ANNEX I

Allgemeine Kriterien für die Zertifizierung

betreffend die

TOMs - Technische und organisatorische Maßnahmen

Version 1.3 vom 29.3.2024

DSGVO-zt GmbH

Inhaltsverzeichnis

1. Präambel

Dieses Dokument enthält die technischen und organisatorischen Maßnahmen, auf die unter Punkt 8. der Allgemeinen Zertifizierungskriterien Bezug genommen wird.

2. Überprüfung der Reife der Organisation des Zertifizierungsantragstellers

Die Zertifizierungsstelle verlangt als grundlegendes Kriterium die Umsetzung der DSGVO in der Organisation des Zertifizierungsantragstellers.

In einem ersten Schritt prüft sie deren Umsetzung innerhalb der Organisation des Zertifizierungsantragstellers mit Fokus auf das Zertifizierungsobjekt. Der Grund für dieses Vorgehen ist, dass eine Organisation die DSGVO-Anforderungen für den Zertifizierungsgegenstand nur dann erfüllen kann, wenn sie selbst über ausreichende Kenntnisse der DSGVO-Anforderungen verfügt und die DSGVO bereits in der entsprechenden Tiefe umgesetzt hat.

3. Überprüfung der Reife der Organisation des Zertifizierungsantragstellers

Die Zertifizierungsstelle verlangt als grundlegendes Kriterium die Umsetzung der Datenschutzgrundverordnung in der Organisation des Zertifizierungsantragstellers.

In einem ersten Schritt prüft sie deren Umsetzung in der Organisation des Zertifizierungsantragstellers mit Fokus auf den Zertifizierungsgegenstand. Der Grund für dieses Vorgehen ist, dass eine Organisation die DSGVO-Anforderungen für den Zertifizierungsgegenstand nur dann erfüllen kann, wenn sie selbst genügend Wissen über die DSGVO-Anforderungen hat und die DSGVO bereits in der entsprechenden Tiefe umgesetzt hat.

Der Auftraggeber hat Maßnahmen gemäß Punkt 8. der Allgemeinen Zertifizierungskriterien umzusetzen. Die umgesetzten Maßnahmen müssen dem aktuellen Stand der Technik entsprechen. Der Stand der Technik ist vor jeder Evaluierung aus allgemein anerkannten Normen und Richtlinien, insbesondere aus der "Handreichung zum Stand der Technik" (https://www.teletrust.de/publikationen/broschueren/stand-der-technik/). des Bundesverbandes IT-Sicherheit e.V. (TeleTrusT) in der jeweils neuesten Fassung.

Der Kunde muss die folgenden Themenbereiche berücksichtigen:

1. Bauliche und infrastrukturelle Maßnahmen 4.1)
2. Zugangskontrolle 4.2)
3. Datenträgerkontrolle 4.3)
4. Organisation des Datenschutzes 4.4)
5. Ausbildungsmaßnahmen 4.5)
6. Benutzerkontrolle 4.6)

7. Zugangskontrolle 4.7)
8. Übertragungssteuerung 4.8)
9. Eingangskontrolle 4.9)
10. Speicherkontrolle 4.10)
11. Transportkontrolle 4.11)
12. Wiederherstellung 4.12)
13. Verlässlichkeit und Datenintegrität 4.13)

Die Schutzmaßnahmen sind im Rahmen der Zertifizierungsanforderungen festzulegen. Sie sind in regelmäßigen Abständen zu überprüfen und an den aktuellen Stand der Technik anzupassen.
Die Auswahl und Durchführung der Schutzmaßnahmen, die Überprüfung ihrer Wirksamkeit und Aktualität sowie die durchgeführten Verbesserungen und Korrekturen sind vom Auftraggeber anhand geeigneter Unterlagen nachzuweisen. Hierzu können insbesondere Aufzeichnungen aus dem Auswahlverfahren, Umsetzungsdokumentationen, interne Bewertungen der

3.1 Strukturelle und infrastrukturelle Maßnahmen

Der Auftraggeber hat geeignete und angemessene Maßnahmen veranlasst, um sicherzustellen, dass Risiken für die Sicherheit des Zertifizierungsobjekts und der darin enthaltenen personenbezogenen Daten bereits im Vorfeld des Betriebs reduziert werden. Zu diesem Zweck wurden bauliche und/oder infrastrukturelle Maßnahmen umgesetzt.
Beispiele für solche Maßnahmen sind u.a. die geeignete Auswahl des Betriebsortes, die Abtrennung und Aufteilung von Sicherheitsbereichen, Maßnahmen zum Einbruch- und Brandschutz oder die geeignete Verlegung von Versorgungs- und Kommunikationsleitungen.
Ziel der Maßnahmen ist es, das Grundrisiko generell zu verringern und die Wirksamkeit der anderen Schutzmaßnahmen zu verbessern. Sie sind so zu gestalten, dass in Kombination mit den anderen Schutzmaßnahmen das Risiko so gering wie möglich bleibt.

3.2 Zugangskontrolle

Der Kunde muss über geeignete und angemessene Maßnahmen verfügen, um sicherzustellen, dass nur befugte Nutzer Zugang zu den personenbezogenen Daten haben, die Gegenstand der Zertifizierung sind. Zu diesem Zweck werden strukturelle, technische und/oder organisatorische Maßnahmen ergriffen.
Beispiele für solche Maßnahmen sind die bauliche Trennung von Gäste- und Besucherbereichen, die Verpflichtung zum Tragen von Besucherausweisen oder elektronische Schließsysteme, die den Zugang zu Sicherheitsbereichen protokollieren.
Die Maßnahmen verfolgen den Zweck, den Zugriff auf zentrale IT-Komponenten (insbesondere

Server, Speichersysteme, Netzwerkkomponenten) sowie relevante Kundensysteme und Netzwerkzugänge des Auftraggebers so zu beschränken, dass Unbefugte keinen Zugang zu diesen Angriffspunkten erhalten. Sie sind so zu gestalten, dass das Risiko minimal bleibt.

3.3 Datenträgerkontrolle

Der Auftraggeber hat durch geeignete und angemessene Maßnahmen sicherzustellen, dass das unbefugte Lesen, Kopieren, Verändern oder Entfernen von Datenträgern verhindert wird. Dabei sind je nach den jeweiligen Gegebenheiten sowohl elektronische Datenträger als auch andere Speichermedien wie insbesondere Papierdokumente zu berücksichtigen.
Beispiele für solche Maßnahmen sind die sichere Aufbewahrung sensibler Datenträger in einem Datenträgerarchiv, die Protokollierung der Nutzung von Datenträgern und die Regelung der Entsorgung oder Löschung von Datenträgern in elektronischer oder Papierform.
Zweck der Maßnahmen ist es, den unbefugten Zugriff auf personenbezogene Informationen des Zertifizierungsobjekts, die auf den Datenträgern des Auftraggebers gespeichert sind, in jeder Form zu verhindern. Sie sind so zu gestalten, dass das Risiko minimal bleibt.

3.4 Organisation des Datenschutzes

Der Auftraggeber ergreift geeignete und angemessene Maßnahmen, um eine sicherheitsbewusste und korrekte Handhabung der Datenschutzaufgaben im Zusammenhang mit den Verarbeitungsvorgängen des Zertifizierungsobjekts zu gewährleisten.
Beispiele für solche Maßnahmen sind u. a. der Erlass einer Datenschutzpolitik, die Zuweisung von Rollen und Zuständigkeiten und die Festlegung von Richtlinien, die das Nutzerverhalten in wichtigen Datenschutzfragen steuern.
Zweck der Maßnahmen ist es, durch organisatorische Regelungen die Einhaltung der datenschutzrechtlichen Pflichten, insbesondere im Bereich der Sicherheit, zu gewährleisten. Sie sind so zu gestalten, dass das Risiko minimal bleibt.

3.5 Ausbildungsmaßnahmen

Der Auftraggeber ergreift geeignete und angemessene Maßnahmen, um ein sicherheitsbewusstes und korrektes Verhalten der im Bereich des Zertifizierungsobjekts tätigen Mitarbeiter zu gewährleisten.
Beispiele für solche Maßnahmen sind insbesondere die Durchführung geeigneter Schulungen zu Sicherheitsmaßnahmen, die Sensibilisierung der Mitarbeiter für Fragen des Datenschutzes und der Informationssicherheit sowie die Sensibilisierung der Mitarbeiter für die bestehenden Regelungen.
Ziel der Maßnahmen ist es, die Einhaltung der vorgesehenen Schutzmaßnahmen und das sichere Verhalten der Beschäftigten zu gewährleisten und Fehlverhalten zu verhindern. Sie sind so zu gestalten, dass das Risiko minimal bleibt.

3.6 Benutzerkontrolle

Der Auftraggeber trifft geeignete und angemessene Maßnahmen, um die Nutzung von Verarbeitungssystemen im Rahmen des Zertifizierungsgegenstandes durch Unbefugte mit Hilfe von Datenübertragungseinrichtungen zu verhindern. Zu diesem Zweck werden technische und organisatorische Maßnahmen getroffen.

Beispiele für solche Maßnahmen sind der Einsatz von Firewalls, geeignete Authentifizierungsmaßnahmen und die Bestimmung der zur Nutzung des Systems berechtigten Mitarbeiter.
Die Maßnahmen richten sich gegen den Zugriff von Unbefugten auf die für die Produktion genutzten IT-Systeme. Sie müssen so gestaltet sein, dass das Risiko minimal bleibt.

3.7 Zugangskontrolle (umbenannt in Berechtigungskonzept – WF)

Der Kunde muss geeignete und angemessene Maßnahmen ergreifen, um sicherzustellen, dass die Nutzer nur auf die personenbezogenen Daten zugreifen können, die unter das Zertifizierungsobjekt fallen und die ihren Zugriffsberechtigungen entsprechen. Diese Berechtigungen sind so einzurichten, dass sie nicht über den tatsächlichen Bedarf hinausgehen, der sich aus der vorgesehenen Funktion des Nutzers ergibt.
Beispiele für solche Maßnahmen sind die Definition eines Berechtigungskonzepts nach dem Needto-know-Prinzip, die Protokollierung der Erteilung und des Entzugs von Zugangsberechtigungen sowie die Protokollierung von Benutzerzugriffen.
Die Maßnahmen verfolgen den Zweck, den unbefugten und unrechtmäßigen Zugriff von Nutzern auf personenbezogene Daten zu verhindern und gleichzeitig deren Aufgabenerfüllung sicherzustellen. Sie sind so zu gestalten, dass das Risiko minimal bleibt.

3.8 Kontrolle der Übertragung

Der Auftraggeber stellt durch geeignete und zumutbare Maßnahmen sicher, dass die Übermittlung oder Bereitstellung personenbezogener Daten mittels Datenübertragungseinrichtungen überprüft, festgestellt und nachvollzogen werden kann. Zu diesem Zweck sind technische und organisatorische Maßnahmen zu treffen.
Beispiele für solche Maßnahmen sind geeignete Verfahren für die Übermittlung von Informationen, die Festlegung und Dokumentation von Übertragungswegen und Empfängern sowie die Verwendung von Protokollierungs- und Verschlüsselungsverfahren für die elektronische Datenübermittlung.
Ziel der Maßnahmen ist es, die Übermittlung personenbezogener Daten einerseits zu sichern und andererseits nachvollziehbar zu machen. Sie sind so zu gestalten, dass das Risiko minimal bleibt.

3.9 Eingabekontrolle

Der Auftraggeber muss durch geeignete und angemessene Maßnahmen sicherstellen, dass nachträglich überprüft und festgestellt werden kann, welche personenbezogenen Daten zu welchem Zeitpunkt und von wem in Verarbeitungsvorgänge im Rahmen des Zertifizierungsgegenstandes eingegeben worden sind. Zu diesem Zweck werden technische und organisatorische Maßnahmen eingesetzt.
Beispiele für solche Maßnahmen sind die Protokollierung von Nutzeraktivitäten, Maßnahmen zum Schutz der Protokolle vor Veränderung oder Löschung sowie Vorschriften oder technische Vorkehrungen für die Protokollauswertung.

Zweck der Maßnahmen ist es, die Nachvollziehbarkeit der Verarbeitung personenbezogener Daten des Zertifizierungsobjekts zu gewährleisten. Sie sind so zu gestalten, dass das Risiko minimal bleibt.

3.10 Kontrolle der Lagerung

Der Auftraggeber hat geeignete und angemessene Maßnahmen zu ergreifen, um einen unbefugten Zugriff auf die im Rahmen der Verarbeitung des Zertifizierungsobjekts gespeicherten personenbezogenen Daten zu verhindern. Dies betrifft sowohl den Lese- und Schreibzugriff als auch die Löschung von Daten.
Beispiele für solche Maßnahmen sind die Verwendung von Authentifizierungsmaßnahmen, die Protokollierung von Nutzeraktivitäten oder die Verwendung von Verschlüsselung.
Zweck der Maßnahmen ist es, alle Arten von unbefugten Änderungen oder Zugriffen auf gespeicherte Daten des Zertifizierungsobjekts zu verhindern. Sie müssen so gestaltet sein, dass das Risiko minimal bleibt.

3.11 Transportkontrolle

Der Auftraggeber hat durch geeignete und angemessene Maßnahmen sichergestellt, dass bei der Übermittlung von Daten und dem Transport von Datenträgern keine personenbezogenen Daten aus Verarbeitungsvorgängen des Zertifizierungsobjekts unbefugt gelesen, kopiert, verändert oder gelöscht werden können.
Beispiele für solche Maßnahmen sind die Beauftragung zuverlässiger Transportunternehmen, die Verwendung sicherer Transportbehälter und der Einsatz geeigneter Verschlüsselungstechniken und -methoden im Rahmen der Datenübertragung.
Die Maßnahmen sollen alle Arten von unbefugtem Zugriff verhindern, die während der Datenübertragung oder des Datenträgertransports auftreten können. Sie sind so zu gestalten, dass das Risiko so gering wie möglich ist.

3.12 Wiederherstellung

Der Kunde muss über geeignete und angemessene Maßnahmen verfügen, um sicherzustellen, dass im Falle eines Ausfalls die Verarbeitungsvorgänge und personenbezogenen Daten des Zertifizierungsobjekts wiederhergestellt werden können. Die Wiederherstellung der Daten und die Wiederaufnahme des Betriebs müssen innerhalb eines Zeitraums möglich sein, der kurz genug ist, um vorhersehbare Schäden für die betroffenen Personen zu vermeiden.
Beispiele für solche Maßnahmen sind die regelmäßige Datensicherung im Rahmen eines Datensicherungs- und Wiederherstellungskonzepts, die Einführung eines Notfallvorsorgekonzepts
und die Durchführung von regelmäßigen Notfall- und Wiederherstellungsübungen.
Die Maßnahmen sollen den Verlust personenbezogener Daten und Schäden, die sich aus der mangelnden Verfügbarkeit ergeben können, verhindern. Sie sind so zu gestalten, dass das Risiko gering bleibt.

3.13 Verlässlichkeit und Datenintegrität

Der Auftraggeber trifft geeignete und angemessene Maßnahmen, um sicherzustellen, dass auftretende Störungen erkannt und gemeldet werden und dass die vom Zertifizierungsgegenstand erfassten personenbezogenen Daten nicht durch Störungen beschädigt werden. Zu diesem Zweck sind technische und organisatorische Maßnahmen zu ergreifen.
Beispiele für solche Maßnahmen sind der Einsatz technischer Lösungen zur Abwehr von Schadsoftware, Systeme zur Erkennung und Verhinderung von Eindringlingen sowie die Einführung eines Systemüberwachungskonzepts.
Zweck der Maßnahmen ist es, Beeinträchtigungen der Datenintegrität zu verhindern und durch rechtzeitiges Erkennen von Störungen oder Fehlern den sicheren Betrieb der Verarbeitungsprozesse zu gewährleisten. Sie sind so zu gestalten, dass das Risiko minimal bleibt.