedlichen Sicherheitszonen wird entsprechend den Sicherheitsanforderungen der verarbeiteten Daten geregelt.

B.07.07 - Zugangsfreigabeprozess für sensible Bereiche

Überblick
Der:die Zertifizierungsantragsteller:in stellt sicher, dass der Zugang zu sensiblen Bereichen geregelt ist.
Detaillierte Anforderungen
Der:die Zertifizierungsantragsteller:in richtet auf Grundlage der Risikobewertung gemäß den Kriterien B.06.01 und B.06.02 ein Verfahren zur Zugangskontrolle für sensible Bereiche ein, in denen personenbezogene Daten verarbeitet werden. Das Verfahren stellt sicher, dass nur autorisierte Personen Zugang erhalten und das Niveau der Zugangskontrolle der Sensibilität der verarbeiteten Daten und den identifizierten Risiken entspricht.

B.07.08 - Schutz vor externen und umweltbedingten Bedrohungen

Überblick
Der:die Zertifizierungsantragsteller:in mindert oder beseitigt potenzielle nachteilige Auswirkungen externer und umweltbedingter Bedrohungen durch geeignete Maßnahmen.
Detaillierte Anforderungen
Der:die Zertifizierungsantragsteller:in setzt auf Grundlage der Risikobewertung gemäß den Kriterien B.06.01 und B.06.02 geeignete Sicherheitsmaßnahmen zum Schutz personenbezogener Daten vor externen und umweltbedingten Bedrohungen um (z. B. Einbrüche, Diebstahl von Hardware oder Datenträgern, Feuer, Überschwemmungen, Stromausfälle).

B.07.09 - Verfahren zur Datenpseudonymisierung oder -anonymisierung

Überblick
Der:die Zertifizierungsantragsteller:in setzt Verfahren zur Pseudonymisierung und Anonymisierung personenbezogener Daten ein, die dem Stand der Technik entsprechen und praktikabel sind.
Detaillierte Anforderungen
Sofern im Rahmen der zu zertifizierenden Verarbeitungstätigkeiten Pseudonymisierungs- und/oder Anonymisierungstechniken eingesetzt werden, stellt der:die Zertifizierungsantragsteller:in sicher, dass diese dem Stand der Technik entsprechen und geeignet sind, die im Rahmen der Risikobewertung gemäß den Kriterien B.06.01 und B.06.02 identifizierten Risiken zu mindern. Die eingesetzten Techniken werden nachvollziehbar dokumentiert. Die Dokumentation beschreibt das jeweilige Verfahren und enthält – soweit möglich – einen Nachweis oder eine Begründung seiner Wirksamkeit.

B.07.10 - Protokollierungsfunktionen für toolgestützte Verarbeitung

Überblick
Der:die Zertifizierungsantragsteller:in stellt sicher, dass beim Einsatz von Tools oder Software zur Unterstützung von Verarbeitungstätigkeiten geeignete Protokollierungsfunktionen implementiert sind.
Detaillierte Anforderungen
Der:die Zertifizierungsantragsteller:in implementiert geeignete Protokollierungsmechanismen, um Zugriffe auf personenbezogene Daten, relevante Verarbeitungsvorgänge sowie Änderungen an personenbezogenen Daten nachvollziehbar zu erfassen. Protokolldaten werden sicher gespeichert und vor unbefugtem Zugriff geschützt. Umfang und technische Umsetzung der Protokollierung richten sich nach der Risikobewertung gemäß den Kriterien B.06.01 und B.06.02.

B.07.11 - Kontinuitätspläne und Wiederherstellungsmaßnahmen

Überblick
Der:die Zertifizierungsantragsteller:in legt Kontinuitätspläne sowie Reaktions- und Wiederherstellungsverfahren fest.
Detaillierte Anforderungen
Der:die Zertifizierungsantragsteller:in setzt auf Grundlage der Risikobewertung gemäß den Kriterien B.06.01 und B.06.02 geeignete Kontinuitäts-, Reaktions- und Wiederherstellungsmaßnahmen um, um die Verfügbarkeit personenbezogener Daten bei Störungen, Notfällen oder Datenverlust rasch wiederherzustellen. Die festgelegten Maßnahmen werden regelmäßig auf ihre Angemessenheit und Wirksamkeit überprüft.

B.07.12 - Festlegungen und Maßnahmen zur Datensicherung (Datensicherungskonzept)

Überblick
Der:die Zertifizierungsantragsteller:in legt ein Sicherungskonzept fest, das den Anforderungen der Organisation an Datenaufbewahrung und Informationssicherheit entspricht.
Detaillierte Anforderungen
Der:die Zertifizierungsantragsteller:in legt eine Backup-Richtlinie fest, die auf die Geschäfts- und Sicherheitsanforderungen der Organisation sowie die Kritikalität der personenbezogenen Daten abgestimmt ist. Die Richtlinie legt insbesondere Umfang und Häufigkeit der Backups fest. Der:die Zertifizierungsantragsteller:in testet die Backups und den Wiederherstellungsprozess regelmäßig, um deren Zuverlässigkeit im Notfall sicherzustellen und Datenverluste zu vermeiden.

B.07.13 - Überwachung der Verfügbarkeit

Überblick
Der:die Zertifizierungsantragsteller:in legt unter Berücksichtigung der geschäftlichen Anforderungen die Verfügbarkeitsanforderungen für IT-Systeme und Anwendungen fest, die zur Verarbeitung personenbezogener Daten eingesetzt werden, und stellt diese durch geeignete technische oder organisatorische Maßnahmen sicher.
Detaillierte Anforderungen
Der:die Zertifizierungsantragsteller:in überwacht die Verfügbarkeit der IT-Systeme und Anwendungen, die im Rahmen der zu zertifizierenden Verarbeitungstätigkeiten personenbezogene Daten verarbeiten. Die Überwachung stellt sicher, dass die festgelegten Verfügbarkeitsanforderungen eingehalten und mögliche Störungen frühzeitig erkannt und behoben werden.

B.07.14 - Verschlüsselungsmaßnahmen

Überblick
Der:die Zertifizierungsantragsteller:in legt Maßnahmen zur Verschlüsselung fest, um gespeicherte und übertragene personenbezogene Daten zu schützen.
Detaillierte Anforderungen
Der:die Zertifizierungsantragsteller:in legt auf Grundlage der Risikobewertung gemäß den Kriterien B.06.01 und B.06.02 geeignete Verschlüsselungsverfahren für die Speicherung und Übertragung personenbezogener Daten fest. Bei der Auswahl geeigneter Verschlüsselungsmethoden können folgende Kriterien berücksichtigt werden: ▶ Verschlüsselungsmethoden und eingesetzte Sicherheitsprotokolle entsprechen dem Stand der Technik; ▶ verwendete Schlüssel entsprechen hinsichtlich ihrer Länge und Komplexität aktuellen Empfehlungen und Standards; ▶ ein sicheres Schlüsselmanagement einschließlich sicherer Speicherung, regelmäßiger Aktualisierung und angemessener Zugriffskontrollen ist gewährleistet; und ▶ bei der Übertragung werden geeignete Protokolle und Mechanismen eingesetzt, welche die Vertraulichkeit der Daten sicherstellen. Der:die Zertifizierungsantragsteller:in weist nach, dass die eingesetzten Sicherheitsprotokolle und deren Konfiguration dem Stand der Technik entsprechen (z. B. kann eine veraltete TLS-Version Sicherheitslücken aufweisen). Verschlüsselungsmethoden, die nicht mehr aktuellen technischen Empfehlungen entsprechen, werden durch geeignete Verfahren ersetzt.

B.07.15 - Umgang mit Passwörtern

Überblick
Der:die Zertifizierungsantragsteller:in stellt sicher, dass für Systeme und Benutzerkonten sichere Passwortverfahren eingesetzt werden.
Detaillierte Anforderungen
Der:die Zertifizierungsantragsteller:in regelt auf Grundlage der Risikobewertung gemäß den Kriterien B.06.01 und B.06.02 die Vergabe, Nutzung und Verwaltung von Passwörtern und legt hierzu eine Passwort-Richtlinie fest. Diese berücksichtigt insbesondere: ▶ Anforderungen an Passwortlänge und -komplexität, Passwortänderungen sowie, soweit zutreffend, den Einsatz von Mehrfaktor-Authentifizierung; ▶ Anforderungen an Passwortzurücksetzungen; und ▶ Vorgaben für die sichere Verwaltung und den Schutz von Passwörtern (z. B. durch die Nutzung sicherer Passwortspeicher, Verschlüsselungstechniken oder andere Maßnahmen zur Gewährleistung der Vertraulichkeit von Passwörtern). Der:die Zertifizierungsantragsteller:in informiert und schult Mitarbeitende zum sicheren Umgang mit Passwörtern und Authentifizierungsverfahren.

B.07.16 – Zuweisung, Entzug oder Anpassung von Benutzerberechtigungen

Überblick
Der:die Zertifizierungsantragsteller:in stellt sicher, dass die Vergabe, Anpassung und der Entzug von Benutzerzugriffsrechten auf einem definierten Prozess basieren.
Detaillierte Anforderungen
Der:die Zertifizierungsantragsteller:in richtet einen Prozess zur Vergabe, Anpassung und zum Entzug von Benutzerberechtigungen für Verarbeitungstätigkeiten und Systeme ein. Dabei gilt insbesondere: ▶ Zugriffsrechte werden auf Grundlage von Rollenkonzepten vergeben; bei sensiblen personenbezogenen Daten erfolgt die Vergabe auf Grundlage eines Genehmigungsprozesses. ▶ Zugriffe auf personenbezogene Daten erfolgen ausschließlich über eindeutig zugeordnete Benutzerkonten. ▶ Gemeinsam genutzte Benutzerkonten sind nur zulässig, wenn sie aus geschäftlichen oder betrieblichen Gründen erforderlich, genehmigt und dokumentiert sind. Der Umfang der Zugriffskontrollmechanismen richtet sich nach der Risikobewertung gemäß den Kriterien B.06.01 und B.06.02.

B.07.17 - Zuweisung von privilegierten Zugriffsrechten

Überblick
Der:die Zertifizierungsantragsteller:in stellt sicher, dass die Vergabe und Nutzung privilegierter Zugriffsrechte beschränkt und kontrolliert erfolgt.
Detaillierte Anforderungen
Der:die Zertifizierungsantragsteller:in stellt sicher, dass privilegierte Zugriffs- oder Sonderrechte für personenbezogene Daten (z. B. Administratorrechte, System- oder Datenbankadministratorrechte) nur einem begrenzten Personenkreis gewährt werden. Vergabe und Umfang der privilegierten Zugriffsrechte werden auf Grundlage der Risikobewertung gemäß den Kriterien B.06.01 und B.06.02 festgelegt.

B.07.18 - Authentifizierungsmethoden

Überblick
Der:die Zertifizierungsantragsteller:in stellt sicher, dass sichere Authentifizierungstechnologien und -verfahren eingesetzt werden.
Detaillierte Anforderungen
Der:die Zertifizierungsantragsteller:in setzt für die zu zertifizierenden Verarbeitungstätigkeiten geeignete Authentifizierungsverfahren ein, um die Identität der Nutzer:innen zu überprüfen und einen legitimen Zugriff sicherzustellen. Wiederholte Identifikations- und Authentifizierungsversuche werden nach einer festgelegten Anzahl fehlgeschlagener Versuche beschränkt. Bei der Auswahl der Authentifizierungsverfahren berücksichtigt der:die Zertifizierungsantragsteller:in insbesondere: ▶ die gemäß den Kriterien B.06.01 und B.06.02 identifizierten Risiken und Bedrohungen; ▶ die Art und Sensibilität der verarbeiteten Daten (sensible oder vertrauliche Daten erfordern in der Regel strengere und sicherere Authentifizierungsmethoden); und ▶ die Nutzer:innen sowie deren Rollen und Berechtigungen (z. B. können Administrator:innen oder privilegierte Nutzer:innen strengere Authentifizierungsmethoden benötigen als reguläre Nutzer:innen).

B.07.19 - Automatische Beendigung der Verbindung zu IT-Systemen aufgrund von Inaktivität

Überblick
Der:die Zertifizierungsantragsteller:in legt ein Verfahren für die Abmeldung an Systemen und Anwendungen fest, um das Risiko unbefugter Zugriffe zu minimieren.
Detaillierte Anforderungen
Der:die Zertifizierungsantragsteller:in setzt Maßnahmen um, durch die Verbindungen zu IT-Systemen nach einem festgelegten Zeitraum der Benutzerinaktivität automatisch beendet werden. Dauer und Bedingungen der automatischen Beendigung werden auf Grundlage der Risikobewertung gemäß den Kriterien B.06.01 und B.06.02 unter Berücksichtigung der Sensibilität der Daten und der Risiken unbefugter Zugriffe festgelegt.

B.07.20 - Regelmäßige Überprüfung von Benutzerkonten, Benutzergruppen und Zugriffsberechtigungen

Überblick
Der:die Zertifizierungsantragsteller:in überprüft die Zugriffsrechte auf personenbezogene Daten gemäß den unternehmensinternen Zugriffsregelungen.
Detaillierte Anforderungen
Der:die Zertifizierungsantragsteller:in überprüft regelmäßig die Nutzer:innen und Nutzer:innengruppen mit Zugang zu personenbezogenen Daten sowie die eingeräumten Zugriffsberechtigungen auf ihre Angemessenheit und Erforderlichkeit. Die Zugriffsberechtigungen müssen den aktuellen geschäftlichen Anforderungen und Tätigkeiten der Nutzer:innen entsprechen. Umfang und Häufigkeit der Überprüfungen werden auf Grundlage der Risikobewertung gemäß den Kriterien B.06.01 und B.06.02 festgelegt. Der:die Zertifizierungsantragsteller:in dokumentiert die Überprüfungen. Die Dokumentation umfasst mindestens: ▶ die überprüften Nutzer:innen und Nutzer:innengruppen; ▶ Zeitpunkt und Verantwortliche der Überprüfung; ▶ die Kriterien zur Bewertung der Angemessenheit und Erforderlichkeit der Zugriffsberechtigungen; und ▶ Änderungen der Zugriffsberechtigungen, die sich aus der Überprüfung ergeben. ▶ sonstige relevante Hinweise oder Beobachtungen zum Überprüfungsprozess.

B.07.21 - Richtlinien für Mitarbeitende zum Umgang mit tragbaren Speichermedien

Überblick
Der:die Zertifizierungsantragsteller:in legt eine Richtlinie zum sicheren Umgang mit tragbaren Speichermedien fest.
Detaillierte Anforderungen
Der:die Zertifizierungsantragsteller:in legt für Mitarbeitende eine Richtlinie zum sicheren Umgang mit tragbaren Speichermedien fest (z. B. externe Festplatten, Speicherkarten, USB-Sticks), die auf dem unternehmensweiten Risikomanagementverfahren basiert und mit diesem im Einklang steht. Die Richtlinie wird allen Mitarbeitenden in geeigneter Weise (über das Intranet, per E-Mail oder ein anderes Kommunikationsmittel) bekannt gemacht.

B.07.22 - Funktionstrennung

Überblick
Der:die Zertifizierungsantragsteller:in trennt Aufgaben und Verantwortungsbereiche, um zu verhindern, dass eine einzelne Person potenziell konfligierende Aufgaben allein ausführt.
Detaillierte Anforderungen
Der:die Zertifizierungsantragsteller:in setzt geeignete Mechanismen zur Funktionstrennung innerhalb der Verarbeitungstätigkeiten und Systeme um. Dies umfasst die funktionale Trennung von Aufgaben und Verantwortlichkeiten sowie die Trennung von Entwicklungs-, Test- und Produktionsumgebungen. Umfang und Ausgestaltung der Maßnahmen werden auf Grundlage der Risikobewertung gemäß den Kriterien B.06.01 und B.06.02 unter Berücksichtigung der potenziellen Auswirkungen auf personenbezogene Daten und der identifizierten Risiken festgelegt.

B.07.23 - Verpflichtung zur Wahrung der Vertraulichkeit

Überblick
Der:die Zertifizierungsantragsteller:in stellt sicher, dass Mitarbeitende vor Beginn der Verarbeitung personenbezogener Daten zur Vertraulichkeit verpflichtet werden, sofern sie nicht bereits einer gesetzlichen Verschwiegenheitspflicht unterliegen.
Detaillierte Anforderungen
Der:die Zertifizierungsantragsteller:in stellt sicher, dass alle Mitarbeitenden, die im Rahmen der zu zertifizierenden Verarbeitungstätigkeiten personenbezogene Daten verarbeiten, durch geeignete Geheimhaltungs- oder Vertraulichkeitsvereinbarungen bzw. betriebliche oder dienstliche Regelungen zur Wahrung der Vertraulichkeit verpflichtet sind. Dies gilt unabhängig davon, ob personenbezogene Daten in automatisierten oder nicht automatisierten Prozessen verarbeitet werden.

B.07.24 - Prüfung der Wirksamkeit technischer und organisatorischer Maßnahmen

Überblick
Der:die Zertifizierungsantragsteller:in führt regelmäßige Prüfungen durch, um die Wirksamkeit der umgesetzten technischen und organisatorischen Maßnahmen zu überprüfen.
Detaillierte Anforderungen
Der:die Zertifizierungsantragsteller:in überprüft die Wirksamkeit der implementierten technischen und organisatorischen Maßnahmen regelmäßig (z. B. alle 12 bis 24 Monate). Die Prüfintervalle werden unter Berücksichtigung der Auswirkungen der jeweiligen Maßnahmen auf den Datenschutz und die organisatorische Sicherheit festgelegt.

Detaillierte Anforderungen

Hierzu richtet der:die Zertifizierungsantragsteller:in einen Prozess ein, der mindestens:

- festlegt, welche Maßnahmen jährlich und welche aufgrund geringerer Risiken in längeren Intervallen überprüft werden;
- die Verantwortlichkeiten für die jeweiligen Prüfbereiche festlegt;
- die Prüfanforderungen einschließlich Methodik, Dokumentation und Umgang mit Nachweisen definiert;
- die Kommunikation der Prüfungsergebnisse regelt; und
- den Umgang mit Feststellungen sowie die Umsetzung von Verbesserungsmaßnahmen festlegt.

Der:die Zertifizierungsantragsteller:in dokumentiert die durchgeführten Prüfungen einschließlich der Feststellungen, identifizierten Verbesserungspotenziale und festgelegten Verbesserungsmaßnahmen.

B.07.25 – Rückgabe oder Löschung von Daten nach Abschluss der Verarbeitungsleistungen

Überblick

Der:die Zertifizierungsantragsteller:in stellt sicher, dass nach Abschluss der Verarbeitungsleistungen alle personenbezogenen Daten und vorhandenen Kopien nach Wahl des:der Verantwortlichen gelöscht oder zurückgegeben werden, sofern keine gesetzliche Verpflichtung zur Speicherung besteht.

Detaillierte Anforderungen

Nach Abschluss der Verarbeitungsleistungen weist der:die Zertifizierungsantragsteller:in nach, dass vollständige Datensätze und einzelne Datenelemente vollständig gelöscht oder an den:die Verantwortliche:n zurückgegeben werden können. Die Löschung erfolgt so, dass eine Wiederherstellung der Daten verhindert wird, beispielsweise durch mehrfaches Überschreiben von Speichermedien wie Festplatten oder CD-RWs.

Die Löschung wird dokumentiert. Dabei bleibt die Vertraulichkeit der gelöschten Daten gewahrt, insbesondere durch sichere Protokolleinträge, die keine Rückschlüsse auf die gelöschten Informationen ermöglichen.

Der:die Zertifizierungsantragsteller:in implementiert automatisierte Löschfunktionen in den vom Zertifizierungsumfang erfassten Datenverarbeitungssystemen.

Vor der Entsorgung oder Weiterverwendung von Hardware werden wesentliche Komponenten wie Festplatten von Computern oder Speicher von Routern entfernt oder sicher gelöscht, um eine Wiederherstellung der Daten zu verhindern. Müssen Informationsträger wie Dokumente, CD-ROMs oder elektronische Token physisch vernichtet werden, kommen wirksame und zuverlässige Verfahren zum Einsatz, die eine vollständige Vernichtung der Daten sicherstellen.

Wird ein Entsorgungsunternehmen mit der Vernichtung beauftragt, bewahrt der:die Zertifizierungsantragsteller:in für jede Entsorgung eine Vernichtungsbestätigung auf. Soweit das Entsorgungsunternehmen personenbezogene Daten im Auftrag verarbeitet, wird mit diesem ein Vertrag gemäß Art. 28 Abs. 3 DSGVO abgeschlossen.

5.8. VERLETZUNGEN DES SCHUTZES PERSONENBEZOGENER DATEN

B.08.01 - Mitteilung von Datenschutzverletzungen an Verantwortliche

Überblick
Der:die Zertifizierungsantragsteller:in implementiert Abläufe und Maßnahmen, um Datenschutzverletzungen zu erkennen, zu bewerten und unverzüglich an Verantwortliche zu melden.
Detaillierte Anforderungen
Zur Sicherstellung einer einheitlichen und nachvollziehbaren Behandlung potenzieller Datenschutzverletzungen werden die hierfür erforderlichen Abläufe und Maßnahmen dokumentiert. Diese umfassen mindestens: ▶ die Festlegung einer zentralen Anlaufstelle für die Identifizierung und Bewertung potenzieller Datenschutzverletzungen; („Single Point of Contact“); ▶ sofern ein:e Datenschutzbeauftragte:r benannt wurde, dessen:deren verpflichtende Einbindung und die Einholung einer Stellungnahme, insbesondere im Zusammenhang mit Mitteilungen an die Aufsichtsbehörde und betroffene Personen; ▶ einen Ablauf zur Bewertung potenzieller Datenschutzverletzungen, der soweit möglich Art, Gegenstand, Umfang und Zwecke der Verarbeitung, die betroffenen Datenkategorien und Datenmengen, die Umstände bzw. Ursachen des Vorfalls sowie die möglichen Risiken für die Rechte und Freiheiten betroffener Personen berücksichtigt, einschließlich einer Risikobewertung; ▶ die eingesetzten Methoden zur Erkennung von Datenschutzverletzungen (z. B. Überwachungssysteme und Tools zur Identifizierung verdächtiger Aktivitäten oder Sicherheitsvorfälle, Intrusion-Detection-Systeme (IDS), Data-Loss-Prevention-Systeme (DLP), Analyse von System- und Anwendungsprotokollen, Threat-Intelligence); ▶ ein Register sämtlicher potenzieller Datenschutzverletzungen, das für jeden Vorfall mindestens eine Beschreibung, die möglichen Auswirkungen auf betroffene Personen und eine Risikobewertung enthält. Mitteilungen an Verantwortliche enthalten, soweit die erforderlichen Informationen zur Verfügung stehen, die Informationen gemäß Art. 33 Abs. 3 DSGVO. Können nicht alle Informationen gleichzeitig bereitgestellt werden, enthält die Erstmeldung die zu diesem Zeitpunkt verfügbaren Informationen; weitere Informationen werden unverzüglich nachgereicht, sobald sie verfügbar sind.

5.9. DATENSCHUTZ-FOLGENABSCHÄTZUNG

B.09.01 - Unterstützung bei der Durchführung einer Datenschutz-Folgenabschätzung

Überblick
Der:die Zertifizierungsantragsteller:in unterstützt Verantwortliche bei der Durchführung einer Datenschutz-Folgenabschätzung und stellt die hierfür erforderlichen Informationen bereit.
Detaillierte Anforderungen
Der:die Zertifizierungsantragsteller:in berücksichtigt bei der Unterstützung insbesondere die vorhandenen Kenntnisse über die eingesetzten Systeme, Datenflüsse und Risikoursachen. Verfügt ausschließlich der:die Zertifizierungsantragsteller:in über die detaillierten Kenntnisse der Systemarchitektur, Datenflüsse und Risikoursachen, die für die Bewertung der daraus resultierenden Risiken und die Festlegung geeigneter Maßnahmen zu deren Minderung erforderlich sind, führt der:die Zertifizierungsantragsteller:in eine beispielhafte Datenschutz-Folgenabschätzung durch. Die Ergebnisse werden dokumentiert und den Verantwortlichen zur Verfügung gestellt.

5.10. DATENSCHUTZBEAUFTRAGTE:R

B.10.01 - Bestellung eines:einer Datenschutzbeauftragten

Überblick
Der:die Zertifizierungsantragsteller:in prüft, ob die Voraussetzungen für die Bestellung eines:einer Datenschutzbeauftragten gemäß Art. 37 Abs. 1 DSGVO erfüllt sind.
Detaillierte Anforderungen
***Anwendbarkeit**: Dieses Kriterium gilt, wenn die Voraussetzungen für die Bestellung eines:einer Datenschutzbeauftragten erfüllt sind oder eine freiwillige Bestellung erfolgt.* Eine Bestellung ist gemäß Art. 37 Abs. 1 DSGVO erforderlich, wenn: ▶ die Verarbeitung von einer Behörde oder öffentlichen Stelle durchgeführt wird, mit Ausnahme von Gerichten, die im Rahmen ihrer justiziellen Tätigkeit handeln; ▶ die Kerntätigkeiten in Verarbeitungsvorgängen bestehen, die aufgrund ihrer Art, ihres Umfangs und/oder ihrer Zwecke eine umfangreiche regelmäßige und systematische Überwachung betroffener Personen erfordern; oder ▶ die Kerntätigkeiten in der umfangreichen Verarbeitung besonderer Kategorien personenbezogener Daten gemäß Art. 9 DSGVO sowie personenbezogener Daten über strafrechtliche Verurteilungen und Straftaten gemäß Art. 10 DSGVO bestehen. Die Begründung für die Bestellung oder Nichtbestellung wird dokumentiert. Ist eine Bestellung erforderlich oder erfolgt diese freiwillig, stellt der:die Zertifizierungsantragsteller:in sicher, dass: ▶ die Bestellung formell und schriftlich erfolgt; ▶ die Dokumentation über die Bestellung oder Benennung aufbewahrt wird; ▶ die Kontaktdaten des:der Datenschutzbeauftragten innerhalb der Organisation zugänglich sind (z. B. Intranet, Onboarding-Unterlagen oder interne Verzeichnisse); und ▶ die Kontaktdaten des:der Datenschutzbeauftragten der zuständigen Aufsichtsbehörde mitgeteilt und gemäß Art. 37 Abs. 7 DSGVO veröffentlicht werden (z. B. auf der Unternehmenswebsite oder in Datenschutzhinweisen).

B.10.02 - Aufgaben- bzw. Tätigkeitsbeschreibung

Überblick
Der:die Zertifizierungsantragsteller:in dokumentiert die Aufgaben des:der Datenschutzbeauftragten in einer Aufgaben- bzw. Tätigkeitsbeschreibung oder – im Fall eines:einer externen Datenschutzbeauftragten – in der Beauftragung.
Detaillierte Anforderungen
***Anwendbarkeit**: Dieses Kriterium gilt, wenn die Voraussetzungen für die Bestellung eines:einer Datenschutzbeauftragten erfüllt sind oder eine freiwillige Bestellung erfolgt.* Die Aufgaben- bzw. Tätigkeitsbeschreibung oder die Beauftragung bei externer Bestellung berücksichtigt die Anforderungen des Art. 39 Abs. 1 und 2 DSGVO. Sie umfasst insbesondere: ▶ die Unterrichtung und Beratung des Unternehmens, der Geschäftsführung sowie der Mitarbeitenden über ihre datenschutzrechtlichen Pflichten; ▶ die Überwachung der Einhaltung der DSGVO, anderer anwendbarer Datenschutzvorschriften und der Strategien des:der Auftragsverarbeiters:in einschließlich der Zuweisung von Verantwortlichkeiten, Sensibilisierung und Schulung der Mitarbeitenden sowie diesbezüglicher Prüfungen; ▶ die Beratung hinsichtlich der Datenschutz-Folgenabschätzung auf Anfrage und die Überwachung ihrer Durchführung gemäß Art. 35 DSGVO; ▶ die Zusammenarbeit mit der Aufsichtsbehörde; und ▶ die Tätigkeit als Anlaufstelle für die Aufsichtsbehörde in Fragen im Zusammenhang mit der Verarbeitung einschließlich der vorherigen Konsultation gemäß Art. 36 DSGVO sowie Beratung in sonstigen Angelegenheiten nach Bedarf. Werden dem:der Datenschutzbeauftragten zusätzliche Aufgaben im Zusammenhang mit der Datenschutzorganisation übertragen (z. B. die Führung des Verzeichnisses von Verarbeitungstätigkeiten oder die Koordinierung von Betroffenenanfragen), dokumentiert der:die Zertifizierungsantragsteller:in auch diese in der Aufgaben- bzw. Tätigkeitsbeschreibung bzw. Beauftragung.

B.10.03 - Aufgaben und Befugnisse

Überblick
Der:die Zertifizierungsantragsteller:in ergreift Maßnahmen, um sicherzustellen, dass der:die Datenschutzbeauftragte die Position und Aufgaben innerhalb der Organisation ordnungsgemäß wahrnehmen kann.
Detaillierte Anforderungen
***Anwendbarkeit**: Dieses Kriterium gilt, wenn die Voraussetzungen für die Bestellung eines:einer Datenschutzbeauftragten erfüllt sind oder eine freiwillige Bestellung erfolgt.* Der:die Zertifizierungsantragsteller:in stellt die ordnungsgemäße und unabhängige Wahrnehmung der Aufgaben des:der Datenschutzbeauftragten durch geeignete organisatorische Maßnahmen sicher und weist insbesondere nach, dass: ▶ schriftliche Qualifikationsanforderungen festgelegt sowie deren Erfüllung überprüft und dokumentiert werden; ▶ sichergestellt und dokumentiert wird, dass der:die Datenschutzbeauftragte zur Wahrung der Geheimhaltung bzw. Vertraulichkeit verpflichtet ist (z. B. durch eine Vertraulichkeitsvereinbarung); ▶ eine unabhängige und weisungsfreie Aufgabenwahrnehmung gewährleistet ist und keine Tätigkeiten ausgeübt werden, die zu Interessenkonflikten führen; Maßnahmen zur Vermeidung von Interessenkonflikten werden dokumentiert (z. B. schriftliche Erklärung zur Interessenkonfliktfreiheit oder Stellenbeschreibung ohne operative Verantwortlichkeiten); ▶ angemessene zeitliche, organisatorische und finanzielle Ressourcen für die Wahrnehmung der Aufgaben bereitgestellt werden; ▶ die Aufrechterhaltung und Weiterentwicklung der fachlichen Expertise unterstützt wird; ▶ eine ordnungsgemäße und frühzeitige Einbindung in Angelegenheiten und Entscheidungen mit Datenschutzbezug erfolgt und diese dokumentiert wird; ▶ die erfolgte Unterrichtung und Beratung der Organisation nachvollziehbar dokumentiert wird (z. B. anhand von Berichten, Schulungsunterlagen oder vergleichbaren Nachweisen); und ▶ regelmäßig über den Status des Datenschutzmanagements an die oberste Leitungsebene berichtet und diese Berichterstattung dokumentiert wird.

5.11. ÜBERMITTLUNG PERSONENBEZOGENER DATEN IN DRITTLÄNDER ODER AN INTERNATIONALE ORGANISATIONEN

Hinweis: *Die Kriterien in Abschnitt B.11 stellen keinen Zertifizierungsmechanismus gemäß Art. 42 Abs. 2 i. V. m. Art. 46 Abs. 2 lit. f DSGVO dar. Die Zertifizierung bestätigt ausschließlich, dass ein Transferinstrument für die zu zertifizierenden Verarbeitungsvorgänge ausgewählt wurde und dass die damit verbundenen Dokumentationsanforderungen erfüllt wurden.*

B.11.01 – Allgemeine Grundsätze der Datenübermittlung gemäß Art. 44 ff. DSGVO

Überblick
Der:die Zertifizierungsantragsteller:in stellt sicher, dass bei Übermittlungen personenbezogener Daten in Drittländer oder an internationale Organisationen ein geeignetes Übermittlungsinstrument gemäß Kapitel V DSGVO eingesetzt wird und das durch die DSGVO gewährleistete Schutzniveau nicht untergraben wird.
Detaillierte Anforderungen
Anwendbarkeit: *Dieses Kriterium gilt, wenn personenbezogene Daten im Rahmen der zu zertifizierenden Verarbeitungstätigkeiten in Drittländer oder an internationale Organisationen übermittelt werden.* Der:die Zertifizierungsantragsteller:in erstellt eine Standardarbeitsanweisung (SOP), die das Verfahren zur Analyse sämtlicher möglicher Übermittlungsmechanismen, deren Eignung für die jeweilige Verarbeitungstätigkeit gemäß Kapitel V DSGVO sowie die Bewertung der Übermittlungsinstrumente im Hinblick auf die Anforderungen der DSGVO beschreibt. Die SOP umfasst mindestens: ▶ Methoden zur Überprüfung des Bestehens und der Anwendbarkeit von Angemessenheitsbeschlüssen, verbindlichen internen Datenschutzvorschriften (BCR), Standard-Datenschutzklauseln, genehmigten Verhaltensregeln und Zertifizierungsmechanismen; und ▶ Verfahren zur fortlaufenden Überwachung und Überprüfung der Wirksamkeit und Konformität des jeweiligen Übermittlungsinstruments. Für die jeweilige Drittlandübermittlung ist die Anwendbarkeit der herangezogenen Übermittlungsgrundlage zu prüfen und zu dokumentieren. Dies umfasst insbesondere: • **Angemessenheitsbeschluss:** die Anwendbarkeit des Angemessenheitsbeschlusses auf das betreffende Drittland, relevante Gebiete innerhalb des Drittlands oder die internationale Organisation; • **verbindliche interne Datenschutzvorschriften (BCR) gemäß Art. 47 DSGVO:** die Anwendbarkeit der verbindlichen internen Datenschutzvorschriften auf die zu zertifizierenden Verarbeitungsvorgänge und ein Transfer Impact Assessment gemäß Kriterium B.11.06; • **Standard-Datenschutzklauseln:** die Anwendbarkeit der Standard-Datenschutzklauseln auf die vorgesehene Drittlandsübermittlung und ein Transfer Impact Assessment gemäß Durchführungsbeschluss (EU) 2021/914 und Kriterium B.11.06; • **genehmigte Verhaltensregeln gemäß Art. 40 DSGVO:** die Anwendbarkeit des Verhaltenskodex auf die zu zertifizierenden Verarbeitungstätigkeiten und die betreffenden Drittlandsübermittlungen und ein Transfer Impact Assessment gemäß Kriterium B.11.06; • **genehmigter Zertifizierungsmechanismus:** das Bestehen einer gültigen Zertifizierung des:der Zertifizierungsantragstellers:in oder des:der Verantwortlichen gemäß Art. 42 Abs. 2 i. V. m. Art. 46 Abs. 2 lit. f DSGVO und ein Transfer Impact Assessment gemäß Kriterium B.11.06; • **vertragliche Klauseln gemäß Art. 46 Abs. 3 lit. a DSGVO:** die Anwendbarkeit der vertraglichen Regelungen auf die zu zertifizierenden Verarbeitungstätigkeiten und die betreffenden Drittlandsübermittlungen und ein Transfer Impact Assessment gemäß Kriterium B.11.06; und • **Verwaltungsvereinbarungen zwischen Behörden oder öffentlichen Stellen gemäß Art. 46 Abs. 3 lit. b DSGVO:** die Anwendbarkeit der Vereinbarungen auf die zu zertifizierenden Verarbeitungstätigkeiten und die betreffenden Drittlandsübermittlungen und ein Transfer Impact Assessment gemäß Kriterium B.11.06.

B.11.02 - Ausnahmen für bestimmte Fälle

Überblick

Der:die Zertifizierungsantragsteller:in stellt sicher, dass in Abwesenheit eines Angemessenheitsbeschlusses gemäß Art. 45 Abs. 3 DSGVO oder geeigneter Garantien gemäß Art. 46 DSGVO eine Übermittlung personenbezogener Daten in ein Drittland oder an eine internationale Organisation nur erfolgt, wenn die Voraussetzungen einer anwendbaren Ausnahme gemäß Art. 49 DSGVO erfüllt sind.

Detaillierte Anforderungen

***Anwendbarkeit**: Dieses Kriterium gilt, wenn der:die Zertifizierungsantragsteller:in im Rahmen der zu zertifizierenden Verarbeitungstätigkeiten personenbezogene Daten in ein Drittland oder an eine internationale Organisation übermittelt und die Übermittlung auf eine Ausnahme gemäß Art. 49 DSGVO gestützt wird.*

Soweit die Voraussetzungen der jeweiligen Ausnahme durch den:die Verantwortliche:n zu erfüllen sind, erfolgt die Übermittlung auf Grundlage einer entsprechenden dokumentierten Weisung des:der Verantwortlichen.

Ausnahmen gemäß Art. 49 Abs. 1 Unterabs. 1 DSGVO

Stützt sich der:die Zertifizierungsantragsteller:in auf eine ausdrückliche Einwilligung gemäß Art. 49 Abs. 1 lit. a DSGVO, informiert er:sie die betroffenen Personen nachweislich über sämtliche möglichen Risiken im Zusammenhang mit der Datenübermittlung und holt eine wirksame ausdrückliche Einwilligung der betroffenen Personen in die vorgesehene Übermittlung ein.

Bei Anwendung der Ausnahmen gemäß Art. 49 Abs. 1 lit. b bis g DSGVO dokumentiert der:die Zertifizierungsantragsteller:in in jedem Fall die Erforderlichkeit der Datenübermittlung:

- **lit. b**: Ist die Datenübermittlung für die Erfüllung eines Vertrags zwischen der betroffenen Person und dem:der Verantwortlichen oder für die Durchführung vorvertraglicher Maßnahmen auf Antrag der betroffenen Person erforderlich, dokumentiert der:die Zertifizierungsantragsteller:in diese Erforderlichkeit. Bei vorvertraglichen Maßnahmen wird zusätzlich nachgewiesen, dass diese auf Antrag der betroffenen Person durchgeführt werden.
- lit. c: Ist die Datenübermittlung für den Abschluss oder die Erfüllung eines im Interesse der betroffenen Person geschlossenen Vertrags zwischen dem:der Verantwortlichen und einer anderen natürlichen oder juristischen Person erforderlich, dokumentiert der:die Zertifizierungsantragsteller:in die Erforderlichkeit der Übermittlung, das Interesse der betroffenen Person sowie den unmittelbaren und objektiven Zusammenhang zwischen der betroffenen Person und dem Zweck des Vertrags.
- lit. d: Ist die Datenübermittlung aus wichtigen Gründen des öffentlichen Interesses erforderlich, dokumentiert der:die Zertifizierungsantragsteller:in dieses wichtige öffentliche Interesse sowie dessen Anerkennung im Unionsrecht oder im österreichischen Recht.
- lit. e: Ist die Datenübermittlung zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen erforderlich, dokumentiert der:die Zertifizierungsantragsteller:in diese Erforderlichkeit.
- lit. f: Ist die Datenübermittlung zum Schutz lebenswichtiger Interessen der betroffenen Person oder anderer Personen erforderlich und ist die betroffene Person aus physischen oder rechtlichen Gründen außerstande, ihre Einwilligung zu geben, dokumentiert der:die Zertifizierungsantragsteller:in das lebenswichtige Interesse sowie den Umstand der physischen oder rechtlichen Unfähigkeit zur Erteilung einer Einwilligung.
- lit. g: Erfolgt die Datenübermittlung aus einem Register, stellt der:die Zertifizierungsantragsteller:in sicher, dass:
  - das Register nach dem Unionsrecht oder dem österreichischen Recht dazu bestimmt ist, der Öffentlichkeit Informationen bereitzustellen, und entweder allgemein öffentlich zugänglich oder allen Personen zugänglich ist, die ein berechtigtes Interesse nachweisen können;
  - die Daten nur übermittelt werden, soweit die unionsrechtlichen oder österreichischen Voraussetzungen für die Einsichtnahme im konkreten Fall erfüllt sind;
  - die Rechtsgrundlage für die Führung des Registers, die Zugangsbedingungen sowie die Voraussetzungen für Datenübermittlungen aus dem Register geprüft und dokumentiert werden;
  - bei einem vom Nachweis eines berechtigten Interesses abhängigen Zugang das berechtigte Interesse der anfragenden Person nachgewiesen und dokumentiert wird;
  - durch geeignete und nachvollziehbar dokumentierte Maßnahmen verhindert wird, dass das gesamte Register oder vollständige Kategorien der darin enthaltenen personenbezogenen Daten übermittelt werden; und
  - bei einem vom Nachweis eines berechtigten Interesses abhängigen Zugang die Übermittlung nur an die anfragende Person oder nur dann erfolgt, wenn diese Person Empfänger:in der Übermittlung ist.

Detaillierte Anforderungen

Ausnahme gemäß Art. 49 Abs. 1 Unterabs. 2 DSGVO

Eine Übermittlung gemäß Art. 49 Abs. 1 Unterabs. 2 DSGVO erfolgt nur auf Grundlage einer entsprechenden dokumentierten Weisung des:der Verantwortlichen. Dabei ist zu dokumentieren, dass die Übermittlung:

- nicht wiederholt erfolgt;
- nur eine begrenzte Anzahl betroffener Personen betrifft;
- auf zwingenden berechtigten Interessen von Verantwortlichen beruht, die nicht durch die Interessen oder Rechte und Freiheiten der betroffenen Personen überwogen werden; und
- auf einer Bewertung der Umstände der Übermittlung durch Verantwortliche beruht und geeignete Garantien zum Schutz personenbezogener Daten vorgesehen wurden.

Die nach Art. 49 Abs. 1 Unterabs. 2 DSGVO erforderliche Bewertung und die vorgesehenen geeigneten Garantien sind entsprechend den gesetzlichen Anforderungen zu dokumentieren.

Die Prüfung und die vorgesehenen geeigneten Garantien werden gemäß Art. 49 Abs. 6 DSGVO im Verzeichnis von Verarbeitungstätigkeiten nach Art. 30 DSGVO dokumentiert.

B.11.03 - Information der Aufsichtsbehörde über eine Datenübermittlung

Überblick

Der:die Zertifizierungsantragsteller:in dokumentiert die Information der zuständigen Aufsichtsbehörde über eine Datenübermittlung.

Detaillierte Anforderungen

***Anwendbarkeit**: Dieses Kriterium gilt, wenn im Rahmen der zu zertifizierenden Verarbeitungstätigkeiten eine Übermittlung personenbezogener Daten gemäß Art. 49 Abs. 1 Unterabs. 2 DSGVO erfolgt.*

Der:die Auftragsverarbeiter:in dokumentiert bei einer Übermittlung gemäß Art. 49 Abs. 1 Unterabs. 2 DSGVO die Information der zuständigen Aufsichtsbehörde und hält einen Nachweis darüber vor.

B.11.04 - Dokumentation der Datenübermittlungen

Überblick

Der:die Zertifizierungsantragsteller:in dokumentiert die im Rahmen der zu zertifizierenden Verarbeitungstätigkeiten vorgenommenen Übermittlungen personenbezogener Daten in Drittländer oder an internationale Organisationen.

Detaillierte Anforderungen

***Anwendbarkeit**: Dieses Kriterium gilt, wenn der:die Zertifizierungsantragsteller:in im Rahmen der zu zertifizierenden Verarbeitungstätigkeiten personenbezogene Daten in ein Drittland oder an eine internationale Organisation übermittelt.*

Der:die Zertifizierungsantragsteller:in dokumentiert die zu zertifizierenden Verarbeitungstätigkeiten, in deren Rahmen personenbezogene Daten in Drittländer oder an internationale Organisationen übermittelt werden, sodass die Zulässigkeit der Übermittlungen nachvollzogen und die Erfüllung der datenschutzrechtlichen Pflichten, einschließlich der Unterstützung des:der Verantwortlichen bei der Bearbeitung von Betroffenenanfragen, sichergestellt werden kann.

Die Dokumentation enthält folgende Informationen: die Arten der betreffenden Daten, die betroffenen Drittländer (einschließlich Transitländer), ob die Übermittlung auf einem Angemessenheitsbeschluss beruht oder — andernfalls — auf welchen geeigneten Garantien gemäß Art. 46 DSGVO, und die für die Übermittlung verwendeten Technologien.

B.11.05 - Regelmäßige Überprüfung der Zulässigkeit der Datenübermittlung

Überblick
Der:die Zertifizierungsantragsteller:in überprüft regelmäßig die Zulässigkeit der von ihm:ihr vorgenommenen Übermittlungen personenbezogener Daten in Drittländer oder an internationale Organisationen gemäß Art. 44 bis 49 DSGVO.
Detaillierte Anforderungen
***Anwendbarkeit**: Dieses Kriterium gilt, wenn der:die Zertifizierungsantragsteller:in im Rahmen der zu zertifizierenden Verarbeitungstätigkeiten personenbezogene Daten in ein Drittland oder an eine internationale Organisation übermittelt.* Der:die Zertifizierungsantragsteller:in überprüft und bewertet mindestens einmal jährlich das angemessene Schutzniveau bzw. die Zulässigkeit der Datenübermittlungen gemäß Art. 44–49 DSGVO für die zu zertifizierenden Verarbeitungstätigkeiten. Dabei werden interne und externe Faktoren berücksichtigt, die die Gültigkeit der gewählten Übermittlungsinstrumente beeinflussen können. Hierzu zählen insbesondere Änderungen des einschlägigen Rechtsrahmens, unternehmerische Veränderungen wie Outsourcing, Fusionen oder Übernahmen, Änderungen der Datenschutzpraktiken, der Einsatz neuer Technologien sowie sonstige organisatorische oder technische Änderungen. Die Bewertung umfasst mindestens: ▶ die Aktualität und Anwendbarkeit eines herangezogenen Angemessenheitsbeschlusses gemäß Art. 45 DSGVO; ▶ das Fortbestehen und die Wirksamkeit geeigneter Garantien gemäß Art. 46 DSGVO einschließlich gegebenenfalls erforderlicher ergänzender Maßnahmen; ▶ bei einer Übermittlung auf Grundlage einer Ausnahme gemäß Art. 49 DSGVO das Fortbestehen der Voraussetzungen für deren Anwendung unter Berücksichtigung der dokumentierten Weisungen von Verantwortlichen sowie ▶ relevante Änderungen bei eingesetzten Unterauftragsverarbeiter:innen, sonstigen Datenimporteuren, Übermittlungswegen sowie den technischen, organisatorischen oder vertraglichen Rahmenbedingungen der Übermittlung. Sofern ein:e Datenschutzbeauftragte:r benannt ist, wird die Stellungnahme in die Bewertung einbezogen. Die Ergebnisse der Überprüfung werden dokumentiert.

B.11.06 - Bewertung der Wirksamkeit des gewählten Übermittlungsinstruments gemäß Art. 46 DSGVO

Überblick
Der:die Zertifizierungsantragsteller:in stellt durch ein „Transfer Impact Assessment“ sicher, dass das durch die DSGVO gewährleistete Schutzniveau durch die Übermittlung personenbezogener Daten in Drittländer oder an internationale Organisationen nicht untergraben wird.
Detaillierte Anforderungen
***Anwendbarkeit**: Dieses Kriterium gilt, wenn der:die Zertifizierungsantragsteller:in im Rahmen der zu zertifizierenden Verarbeitungstätigkeiten personenbezogene Daten in ein Drittland oder an eine internationale Organisation übermittelt und die Übermittlung auf geeignete Garantien gemäß Art. 46 DSGVO gestützt wird.* Der:die Zertifizierungsantragsteller:in prüft, ob die Wirksamkeit der geeigneten Garantien des gemäß Art. 46 DSGVO gewählten Übermittlungsinstruments im Kontext der beabsichtigten Übermittlung durch die im Drittland geltenden Gesetze oder Praktiken beeinträchtigt werden kann. Erfolgt die Datenübermittlung aufgrund eines Angemessenheitsbeschlusses der Europäischen Kommission oder einer Ausnahme gemäß Art. 49 DSGVO, ist kein Transfer Impact Assessment erforderlich. Im Rahmen des Transfer Impact Assessments werden mindestens folgende Aspekte in strukturierter Form (z. B. anhand eines Fragebogens) berücksichtigt und dokumentiert: ▶ konkrete Umstände der Datenübermittlung: Identifikation des Datenexporteurs und Datenimporteurs sowie Rechtsgrundlage der Datenübermittlung gemäß Art. 44 ff. DSGVO; ▶ Übermittlungsumstände: Kategorien personenbezogener Daten (z. B. Arbeitnehmer:innen, Kund:innen), Arten der übermittelten Daten (z. B. E-Mail-Adressen, IP-Adressen), Häufigkeit der Übermittlung (z. B. einmalig, gelegentlich), Übermittlungsmethode (z. B. E-Mail, Secure File Transfer Protocol, Remote-Zugriff); ▶ Anwendbares Recht des Bestimmungslandes: Beschreibung der relevanten Gesetze für die Verarbeitung im Drittland, einschließlich Übersicht über Gesetze, die staatliche Stellen betreffen; ▶ Bewertung der Rechtslage im Drittland: Bewertung, inwieweit die Rechtsvorschriften im Drittland den Schutz der personenbezogenen Daten und der Rechte betroffener Personen gewährleisten;

Detaillierte Anforderungen

- Risiken für betroffene Personen: Bewertung der inhärenten Risiken, die sich aus der geplanten Verarbeitung im Drittland für betroffene Personen ergeben;
- Risiko behördlicher Zugriffe, soweit zutreffend: Bewertung der Rechtslage im Drittland hinsichtlich der Wahrscheinlichkeit eines Zugriffs staatlicher Stellen (z. B. im Fall der USA Prüfung, ob Datenempfänger:innen als Anbieter:innen elektronischer Kommunikationsdienste einzustufen sind und ob sie personenbezogene Daten im Klartext einsehen können); und
- Schlussfolgerung: abschließende Bewertung, ob die Verarbeitung im Drittland den Anforderungen der DSGVO und der Rechtsprechung des EuGH entspricht (für die abschließende Bewertung kann ein Scoring-Modell oder eine Risikomatrix verwendet werden, um den Entscheidungsprozess für Dritte nachvollziehbar zu machen);

Ergibt die Bewertung, dass das gewählte Übermittlungsinstrument kein ausreichendes Schutzniveau gewährleistet, werden ergänzende technische, organisatorische oder vertragliche Maßnahmen umgesetzt und dokumentiert.

Der:die Zertifizierungsantragsteller:in überprüft die dem Transfer Impact Assessment zugrunde liegende Bewertung in angemessenen Abständen sowie anlassbezogen, wenn Entwicklungen im Drittland oder Änderungen der Übermittlung die ursprüngliche Bewertung oder die Wirksamkeit der getroffenen Maßnahmen beeinflussen können.

Der:die Zertifizierungsantragsteller:in stellt sicher, dass die Übermittlung ausgesetzt oder beendet wird, wenn der Datenimporteur seine Verpflichtungen aus dem Übermittlungsinstrument gemäß Art. 46 DSGVO nicht mehr erfüllen kann oder die getroffenen ergänzenden Maßnahmen nicht mehr wirksam sind.

WE SEARCH FOR GREATNESS.

BDO Consulting GmbH
QBC 4 – Am Belvedere 4
(Eingang Karl-Popper-Straße 4)
1100 Wien

bdo.at