Anlage zu Anhang I

zu den

Allgemeinen Kriterien für die Zertifizierung

Betreffend die

TOMs -Technische und organisatorische Maßnahmen

Zertifizierungsanforderungen

Version 2.0 vom 14.08.2024

DSGVO-**zt** GmbH

I N H A L T S V E R Z E I C H N I S

1 Präambel

Dieses Dokument spezifiziert Anforderungen für die in Anhang I aufgeführten technischen und organisatorischen Maßnahmen.

Diese Anforderungen werden laufend an aktuelle Entwicklungen angepasst, insbesondere im Hinblick auf die Einstufung des Schutzbedarfs, die Erkennung neuer Bedrohungen und den Stand der Technik. Die Überprüfung erfolgt mindestens einmal pro Jahr oder ad hoc.

2 Maßnahmen

Der Kunde wählt geeignete Maßnahmen gemäß Punkt 8. der Allgemeinen Zertifizierungskriterien. Die korrekte Umsetzung der getroffenen Maßnahmen wird von der Zertifizierungsstelle gemäß Art. 43 DSGVO überprüft.

Die Durchführung der Sicherheitsmaßnahmen, die Überprüfung ihrer Wirksamkeit und Aktualität sowie durchgeführte Verbesserungen und Korrekturen sind vom Auftraggeber durch eine geeignete Dokumentation nachzuweisen.

2.1 Bauliche und infrastrukturelle Maßnahmen

N°	Maßnahme	Erläuterung
2.1.1	Bauliche und infrastrukturelle Maßnahmen	Bauliche Maßnahmen umfassen Themen wie Standortwahl, Einbruchschutz, Brandschutz oder Perimeterschutz. Infrastrukturelle Maßnahmen betreffen die Streckenführung von Kabel, geeignete Aufstellungsorte, Aufteilung der Teilsysteme in "Käfige" usw.

2.2 Physischer Zugang

Je nach dem Schutzbedarf der verarbeiteten Informationen sowie den zu erwartenden Risiken, den vorhandenen Gegebenheiten und der Anwendbarkeit auf die Verarbeitungen des Zertifizierungsgegenstandes sind die folgenden Maßnahmen zu ergreifen:

N°	Maßnahme	Erläuterung
2.2.1	Anmeldung an der Rezeption mit Identitätskontrolle	Identifizierung und Kontrolle: Beim Betreten des Firmengeländes müssen alle unternehmensfremden Personen (Besucher, Kunden, Dienstleister, Zulieferer...) identifiziert und der Grund des Besuchs sowie die Kontaktperson vermerkt werden. Diese Maßnahme ist für mittlere bis hohe Schutzbedürfnisse gedacht. Sie ist nicht erforderlich, wenn geeignete technische Schutz- und Überwachungsmaßnahmen zur Sicherung gefährdeter Bereiche vorhanden sind und eine bauliche Trennung zwischen Besuchs- und Arbeitsbereich besteht.
2.2.2	Tragen von Firmen-/Besucherausweisen	Die Pflicht zum sichtbaren Tragen von Firmen- und Besucherausweisen stellt eine ergänzende Schutzmaßnahme zu 2.2.1 dar. Diese Maßnahme ist für ein mittleres bis hohes Schutzbedürfnis mit einer größeren Anzahl von Beschäftigten und verteilten Standorten vorgesehen.
2.2.3	Begleitung von Besuchern im Firmengebäude	Diese Maßnahme sollte in Ergänzung zu 2.2.2 durchgeführt werden. Die zuverlässige Einhaltung durch die Mitarbeiter muss durch Richtlinien, Anweisungen und Schulungen sichergestellt werden. Diese Maßnahme ist für ein mittleres bis hohes Schutzbedürfnis vorgesehen.

2.2.4	Wachdienst	Die Räumlichkeiten müssen von einem Sicherheitsdienst auf unbefugte Personen kontrolliert werden, insbesondere außerhalb der Betriebszeiten. Die Maßnahme ist insbesondere für ein mittleres bis hohes Schutzniveau vorgesehen. Sie kann durch geeignete technische Schutz- und Überwachungsmaßnahmen ersetzt werden - siehe 2.2.5.
2.2.5	Technische Schutz- und Überwachungsmaßnahmen	Technische Sicherheitsmaßnahmen können alternativ oder zusätzlich zu einem Wachdienst (2.2.4) zur Sicherung der Räumlichkeiten, insbesondere außerhalb der Betriebszeiten, eingesetzt werden. Dazu gehören u.a. die Videoüberwachung des Geländes, Schließ- und Alarmanlagen, Personentrennsysteme sowie einbruchsichere Sicherungsmaßnahmen wie Mauern, Zäune und Schranken.
2.2.6	Passwortpolitik mit Passwörter-Qualitätsprüfung	Die Sicherheit der Benutzerauthentifizierung muss durch eine Passwortpolitik gewährleistet werden, die die Benutzer bei der Erstellung sicherer Passwörter unterstützt und den richtigen Umgang mit Passwörtern regelt. Darüber hinaus muss durch technische Maßnahmen sichergestellt werden, dass ausreichend lange und komplexe Passwörter gewählt werden. Weitere Vorgaben zur technischen Sicherheit (Sperrung von Konten nach mehrfacher Falschanmeldung, automatische Aufhebung der Kontosperre, Passwortänderungsintervalle etc.) sind je nach Anwendung, technischem und organisatorischem Umfeld sowie Schutzbedarf zu treffen. Die Maßnahme muss durch Schulungs- und Sensibilisierungsmaßnahmen für die Nutzer unterstützt werden (siehe Kapitel 2.5).
2.2.7	Regelmäßige Überprüfung der Zugangsberechtigungen	Dies betrifft sowohl den physischen (Schlüssel usw.) als auch den elektronischen Zugang (Passwörter, Schlüsselcodes, ...), wobei Auf die Abstimmung zwischen den beiden muss geachtet werden. Für das Betreten, Verlassen und den Wechsel des Arbeitsplatzes von Arbeitnehmern sind entsprechende Vorkehrungen zu treffen (siehe auch 2.2.11 und 2.7.9).
2.2.8	Protokollierung der physischen Zugänge und Ausgänge	Die Protokollierung kann zusätzlich zu 2.2.1 oder auf der Basis von elektronischen Schließanlagen erfolgen. Diese Maßnahmen sind insbesondere für IT-Sicherheitsbereiche (Serverräume, Netzwerkverteiler) vorgesehen. Erforderlichenfalls muss sie von arbeitsrechtlichen Maßnahmen begleitet werden (BV, individuelle Vereinbarung).

2.29	Protokollierung von System- und -abmeldungen sowie von Anmeldeversuchen am Zertifizierungsgegenstand	Siehe Punkte 2.6.4, 2.7.4, 2.7.11 und 2.7.15
2.2.10	Protokollierung von System- und -abmeldungen sowie von Anmeldeversuchen am Zertifizierungsgegenstand	Siehe Punkte 2.6.4, 2.7.4, 2.7.11 und 2.7.15
2.2.10	Zugangsbeschränkungen für sensible Unternehmensbereiche	Die Maßnahme ist insbesondere für IT-Sicherheitsbereiche (Serverräume, Netzwerkverteiler) sowie Räume, in denen Datenträger mit hohem Schutzbedarf (z.B. Sicherungsmedien, Patientenakten) gelagert werden, vorgesehen. Maßnahmen nach Die Nummern 2.2.7 und 2.2.8 sollten hinzugefügt werden.
2.2.11	Festlegung der zur Nutzung der Netzzugänge berechtigten Personen	Es sind organisatorische Maßnahmen zu treffen, um festzustellen, welche Personen zur Nutzung der Netzzugänge berechtigt sind. Zu diesem Zweck werden Verfahren für die Erteilung, den Widerruf und die regelmäßige Überprüfung von Berechtigungen festgelegt.
2.2.12	Bildschirmsperre beim Verlassen des Arbeitsplatzes	Die Arbeitnehmer müssen verpflichtet werden, die Bildschirmsperre zu aktivieren, wenn sie ihren Arbeitsplatz verlassen. Dies kann zusätzlich zu den automatischen Bildschirmsperren (2.7.2) erfolgen und ist insbesondere für einen mittleren bis hohen Schutzbedarf vorgesehen.
2.2.13	Clear-Desk-Policy	Der unbefugte Zugang zu sensiblen Daten kann durch eine "Clear-Desk-Policy" verhindert werden, die die Nutzer dazu verpflichtet, alle Datenträger und Papierdokumente mit vertraulichem Inhalt zu entfernen und sicher zu verwahren, wenn der Arbeitsplatz nicht besetzt ist. Je nach baulicher und betrieblicher Situation gilt dies sowohl für den Zugriff externer Personen als auch für den anderer Mitarbeiter. Diese Maßnahme ist insbesondere für mittlere bis hohe Schutzbedürfnisse gedacht.

2.3 Datenträgerkontrolle

Je nach dem Schutzbedarf der verarbeiteten Informationen sowie den zu erwartenden Risiken, den vorhandenen Gegebenheiten und der Anwendbarkeit auf die Verarbeitungen des Zertifizierungsgegenstandes sind die folgenden Maßnahmen zu ergreifen:

N°	Maßnahme	Erläute-

2.3.1	Datenträgerarchiv, Bestandskontrolle und sichere Aufbewahrung von Speichermedien	Im Rahmen eines Datenträgerarchivs müssen alle Datenträger gesichert werden, deren unberechtigte Manipulation oder Verlust mit einem mittleren bis hohen Risiko verbunden ist. Die Bestandskontrolle dient als Unterstützung bei der Erkennung von Sicherheitsvorfällen. Das Archiv muss vor unberechtigtem Zugriff und möglichen Gefährdungen durch Feuer, Wasser, Naturkatastrophen etc. ausreichend geschützt sein.
2.3.2	Protokollierung des autorisierten Transfers von Datenträgern	Die Protokollierung des Datenträgertransfers

2.3.3	Kontrolle kopieren	Papierdokumente: Papierdokumente dürfen nur für unbedingt notwendige interne Vorgänge kopiert werden. Das Kopieren und insbesondere die Weitergabe von Dokumenten (z.B. an das Home-Office) sollte durch Genehmigungsverfahren geregelt werden, die dem jeweiligen Schutzbedarf angepasst sind. Elektronische Dokumente: Durch technische Maßnahmen, insbesondere zur Regelung der Nutzung von Wechseldatenträgern, kann das Kopieren von Daten auf bestimmte Benutzer, Arbeitsplätze oder autorisierte Datenträger beschränkt werden. Diese Maßnahme muss immer von einer technischen Protokollierung
2.3.4	Datenschutzkonforme	Es müssen geeignete Möglichkeiten zur Entsorgung von Datenträgern zur Verfügung gestellt werden (Shredder, gesicherte Entsorgungsbehälter) und verbindliche organisatorische Regelungen getroffen werden. Die nicht mehr benötigten Datenträger müssen auf sichere Weise entsorgt werden. Dazu gehört entweder eine Entsorgungsbestätigung durch zertifizierte Entsorgungspartner oder die Dokumentation und Protokollierung der innerbetrieblichen Entsorgung durch den Mitarbeiter, der die Entsorgung durchführt.
2.3.5	Wiederverwendung von Datenträgern	Vor der Wiederverwendung gebrauchter Datenträger müssen deren Inhalte mit technischen Mitteln unwiederbringlich gelöscht werden. Das genaue Verfahren ist im Rahmen eines Organisationsreglements verbindlich zu regeln.

2.4 Organisation des Datenschutzes

Je nach dem Schutzbedarf der verarbeiteten Informationen sowie den zu erwartenden Risiken, den vorhandenen Gegebenheiten und der Anwendbarkeit auf die Verarbeitungen des Zertifizierungsgegenstandes sind die folgenden Maßnahmen zu ergreifen:

2.4.1	Datenschutzpolitik	In Form einer Erklärung, die von der obersten Leitung in Kraft gesetzt und intern veröffentlicht wird, werden grundlegende Ziele und Orientierungen zum Datenschutz festgelegt. Diese Maßnahme ist insbesondere für mittlere bis große Organisationen.
2.4.2	Zuweisung von Rollen und Zuständigkeiten für den Schutz der Daten	Es wurden differenzierte Rollen, Aufgaben und Verantwortlichkeiten für den Datenschutz definiert und den Mitarbeitern zugewiesen. Dies kann auf unterschiedliche Weise geschehen, z. B. im Rahmen eines Grundsatzpapiers, einer Rollen- oder Stellenbeschreibung oder im Rahmen des Arbeitsvertrags. Diese Maßnahme ist für mittlere bis große Organisationen gedacht und wird insbesondere für komplexe Organisationsstrukturen und/oder geographisch verteilte Standorte mit mittlerem bis hohem Schutzbedarf empfohlen.
2.4.3	Benutzerleitfaden und Handlungsanweisungen zum Datenschutz	Zu wichtigen Datenschutzthemen wie Betroffenenanfragen, Datenschutzverletzungen oder Datenlöschung wurden schriftliche Richtlinien erstellt, die von den Mitarbeitern bei Bedarf jederzeit abgerufen werden können. Die Mitarbeiter werden sensibilisiert und im Rahmen von Fortbildungsmaßnahmen in diesen Leitlinien geschult werden (2.5).

2.5 Ausbildungsmaßnahmen

2.5.1	Regelmäßige Schulungen	Der Kunde sorgt für eine regelmäßige Schulung und Sensibilisierung des Personals. Dabei sind die verschiedenen Ebenen der Mitarbeiter bzw. ihre Rolle im Unternehmen zu berücksichtigen. Wenn möglich, sollten die Häufigkeit und Der Inhalt der Schulung sollte an die jeweilige Situation angepasst werden und der damit verbundenen Schutzbedürftigkeit. Die Teilnahme an Schulungsmaßnahmen ist zu dokumentieren.
2.5.2	Erinnerung an technische und organisatorische Maßnahmen und Schulungen	In regelmäßigen Abständen sowie ad hoc (z.B. bei akuten Bedrohungen) müssen die Mitarbeiter an die Inhalte der technisch-organisatorischen Schutzmaßnahmen erinnert bzw. in deren Einhaltung geschult werden. Diese Erinnerung kann in unterschiedlicher Form erfolgen, z.B. abteilungsweise durch Führungskräfte, individuell durch IT-Betreuer, unternehmensweite E-Mails oder andere Maßnahmen, die für den konkreten Fall und das Schutzbedürfnis wirksam sind.

2.6 Benutzerkontrolle

2.6 Benutzerkontrolle

Je nach dem Schutzbedarf der verarbeiteten Informationen sowie den zu erwartenden Risiken, den vorhandenen Gegebenheiten und der Anwendbarkeit auf die Verarbeitungen des Zertifizierungsgegenstandes sind die folgenden Maßnahmen zu ergreifen:

N°	Maßnahme	Erläuterung
2.6.1	Bestimmung der zur Nutzung berechtigten Personen	Es ist durch organisatorische Maßnahmen festzulegen, welche Personen zur Nutzung der IT-Ressourcen berechtigt sind. Zu diesem Zweck sind Verfahren für die Vergabe, den Widerruf und die regelmäßige Überprüfung von Berechtigungen festzulegen (siehe 2.2.11).
2.6.2	Kennwortrichtlinie mit Kennwortqualitätsprüfung	Die Sicherheit der Benutzerauthentifizierung ist durch eine Passwortpolitik zu gewährleisten, die die Benutzer bei der Erstellung sicherer Passwörter unterstützt und den ordnungsgemäßen Umgang mit Passwörtern regelt. Darüber hinaus ist durch technische Maßnahmen sicherzustellen, dass ausreichend lange und komplexe Passwörter gewählt werden. Weitere Festlegungen zur technischen Sicherheit (Kontosperrung nach mehrfacher unkorrekter Anmeldung, automatische Aufhebung der Kontosperrung, Passwortänderungsintervalle, etc.) sind je nach Anwendungsfall, technischem und organisatorischem Umfeld sowie Schutzbedürfnis zu treffen. Die

		Maßnahme muss durch Schulungs- und Sensibilisierungsmaßnahmen für die Nutzer unterstützt werden (siehe 2.5).

2.6.3	Benutzeridentifizierung und -authentifizierung	Die Nutzung der Verarbeitungssysteme darf nur nach Anmeldung und Authentifizierung des Nutzers möglich sein. Im Mindestfall ist eine Anmeldung mittels Benutzername und Passwort vorzusehen. Vom Medium bis hoher Schutz erfordert erweiterte Authentifizierung

		Methoden (Zwei-, Drei-Faktor-Authentifizierung) oder schrittweise Anmeldungen an verschiedenen Sicherheitssystemen (VPN, Betriebssystem, Anwendung) können je nach den technischen Gegebenheiten vorgesehen werden.
2.6.4	Protokollierung der Benutzer und ihrer Aktivitäten	Je nach Schutzbedarf und Zugriffsart sind die Aktivitäten der Benutzer zu protokollieren. Zu protokollieren sind mindestens die An- und Abmeldungen der Benutzer sowie die fehlgeschlagenen Anmeldeversuche. Soweit das jeweilige Verarbeitungssystem dies technisch ermöglicht, sind insbesondere die Aktivitäten von Nutzern mit erweiterten Rechten (Administratoren) detailliert zu protokollieren. (Siehe 2.7.).
2.6.5	Einsatz von Firewalls, Systemen zur Erkennung und Verhinderung von Eindringlingen	Der Einsatz von Netzsicherheitsgeräten an allen Schnittstellen zu offenen Netzen ist eine Mindestanforderung. Je nach Art und Schutzbedarf der Verarbeitungsprozesse müssen Firewall- Konstruktionen unterschiedlicher Komplexität und Leistungsfähigkeit eingesetzt werden, wobei in jedem Fall eine ordnungsgemäße und sichere Konfiguration gewährleistet sein muss. Die kontinuierliche Sicherheit muss durch laufende Wartung und externe Kontrollen gewährleistet werden, die je nach Bedrohungslage regelmäßig wiederholt werden müssen. Bei mittlerem bis hohem Schutzbedarf können zusätzlich Intrusion Detection/Prevention-Systeme eingesetzt werden, mit deren Hilfe Angriffe rechtzeitig erkannt und abgewehrt werden können.

2.7 Logischer Zugriff

Je nach dem Schutzbedarf der verarbeiteten Informationen sowie den zu erwartenden Risiken, den vorhandenen Gegebenheiten und der Anwendbarkeit auf die Verarbeitungen des Zertifizierungsgegenstandes sind die folgenden Maßnahmen zu ergreifen:

N°	Maßnahme	Erläuterung
2.7.1	Einsatz von Maßnahmen zur Benutzeridentifizierung und -authentifizierung	Für den Zugriff auf gespeicherte Inhalte ist mindestens eine Anmeldung mit Benutzernamen und Passwort erforderlich. Bei mittlerem bis hohem Schutzbedarf können je nach den technischen Gegebenheiten der jeweiligen Anwendung erweiterte Authentifizierungsmethoden (Zwei-, Drei-Faktor-Authentifizierung) eingesetzt werden. Siehe auch 2.6.3.

2.7.2	Bildschirmsperre bei längerer Inaktivität des Benutzers	Unbefugter Zugriff auf ungenutzte Geräte kann durch eine automatische Bildschirmsperre verhindert werden. die das Terminal erst nach der Freigabe neuer Benutzer au-

		thentifizierung. Einfache Benutzer sollten nicht in der Lage sein, die automatische Bildschirmsperre zu deaktivieren. Das Intervall für die Aktivierung der Bildschirmsperre sollte praktisch und ausreichend sicher festgelegt werden.
2.7.4	Protokollierung des Nutzerverhaltens	Je nach dem für die betreffenden Daten erforderlichen Schutzniveau können die Benutzeraktivitäten (Lesen, Schreiben, Löschen, Ändern, Kopieren) in Bezug auf diese Daten protokolliert werden. Zumindest müssen der Benutzer, die Art des Zugriffs und der Zeitstempel aufgezeichnet werden. Dabei ist auf die Angemessenheit des technischen Aufwands und die laufende Auswertung der Protokolle zu achten. Siehe auch 2.6.4.
2.7.5	Berechtigungskonzept für berechtigte Personen mit transparentem Zugang zu personenbezogenen Daten	Die Vergabe von Zugriffsberechtigungen auf personenbezogene Daten und Dokumente muss auf der Grundlage eines Berechtigungskonzepts erfolgen, das die zulässigen Zugriffe pro Benutzer oder Benutzergruppe nachvollziehbar darstellt.
2.7.6	Berücksichtigung des Need-to-know-Prinzips im Berechtigungskonzept (nur diejenigen Personen, die die Daten zur Erfüllung ihrer Aufgaben unbedingt benötigen)	Bei der Vergabe von Zugriffsberechtigungen ist das Need-to-know-Prinzip umzusetzen, d.h. der tatsächliche Bedarf zur Erfüllung der zugewiesenen Aufgaben oder Funktionen der Nutzer oder Nutzergruppen bestimmt den Umfang und die Reichweite der Berechtigungen.
2.7.7	Dokumentation über den Entzug oder die Anpassung von Zugangsberechtigungen	Änderungen und Widerrufe von Berechtigungen müssen protokolliert werden. Dies umfasst sowohl den betrieblich-organisatorischen Teil (Berechtigungen, Anweisungen usw.) als auch die technische Protokollierung.
2.7.8	Konzept für die Verwaltung des Zertifizierungsobjekts	Die sach- und fachgerechte Verwaltung des Zertifizierungsobjekts soll durch ein geeignetes Betreuungskonzept sichergestellt werden. Das Konzept sollte in jedem Fall die Vergabe und Zuordnung von Administrationsrechten sowie Berechtigungen für Soft- und Hardwareinstallationen regeln.
2.7.9	Überprüfung der Zugriffsberechtigungen der Benutzer	Die zugewiesenen Zugangsberechtigungen müssen in regelmäßigen Abständen überprüft werden, insbesondere um nicht mehr benötigte Berechtigungen zu entfernen. Darüber hinaus ist zu prüfen, ob die Berechtigungen von ausgeschiedenen Benutzern irrtümlich im System verblieben sind.

2.7.10	Zeitliche Begrenzung der Zugangsmöglichkeiten	Bei befristeten Arbeitsverhältnissen oder befristeten Diensten kann, soweit technisch möglich, ein Verfallsdatum für die Zugangsberechtigung festgelegt werden. Darüber hinaus, insbesondere bei mittlerem bis hohem Risiko, Zugangsmöglichkeiten können auf bestimmte Zeiten beschränkt werden

		Fenster (Bürozeiten) durch System- oder Netzmaßnahmen.
2.7.11	Benutzerbezogene Protokollierung von Zugriffen	Siehe auch 2.7.4 und 2.6.4.
2.7.12	Dokumentation der Maßnahmen zur Datenvernichtung	Die Löschung der Daten ist zu protokollieren und durch organisatorische oder technische Maßnahmen zu dokumentieren. Diese Maßnahme ist in Abhängigkeit von den konkreten betrieblichen und technischen Gegebenheiten sowie dem Schutzbedürfnis zu realisieren.
2.7.13	Warnsystem gegen Hackerangriffe	Insbesondere bei mittlerem bis hohem Schutzbedarf müssen Systeme zur Früherkennung von Hackerangriffen implementiert werden. Dazu können Intrusion Detection/Prevention Systeme, spezielle Funktionen der Firewall oder Virenschutzsoftware sowie Systeme zur Log- Auswertung und Erkennung von statistischen Anomalien eingesetzt werden.
2.7.14	Kontrolle kopieren	Siehe auch 2.3.3.
2.7.15	Ablehnung und Protokollierung von unbefugtem Zugriff auf das Netz	Unbefugter Zugriff über das Netz muss zuverlässig verhindert werden. Der Vorfall ist zu protokollieren. Siehe auch 2.2.11, 2.6.3, 2.6.4 und 2.6.5.
2.7.16	Trennung von Test- und Produktionsbetrieb	Echte Daten aus dem Produktionsbetrieb dürfen nicht oder nur in anonymisierter Form im Rahmen von Tests verwendet werden. Siehe auch 2.10.3.

2.8 Kontrolle der Übertragung

Je nach dem Schutzbedarf der verarbeiteten Informationen sowie den zu erwartenden Risiken, den vorhandenen Gegebenheiten und der Anwendbarkeit auf die Verarbeitungen des Zertifizierungsgegenstandes sind die folgenden Maßnahmen zu ergreifen:

N°	Maßnahme	Erläuterung
2.8.1	Leitlinien und Verfahren für die Übermittlung von Informationen	Die organisatorische Festlegung geeigneter Verfahren zur Übermittlung von Informationen ist die Grundlage für die sichere Datenübertragung. Richtlinien dienen der Klärung und Absicherung untergeordneter Verfahren und Methoden.
2.8.2	Ermittlung und Dokumentation der Übertragungswege und der Datenempfänger	Die Datenempfänger müssen erfasst und definiert werden. Je nach technischen Möglichkeiten, Schutzbedarf und Risiko müssen für die jeweiligen Daten und Empfänger geeignete Übertragungswege definiert werden.

2.8.3	Verschlüsselung aller mobilen Datenträger	Datenträger, die für die Übermittlung personenbezogener Daten verwendet werden, müssen vor unbefugtem Zugriff geschützt sein.

		durch geeignete und sichere kryptographische Verfahren. Siehe auch 2.10.1 und 2.11.5.
2.8.4	Tool zum Versenden von Dateianhängen per E-Mail	Der Versand von E-Mails, insbesondere von besonderen Kategorien personenbezogener Daten, muss durch geeignete Schutzmaßnahmen, einschließlich Ende-zu-Ende-Verschlüsselung und Authentifizierung, gesichert werden. Soll dieser Übertragungsweg genutzt werden, sind geeignete technische Möglichkeiten vorzusehen.
2.8.5	Schutzbedürftige Informationen werden entsprechend ihrem Schutzbedarf durch Löschung oder Vernichtung beseitigt.	Daten und Datenträger, die nicht mehr benötigt werden, sind in geeigneter Weise zu löschen oder zu vernichten. Dazu gehören auch Sicherungsdaten und -medien. Das Wiederherstellungsrisiko ist in Abhängigkeit vom jeweiligen Schutzbedarf durch Einhaltung gängiger Normen und Standards wie ÖNORM S 2109 oder DIN 66399 und dem Stand der Technik zu minimieren. Die Löschung oder Vernichtung ist zu dokumentieren, siehe auch 2.7.12.
2.8.6	Es muss nachvollziehbar dokumentiert werden, welcher Empfänger wann welche Daten erhalten hat.	Die Übermittlung personenbezogener Daten an Dritte muss unter Angabe des Zeitpunkts, des Absenders, des Empfängers und des übermittelten Inhalts dokumentiert werden. Dies kann je nach Übermittlungsart durch schriftliche Dokumentation, technische Protokollierung oder Aufbewahrung von Kopien der Übermittlungen erfolgen.
2.8.7	Dokumentation der Abruf- und Übermittlungsprogramme	Der Einsatz von Software, die zur Übertragung oder zum Abruf von Daten verwendet wird, muss organisatorisch festgelegt und dokumentiert werden.
2.8.8	Protokollierung der Datenübertragungen	Die Übermittlung personenbezogener Daten wird unter Angabe des Zeitpunkts, des Absenders, des Empfängers und des übermittelten Inhalts protokolliert.
2.8.9	Auswertungsmöglichkeiten der Übertragungsprotokolle, um die Empfänger oder Abrufer gezielt bestimmen zu können	Die Übertragungsprotokolle müssen für die verantwortlichen Personen abrufbar und auswertbar sein. Erforderlichenfalls sind technische Mittel zur Auswertung bereitzustellen. Siehe 2.9.7.
2.8.10	Verschlüsselte Übertragung von Inhalten in öffentlichen Netzen (VPN-Technologie im Internet)	Die Übermittlung von personenbezogenen Daten über öffentliche Netze darf nur in verschlüsselter Form erfolgen. Hierfür sind geeignete kryptographische Verfahren zu verwenden, siehe auch 2.8.12.

2.8.11	Kontrolliert und dokumentiertes Kopieren	Siehe 2.3.3.
2.8.12	Verschlüsselungsmethoden, die dem aktuellen Stand der Technik entsprechen	Die zur Verschlüsselung verwendeten kryptographischen Verfahren müssen dem aktuellen Stand der Technik entsprechen oder für den jeweiligen Bereich als ausreichend sicher anerkannt sein

		der Anwendung. Dies muss durch die ständige Überwachung der kryptografischen Entwicklungen gewährleistet werden.
2.8.13	Protokollierung an der Firewall	Soweit technisch möglich, werden die Datenübertragungen im Rahmen der Firewall-Protokollierung aufgezeichnet.
2.8.14	Transportverschlüsselung mit TLS	Bei Datenübertragungen über öffentliche Netze muss eine Transportverschlüsselung mittels TLS verwendet werden. Dies gilt für den Zugriff auf Webseiten, die Übermittlung oder den Abruf von E- Mails, FTP-Übertragungen, etc. Es sind nur TLS- Versionen zu verwenden, die dem aktuellen Stand der Technik entsprechen und als ausreichend sicher angesehen werden (siehe 2.8.12).
2.8.15	E-Mail-Verschlüsselung	E-Mails, die personenbezogene Daten enthalten, müssen vor unbefugtem Zugriff geschützt werden; zu diesem Zweck ist eine Transport- oder Ende-zu-Ende-Verschlüsselung zu verwenden.

2.9 Eingabekontrolle

Je nach dem Schutzbedarf der verarbeiteten Informationen sowie den zu erwartenden Risiken, den vorhandenen Gegebenheiten und der Anwendbarkeit auf die Verarbeitungen des Zertifizierungsgegenstandes sind die folgenden Maßnahmen zu ergreifen:

N°	Maßnahme	Erläuterung
2.9.1	Definition der Personen, die befugt sind, personenbezogene Daten einzugeben, zu ändern und zu löschen	Nutzer, die zur Verarbeitung personenbezogener Daten berechtigt sind, müssen vorab anhand ihrer Aufgaben und Funktionen definiert werden. Gleichzeitig müssen auch die entsprechenden Rollen und Zugriffsberechtigungen definiert werden
2.9.2	Definition von Plausibilitätskontrollen für die Eingabe, Änderung und Löschung von personenbezogenen Daten	Soweit technisch möglich, sind programmatische Plausibilitätsprüfungen und Eingabebeschränkungen vorzusehen, um Fehler und unbeabsichtigte Änderungen zu verhindern.
2.9.3	Sichere Ablage und rechtzeitige Löschung von Protokollen	Protokolle zur Verfolgung des Nutzerverhaltens sind sicher zu speichern und vor Veränderung und Löschung zu schützen. Bei mittlerem bis hohem Schutzbedarf sind unabhängige Protokollserver oder Einrichtungen zur revisionssicheren Protokollierung zu verwenden. Geeignete Aufbewahrungsfristen für Protokolle sind zu definieren und, wenn möglich, technisch umzusetzen.

2.9.4	Nachvollziehbarkeit von Eingabe, Änderung und Löschung von Daten durch individuelle Benutzernamen	Die Nachvollziehbarkeit der Protokollierung von Nutzeraktivitäten ist nur dann gegeben, wenn diese unter individuellen Nutzernamen erfolgen. Die Verwendung von "Sammelkonten" oder generischen Benutzerkonten ist daher auf ein Minimum zu beschränken und darf nur dann verwendet werden, wenn dies aufgrund technischer Beschränkungen oder bestimmter betrieblicher Abläufe unvermeidbar ist.

2.9.5	Benutzeridentifizierung und -authentifizierung	Siehe 2.7.1 und 2.6.3.
2.9.6	Protokollierung der Eingabe, Änderung und Löschung von Daten (auch für Log-Dateien)	Siehe 2.7.4 und 2.9.3.
2.9.7	Verwendung von Protokollbewertungssystemen	Um unberechtigte oder ungeplante Änderungen zu erkennen, müssen die Protokolle je nach Schutzbedürfnis laufend oder in regelmäßigen Abständen überprüft und ausgewertet werden. Die personellen Zuständigkeiten sowie die Häufigkeit der Auswertung müssen organisatorisch festgelegt werden. Zur Unterstützung der Auswertung können elektronische Auswertungssysteme eingesetzt werden, die das Herausfiltern bestimmter Zugriffe und das Erkennen von Auffälligkeiten erleichtern.

2.10 Kontrolle der Lagerung

Abhängig vom Schutzbedarf der verarbeiteten Informationen sowie den zu erwartenden Risiken, den vorhandenen Gegebenheiten und der Anwendbarkeit auf die Verarbeitungen des Zertifizierungsgegenstandes sind die folgenden Maßnahmen zu ergreifen:

N°	Maßnahme	Erläuterung
2.10.1	Verschlüsselte Speicherung von Daten (Mo- bile Datenträger und Festplatten)	Insbesondere Datenträger, die durch Maßnahmen der Zugriffskontrolle (2.2) nicht ausreichend geschützt werden können, müssen durch kryptografische Verfahren gegen unbefugten Lese- und Schreibzugriff gesichert werden. Dazu gehören vor allem mobile Datenträger wie externe Festplatten, USB-Sticks und Speicherkarten, aber auch die Massenspeicher von mobilen Endgeräten (Notebooks, Smartphones, Tablets).
2.10.2	Pseudonymisierung	Pseudonymisierungsmaßnahmen schützen Daten vor der Einsichtnahme durch Unbefugte. Darüber hinaus kann das Need-to-know-Prinzip unterstützt werden, indem Informationen, die für die Erfüllung der Aufgabe nicht notwendig sind, ausgeblendet werden. Bei der Pseudonymisierung müssen Daten und Identifikationsschlüssel getrennt von pseudonymisierten personenbezogenen Daten gespeichert werden. Der Zugriff auf die Identifikationsschlüssel muss organisatorisch geregelt sein.

2.10.3	Trennung von Test- und Produktionsbetrieb	Eine strikte Trennung von Test- und Produktionsbetrieb muss typische Schwachstellen in Testumgebungen (fehlende Sicherheitsmaßnahmen, schwache oder erratbare Passwörter) verhindern. Wörter usw.) die Sicherheit der realen Daten nicht beeinträchtigen. Gleichzeitig muss darauf geachtet werden, dass

		Personenbezogene Daten werden nicht oder nur in anonymisierter Form für Testzwecke verwendet.

2.11 Transportkontrolle

Je nach dem Schutzbedarf der verarbeiteten Informationen sowie den zu erwartenden Risiken, den vorhandenen Gegebenheiten und der Anwendbarkeit auf die Verarbeitungen des Zertifizierungsgegenstandes sind die folgenden Maßnahmen zu ergreifen:

N°	Maßnahme	Erläuterung
2.11.1	Eskalation für Sicherheitsmeldungen	Für Sicherheitsvorfälle während der Beförderung sind geeignete Maßnahmen vorzusehen, die zumindest die Meldung an die zuständigen Personen und die Dokumentation des Vorfalls umfassen.
2.11.2	Inbetriebnahme von zuverlässiger Transportunternehmen	Für den Transport von Datenträgern mit mittlerem bis hohem Schutzbedarf dürfen nur zuverlässige, einschlägig zertifizierte Unternehmen eingesetzt werden. Unternehmenszertifizierungen, die die Sicherheit der Transportprozesse einschließen, z. B. nach ISO 9001 oder ISO 27001, können bei der Beurteilung der Zuverlässigkeit eines Anbieters berücksichtigt werden.
2.11.3	Dokumentation des Transportweges	Dies bezieht sich nur auf physische Übertragungen, d. h. den Medientransport. Digitale Übertragungen können nur innerhalb des internen Netzes der Organisation durchgeführt werden. Zur Sicherheit von digitalen Übertragungskanälen siehe 2.8.10, 2.11.10.
2.11.4	Führen eines Datenträgereingangs- oder -ausgangsbuches	Der Schutz von Datenträgern mit mittlerem bis hohem Schutzbedarf vor Diebstahl oder Verlust kann durch ein entsprechendes Datenträger-Management verbessert werden. Diese Maßnahme ist insbesondere im Zusammenhang mit der Bestandskontrolle vorzusehen. 2.3.1.
2.11.5	Zusätzlicher Passwortschutz für Dokumente vor der Übermittlung mit separater Übermittlung des Passwortes	Elektronisch gespeicherte Dokumente sind während der Übermittlung durch Verschlüsselung vor unbefugtem Zugriff zu schützen. Das für die Entschlüsselung erforderliche Passwort ist getrennt vom geschützten Inhalt und nach Möglichkeit auf einem anderen Transportweg zu übermitteln.

	2.11.6	Verwendung von sicheren Transportbehältern	Für den Transport von schutzbedürftigen Dokumenten und Datenträgern müssen verschlossene, sichere Transportbehälter verwendet werden. Die Sicherheitsstufe muss an den Schutzbedarf des transportierten Inhalts angepasst sein.	
	2.11.7	Überwachung der Transportzeit	Um Sicherheitsvorfälle oder Sicherheitslücken zu erkennen, kann die Transportzeit überwacht werden. Zu diesem Zweck müssen die Zeiten der Ein- und Ausreise abgeglichen werden, z. B. durch	

		Bereitstellung der entsprechenden Daten durch das Verkehrsunternehmen.
2.11.8	Verschlüsselungsmethoden, die dem aktuellen Stand der Technik entsprechen	Siehe 2.8.12.
2.11.9	Verschlüsselte Speicherung von Daten auf Datenträgern	Siehe 2.10.1, 2.8.3 und 2.11.5.
2.11.10	Sicherer Zugang über verschlüsseltes VPN	Siehe 2.8.10.
2.11.11	Schutz von Datenübertragungen und Datenträgern vor Malware (Viren etc.)	Datenträger, die zur Speicherung und zum Transport elektronischer Inhalte verwendet werden, müssen vor der Nutzung mit geeigneter und aktueller Virenschutzsoftware auf Schadsoftware überprüft werden. Je nach zu erwartender Bedrohungslage müssen auch elektronisch übermittelte Daten auf Schadsoftware überprüft werden.
2.11.12	Protokollierung an der Firewall	Siehe 2.8.13.
2.11.13	Verschlüsselung von Dateianhängen beim Versand von E-Mails	Siehe 2.8.15.
2.11.14	Transportverschlüsselung mit TLS	Siehe 2.8.14.

2.12 Wiederherstellung

Je nach dem Schutzbedarf der verarbeiteten Informationen sowie den zu erwartenden Risiken, den vorhandenen Gegebenheiten und der Anwendbarkeit auf die Verarbeitungen des Zertifizierungsgegenstandes sind die folgenden Maßnahmen zu ergreifen:

N°	Maßnahme	Erläuterung
2.12.1	Konzept für die Notfallvorsorge	Verfügbarkeitsverluste können durch die Erstellung eines Notfallvorsorgekonzepts minimiert werden. Diese Maßnahme ist insbesondere dann erforderlich, wenn vorübergehende Unterbrechungen der Verarbeitung zu mittleren bis hohen Risiken für die Betroffenen führen können.
2.12.2	Regelmäßig geübte Notfallpläne	Die Festlegungen im Rahmen eines Notfallvorsorgekonzeptes (2.12.1) oder eines Wiederherstellungskonzeptes (2.12.3) sind durch regelmäßige Notfallübungen zu überprüfen und zu üben. Der Zeitplan für Notfallübungen ist organisatorisch festzulegen und die notwendigen Ressourcen sind bereitzustellen.

2.12.3	Konzept zur Datensicherung und -wiederherstellung	Im Rahmen eines Datensicherungskonzepts werden der Umfang der zu sichernden Daten, das Sicherungsintervall und die Wert, Zeitpunkt, Methode und Aufbewahrungsfrist der

		Backups sind transparent zu definieren. Es ist festzulegen, wer für die Durchführung und Kontrolle der Backups verantwortlich ist. Darüber hinaus regelt ein Restore-Konzept das Vorgehen im Falle eines Restores, das die unten aufgeführten Anforderungen beinhaltet. 2.12.5 spezi- fikationen.
2.12.4	Sichere Aufbewahrung der Sicherungsdatenträger sowie eine lückenlose Dokumentation der Speichermedien	Die Sicherungsmedien sind vor unberechtigtem Zugriff und Zerstörung geschützt aufzubewahren. Die Dokumentation und Bestandskontrolle der Sicherungsmedien dient der Aufdeckung von Sicherheitsvorfällen. Siehe auch 2.3.1 und 2.11.4.
2.12.5	Vorgaben wiederherstellen (genaue Planung des Wiederaufbaus, umgesetzte Übungspläne und Abstimmung mit Notfallvorsorgekonzept)	Im Rahmen dieser Vorgaben sind der Ablauf der Wiederherstellung sowie verschiedene Wiederherstellungsfälle (Bare Metal Restore, Einzeldaten, virtuelle Ma- chen, etc.) zu behandeln. Die Wiederherstellung muss in regelmäßigen Abständen getestet und geübt werden. Es ist darauf zu achten, dass eine genaue und angemessene Abstimmung mit einem Notfallvorsorgekonzept erfolgt (2.12.1).
2.12.6	Regelmäßige Datensicherung nach dem Stand der Technik (Sicherung von Anwendungsdaten, Systemdaten und Logdaten)	Die Datensicherungen sind an den jeweiligen Stand der Technik anzupassen. Dabei sind u.a. Herstellerspezifika zum Umfang der Datensicherungen und organisatorische Anforderungen zu berücksichtigen.

2.13 Verlässlichkeit und Datenintegrität

Je nach dem Schutzbedarf der verarbeiteten Informationen sowie den zu erwartenden Risiken, den vorhandenen Gegebenheiten und der Anwendbarkeit auf die Verarbeitungen des Zertifizierungsgegenstandes sind die folgenden Maßnahmen zu ergreifen:

N°	Maßnahme	Erläuterung
2.13.1	Konzept zur Datensicherung und -wiederherstellung	Siehe 2.12.3.
2.13.2	Konzept der Systemüberwachung	Im Rahmen eines Systemüberwachungskonzepts müssen Maßnahmen zur Vermeidung von Störungen und Ausfällen der IT-Systeme geregelt werden. Dazu gehören sowohl manuelle Überwachungsmaßnahmen als auch technische Maßnahmen wie System- und Netzwerküberwachungslösungen. Personelle Zuständigkeiten, Meldungen und Eskalationswege müssen festgelegt werden.

		aktualisiert und auf korrekte Funktion überwacht werden. Eine Deaktivierung der Virenschutzsoftware durch einfache Benutzer muss verhindert werden. Bei Fehlfunktionen der Software und dem Auffinden von Schadsoftware sind die zuständigen Personen zu benachrichtigen.
2.13.3	Schutz von Daten und Datenträgern vor Malware (Viren usw.)	Zum Schutz der gespeicherten Daten und der Verarbeitung vor Schadsoftware muss auf allen Systemen eine geeignete Virenschutzsoftware betrieben werden, die laufend aktualisiert und auf ihre Funktionstüchtigkeit überwacht wird. Eine Deaktivierung der Virenschutzsoftware durch einfache Benutzer muss verhindert werden. Bei Fehlfunktionen der Software und dem Auffinden von Schadsoftware sind die Verantwortlichen zu benachrichtigen.
2.13.4	Benutzeridentifizierung und -authentifizierung	Siehe 2.6.1 und 2.6.3.
2.13.5	Sicherer Zugang über verschlüsseltes VPN	Siehe 2.8.10.
2.13.6	Transportverschlüsselung mit TLS	Siehe 2.8.14.
2.13.7	Einsatz von Firewalls, Systemen zur Erkennung und Verhinderung von Eindringlingen	Siehe 2.6.5 und 2.7.13.