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

[KBV_ITV_FMEX_TOM_370a]

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

INHALT

1 MAßNAHMEN ZUM ZUTRITT ZU SYSTEMEN

	FRAGE	SCHUTZ-STUFE	MINDESTANFORDERUNG	ERLÄUTERUNGEN ODER DARSTELLUNG GLEICHWERTIGER MAßNAHMEN DES AUFTRAGNEHMERS
1.1	Werden personenbezogene Daten in Serverräumen oder Rechenzentren (zwischen-)gespeichert oder weitergeleitet, die von dem Auftragnehmer verantwortet werden? ☐ ja ☐ nein	A		
	Wenn 1.1 nein: In diesem Fall müssen die weiteren Fragen zu 1 nicht beantwortet werden, sondern sogleich die Fragen ab 2. Auch die Fragen zu 6 und 7 entfallen.			
1.2	Standort(e) an denen der Auftragnehmer die Systeme betreibt: bitte angeben	B	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,	

	FRAGE	SCHUTZ-STUFE	MINDESTANFORDERUNG	ERLÄUTERUNGEN ODER DARSTELLUNG GLEICHWERTIGER MAßNAHMEN DES AUFTRAGNEHMERS
			liegen.	
1.3	Sind die personenbezogenen Daten auf mehr als einem System je Standort verteilt (z. B. für Backup / Datenreplikation / Nutzung von Cloud-Dienstleistungen)? ☐ ja ☐ nein	B		
1.4	Aus welchem Material bestehen die Zugangstüren zu den Serverräumen (Stahl oder sonstiges Material)? bitte angeben	B	Alle Bauelemente der Gebäudehülle müssen mindestens RC 2 gemäß DIN EN 1627-1630:11 erfüllen.	
1.5	Sind Serverräume fensterlos? ☐ ja ☐ nein	B		
1.6	**Wenn 1.5 nein:** Wie sind die Fenster vor Einbruch geschützt? bitte angeben	B	Alle Bauelemente der Gebäudehülle müssen mindestens RC 2 gemäß DIN EN 1627-1630:11 erfüllen.	
1.7	Sind Serverräume / RZ mittels einer Einbruchmeldeanlage (EMA) alarmgesichert? ☐ ja	B	Einbruchmeldeanlage muss vorhanden sein.	

	FRAGE	SCHUTZ-STUFE	MINDESTANFORDERUNG	ERLÄUTERUNGEN ODER DARSTELLUNG GLEICHWERTIGER MAßNAHMEN DES AUFTRAGNEHMERS
	☐ nein			
1.8	**Wenn 1.7 ja:** Wer wird informiert, wenn die EMA auslöst? **Mehrfachantworten möglich!** ☐ beauftragter Wachdienst ☐ Administrator ☐ Leiter IT ☐ Sonstiges: bitte angeben	C	Eine Alarmaufschaltung ist verpflichtend. Mindestens eine der zu alarmierenden Stellen muss 24/7 erreichbar sein und reagieren.	
1.9	Sind Serverräume / RZ videoüberwacht? ☐ ja ☐ nein	B	Eine Videoüberwachung ist verpflichtend.	
1.10	**Wenn 1.9 ja:** Wie lange werden die Bilddaten gespeichert? bitte angeben	B	Die Videoaufzeichnungen müssen mindestens 24 h vorgehalten werden.	
1.11	Wie viele Personen haben Zutritt zu den Serverräumen und welche Funktionen haben diese inne? bitte angeben	B	Nur ausgewählte, berechtigte Personen dürfen Zutritt erlangen. Die Zutrittsberechtigung darf nur personengebunden vergeben werden.	
1.12	Existiert ein Prozess zur Vergabe von Zutrittsberechtigungen bei der Neueinstellung und beim Ausscheiden	A	Ein definierter Freigabeprozess ist erforderlich.	

	FRAGE	SCHUTZ-STUFE	MINDESTANFORDERUNG	ERLÄUTERUNGEN ODER DARSTELLUNG GLEICHWERTIGER MAßNAHMEN DES AUFTRAGNEHMERS
	von Mitarbeitenden bzw. bei organisatorischen Veränderungen? ☐ definierter Freigabeprozess ☐ kein definierter Freigabeprozess, auf Zuruf ☐ Sonstige Vergabeweise: bitte angeben			
1.13	Sind Serverräume mit einem elektronischen Schließsystem versehen? ☐ ja ☐ nein	B	Ein elektronisches Schließsystem ist erforderlich.	
1.14	**Wenn 1.13 ja:** Welche Zutrittstechnik kommt zum Einsatz? **Mehrfachantworten möglich!** bitte angeben	B	Mindestens zwei aus drei Authentifizierungskomponenten (Besitz, Wissen oder biometrische Charakteristika) sind für den Zutritt erforderlich.	
1.15	**Wenn 1.13 ja:** Werden die Zutritte zu Serverräumen protokolliert? ☐ ja ☐ nein	B		
1.16	**Wenn 1.15 ja:** Wie lange werden die Zutrittsdaten gespeichert? bitte angeben	B		

	FRAGE	SCHUTZ-STUFE	MINDESTANFORDERUNG	ERLÄUTERUNGEN ODER DARSTELLUNG GLEICHWERTIGER MAßNAHMEN DES AUFTRAGNEHMERS
1.17	**Wenn 1.15 ja:** Werden die Protokolle regelmäßig ausgewertet? ☐ ja ☐ nein	B		
1.18	Ist der Zutritt zu den Serverräumen (auch) mechanisch mit Schlüssel möglich? ☐ ja ☐ nein	B		
1.19	**Wenn 1.17 ja:** Wo werden die Schlüssel aufbewahrt und wer gibt sie aus? bitte angeben	B		
1.20	Existiert ein Pförtnerdienst / Wachdienst / besetzter Empfangsbereich o. ä. zum Rechenzentrum/Serverraum? ☐ ja ☐ nein	B		
1.21	Werden die Serverräume neben ihrer eigentlichen Funktion noch für andere Zwecke genutzt?	A		

	FRAGE	SCHUTZ-STUFE	MINDESTANFORDERUNG	ERLÄUTERUNGEN ODER DARSTELLUNG GLEICHWERTIGER MAßNAHMEN DES AUFTRAGNEHMERS
	☐ ja ☐ nein	B	Die Nutzung von Serverräumen für andere Zwecke ist nicht erlaubt.	
1.22	**Wenn 1.19 ja:** Für welche Zwecke werden die Serverräume noch genutzt? bitte angeben	B		
1.23	Gibt es offizielle Zutrittsregelung für betriebsfremde Personen (bspw. Besucher) zu den Serverräumen? ☐ ja, bitte angeben ☐ nein	A	Eine offizielle Zutrittsregelung für betriebsfremde Personen ist zwingend erforderlich.	
	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		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.	

	FRAGE	SCHUTZ-STUFE	MINDESTANFORDERUNG	ERLÄUTERUNGEN ODER DARSTELLUNG GLEICHWERTIGER MAßNAHMEN DES AUFTRAGNEHMERS
	☐ begrenzt geeignet ☐ ungeeignet Begründung: bitte angeben			

2 MAßNAHMEN ZUM ZUTRITT ZU BÜRORÄUMEN

	FRAGE	SCHUTZ-STUFE	MINDESTANFORDERUNG	ERLÄUTERUNGEN ODER DARSTELLUNG GLEICHWERTIGER MAßNAHMEN DES AUFTRAGNEHMERS
2.1	An welchen Standorten wird über Clientarbeitsplätze auf personenbezogene Daten zugegriffen? bitte angeben	A		
2.2	Existiert ein Pförtnerdienst / Wachdienst / besetzter Empfangsbereich o. ä. zum Gebäude bzw. zu Ihren Büros? ☐ ja ☐ nein	B		
2.3	Ist das Gebäude oder sind die Büroräume mittels einer Einbruchmeldeanlage (EMA) alarmgesichert? ☐ ja ☐ nein	C	Einbruchmeldeanlage muss vorhanden sein.	
2.4	**Wenn 2.3 ja:** Wer wird informiert, wenn die EMA auslöst? **Mehrfachantworten möglich!** ☐ beauftragter Wachdienst ☐ Administrator ☐ Leiter IT	C	Eine Alarmaufschaltung ist verpflichtend. Mindestens eine der zu alarmierenden Stellen muss 24/7 erreichbar sein und reagieren.	

	FRAGE	SCHUTZ-STUFE	MINDESTANFORDERUNG	ERLÄUTERUNGEN ODER DARSTELLUNG GLEICHWERTIGER MAßNAHMEN DES AUFTRAGNEHMERS
	☐ Sonstiges: bitte angeben			
2.5	Werden das Bürogebäude bzw. seine Zugänge videoüberwacht? ☐ ja, ohne Bildaufzeichnung ☐ ja, mit Bildaufzeichnung ☐ nein	B		
2.6	**Wenn 2.5 „ja, mit Bildaufzeichnung“:** Wie lange werden die Bilddaten gespeichert? bitte angeben	B		
2.7	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	A		
		C	Ein elektronisches Schließsystem ist erforderlich.	
2.8	**Wenn 2.7 ja:** Welche Zutrittstechnik kommt zum Einsatz? ☐ RFID	A		

	FRAGE	SCHUTZ-STUFE	MINDESTANFORDERUNG	ERLÄUTERUNGEN ODER DARSTELLUNG GLEICHWERTIGER MAßNAHMEN DES AUFTRAGNEHMERS
	☐ PIN ☐ Biometrie ☐ Sonstiges: bitte angeben	C	Mindestens zwei verschiedene Techniken müssen genutzt werden.	
2.9	**Wenn 2.7 ja:** Werden die Zutritte im Zutrittssystem protokolliert? ☐ ja, sowohl erfolgreiche als auch erfolglose Zutrittsversuche ☐ ja, aber nur erfolgreiche Zutrittsversuche ☐ ja, aber nur erfolglose Zutrittsversuche ☐ nein, das Schloss wird nur freigegeben oder nicht	A		
		C	Es muss mindestens ein „Ja“ ausgewählt werden.	
2.10	**Wenn 2.9 ja:** Wie lange werden diese Protokolldaten aufbewahrt? bitte angeben	B		
2.11	**Wenn 2.9 ja:** Werden die Protokolle regelmäßig ausgewertet? ☐ ja ☐ nein	B		
2.12	Existiert ein mechanisches Schloss für die Gebäude / Büroräume? ☐ ja	A		

	FRAGE	SCHUTZ-STUFE	MINDESTANFORDERUNG	ERLÄUTERUNGEN ODER DARSTELLUNG GLEICHWERTIGER MAßNAHMEN DES AUFTRAGNEHMERS
	☐ nein			
2.13	**Wenn 2.12 ja:** Wird die Ausgabe der (mechanischen und/oder elektronischen) Schlüssel protokolliert? ☐ ja, bitte angeben ☐ nein	A		
2.14	**Wenn 2.12 ja:** Wer gibt die (mechanischen und/oder elektronischen) Schlüssel aus? bitte angeben	A	Es muss festgelegt sein, wer eine Schlüsselausgabe vornehmen darf.	
2.15	Werden die Zutrittsrechte/Schlüssel zu Büros personenbezogen vergeben? ☐ ja ☐ nein	A		
		B	Personenbezogene Zutrittsrechte/Schlüssel sind zwingend erforderlich.	
2.16	Gibt es offizielle Zutrittsregelung für betriebsfremde Personen (bspw. Besucher) zu den Büroräumen? ☐ ja, bitte angeben ☐ nein	A	Eine offizielle Zutrittsregelung für betriebsfremde Personen ist zwingend erforderlich.	
	Sind die dokumentierten Maßnahmen aus Ihrer Sicht unter Berücksichtigung		Es muss bestätigt werden, dass die getroffenen Maßnahmen geeignet	

	FRAGE	SCHUTZ-STUFE	MINDESTANFORDERUNG	ERLÄUTERUNGEN ODER DARSTELLUNG GLEICHWERTIGER MAßNAHMEN DES AUFTRAGNEHMERS
	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		sein, um ein angemessenes Schutzniveau zu gewährleisten. Bei der Angabe „begrenzt geeignet“ muss eine Begründung erfolgen.	

3 MAßNAHMEN ZUM ZUGANG UND ZUGRIFF

	FRAGE	SCHUTZ-STUFE	MINDESTANFORDERUNG	ERLÄUTERUNGEN ODER DARSTELLUNG GLEICHWERTIGER MAßNAHMEN DES AUFTRAGNEHMERS
3.1	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	A	Ein definierter Freigabeprozess ist erforderlich.	
3.2	Werden die Vergabe bzw. Änderungen von Zugriffsberechtigungen protokolliert? ☐ ja ☐ nein	B	Eine Protokollierung ist erforderlich.	
3.3	Authentisieren sich die Mitarbeitenden über eine individuelle Kennung gegenüber dem zentralen Verzeichnisdienst? ☐ ja ☐ nein	B	Authentisierung gegen einen zentralen Verzeichnisdienst ist erforderlich.	

	FRAGE	SCHUTZ-STUFE	MINDESTANFORDERUNG	ERLÄUTERUNGEN ODER DARSTELLUNG GLEICHWERTIGER MAßNAHMEN DES AUFTRAGNEHMERS
3.4	Existieren verbindliche Passwortparameter im Unternehmen? ☐ ja ☐ nein	A	Verbindliche Password-Policy ist erforderlich.	
3.5	**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): (~! @ # $% ^& * -+ = ' | \ \ (){}\ []:; "' <>,.? /)	A	Die Passwortlänge muss mindestens 10 Zeichen sein. Für die Passwortkomplexität müssen drei der vier Kategorien (Großbuchstaben, Kleinbuchstaben, Ziffern oder nicht alphanumerische Zeichen) enthalten sein.	
		B	Die Passwortlänge muss mindestens 12 Zeichen sein. Für die Passwortkomplexität müssen drei der vier Kategorien (Großbuchstaben, Kleinbuchstaben, Ziffern oder nicht alphanumerische Zeichen) enthalten sein.	
		C	Die Passwortlänge muss mindestens 12 Zeichen sein. Für die Passwortkomplexität müssen alle vier Kategorien (Großbuchstaben, Kleinbuchstaben, Ziffern oder nicht alphanumerische Zeichen) enthalten sein. - ODER -	

	FRAGE	SCHUTZ-STUFE	MINDESTANFORDERUNG	ERLÄUTERUNGEN ODER DARSTELLUNG GLEICHWERTIGER MAßNAHMEN DES AUFTRAGNEHMERS
			Es wird eine Multi-Faktor-Authentifizierung eingesetzt.	
3.6	Zwingt das IT System den Nutzer zur Einhaltung der oben genannten Passwortvorgaben? ☐ ja ☐ nein	B	Die IT-technische Unterstützung der Einhaltung der Password-Policy ist erforderlich.	
3.7	Wird der Bildschirm bei Inaktivität des Benutzers gesperrt? ☐ ja, nach bitte Anzahl angeben Minuten ☐ nein	A	Die Bildschirmsperre muss automatisch aktiviert werden.	
		B	Die Bildschirmsperre muss automatisch nach spätestens 10 Minuten Inaktivität aktiviert werden.	
3.8	Welche Maßnahmen ergreifen Sie bei Verlust, Vergessen oder Ausspähen eines Passworts? bitte angeben	A	Ein definierter Prozess muss existieren.	
3.9	Gibt es eine Begrenzung von erfolglosen Anmeldeversuchen?	A	Es muss eine Anmeldesperre eingerichtet sein.	

	FRAGE	SCHUTZ-STUFE	MINDESTANFORDERUNG	ERLÄUTERUNGEN ODER DARSTELLUNG GLEICHWERTIGER MAßNAHMEN DES AUFTRAGNEHMERS
	☐ ja, nach bitte Anzahl angeben erfolglosen Versuchen. ☐ nein	B	Es muss eine Anmeldesperre spätestens nach 10 erfolglosen Anmeldeversuchen eingerichtet sein.	
3.10	**Wenn 3.9 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 Minuten gesperrt.	A		
		C	Zugänge müssen bis zur manuellen Aufhebung gesperrt bleiben.	
3.11	Ist der Zugriff auf Daten aus dem Internet (z. B. im Home Office) möglich? ☐ ja ☐ nein	A		
3.12	**Wenn 3.11 ja:** Wie erfolgt die Authentisierung: ☐ (RSA) Token ☐ VPN-Zertifikat	A	Mindestens eine aus drei Authentifizierungskomponenten (Besitz, Wissen oder biometrische Charakteristika) sind für den Zugriff erforderlich.	

	FRAGE	SCHUTZ-STUFE	MINDESTANFORDERUNG	ERLÄUTERUNGEN ODER DARSTELLUNG GLEICHWERTIGER MAßNAHMEN DES AUFTRAGNEHMERS
	☐ pre-shared key ☐ Benutzeraccount	B	Mindestens zwei aus drei Authentifizierungskomponenten (Besitz, Wissen oder biometrische Charakteristika) sind für den Zugriff erforderlich.	
3.13	**Wenn 3.11 ja:** Gibt es eine Begrenzung von erfolglosen Anmeldeversuchen bei Fernzugängen? ☐ ja, bitte Anzahl angeben Versuche pro Tag ☐ nein	A	Es muss eine Anmeldesperre eingerichtet sein.	
		B	Es muss eine Anmeldesperre spätestens nach 10 erfolglosen Anmeldeversuchen eingerichtet sein.	
3.14	**Wenn 3.13 ja:** Wie lange bleiben Zugänge gesperrt, wenn die maximale Zahl erfolgloser Anmeldeversuche erreicht worden ist? ☐ Die Zugänge bleiben bis zur manuellen Aufhebung der Sperre gesperrt ☐ Die Zugänge bleiben für bitte Anzahl Minuten gesperrt.	A		
		C	Zugänge müssen bis zur manuellen Aufhebung gesperrt bleiben.	
3.15	Werden Firewalls eingesetzt? ☐ ja ☐ nein	A	Firewalls sind zwingend erforderlich.	

	FRAGE	SCHUTZ-STUFE	MINDESTANFORDERUNG	ERLÄUTERUNGEN ODER DARSTELLUNG GLEICHWERTIGER MAßNAHMEN DES AUFTRAGNEHMERS
3.16	Wer administriert die Firewall des Auftragnehmers? ☐ eigene IT ☐ Externer Dienstleister	A		
3.17	**Wenn ein externer DL zum Einsatz kommt**: Kann sich dieser ohne Aufsicht durch Ihre IT auf ein System aufschalten? ☐ ja ☐ nein	B	Eine Remote-Administration der Firewall ohne Beaufsichtigung durch eigenes Personal ist nicht zulässig, es sei denn, es handelt sich um den beauftragten IT-Dienstleister.	
3.18	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	B		
	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		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.	

	FRAGE	SCHUTZ-STUFE	MINDESTANFORDERUNG	ERLÄUTERUNGEN ODER DARSTELLUNG GLEICHWERTIGER MAßNAHMEN DES AUFTRAGNEHMERS
	und Freiheiten der Betroffenen geeignet, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten? ☐ geeignet ☐ begrenzt geeignet ☐ ungeeignet Begründung: bitte angeben			

4 MAßNAHMEN ZUM UMGANG MIT DATENTRÄGERN (ANALOG & DIGITAL)

	FRAGE	SCHUTZ-STUFE	MINDESTANFORDERUNG	ERLÄUTERUNGEN ODER DARSTELLUNG GLEICHWERTIGER MAßNAHMEN DES AUFTRAGNEHMERS
4.1	Erfolgt eine Klassifizierung und ggf. Kennzeichnung sensibler Informationen? ☐ ja ☐ nein	B	Sensible Informationen müssen klassifiziert und ggf. gekennzeichnet um den korrekten Umgang mit ihnen zu gewährleisten.	
4.2	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	A	Es ist eine datenschutzkonforme sichere Vernichtungsart zu wählen.	
4.3	Wie werden nicht mehr benötigte Datenträger (USB Sticks, Festplatten), auf denen personenbezogene Daten gespeichert sind, entsorgt?	A	Es ist eine sichere Vernichtungsart zu wählen.	

	FRAGE	SCHUTZ-STUFE	MINDESTANFORDERUNG	ERLÄUTERUNGEN ODER DARSTELLUNG GLEICHWERTIGER MAßNAHMEN DES AUFTRAGNEHMERS
	☐ Physische Zerstörung durch eigene IT. ☐ Physische Zerstörung durch externen Dienstleister. ☐ Löschen der Daten durch Überschreibungen ☐ Sonstiges: bitte angeben			
4.4	Dürfen im Unternehmen mobile Datenträger verwendet werden (z.B. USB-Sticks) ☐ ja ☐ nein	A		
4.5	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.	A		
		B	Verwendung ist nur nach Genehmigung und Überprüfung erlaubt oder auf unternehmenseigene Speichermedien beschränkt.	
		C	Die Verwendung ist auf unternehmenseigene Speichermedien beschränkt.	

	FRAGE	SCHUTZ-STUFE	MINDESTANFORDERUNG	ERLÄUTERUNGEN ODER DARSTELLUNG GLEICHWERTIGER MAßNAHMEN DES AUFTRAGNEHMERS
4.6	Werden personenbezogene Daten auf mobilen Endgeräten verschlüsselt? ☐ Verschlüsselung der Festplatte/des Speichers ☐ Verschlüsselung einzelner Verzeichnisse ☐ keine Maßnahmen	B	Die Daten sind zu verschlüsseln.	
4.7	Verarbeiten Mitarbeitende personenbezogene Daten auch auf eigenen privaten Geräten (bring your own device)? ☐ ja ☐ nein	A	Das Halten personenbezogener Daten des Auftraggebers auf privaten Geräten des Auftragnehmers ist untersagt.	
	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		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.	

	FRAGE	SCHUTZ-STUFE	MINDESTANFORDERUNG	ERLÄUTERUNGEN ODER DARSTELLUNG GLEICHWERTIGER MAßNAHMEN DES AUFTRAGNEHMERS
	angemessenes Schutzniveau zu gewährleisten? ☐ geeignet ☐ begrenzt geeignet ☐ ungeeignet Begründung: bitte angeben			

5 MAßNAHMEN ZUR DATENÜBERTRAGUNG

	FRAGE	SCHUTZ-STUFE	MINDESTANFORDERUNG	ERLÄUTERUNGEN ODER DARSTELLUNG GLEICHWERTIGER MAßNAHMEN DES AUFTRAGNEHMERS
	Werden keine personenbezogenen Daten übertragen, müssen die Fragen zu 5 nicht beantwortet werden.			
5.1	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	A	Beim Transfer personenbezogener Daten muss durch Verschlüsselung sichergestellt werden, dass keine unberechtigte Einsichtnahme Dritter möglich ist.	
5.2	Wer verwaltet die Schlüssel bzw. die Zertifikate? ☐ Anwender selbst ☐ eigene IT ☐ Externer Dienstleister	A		
5.3	Werden die Übertragungsvorgänge protokolliert?	A		

	FRAGE	SCHUTZ-STUFE	MINDESTANFORDERUNG	ERLÄUTERUNGEN ODER DARSTELLUNG GLEICHWERTIGER MAßNAHMEN DES AUFTRAGNEHMERS
	☐ ja ☐ nein			
5.4	**Wenn 5.3 ja:** Wie lange werden diese Protokolldaten aufbewahrt? bitte angeben	A		
5.5	**Wenn 5.3 ja:** Werden die Protokolle regelmäßig ausgewertet? ☐ ja, über eine Security Information and Event Management-Lösung (SIEM) ☐ nein, eine Auswertung wäre aber im Bedarfsfall möglich	A		
	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		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.	

	FRAGE	SCHUTZ-STUFE	MINDESTANFORDERUNG	ERLÄUTERUNGEN ODER DARSTELLUNG GLEICHWERTIGER MAßNAHMEN DES AUFTRAGNEHMERS
	☐ ungeeignet Begründung: bitte angeben			

6 MAßNAHMEN FÜR SICHERE SERVERRÄUME / RECHENZENTRUMSGEBÄUDE

	FRAGE	SCHUTZ-STUFE	MINDESTANFORDERUNG	ERLÄUTERUNGEN ODER DARSTELLUNG GLEICHWERTIGER MAßNAHMEN DES AUFTRAGNEHMERS
6.1	Verfügen die Serverräume über feuerfeste bzw. feuerhemmende Zugangstüren? ☐ ja ☐ nein	B	Zugangstüren müssen feuerhemmend bzw. feuerfest sein.	
6.2	Sind die Serverräume / RZ mit Rauchmeldern ausgestattet? ☐ ja ☐ nein	B	Es müssen Rauchmelder vorhanden sein.	
6.3	Sind die Serverräume / RZ an eine Brandmeldezentrale angeschlossen? ☐ ja ☐ nein	B	Der Anschluss an eine Brandmeldezentrale ist Pflicht.	
6.4	Sind die Serverräume / RZ mit Löschsystemen ausgestattet? ☐ ja ☐ nein	B	Es muss ein Löschsystem vorhanden sein.	
6.5	Woraus bestehen die Außenwände der Serverräume / RZ? bitte angeben	B		

	FRAGE	SCHUTZ-STUFE	MINDESTANFORDERUNG	ERLÄUTERUNGEN ODER DARSTELLUNG GLEICHWERTIGER MAßNAHMEN DES AUFTRAGNEHMERS
6.6	Sind die Serverräume / RZ klimatisiert? ☐ ja ☐ nein	B	Die Klimatisierung ist zwingend erforderlich.	
6.7	Verfügen die Serverräume / RZ über eine unterbrechungsfreie Stromversorgung (USV)? ☐ ja ☐ nein	B	Der Einsatz einer USV ist zwingend erforderlich.	
6.8	Wird die Stromversorgung der Serverräume / RZ zusätzlich über ein Dieselaggregat abgesichert? ☐ ja ☐ nein	B		
6.9	Werden die Funktionalität 6.2, 6.3, 6.4, 6.6, 6.7 und 6.8, sofern vorhanden, regelmäßig getestet? ☐ ja ☐ nein	B		
6.10	Sind die internen Managementnetze/Betriebsnetze (z. B. zur Gebäudeleittechnik, Videoüberwachung, Zutrittskontrolle) vor externem Zugriff geschützt?	B	Es muss mindestens eine logische Trennung der Netze erfolgen.	
		C	Ein zusätzlicher Schutz durch angemessenes Zugriffs- (z. B. Passwort, 2FA,…) und	

	FRAGE	SCHUTZ-STUFE	MINDESTANFORDERUNG	ERLÄUTERUNGEN ODER DARSTELLUNG GLEICHWERTIGER MAßNAHMEN DES AUFTRAGNEHMERS
	☐ ja, bitte angeben ☐ nein		Rechtemanagement ist zu gewährleisten.	
	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 ZUM BACKUP

	FRAGE	SCHUTZ-STUFE	MINDESTANFORDERUNG	ERLÄUTERUNGEN ODER DARSTELLUNG GLEICHWERTIGER MAßNAHMEN DES AUFTRAGNEHMERS
7.1	Existiert ein Backupkonzept für Systeme, auf denen personenbezogene Daten gespeichert sind? ☐ ja ☐ nein	A		
		B	Ein Backupkonzept muss vorhanden sein.	
7.2	**Wenn 7.1 nein:** fortfahren mit 8.1			
7.3	Wird die Funktionalität der Backup / Wiederherstellung regelmäßig getestet? ☐ ja ☐ nein	A		
7.4	In welchem Rhythmus werden Backups von Systemen angefertigt, auf denen personenbezogene Daten gespeichert werden? bitte angeben	A		
7.5	**Im Falle eines Transports der Backups:** Wie wird dieser durchgeführt? bitte angeben	C		
	Sind die Backups verschlüsselt?	A		

	FRAGE	SCHUTZ-STUFE	MINDESTANFORDERUNG	ERLÄUTERUNGEN ODER DARSTELLUNG GLEICHWERTIGER MAßNAHMEN DES AUFTRAGNEHMERS
7.6	☐ ja ☐ nein	C	Backups müssen verschlüsselt sein.	
7.7	Befindet sich der Aufbewahrungsort der Backups in einem (von den Serverräumen aus betrachtet) getrennten Brandabschnitt bzw. Gebäudeteil? ☐ ja ☐ nein	B	Backups müssen in einem getrennten Brandabschnitt bzw. Gebäudeteil aufbewahrt 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:		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.	

	FRAGE	SCHUTZ-STUFE	MINDESTANFORDERUNG	ERLÄUTERUNGEN ODER DARSTELLUNG GLEICHWERTIGER MAßNAHMEN DES AUFTRAGNEHMERS
	bitte angeben			

8 MAßNAHMEN ZUR ABWEHR VON ANGRIFFEN

	FRAGE	SCHUTZ-STUFE	MINDESTANFORDERUNG	ERLÄUTERUNGEN ODER DARSTELLUNG GLEICHWERTIGER MAßNAHMEN DES AUFTRAGNEHMERS
8.1	Sind die IT Systeme technisch vor Angriffen geschützt? ☐ ja ☐ nein	A		
8.2	**Wenn 8.1 ja:** Wer ist für die Aktualisierung von Virenschutz, Anti-Spyware und Spamfilter zuständig? bitte angeben	A		
8.3	Erfolgt eine Separierung von Netzen unterschiedlichen Schutzbedarfs (z. B. DMZ und Intern)? ☐ ja ☐ nein	A	Eine Netztrennung ist zwingend erforderlich.	
8.4	Werden Systeme gehärtet? ☐ ja: ☐ Patchmanagement ☐ Deaktivierung unnötiger Komponenten ☐ Aktivierung hardwarenaher Schutzfunktionen ☐ Sicherheitskonfiguration	B	Systeme müssen durch mehrere Maßnahmen gehärtet werden.	
		C	Systeme müssen durch möglichst alle aufgeführten Maßnahmen gehärtet werden. Nicht umgesetzte Maßnahmen müssen begründet werden.	

	FRAGE	SCHUTZ-STUFE	MINDESTANFORDERUNG	ERLÄUTERUNGEN ODER DARSTELLUNG GLEICHWERTIGER MAßNAHMEN DES AUFTRAGNEHMERS
	☐ Minimale Vergabe von Berechtigungen (z. B. Role Based Access Control) ☐ Konten und Kennwörter ☐ Einschränkung der Netzwerkkommunikation ☐ Protokollierung ☐ Sonstiges: bitte angeben ☐ nein			
8.5	Werden im Falle eines Angriffes Betroffene zeitnah informiert? ☐ ja: ☐ durch ein ungeregeltes Vorgehen ☐ durch ein geregeltes Vorgehen ☐ durch ein geregeltes Vorgehen inklusive Rollen- und Kommunikationsvorgaben ☐ nein	A	Meldungen zu Informationssicherheitsvorfällen müssen zeitnah erfolgen.	
		B	Meldungen zu Informationssicherheitsvorfällen müssen zeitnah erfolgen und geregelt sein.	
		C	Meldungen zu Informationssicherheitsvorfällen müssen zeitnah erfolgen und Verantwortlichkeiten im Prozess geklärt sein.	
8.6	Werden im Anschluss an einen erfolgreichen Angriff Betroffene über	A	Details zu Informationssicherheitsvorfällen müssen kommuniziert werden.	

	FRAGE	SCHUTZ-STUFE	MINDESTANFORDERUNG	ERLÄUTERUNGEN ODER DARSTELLUNG GLEICHWERTIGER MAßNAHMEN DES AUFTRAGNEHMERS
	Angriffsdetails und Maßnahmen informiert? ☐ ja: ☐ durch ein ungeregeltes Vorgehen ☐ durch ein geregeltes Vorgehen ☐ durch ein geregeltes Vorgehen inklusive Rollen- und Kommunikationsvorgaben ☐ nein	B	Details zu Informationssicherheitsvorfällen müssen geregelt kommuniziert werden..	
		C	Details zu Informationssicherheitsvorfällen müssen, geregelt durch Verantwortlichkeiten im Prozess, kommuniziert 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:		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.	

	FRAGE	SCHUTZ-STUFE	MINDESTANFORDERUNG	ERLÄUTERUNGEN ODER DARSTELLUNG GLEICHWERTIGER MAßNAHMEN DES AUFTRAGNEHMERS
	bitte angeben			

9 WEITERE MAßNAHMEN ZUR PRÄVENTION UND REAKTION

	FRAGE	SCHUTZ-STUFE	MINDESTANFORDERUNG	ERLÄUTERUNGEN ODER DARSTELLUNG GLEICHWERTIGER MAßNAHMEN DES AUFTRAGNEHMERS
9.1	Existiert ein dokumentierter Prozess zum Software- bzw. Patchmanagement? ☐ ja ☐ nein	B	Ein Update der Systeme ist regelmäßig erforderlich.	
9.2	**Wenn 9.1 ja:** Wer ist für die Installation von Updates bzw. Patches zuständig? bitte angeben	B		
9.3	Existiert ein Prozess zum Assetmanagement? ☐ ja, dieser wird gelebt ☐ ja, dieser ist dokumentiert und wird gelebt ☐ nein	B	Ein Assetmangementprozess ist vorhanden.	
		C	Der Assetmanagementprozess ist vorhanden und dokumentiert.	
9.4	Werden regelmäßige Schwachstellenprüfungen durchgeführt? ☐ ja ☐ nein	B	Regelmäßige Schwachstellenprüfungen sind erforderlich.	
9.5	Existiert ein Notfallkonzept (bspw. Notfallmaßnahmen bei	A		

	FRAGE	SCHUTZ-STUFE	MINDESTANFORDERUNG	ERLÄUTERUNGEN ODER DARSTELLUNG GLEICHWERTIGER MAßNAHMEN DES AUFTRAGNEHMERS
	Hardwaredefekt / Brand / Totalverlust etc.)? ☐ ja ☐ nein			
9.6	Verfügt das Unternehmen über eine redundante Internetanbindung? ☐ ja ☐ nein	A		
9.7	Sind die einzelnen Standorte des Unternehmens redundant miteinander verbunden? ☐ ja ☐ nein	A		
9.8	Wer ist für die Netzanbindung des Unternehmens verantwortlich? ☐ eigene IT ☐ Externer Dienstleister	A		
9.9	Es werden nur zuverlässige Personen zur Leistungserbringung eingesetzt, die über entsprechende Kenntnisse und Fähigkeiten für ihre Aufgaben verfügen: ☐ ja ☐ nein	A		

	FRAGE	SCHUTZ-STUFE	MINDESTANFORDERUNG	ERLÄUTERUNGEN ODER DARSTELLUNG GLEICHWERTIGER MAßNAHMEN DES AUFTRAGNEHMERS
	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 REGELMÄßIGEN ÜBERPRÜFUNG, BEWERTUNG UND EVALUIERUNG DER WIRKSAMKEIT DER TECHNISCH-ORGANISATORISCHEN MAßNAHMEN

	FRAGE	SCHUTZ-STUFE	MINDESTANFORDERUNG	ERLÄUTERUNGEN ODER DARSTELLUNG GLEICHWERTIGER MAßNAHMEN DES AUFTRAGNEHMERS
10.1	**Wenn 8.4 ja:** Werden die Maßnahmen zur Härtung von Servern regelmäßig bei in Betrieb befindlichen Systemen überprüft? ☐ ja ☐ nein	B		
10.2	Findet eine unabhängige Überprüfung der IT-Systeme oder des Netzwerkes statt? ☐ ja: ☐ Penetrationstests ☐ Sonstiges: bitte angeben ☐ nein	B		

	FRAGE	SCHUTZ-STUFE	MINDESTANFORDERUNG	ERLÄUTERUNGEN ODER DARSTELLUNG GLEICHWERTIGER MAßNAHMEN DES AUFTRAGNEHMERS
10.3	Finden umfassendere Überprüfungen, Bewertungen und Evaluierungen der technisch-organisatorischen Maßnahmen statt? ☐ ja: ☐ Interne Audits ☐ Externe Audits ☐ Überprüfung durch Wirtschaftsprüfer ☐ Interne Revision ☐ Prüfung durch Compliance-Beauftragten ☐ Austausch zwischen Informationssicherheitsbeauftragten und Datenschutzbeauftragten ☐ Überprüfung durch die Rechtsaufsicht ☐ Aufrechterhaltung von Zertifikaten: bitte Zertifikate angeben ☐ Sonstiges: bitte angeben ☐ nein	B	Es muss durch mindestens ein geeignetes Verfahren sichergestellt werden, dass eine regelmäßige Prüfung, Aktualisierung und Dokumentation der technisch-organisatorischen Maßnahmen stattfindet.	
		C	Es muss durch mindestens zwei geeignete Verfahren sichergestellt werden, dass eine regelmäßige Prüfung, Aktualisierung und Dokumentation der technisch-organisatorischen Maßnahmen stattfindet.	
	Sind die dokumentierten Maßnahmen aus Ihrer Sicht unter Berücksichtigung des Stands der Technik, der Implementierungskosten, der Art, des		Es muss bestätigt werden, dass die getroffenen Maßnahmen geeignet sein, um ein angemessenes Schutzniveau zu gewährleisten. Bei	

	FRAGE	SCHUTZ-STUFE	MINDESTANFORDERUNG	ERLÄUTERUNGEN ODER DARSTELLUNG GLEICHWERTIGER MAßNAHMEN DES AUFTRAGNEHMERS
	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		der Angabe „begrenzt geeignet“ muss eine Begründung erfolgen.	