TECHNISCH-ORGANISATORISCHE MAßNAHMEN FÜR DIE SCHNITTSTELLE FÜR DRITTE GEMÄß § 370A ABS. 2 SGB V

[KBV_ITV_FMEX_TOM_370a]

Die Technisch-Organisatorische Maßnahmen (TOMs) zur Nutzung des elektronischen Systems zur Vermittlung von Behandlungsterminen und telemedizinischen Leistungen durch Nutzer der Schnittstelle sind im Rahmen der Zertifizierung der Schnittstelle für Dritte gemäß § 370A Abs. 2 SGB V auszufüllen, einzureichen und werden im Zertifizierungsverfahren geprüft.

Die nachfolgend aufgeführten Maßnahmen gelten für die Schutzstufe C und müssen vom Nutzer der Schnittstelle nachweislich erfüllt sein.

INHALT

1 ALLGEMEINE MAßNAHMEN

ID	FRAGE	MINDESTANFORDERUNG	ERLÄUTERUNGEN ODER DARSTELLUNG GLEICHWERTIGER MAßNAHMEN DES NUTZERS DER SCHNITTSTELLE
01.01	Existieren eine Richtlinie zur Informationssicherheit und nachgelagerte gelenkte Richtlinien und Anweisungen, auf die Mitarbeitende geschult werden? ☐ ja ☐ nein	Richtlinien und Anweisungen zur Informationssicherheit müssen existieren und Mitarbeitende darauf geschult werden.	Bei vorhandenem C5 Testat: Abgedeckt über OIS-02
01.02	Gibt es klare Regeln zur Nutzung geistigen Eigentums und lizenzierter Software? ☐ ja ☐ nein		
01.03	Gibt es ein festgelegtes Verfahren zum Umgang mit Fehlverhalten und Regelverstößen (Maßregelungsprozess)? ☐ ja ☐ nein		
01.04	Ist vertraglich sichergestellt, dass Mitarbeitende auch nach Beendigung ihres Arbeits- oder Vertragsverhältnisses weiterhin zur Einhaltung der Vertraulichkeit verpflichtet bleiben? ☐ ja ☐ nein	Eine Verpflichtung muss erfolgen.	Bei vorhandenem C5 Testat: Abgedeckt über HR-05
01.05	Gibt es Vorgaben zum Arbeiten in Sicherheitsbereichen? ☐ ja ☐ nein		

ID	FRAGE	MINDESTANFORDERUNG	ERLÄUTERUNGEN ODER DARSTELLUNG GLEICHWERTIGER MAßNAHMEN DES NUTZERS DER SCHNITTSTELLE
	Sind die dokumentierten Maßnahmen aus Ihrer Sicht unter Berücksichtigung des Stands der Technik, der Implementierungskosten, der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten der Betroffenen geeignet, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten? ☐ geeignet ☐ begrenzt geeignet ☐ ungeeignet Begründung: bitte angeben	Es muss bestätigt werden, dass die getroffenen Maßnahmen geeignet sein, um ein angemessenes Schutzniveau zu gewährleisten. Bei der Angabe „begrenzt geeignet“ muss eine Begründung erfolgen.	

2 MAßNAHMEN ZUM ZUTRITT ZU SYSTEMEN

ID	FRAGE	MINDESTANFORDERUNG	ERLÄUTERUNGEN ODER DARSTELLUNG GLEICHWERTIGER MAßNAHMEN DES NUTZERS DER SCHNITTSTELLE
02.01	Werden personenbezogene Daten in Serverräumen oder Rechenzentren (zwischen-) gespeichert oder weitergeleitet, die von dem Auftragnehmer verantwortet werden? ☐ ja ☐ nein		
	Wenn 02.01 nein: In diesem Fall müssen die weiteren Fragen zu 2 nicht beantwortet werden, sondern sogleich die Fragen ab 3. Auch die Fragen zu 7 und 8 entfallen.		
02.02	Standort(e) an denen der Auftragnehmer die Systeme betreibt: bitte angeben	Der Standort muss in • der EU, • des Europäischen Wirtschaftsraums, • der Schweiz, oder • in einem Drittstaat nur, sofern ein Angemessenheitsbeschluss gemäß Artikel 45 DSGVO vorliegt und zusätzlich die sich aus dem Angemessenheitsbeschluss ergebenden Voraussetzungen (wie zum Beispiel erforderliche Zertifizierungen) vorliegen, liegen.	

ID	FRAGE	MINDESTANFORDERUNG	ERLÄUTERUNGEN ODER DARSTELLUNG GLEICHWERTIGER MAßNAHMEN DES NUTZERS DER SCHNITTSTELLE
02.03	Sind die personenbezogenen Daten auf mehr als einem System je Standort verteilt (z. B. für Backup / Datenreplikation / Nutzung von Cloud-Dienstleistungen)? ☐ ja ☐ nein		
02.04	Aus welchem Material bestehen die Zugangstüren zu den Serverräumen (Stahl oder sonstiges Material)? bitte angeben	Alle Bauelemente der Gebäudehülle müssen mindestens RC 2 gemäß DIN EN 1627-1630:11 erfüllen.	Bei vorhandenem C5 Testat: Abgedeckt über PS-03
02.05	Sind Serverräume fensterlos? ☐ ja ☐ nein		
02.06	**Wenn 02.05 nein:** Wie sind die Fenster vor Einbruch geschützt? bitte angeben	Alle Bauelemente der Gebäudehülle müssen mindestens RC 2 gemäß DIN EN 1627-1630:11 erfüllen.	Bei vorhandenem C5 Testat: Abgedeckt über PS-03
02.07	Sind Serverräume / RZ mittels einer Einbruchmeldeanlage (EMA) alarmgesichert? ☐ ja ☐ nein	Einbruchmeldeanlage muss vorhanden sein.	
02.08	**Wenn 02.07 ja:** Wer wird informiert, wenn die EMA auslöst? **Mehrfachantworten möglich!** ☐ beauftragter Wachdienst ☐ Administrator ☐ Leiter IT ☐ Sonstiges: bitte angeben	Eine Alarmaufschaltung ist verpflichtend. Mindestens eine der zu alarmierenden Stellen muss 24/7 erreichbar sein und reagieren.	

ID	FRAGE	MINDESTANFORDERUNG	ERLÄUTERUNGEN ODER DARSTELLUNG GLEICHWERTIGER MAßNAHMEN DES NUTZERS DER SCHNITTSTELLE
02.09	Sind Serverräume / RZ videoüberwacht? ☐ ja ☐ nein	Eine Videoüberwachung ist verpflichtend.	
02.10	**Wenn 02.09 ja:** Wie lange werden die Bilddaten gespeichert? bitte angeben	Die Videoaufzeichnungen müssen mindestens 24 h vorgehalten werden.	
02.11	Wie viele Personen haben Zutritt zu den Serverräumen und welche Funktionen haben diese inne? bitte angeben	Nur ausgewählte, berechtigte Personen dürfen Zutritt erlangen. Die Zutrittsberechtigung darf nur personengebunden vergeben werden.	Bei vorhandenem C5 Testat: Abgedeckt über PS-04
02.12	Existiert ein Prozess zur Vergabe von Zutrittsberechtigungen bei der Neueinstellung und beim Ausscheiden von Mitarbeitenden bzw. bei organisatorischen Veränderungen? ☐ definierter Freigabeprozess ☐ kein definierter Freigabeprozess, auf Zuruf ☐ Sonstige Vergabeweise: bitte angeben	Ein definierter Freigabeprozess ist erforderlich.	Bei vorhandenem C5 Testat: Abgedeckt über PS-04
02.13	Sind Serverräume mit einem elektronischen Schließsystem versehen? ☐ ja ☐ nein	Ein elektronisches Schließsystem ist erforderlich.	
02.14	**Wenn 02.13 ja:** Welche Zutrittstechnik kommt zum Einsatz? **Mehrfachantworten möglich!** bitte angeben	Mindestens zwei aus drei Authentifizierungskomponenten (Besitz, Wissen oder biometrische Charakteristika) sind für den Zutritt erforderlich.	Bei vorhandenem C5 Testat: Abgedeckt über PS-04

ID	FRAGE	MINDESTANFORDERUNG	ERLÄUTERUNGEN ODER DARSTELLUNG GLEICHWERTIGER MAßNAHMEN DES NUTZERS DER SCHNITTSTELLE
02.15	**Wenn 02.13 ja:** Werden die Zutritte zu Serverräumen protokolliert? ☐ ja ☐ nein		
02.16	**Wenn 02.15 ja:** Wie lange werden die Zutrittsdaten gespeichert? bitte angeben		
02.17	**Wenn 02.15 ja:** Werden die Protokolle regelmäßig ausgewertet? ☐ ja ☐ nein		
02.18	Ist der Zutritt zu den Serverräumen (auch) mechanisch mit Schlüssel möglich? ☐ ja ☐ nein		
02.19	**Wenn 02.18 ja:** Wo werden die Schlüssel aufbewahrt und wer gibt sie aus? bitte angeben		
02.20	Existiert ein Pförtnerdienst / Wachdienst / besetzter Empfangsbereich o. ä. zum Rechenzentrum/Serverraum? ☐ ja ☐ nein		

ID	FRAGE	MINDESTANFORDERUNG	ERLÄUTERUNGEN ODER DARSTELLUNG GLEICHWERTIGER MAßNAHMEN DES NUTZERS DER SCHNITTSTELLE
02.21	Werden die Serverräume neben ihrer eigentlichen Funktion noch für andere Zwecke genutzt? ☐ ja ☐ nein	Die Nutzung von Serverräumen für andere Zwecke ist nicht erlaubt.	
02.22	Gibt es offizielle Zutrittsregelung für betriebsfremde Personen (bspw. Besucher) zu den Serverräumen? ☐ ja, bitte angeben ☐ nein	Eine offizielle Zutrittsregelung für betriebsfremde Personen ist zwingend erforderlich.	Bei vorhandenem C5 Testat: Abgedeckt über PS-04
	Sind die dokumentierten Maßnahmen aus Ihrer Sicht unter Berücksichtigung des Stands der Technik, der Implementierungskosten, der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten der Betroffenen geeignet, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten? ☐ geeignet ☐ begrenzt geeignet ☐ ungeeignet Begründung: bitte angeben	Es muss bestätigt werden, dass die getroffenen Maßnahmen geeignet sein, um ein angemessenes Schutzniveau zu gewährleisten. Bei der Angabe „begrenzt geeignet“ muss eine Begründung erfolgen.	

3 MAßNAHMEN ZUM ZUTRITT ZU BÜRORÄUMEN

ID	FRAGE	MINDESTANFORDERUNG	ERLÄUTERUNGEN ODER DARSTELLUNG GLEICHWERTIGER MAßNAHMEN DES NUTZERS DER SCHNITTSTELLE
03.01	An welchen Standorten wird über Clientarbeitsplätze auf personenbezogene Daten zugegriffen? bitte angeben		
03.02	Existiert ein Pförtnerdienst / Wachdienst / besetzter Empfangsbereich o. ä. zum Gebäude bzw. zu Ihren Büros? ☐ ja ☐ nein		
03.03	Ist das Gebäude oder sind die Büroräume mittels einer Einbruchmeldeanlage (EMA) alarmgesichert? ☐ ja ☐ nein	Einbruchmeldeanlage muss vorhanden sein.	
03.04	**Wenn 03.03 ja:** Wer wird informiert, wenn die EMA auslöst? **Mehrfachantworten möglich!** ☐ beauftragter Wachdienst ☐ Administrator ☐ Leiter IT ☐ Sonstiges: bitte angeben	Eine Alarmaufschaltung ist verpflichtend. Mindestens eine der zu alarmierenden Stellen muss 24/7 erreichbar sein und reagieren.	
03.05	Werden das Bürogebäude bzw. seine Zugänge videoüberwacht? ☐ ja, ohne Bildaufzeichnung ☐ ja, mit Bildaufzeichnung ☐ nein		

ID	FRAGE	MINDESTANFORDERUNG	ERLÄUTERUNGEN ODER DARSTELLUNG GLEICHWERTIGER MAßNAHMEN DES NUTZERS DER SCHNITTSTELLE
03.06	**Wenn 03.05 „ja, mit Bildaufzeichnung“:** Wie lange werden die Bilddaten gespeichert? bitte angeben		
03.07	Sind die Räumlichkeiten mit einem elektronischen Schließsystem versehen? ☐ ja, die Büroräume sind elektronisch verschlossen. ☐ ja, die Büroetagen sind elektronisch verschlossen. ☐ ja, das gesamte Gebäude ist elektronisch verschlossen. ☐ nein	Ein elektronisches Schließsystem ist erforderlich.	
03.08	**Wenn 03.07 ja:** Welche Zutrittstechnik kommt zum Einsatz? ☐ RFID ☐ PIN ☐ Biometrie ☐ Sonstiges: bitte angeben	Mindestens zwei verschiedene Techniken müssen genutzt werden.	Bei vorhandenem C5 Testat: Abgedeckt über PS-04
03.09	**Wenn 03.07 ja:** Werden die Zutritte im Zutrittssystem protokolliert? ☐ ja, erfolgreiche und -lose Versuche ☐ ja, nur erfolgreiche Versuche ☐ ja, nur erfolglose Versuche ☐ nein	Mindestens erfolglose Versuche müssen protokolliert werden.	
03.10	**Wenn 03.09 ja:** Wie lange werden diese Protokolldaten aufbewahrt? bitte angeben		

ID	FRAGE	MINDESTANFORDERUNG	ERLÄUTERUNGEN ODER DARSTELLUNG GLEICHWERTIGER MAßNAHMEN DES NUTZERS DER SCHNITTSTELLE
03.11	**Wenn 03.09 ja:** Werden die Protokolle regelmäßig ausgewertet? ☐ ja ☐ nein		
03.12	Existiert ein mechanisches Schloss für die Gebäude / Büroräume? ☐ ja ☐ nein		
03.13	**Wenn 03.07 oder 03.12 ja:** Wird die Ausgabe der (mechanischen / elektronischen) Schlüssel/Token protokolliert? ☐ ja, bitte angeben ☐ nein		
03.14	**Wenn 03.07 oder 03.12 ja:** Wer gibt die Schlüssel (mechanisch/elektronisch) aus? bitte angeben	Es muss festgelegt sein, wer eine Schlüsselausgabe vornehmen darf.	
03.15	Werden die Zutrittsrechte/Schlüssel zu Büros personenbezogen vergeben? ☐ ja ☐ nein	Personenbezogene Zutrittsrechte/ Schlüssel sind zwingend erforderlich.	Bei vorhandenem C5 Testat: Abgedeckt über PS-04
03.16	Gibt es offizielle Zutrittsregelung für betriebsfremde Personen (bspw. Besucher) zu den Büroräumen? ☐ ja, bitte angeben ☐ nein	Eine offizielle Zutrittsregelung für betriebsfremde Personen ist zwingend erforderlich.	Bei vorhandenem C5 Testat: Abgedeckt über PS-04

ID	FRAGE	MINDESTANFORDERUNG	ERLÄUTERUNGEN ODER DARSTELLUNG GLEICHWERTIGER MAßNAHMEN DES NUTZERS DER SCHNITTSTELLE
	Sind die dokumentierten Maßnahmen aus Ihrer Sicht unter Berücksichtigung des Stands der Technik, der Implementierungskosten, der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten der Betroffenen geeignet, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten? ☐ geeignet ☐ begrenzt geeignet ☐ ungeeignet Begründung: bitte angeben	Es muss bestätigt werden, dass die getroffenen Maßnahmen geeignet sein, um ein angemessenes Schutzniveau zu gewährleisten. Bei der Angabe „begrenzt geeignet“ muss eine Begründung erfolgen.	

4 MAßNAHMEN ZUM ZUGANG UND ZUGRIFF

ID	FRAGE	MINDESTANFORDERUNG	ERLÄUTERUNGEN ODER DARSTELLUNG GLEICHWERTIGER MAßNAHMEN DES NUTZERS DER SCHNITTSTELLE
04.01	Existiert ein Prozess zur Vergabe von Benutzerkennungen und Zugriffsberechtigungen bei der Neueinstellung und beim Ausscheiden von Mitarbeitenden bzw. bei organisatorischen Veränderungen? ☐ definierter Freigabeprozess ☐ kein definierter Freigabeprozess, auf Zuruf ☐ Sonstige Vergabeweise: bitte angeben	Ein definierter Freigabeprozess ist erforderlich.	Bei vorhandenem C5 Testat: Abgedeckt über IDM-01
04.02	Werden Zugriffsberechtigungen nach dem Need-to-Know und Least-Privilege Prinzip auf Basis eines Rollen- und Rechtekonzeptes vergeben? ☐ ja ☐ nein	Need-to-Know und Least-Privilege Prinzipien auf Basis eines Rollen- und Rechtekonzeptes sind erforderlich.	Bei vorhandenem C5 Testat: Abgedeckt über PSS-08
04.03	Werden die Vergabe bzw. Änderungen von Zugriffsberechtigungen protokolliert? ☐ ja ☐ nein	Eine Protokollierung ist erforderlich.	
04.04	Authentisieren sich die Mitarbeitenden über eine individuelle Kennung gegenüber dem zentralen Verzeichnisdienst? ☐ ja ☐ nein	Authentisierung gegen einen zentralen Verzeichnisdienst ist erforderlich.	
04.05	Existieren verbindliche Passwortvorgaben im Unternehmen? ☐ ja ☐ nein	Verbindliche Password-Policy ist erforderlich.	Bei vorhandenem C5 Testat: Abgedeckt über IDM-09

ID	FRAGE	MINDESTANFORDERUNG	ERLÄUTERUNGEN ODER DARSTELLUNG GLEICHWERTIGER MAßNAHMEN DES NUTZERS DER SCHNITTSTELLE
04.06	**Passwort-Zeichenlänge:** bitte angeben **Das Passwort enthält Zeichen aus den folgenden Kategorien entsprechend den Mindestanforderungen der Schutzstufe:** ☐ Großbuchstaben (A bis Z) ☐ Kleinbuchstaben (a bis z) ☐ Ziffern (0 bis 9) ☐ Nicht alphanumerische Zeichen (Sonderzeichen): (~! @ # $% ^& * -+ = ' | \ \ (){}\ []:; "' <>,.? /)	Die Passwortlänge muss mindestens 12 Zeichen sein. Für die Passwortkomplexität müssen alle vier Kategorien (Großbuchstaben, Kleinbuchstaben, Ziffern oder nicht alphanumerische Zeichen) enthalten sein. - ODER - Es wird eine Multi-Faktor-Authentifizierung eingesetzt.	Bei vorhandenem C5 Testat: Abgedeckt über IDM-09
04.07	Zwingt das IT-System den Nutzer zur Einhaltung der oben genannten Passwortvorgaben? ☐ ja ☐ nein	Die technische Unterstützung der Einhaltung der Password-Policy ist erforderlich.	Bei vorhandenem C5 Testat: Abgedeckt über IDM-08
04.08	Wird der Bildschirm bei Inaktivität des Benutzers gesperrt? ☐ ja, nach bitte Anzahl angeben Minuten ☐ nein	Die Bildschirmsperre muss automatisch nach spätestens 10 Minuten Inaktivität aktiviert werden.	
04.09	Welche Maßnahmen ergreifen Sie bei Verlust, Vergessen oder Ausspähen eines Passworts? bitte angeben	Ein definierter Prozess muss existieren.	
04.10	Gibt es eine Begrenzung von erfolglosen Anmeldeversuchen? ☐ ja, nach bitte Anzahl angeben erfolglosen Versuchen. ☐ nein	Es muss eine Anmeldesperre spätestens nach 10 erfolglosen Anmeldeversuchen eingerichtet sein.	

ID	FRAGE	MINDESTANFORDERUNG	ERLÄUTERUNGEN ODER DARSTELLUNG GLEICHWERTIGER MAßNAHMEN DES NUTZERS DER SCHNITTSTELLE
04.11	**Wenn 04.10 ja:** Wie lange bleiben Zugänge gesperrt, wenn die maximale Zahl erfolgloser Anmeldeversuche erreicht wurde? ☐ Die Zugänge bleiben bis zur manuellen Aufhebung der Sperre gesperrt. ☐ Die Zugänge bleiben für bitte Anzahl angeben Minuten gesperrt.	Zugänge müssen bis zur manuellen Aufhebung gesperrt bleiben.	
04.12	Ist der Zugriff auf Daten aus dem Internet (z. B. im Home-Office) möglich? ☐ ja ☐ nein		
04.13	**Wenn 04.12 ja:** Wie erfolgt die Authentisierung beim Zugriff auf Daten aus dem Internet: ☐ (RSA) Token ☐ VPN-Zertifikat ☐ pre-shared key ☐ Benutzeraccount	Mindestens zwei aus drei Authentifizierungskomponenten (Besitz, Wissen oder biometrische Charakteristika) sind für den Zugriff erforderlich.	Bei vorhandenem C5 Testat: Abgedeckt über IDM-09
04.14	**Wenn 04.12 ja:** Gibt es eine Begrenzung von erfolglosen Anmeldeversuchen bei Fernzugängen? ☐ ja, bitte Anzahl angeben Versuche pro Tag ☐ nein	Es muss eine Anmeldesperre spätestens nach 10 erfolglosen Anmeldeversuchen eingerichtet sein.	

ID	FRAGE	MINDESTANFORDERUNG	ERLÄUTERUNGEN ODER DARSTELLUNG GLEICHWERTIGER MAßNAHMEN DES NUTZERS DER SCHNITTSTELLE
04.15	**Wenn 04.14 ja:** Wie lange bleiben Zugänge gesperrt, wenn die maximale Zahl erfolgloser Anmeldeversuche erreicht worden ist? ☐ Die Zugänge bleiben bis zur manuellen Aufhebung gesperrt. ☐ Die Zugänge bleiben für bitte Anzahl angeben Minuten gesperrt.	Zugänge müssen bis zur manuellen Aufhebung gesperrt bleiben.	
04.16	Werden Firewalls eingesetzt? ☐ ja ☐ nein	Firewalls sind zwingend erforderlich.	Bei vorhandenem C5 Testat: Abgedeckt über COS-03
04.17	Wer administriert die Firewall des Auftragnehmers? ☐ eigene IT ☐ Externer Dienstleister		
04.18	**Wenn ein externer DL zum Einsatz kommt**: Kann sich dieser ohne Aufsicht durch Ihre IT auf ein System aufschalten? ☐ ja ☐ nein	Eine Remote-Administration der Firewall ohne Beaufsichtigung durch eigenes Personal ist nicht zulässig, es sei denn, es handelt sich um den beauftragten IT-Dienstleister.	
04.19	Werden die Zugriffsprotokolle (z. B. Anmeldungen und Firewall Logs) regelmäßig ausgewertet? ☐ ja, über eine Security Information and Event Management-Lösung (SIEM) ☐ nein, eine Auswertung wäre aber im Bedarfsfall möglich		

ID	FRAGE	MINDESTANFORDERUNG	ERLÄUTERUNGEN ODER DARSTELLUNG GLEICHWERTIGER MAßNAHMEN DES NUTZERS DER SCHNITTSTELLE
04.20	Werden Mitarbeitende vor der Nutzung von internen und externen Assets und Informationen auf deren zulässigen Gebrauch verpflichtet? ☐ ja, im Rahmen des Arbeitsvertrags ☐ ja, dediziert vor jedem neuen Gebrauch ☐ nein	Mitarbeitende müssen auf einen zulässigen Gebrauch verpflichtet werden.	Bei vorhandenem C5 Testat: Abgedeckt über AM-05
	Sind die dokumentierten Maßnahmen aus Ihrer Sicht unter Berücksichtigung des Stands der Technik, der Implementierungskosten, der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten der Betroffenen geeignet, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten? ☐ geeignet ☐ begrenzt geeignet ☐ ungeeignet Begründung: bitte angeben	Es muss bestätigt werden, dass die getroffenen Maßnahmen geeignet sein, um ein angemessenes Schutzniveau zu gewährleisten. Bei der Angabe „begrenzt geeignet“ muss eine Begründung erfolgen.	

5 MAßNAHMEN ZUM UMGANG MIT DATENTRÄGERN (ANALOG & DIGITAL)

ID	FRAGE	MINDESTANFORDERUNG	ERLÄUTERUNGEN ODER DARSTELLUNG GLEICHWERTIGER MAßNAHMEN DES NUTZERS DER SCHNITTSTELLE
05.01	Erfolgt eine Klassifizierung und ggf. Kennzeichnung sensibler Informationen? ☐ ja ☐ nein	Sensible Informationen müssen klassifiziert und ggf. gekennzeichnet werden, um den korrekten Umgang mit ihnen zu gewährleisten.	Bei vorhandenem C5 Testat: Abgedeckt über AM-06
05.02	Wie werden nicht mehr benötigte Papier-Unterlagen mit personenbezogenen Daten (bspw. Ausdrucke / Akten / Schriftwechsel) entsorgt? ☐ Altpapier / Restmüll ☐ Es stehen hierfür Schredder zur Verfügung, deren Nutzung angewiesen ist. ☐ Es sind verschlossene Datentonnen aufgestellt, die von einem Entsorgungsdienstleister zur datenschutzkonformen Vernichtung abgeholt werden. ☐ Sonstiges: bitte angeben	Es ist eine datenschutzkonforme sichere Vernichtungsart zu wählen.	
05.03	Wie werden nicht mehr benötigte Datenträger (USB-Sticks, Festplatten), auf denen personenbezogene Daten gespeichert sind, entsorgt? ☐ Physische Zerstörung durch eigene IT. ☐ Physische Zerstörung durch externen Dienstleister. ☐ Löschen der Daten durch bitte Anzahl angeben Überschreibungen ☐ Sonstiges: bitte angeben	Es ist eine sichere Vernichtungsart zu wählen.	Bei vorhandenem C5 Testat: Abgedeckt über AM-04
05.04	Dürfen im Unternehmen mobile Datenträger verwendet werden? (z. B. USB-Sticks) ☐ ja ☐ nein		

ID	FRAGE	MINDESTANFORDERUNG	ERLÄUTERUNGEN ODER DARSTELLUNG GLEICHWERTIGER MAßNAHMEN DES NUTZERS DER SCHNITTSTELLE
05.05	Dürfen die Mitarbeitenden private Datenträger (z. B. USB Sticks) verwenden? ☐ ja, aber Mitarbeitende sind angehalten, vorher einen Virencheck durchführen zu lassen. ☐ ja, aber nur nach Genehmigung und Überprüfung des Speichermediums durch die IT. ☐ nein, alle benötigten Speichermedien werden vom Unternehmen gestellt.	Die Verwendung ist auf unternehmenseigene Speichermedien beschränkt.	Bei vorhandenem C5 Testat: Abgedeckt über AM-03
05.06	Werden personenbezogene Daten beim Speichern verschlüsselt? ☐ Verschlüsselung auf dezentralen Endgeräten ☐ Verschlüsselung auf allen Systemen und Endgeräten ☐ keine Verschlüsselung	Die Daten auf Endgeräten sind zu verschlüsseln.	Bei vorhandenem C5 Testat: Abgedeckt über CRY-03
05.07	Verarbeiten Mitarbeitende personenbezogene Daten auch auf eigenen privaten Geräten (bring your own device)? ☐ ja ☐ nein	Das Halten personenbezogener Daten des Auftraggebers auf privaten Geräten des Auftragnehmers ist untersagt.	

ID	FRAGE	MINDESTANFORDERUNG	ERLÄUTERUNGEN ODER DARSTELLUNG GLEICHWERTIGER MAßNAHMEN DES NUTZERS DER SCHNITTSTELLE
	Sind die dokumentierten Maßnahmen aus Ihrer Sicht unter Berücksichtigung des Stands der Technik, der Implementierungskosten, der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten der Betroffenen geeignet, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten? ☐ geeignet ☐ begrenzt geeignet ☐ ungeeignet Begründung: bitte angeben	Es muss bestätigt werden, dass die getroffenen Maßnahmen geeignet sein, um ein angemessenes Schutzniveau zu gewährleisten. Bei der Angabe „begrenzt geeignet“ muss eine Begründung erfolgen.	

6 MAßNAHMEN ZUR DATENÜBERTRAGUNG

ID	FRAGE	MINDESTANFORDERUNG	ERLÄUTERUNGEN ODER DARSTELLUNG GLEICHWERTIGER MAßNAHMEN DES NUTZERS DER SCHNITTSTELLE
	Werden keine personenbezogenen Daten übertragen, sind die Fragen zu 6 nicht zu beantworten.		
06.01	Erfolgt der Transfer personenbezogener Daten durchgängig verschlüsselt? ☐ ja: ☐ per verschlüsselter Datei als Mailanhang ☐ per PGP / SMime ☐ per verschlüsseltem Datenträger ☐ per VPN ☐ per https / TLS ☐ per SFTP ☐ Sonstiges: bitte angeben ☐ nein	Beim Transfer personenbezogener Daten muss durch Verschlüsselung sichergestellt werden, dass keine unberechtigte Einsichtnahme Dritter möglich ist.	Bei vorhandenem C5 Testat: Abgedeckt über CRY-02
06.02	Wer verwaltet die Schlüssel/ Zertifikate? ☐ Anwender selbst ☐ eigene IT ☐ Externer Dienstleister		
06.03	Werden die Übertragungsvorgänge protokolliert? ☐ ja ☐ nein		
06.04	**Wenn 06.03 ja:** Wie lange werden diese Protokolldaten aufbewahrt? bitte angeben		

ID	FRAGE	MINDESTANFORDERUNG	ERLÄUTERUNGEN ODER DARSTELLUNG GLEICHWERTIGER MAßNAHMEN DES NUTZERS DER SCHNITTSTELLE
06.05	**Wenn 06.03 ja:** Werden die Protokolle regelmäßig ausgewertet? ☐ ja, über eine Security Information and Event Management-Lösung (SIEM) ☐ nein, eine Auswertung wäre aber im Bedarfsfall möglich		
06.06	Werden alle Systeme auf eine verlässliche gemeinsame Zeitquelle synchronisiert? ☐ ja ☐ nein	Systeme müssen auf eine gemeinsame Zeitquelle synchronisiert werden.	
	Sind die dokumentierten Maßnahmen aus Ihrer Sicht unter Berücksichtigung des Stands der Technik, der Implementierungskosten, der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten der Betroffenen geeignet, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten? ☐ geeignet ☐ begrenzt geeignet ☐ ungeeignet Begründung: bitte angeben	Es muss bestätigt werden, dass die getroffenen Maßnahmen geeignet sein, um ein angemessenes Schutzniveau zu gewährleisten. Bei der Angabe „begrenzt geeignet“ muss eine Begründung erfolgen.	

7 MAßNAHMEN FÜR SICHERE SERVERRÄUME / RECHENZENTRUMSGEBÄUDE

ID	FRAGE	MINDESTANFORDERUNG	ERLÄUTERUNGEN ODER DARSTELLUNG GLEICHWERTIGER MAßNAHMEN DES NUTZERS DER SCHNITTSTELLE
07.01	Verfügen die Serverräume über feuerfeste bzw. feuerhemmende Zugangstüren? ☐ ja ☐ nein	Zugangstüren müssen feuerhemmend bzw. feuerfest sein.	Bei vorhandenem C5 Testat: Abgedeckt über PS-05
07.02	Sind die Serverräume / RZ mit Rauchmeldern ausgestattet? ☐ ja ☐ nein	Es müssen Rauchmelder vorhanden sein.	Bei vorhandenem C5 Testat: Abgedeckt über PS-05
07.03	Sind die Serverräume / RZ an eine Brandmeldezentrale angeschlossen? ☐ ja ☐ nein	Der Anschluss an eine Brandmeldezentrale ist Pflicht.	Bei vorhandenem C5 Testat: Abgedeckt über PS-05
07.04	Sind die Serverräume / RZ mit Löschsystemen ausgestattet? ☐ ja ☐ nein	Es muss ein Löschsystem vorhanden sein.	Bei vorhandenem C5 Testat: Abgedeckt über PS-05
07.05	Woraus bestehen die Außenwände der Serverräume / RZ? bitte angeben		
07.06	Sind die Serverräume / RZ klimatisiert? ☐ ja ☐ nein	Die Klimatisierung ist zwingend erforderlich.	Bei vorhandenem C5 Testat: Abgedeckt über PS-06

ID	FRAGE	MINDESTANFORDERUNG	ERLÄUTERUNGEN ODER DARSTELLUNG GLEICHWERTIGER MAßNAHMEN DES NUTZERS DER SCHNITTSTELLE
07.07	Verfügen die Serverräume / RZ über eine unterbrechungsfreie Stromversorgung (USV)? ☐ ja ☐ nein	Der Einsatz einer USV ist zwingend erforderlich.	Bei vorhandenem C5 Testat: Abgedeckt über PS-06
07.08	Wird die Stromversorgung der Serverräume / RZ zusätzlich über ein Dieselaggregat abgesichert? ☐ ja ☐ nein		
07.09	Werden die Funktionalität 07.02, 07.03, 07.04, 07.06, 07.07 und 07.08, sofern vorhanden, regelmäßig getestet? ☐ ja ☐ nein		
07.10	Sind die internen Managementnetze/Betriebs-netze (z. B. zur Gebäudeleittechnik, Videoüberwachung, Zutrittskontrolle) vor externem Zugriff geschützt? ☐ ja, bitte angeben ☐ nein	Ein zusätzlicher Schutz durch angemessenes Zugriffs- (z. B. Passwort, 2FA, …) und Rechtemanagement ist zu gewährleisten.	Bei vorhandenem C5 Testat: Abgedeckt über COS-05
07.11	Erfolgt eine regelmäßige Wartung von Geräten und Betriebsmitteln? ☐ ja ☐ nein	Es erfolgt eine regelmäßige Wartung.	Bei vorhandenem C5 Testat: Abgedeckt über PS-06

ID	FRAGE	MINDESTANFORDERUNG	ERLÄUTERUNGEN ODER DARSTELLUNG GLEICHWERTIGER MAßNAHMEN DES NUTZERS DER SCHNITTSTELLE
	Sind die dokumentierten Maßnahmen aus Ihrer Sicht unter Berücksichtigung des Stands der Technik, der Implementierungskosten, der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten der Betroffenen geeignet, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten? ☐ geeignet ☐ begrenzt geeignet ☐ ungeeignet Begründung: bitte angeben	Es muss bestätigt werden, dass die getroffenen Maßnahmen geeignet sein, um ein angemessenes Schutzniveau zu gewährleisten. Bei der Angabe „begrenzt geeignet“ muss eine Begründung erfolgen.	

8 MAßNAHMEN ZUM BACKUP

ID	FRAGE	MINDESTANFORDERUNG	ERLÄUTERUNGEN ODER DARSTELLUNG GLEICHWERTIGER MAßNAHMEN DES NUTZERS DER SCHNITTSTELLE
08.01	Existiert ein Backupkonzept für Systeme, auf denen personenbezogene Daten gespeichert sind? ☐ ja ☐ nein	Ein Backupkonzept muss vorhanden sein.	Bei vorhandenem C5 Testat: Abgedeckt über OPS-06
	Wenn 08.01 nein: fortfahren mit **09.01**		
08.02	Wird die Funktionalität der Backup / Wiederherstellung regelmäßig getestet? ☐ ja ☐ nein		Bei vorhandenem C5 Testat: Abgedeckt über OPS-08
08.03	In welchem Rhythmus werden Backups von Systemen angefertigt, auf denen personenbezogene Daten gespeichert werden? bitte angeben		
08.04	**Im Falle eines Transports der Backups:** Wie wird dieser durchgeführt? bitte angeben		
08.05	Sind die Backups verschlüsselt? ☐ ja ☐ nein	Backups müssen verschlüsselt sein.	Bei vorhandenem C5 Testat: Abgedeckt über OPS-06

ID	FRAGE	MINDESTANFORDERUNG	ERLÄUTERUNGEN ODER DARSTELLUNG GLEICHWERTIGER MAßNAHMEN DES NUTZERS DER SCHNITTSTELLE
08.06	Befindet sich der Aufbewahrungsort der Backups in einem (von den Serverräumen aus betrachtet) getrennten Brandabschnitt bzw. Gebäudeteil? ☐ ja ☐ nein	Backups müssen in einem getrennten Brandabschnitt bzw. Gebäudeteil aufbewahrt werden.	Bei vorhandenem C5 Testat: Abgedeckt über OPS-09
	Sind die dokumentierten Maßnahmen aus Ihrer Sicht unter Berücksichtigung des Stands der Technik, der Implementierungskosten, der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten der Betroffenen geeignet, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten? ☐ geeignet ☐ begrenzt geeignet ☐ ungeeignet Begründung: bitte angeben	Es muss bestätigt werden, dass die getroffenen Maßnahmen geeignet sein, um ein angemessenes Schutzniveau zu gewährleisten. Bei der Angabe „begrenzt geeignet“ muss eine Begründung erfolgen.	

9 MAßNAHMEN ZUR ABWEHR VON ANGRIFFEN

ID	FRAGE	MINDESTANFORDERUNG	ERLÄUTERUNGEN ODER DARSTELLUNG GLEICHWERTIGER MAßNAHMEN DES NUTZERS DER SCHNITTSTELLE
09.01	Werden aktive Kontakte zu relevanten Behörden und Fachgremien gepflegt (z. B. für Bedrohungsinformationen)? ☐ ja ☐ nein	Kontakte müssen gepflegt werden.	Bei vorhandenem C5 Testat: Abgedeckt über OIS-05
09.02	Sind die IT-Systeme technisch vor Angriffen geschützt? ☐ ja ☐ nein		
09.03	**Wenn 09.02 ja:** Wer ist für die Aktualisierung von Virenschutz, Anti-Spyware und Spamfilter zuständig? bitte angeben		
09.04	Erfolgt eine Separierung von Netzen unterschiedlichen Schutzbedarfs (z. B. DMZ und Intern, Produktions- und Entwicklungsnetz)? ☐ ja ☐ nein	Eine Netztrennung ist zwingend erforderlich.	Bei vorhandenem C5 Testat: Abgedeckt über DEV-10 & COS-03
09.05	Werden gefährliche/unerwünschte Websites für Mitarbeitende gesperrt? ☐ ja ☐ nein	Gefährliche oder unerwünschte Websites werden gesperrt.	

ID	FRAGE	MINDESTANFORDERUNG	ERLÄUTERUNGEN ODER DARSTELLUNG GLEICHWERTIGER MAßNAHMEN DES NUTZERS DER SCHNITTSTELLE
09.06	Werden Systeme gehärtet? ☐ ja: ☐ Patchmanagement ☐ Deaktivierung unnötiger Komponenten ☐ Aktivierung hardwarenaher Schutzfunktionen ☐ Sicherheitskonfiguration ☐ Minimale Vergabe von Berechtigungen (z. B. Role Based Access Control) ☐ Konten und Kennwörter ☐ Einschränkung der Netzwerkkommunikation ☐ Protokollierung ☐ Sonstiges: bitte angeben ☐ nein	Systeme müssen durch möglichst alle aufgeführten Maßnahmen gehärtet werden. Nicht umgesetzte Maßnahmen müssen begründet werden.	Bei vorhandenem C5 Testat: Abgedeckt über AM-02, OPS-05, PSS-08, OPS-13 & OPS-23
09.07	Existiert ein Ablauf zur Erkennung und Bearbeitung von Vorfällen? ☐ ja ☐ nein	Es gibt einen Incidentmanagementprozess.	Bei vorhandenem C5 Testat: Abgedeckt über SIM-01
09.08	Werden Betroffene zeitnah über Angriffe informiert? ☐ ja: ☐ durch ein ungeregeltes Vorgehen ☐ durch ein geregeltes Vorgehen ☐ durch ein geregeltes Vorgehen (inkl. Rollen- und Kommunikations-vorgaben) ☐ nein	Meldungen zu Informationssicher-heitsvorfällen müssen zeitnah erfolgen und Verantwortlichkeiten im Prozess geklärt sein.	Bei vorhandenem C5 Testat: Abgedeckt über SIM-01

ID	FRAGE	MINDESTANFORDERUNG	ERLÄUTERUNGEN ODER DARSTELLUNG GLEICHWERTIGER MAßNAHMEN DES NUTZERS DER SCHNITTSTELLE
09.09	Werden im Anschluss an einen erfolgreichen Angriff Betroffene über Angriffsdetails und Maßnahmen informiert? ☐ ja: ☐ durch ein ungeregeltes Vorgehen ☐ durch ein geregeltes Vorgehen ☐ durch ein geregeltes Vorgehen (inkl. Rollen- und Kommunikations-vorgaben) ☐ nein	Details zu Informationssicherheitsvorfällen müssen, geregelt durch Verantwortlichkeiten im Prozess, kommuniziert werden.	Bei vorhandenem C5 Testat: Abgedeckt über SIM-01
	Sind die dokumentierten Maßnahmen aus Ihrer Sicht unter Berücksichtigung des Stands der Technik, der Implementierungskosten, der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten der Betroffenen geeignet, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten? ☐ geeignet ☐ begrenzt geeignet ☐ ungeeignet Begründung: bitte angeben	Es muss bestätigt werden, dass die getroffenen Maßnahmen geeignet sein, um ein angemessenes Schutzniveau zu gewährleisten. Bei der Angabe „begrenzt geeignet“ muss eine Begründung erfolgen.	

10 WEITERE MAßNAHMEN ZUR PRÄVENTION UND REAKTION

ID	FRAGE	MINDESTANFORDERUNG	ERLÄUTERUNGEN ODER DARSTELLUNG GLEICHWERTIGER MAßNAHMEN DES NUTZERS DER SCHNITTSTELLE
10.01	Existiert ein dokumentierter Prozess zum Change- und Patchmanagement? ☐ ja ☐ nein	Koordinierte regelmäßige Updates der Systeme sind erforderlich.	Bei vorhandenem C5 Testat: Abgedeckt über DEV-03
10.02	**Wenn 10.01 ja:** Wer ist für die Installation von Updates bzw. Patches zuständig? bitte angeben		
10.03	Werden Änderungen an System- und Entwicklungstools protokolliert? ☐ ja ☐ nein	Eine Protokollierung bzw. Versionierung ist erforderlich.	Bei vorhandenem C5 Testat: Abgedeckt über DEV-07
10.04	Werden Anwendungen über ihren gesamten Lebenszyklus nach klar definierten Sicherheitsanforderungen entwickelt, betrieben und geschützt? ☐ ja ☐ nein	Es muss ein sicherer Entwicklungsprozess existieren.	Bei vorhandenem C5 Testat: Abgedeckt über DEV-01
10.05	Werden neue oder geänderte Systeme getestet? ☐ ja ☐ nein	Ein Test ist erforderlich.	Bei vorhandenem C5 Testat: Abgedeckt über DEV-06
10.06	Existiert ein Prozess zum Assetmanagement? ☐ ja, dieser wird gelebt ☐ ja, dieser ist dokumentiert und wird gelebt ☐ nein	Ein Assetmangementprozess ist vorhanden und dokumentiert.	Bei vorhandenem C5 Testat: Abgedeckt über AM-01

ID	FRAGE	MINDESTANFORDERUNG	ERLÄUTERUNGEN ODER DARSTELLUNG GLEICHWERTIGER MAßNAHMEN DES NUTZERS DER SCHNITTSTELLE
10.07	Werden regelmäßige Schwachstellenprüfungen durchgeführt? ☐ ja ☐ nein	Regelmäßige Schwachstellenprüfungen sind erforderlich.	Bei vorhandenem C5 Testat: Abgedeckt über OPS-22
10.08	Existiert ein Notfallkonzept (bspw. Notfallmaßnahmen bei Hardware-defekt, Brand, Totalverlust etc.) und findet ein regelmäßiger Test dieses bzw. von Teilen davon statt? ☐ Notfallkonzept existiert ☐ Notfallkonzept wird regelmäßig getestet ☐ nein	Notfallkonzept wird regelmäßig getestet.	Bei vorhandenem C5 Testat: Abgedeckt über BCM-03
10.09	Gibt es eine redundante Systemarchitektur? ☐ ja ☐ nein		
10.10	Verfügt das Unternehmen über eine redundante Internetanbindung? ☐ ja ☐ nein		
10.11	Sind die einzelnen Standorte des Unternehmens redundant miteinander verbunden? ☐ ja ☐ nein		
10.12	Wer ist für die Netzanbindung des Unternehmens verantwortlich? ☐ eigene IT ☐ Externer Dienstleister		

ID	FRAGE	MINDESTANFORDERUNG	ERLÄUTERUNGEN ODER DARSTELLUNG GLEICHWERTIGER MAßNAHMEN DES NUTZERS DER SCHNITTSTELLE
10.13	Es werden nur zuverlässige Personen zur Leistungserbringung eingesetzt, die über entsprechende Kenntnisse und Fähigkeiten für ihre Aufgaben verfügen: ☐ ja ☐ nein		
10.14	Werden Personal- und IT-Ressourcen geplant und überwacht? ☐ ja ☐ nein	Personal- und IT-Ressourcen werden geplant und überwacht.	Bei vorhandenem C5 Testat: Abgedeckt über OPS-01 & OPS-02
10.15	Werden personenbezogene Daten pseudonymisiert verarbeitet ☐ ja ☐ ja, eine Zuordnung zu einer betroffenen Person ist nur mit zusätzlichen, gesondert aufbewahrten Informationen möglich ☐ nein	Die Pseudonymisierung besonders schutzbedürftiger Daten erfolgt mittels kryptografisch sicherer. Eine Re-Identifizierung ist technisch erschwert, streng reglementiert und vollständig protokolliert.	Bei vorhandenem C5 Testat: Abgedeckt über OPS-11
10.16	**Wenn 10.15 ja:** Erfolgt Pseudonymisierung auch in Test-, Analyse- oder Entwicklungsumgebungen? ☐ ja ☐ nein	Bei Test-, Analyse- oder Entwicklungsumgebungen muss Pseudonymisierung eingesetzt werden.	

ID	FRAGE	MINDESTANFORDERUNG	ERLÄUTERUNGEN ODER DARSTELLUNG GLEICHWERTIGER MAßNAHMEN DES NUTZERS DER SCHNITTSTELLE
	Sind die dokumentierten Maß-nahmen aus Ihrer Sicht unter Berücksichtigung des Stands der Technik, der Implementierungs-kosten, der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten der Betroffenen geeignet, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten? ☐ geeignet ☐ begrenzt geeignet ☐ ungeeignet Begründung: bitte angeben	Es muss bestätigt werden, dass die getroffenen Maßnahmen geeignet sein, um ein angemessenes Schutzniveau zu gewährleisten. Bei der Angabe „begrenzt geeignet“ muss eine Begründung erfolgen.	

11 REGELMÄßIGE ÜBERPRÜFUNG, BEWERTUNG UND EVALUIERUNG DER WIRKSAMKEIT DER TECHNISCH-ORGANISATORISCHEN MAßNAHMEN

ID	FRAGE	MINDESTANFORDERUNG	ERLÄUTERUNGEN ODER DARSTELLUNG GLEICHWERTIGER MAßNAHMEN DES NUTZERS DER SCHNITTSTELLE
11.01	**Wenn 09.06 ja:** Wird die Härtung regelmäßig bei laufenden Systemen geprüft? ☐ ja ☐ nein		
11.02	Findet eine unabhängige Überprüfung der IT-Systeme/des Netzwerkes statt? ☐ ja: ☐ Penetrationstests ☐ Sonstiges: bitte angeben ☐ nein		
11.03	Werden Tests im Rahmen von Audits mit minimalem Zugriff, ohne Störungen und mit vollständiger Protokollierung durchgeführt? ☐ ja ☐ nein	Es existieren Vorgaben zur reibungslosen Durchführung von Audits.	Bei vorhandenem C5 Testat: Abgedeckt über COM-02
11.04	Erfolgt eine Überprüfung, Bewertung und Evaluierung der technisch-organisatorischen Maßnahmen? ☐ ja: ☐ Interne Audits	Es muss durch mindestens zwei geeignete Verfahren sichergestellt werden, dass eine regelmäßige Prüfung, Aktualisierung und Dokumentation der technisch-	Bei vorhandenem C5 Testat: Abgedeckt über SSO-04

ID	FRAGE	MINDESTANFORDERUNG	ERLÄUTERUNGEN ODER DARSTELLUNG GLEICHWERTIGER MAßNAHMEN DES NUTZERS DER SCHNITTSTELLE
	☐ Externe Audits ☐ Überprüfung durch Wirtschaftsprüfer ☐ Interne Revision ☐ Prüfung durch Compliance-Beauftragten ☐ Austausch zwischen Informations-sicherheitsbeauftragten und Datenschutzbeauftragten ☐ Überprüfung durch Rechtsaufsicht ☐ Aufrechterhaltung von Zertifikaten: bitte Zertifikate angeben ☐ Sonstiges: bitte angeben ☐ nein	organisatorischen Maßnahmen stattfindet. Davon erfolgt mindestens eine Maßnahme durch Dritte.	
	Sind die dokumentierten Maßnahmen aus Ihrer Sicht unter Berücksichtigung des Stands der Technik, der Imple-mentierungskosten, der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrschein-lichkeit und Schwere des Risikos für die Rechte und Freiheiten der Betroffenen geeignet, um ein dem Risiko angemes-senes Schutzniveau zu gewährleisten? ☐ geeignet ☐ begrenzt geeignet ☐ ungeeignet Begründung: bitte angeben	Es muss bestätigt werden, dass die getroffenen Maßnahmen geeignet sein, um ein angemessenes Schutzniveau zu gewährleisten. Bei der Angabe „begrenzt geeignet“ muss eine Begründung erfolgen.	