

## 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.

# INHALT

1	MAßNAHMEN ZUM ZUTRITT ZU SYSTEMEN	3
2	MAßNAHMEN ZUM ZUTRITT ZU BÜRORÄUMEN	10
3	MAßNAHMEN ZUM ZUGANG UND ZUGRIFF	15
4	MAßNAHMEN ZUM UMGANG MIT DATENTRÄGERN (ANALOG & DIGITAL)	22
5	MAßNAHMEN ZUR DATENÜBERTRAGUNG	26
6	MAßNAHMEN FÜR SICHERE SERVERRÄUME / RECHENZENTRUMSGEBÄUDE	29
7	MAßNAHMEN ZUM BACKUP	32
8	MAßNAHMEN ZUR ABWEHR VON ANGRIFFEN	35
9	WEITERE MAßNAHMEN ZUR PRÄVENTION UND REAKTION	39
10	REGELMÄßIGEN ÜBERPRÜFUNG, BEWERTUNG UND EVALUIERUNG DER WIRKSAMKEIT DER TECHNISCH-ORGANISATORISCHEN MAßNAHMEN	42

# 1 MAßNAHMEN ZUM ZUTRITT ZU SYSTEMEN

FRAGE	SCHUTZ- STUFE	MINDESTANFORDERUNG	ERLÄUTERUNGEN ODER DARSTELLUNG GLEICHWERTIGER MAßNAHMEN DES AUFTRAGNEHMERS
<b>1.1</b> Werden personenbezogene Daten in Serverräumen oder Rechenzentren (zwischen-)gespeichert oder weitergeleitet, die von dem Auftragnehmer verantwortet werden?  <input type="checkbox"/> ja <input type="checkbox"/> nein	A		
<b>Wenn 1.1 nein:</b> In diesem Fall müssen die weiteren Fragen zu 1 <u>nicht beantwortet werden</u> , sondern sogleich die Fragen ab 2. Auch die Fragen zu 6 und 7 entfallen.			
<b>1.2</b> Standort(e) an denen der Auftragnehmer die Systeme betreibt:  bitte angeben	B	Der Standort muss in <ul style="list-style-type: none"> <li>• der EU,</li> <li>• des Europäischen Wirtschaftsraums,</li> <li>• der Schweiz, <u>oder</u></li> <li>• 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,</li> </ul>	

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

FRAGE		SCHUTZ- STUFE	MINDESTANFORDERUNG	ERLÄUTERUNGEN ODER DARSTELLUNG GLEICHWERTIGER MAßNAHMEN DES AUFTRAGNEHMERS
	<input type="checkbox"/> nein			
1.8	<b>Wenn 1.7 ja:</b> Wer wird informiert, wenn die EMA auslöst? <b>Mehrfachantworten möglich!</b> <input type="checkbox"/> beauftragter Wachdienst <input type="checkbox"/> Administrator <input type="checkbox"/> Leiter IT <input type="checkbox"/> 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?  <input type="checkbox"/> ja <input type="checkbox"/> nein	B	Eine Videoüberwachung ist verpflichtend.	
1.10	<b>Wenn 1.9 ja:</b> 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, berechnigte Personen dürfen Zutritt erlangen. Die Zutrittsberechnigung darf nur personengebunden vergeben werden.	
1.12	Existiert ein Prozess zur Vergabe von Zutrittsberechnigungen 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? <input type="checkbox"/> definierter Freigabeprozess <input type="checkbox"/> kein definierter Freigabeprozess, auf Zuruf <input type="checkbox"/> Sonstige Vergabeweise: bitte angeben			
1.13	Sind Serverräume mit einem elektronischen Schließsystem versehen? <input type="checkbox"/> ja <input type="checkbox"/> nein	B	Ein elektronisches Schließsystem ist erforderlich.	
1.14	<b>Wenn 1.13 ja:</b> Welche Zutrittstechnik kommt zum Einsatz? <b>Mehrfachantworten möglich!</b> bitte angeben	B	Mindestens zwei aus drei Authentifizierungskomponenten (Besitz, Wissen oder biometrische Charakteristika) sind für den Zutritt erforderlich.	
1.15	<b>Wenn 1.13 ja:</b> Werden die Zutritte zu Serverräumen protokolliert? <input type="checkbox"/> ja <input type="checkbox"/> nein	B		
1.16	<b>Wenn 1.15 ja:</b> Wie lange werden die Zutrittsdaten gespeichert? bitte angeben	B		

	FRAGE	SCHUTZ- STUFE	MINDESTANFORDERUNG	ERLÄUTERUNGEN ODER DARSTELLUNG GLEICHWERTIGER MAßNAHMEN DES AUFTRAGNEHMERS
1.17	<b>Wenn 1.15 ja:</b> Werden die Protokolle regelmäßig ausgewertet?  <input type="checkbox"/> ja <input type="checkbox"/> nein	B		
1.18	Ist der Zutritt zu den Serverräumen (auch) mechanisch mit Schlüssel möglich?  <input type="checkbox"/> ja <input type="checkbox"/> nein	B		
1.19	<b>Wenn 1.17 ja:</b> 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?  <input type="checkbox"/> ja <input type="checkbox"/> 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
	<input type="checkbox"/> ja <input type="checkbox"/> nein	B	Die Nutzung von Serverräumen für andere Zwecke ist nicht erlaubt.	
1.22	<b>Wenn 1.19 ja:</b> 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? <input type="checkbox"/> ja, bitte angeben <input type="checkbox"/> nein	A	Eine offizielle Zutrittsregelung für betriebsfremde Personen ist zwingend erforderlich.	
	<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 und Freiheiten der Betroffenen geeignet, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten?</b> <input type="checkbox"/> 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
<input type="checkbox"/> begrenzt geeignet <input type="checkbox"/> 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?  <input type="checkbox"/> ja <input type="checkbox"/> nein	B		
2.3	Ist das Gebäude oder sind die Büroräume mittels einer Einbruchmeldeanlage (EMA) alarmgesichert?  <input type="checkbox"/> ja <input type="checkbox"/> nein	C	Einbruchmeldeanlage muss vorhanden sein.	
2.4	<b>Wenn 2.3 ja:</b> Wer wird informiert, wenn die EMA auslöst? <b>Mehrfachantworten möglich!</b>  <input type="checkbox"/> beauftragter Wachdienst <input type="checkbox"/> Administrator <input type="checkbox"/> 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
	<input type="checkbox"/> Sonstiges: bitte angeben			
2.5	<p>Werden das Bürogebäude bzw. seine Zugänge videoüberwacht?</p> <p><input type="checkbox"/> ja, ohne Bildaufzeichnung</p> <p><input type="checkbox"/> ja, mit Bildaufzeichnung</p> <p><input type="checkbox"/> nein</p>	B		
2.6	<p><b>Wenn 2.5 „ja, mit Bildaufzeichnung“:</b></p> <p>Wie lange werden die Bilddaten gespeichert?</p> <p>bitte angeben</p>	B		
2.7	<p>Sind die Räumlichkeiten mit einem elektronischen Schließsystem versehen?</p> <p><input type="checkbox"/> ja, die Büroräume sind elektronisch verschlossen.</p> <p><input type="checkbox"/> ja, die Büroetagen sind elektronisch verschlossen.</p> <p><input type="checkbox"/> ja, das gesamte Gebäude ist elektronisch verschlossen.</p> <p><input type="checkbox"/> nein</p>	A		
		C	Ein elektronisches Schließsystem ist erforderlich.	
2.8	<p><b>Wenn 2.7 ja:</b> Welche Zutrittstechnik kommt zum Einsatz?</p> <p><input type="checkbox"/> RFID</p>	A		

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

FRAGE		SCHUTZ- STUFE	MINDESTANFORDERUNG	ERLÄUTERUNGEN ODER DARSTELLUNG GLEICHWERTIGER MAßNAHMEN DES AUFTRAGNEHMERS
	<input type="checkbox"/> nein			
2.13	<b>Wenn 2.12 ja:</b> Wird die Ausgabe der (mechanischen und/oder elektronischen) Schlüssel protokolliert?  <input type="checkbox"/> ja, bitte angeben <input type="checkbox"/> nein	A		
2.14	<b>Wenn 2.12 ja:</b> 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?  <input type="checkbox"/> ja <input type="checkbox"/> nein	A		
		B	Personenbezogene Zutrittsrechte/Schlüssel sind zwingend erforderlich.	
2.16	Gibt es offizielle Zutrittsregelung für betriebsfremde Personen (bspw. Besucher) zu den Büroräumen?  <input type="checkbox"/> ja, bitte angeben <input type="checkbox"/> nein	A	Eine offizielle Zutrittsregelung für betriebsfremde Personen ist zwingend erforderlich.	
	<b>Sind die dokumentierten Maßnahmen aus Ihrer Sicht unter Berücksichtigung</b>		Es muss bestätigt werden, dass die getroffenen Maßnahmen geeignet	

FRAGE	SCHUTZ- STUFE	MINDESTANFORDERUNG	ERLÄUTERUNGEN ODER DARSTELLUNG GLEICHWERTIGER MAßNAHMEN DES AUFTRAGNEHMERS
<p><b>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?</b></p> <p><input type="checkbox"/> geeignet</p> <p><input type="checkbox"/> begrenzt geeignet</p> <p><input type="checkbox"/> ungeeignet</p> <p>Begründung: bitte angeben</p>		<p>sein, um ein angemessenes Schutzniveau zu gewährleisten. Bei der Angabe „begrenzt geeignet“ muss eine Begründung erfolgen.</p>	

### 3 MAßNAHMEN ZUM ZUGANG UND ZUGRIFF

FRAGE	SCHUTZ- STUFE	MINDESTANFORDERUNG	ERLÄUTERUNGEN ODER DARSTELLUNG GLEICHWERTIGER MAßNAHMEN DES AUFTRAGNEHMERS
<b>3.1</b> Existiert ein Prozess zur Vergabe von Benutzerkennungen und Zugriffsberechtigungen bei der Neueinstellung und beim Ausscheiden von Mitarbeitenden bzw. bei organisatorischen Veränderungen?  <input type="checkbox"/> definierter Freigabeprozess <input type="checkbox"/> kein definierter Freigabeprozess, auf Zuruf <input type="checkbox"/> Sonstige Vergabeweise: bitte angeben	A	Ein definierter Freigabeprozess ist erforderlich.	
<b>3.2</b> Werden die Vergabe bzw. Änderungen von Zugriffsberechtigungen protokolliert?  <input type="checkbox"/> ja <input type="checkbox"/> nein	B	Eine Protokollierung ist erforderlich.	
<b>3.3</b> Authentisieren sich die Mitarbeitenden über eine individuelle Kennung gegenüber dem zentralen Verzeichnisdienst?  <input type="checkbox"/> ja <input type="checkbox"/> 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?  <input type="checkbox"/> ja <input type="checkbox"/> nein	A	Verbindliche Password-Policy ist erforderlich.	
3.5	<b>Passwort-Zeichenlänge:</b> bitte angeben  <b>Das Passwort enthält Zeichen aus den folgenden Kategorien entsprechend den Mindestanforderungen der Schutzstufe:</b>  <input type="checkbox"/> Großbuchstaben (A bis Z) <input type="checkbox"/> Kleinbuchstaben (a bis z) <input type="checkbox"/> Ziffern (0 bis 9) <input type="checkbox"/> 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	<p>Zwingt das IT System den Nutzer zur Einhaltung der oben genannten Passwortvorgaben?</p> <p><input type="checkbox"/> ja</p> <p><input type="checkbox"/> nein</p>	B	Die IT-technische Unterstützung der Einhaltung der Password-Policy ist erforderlich.	
3.7	<p>Wird der Bildschirm bei Inaktivität des Benutzers gesperrt?</p> <p><input type="checkbox"/> ja, nach bitte Anzahl angeben Minuten</p> <p><input type="checkbox"/> nein</p>	A	Die Bildschirmsperre muss automatisch aktiviert werden.	
		B	Die Bildschirmsperre muss automatisch nach spätestens 10 Minuten Inaktivität aktiviert werden.	
3.8	<p>Welche Maßnahmen ergreifen Sie bei Verlust, Vergessen oder Ausspähen eines Passworts?</p> <p>bitte angeben</p>	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
	<input type="checkbox"/> ja, nach bitte Anzahl angeben erfolglosen Versuchen. <input type="checkbox"/> nein	B	Es muss eine Anmeldesperre spätestens nach 10 erfolglosen Anmeldeversuchen eingerichtet sein.	
3.10	<b>Wenn 3.9 ja:</b> Wie lange bleiben Zugänge gesperrt, wenn die maximale Zahl erfolgloser Anmeldeversuche erreicht wurde? <input type="checkbox"/> Die Zugänge bleiben bis zur manuellen Aufhebung der Sperre gesperrt. <input type="checkbox"/> Die Zugänge bleiben für bitte Anzahl angeben 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? <input type="checkbox"/> ja <input type="checkbox"/> nein	A		
3.12	<b>Wenn 3.11 ja:</b> Wie erfolgt die Authentisierung: <input type="checkbox"/> (RSA) Token <input type="checkbox"/> 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
	<input type="checkbox"/> pre-shared key <input type="checkbox"/> Benutzeraccount	B	Mindestens zwei aus drei Authentifizierungskomponenten (Besitz, Wissen oder biometrische Charakteristika) sind für den Zugriff erforderlich.	
3.13	<b>Wenn 3.11 ja:</b> Gibt es eine Begrenzung von erfolglosen Anmeldeversuchen bei Fernzugängen?  <input type="checkbox"/> ja, bitte Anzahl angeben Versuche pro Tag <input type="checkbox"/> nein	A	Es muss eine Anmeldesperre eingerichtet sein.	
		B	Es muss eine Anmeldesperre spätestens nach 10 erfolglosen Anmeldeversuchen eingerichtet sein.	
3.14	<b>Wenn 3.13 ja:</b> Wie lange bleiben Zugänge gesperrt, wenn die maximale Zahl erfolgloser Anmeldeversuche erreicht worden ist?  <input type="checkbox"/> Die Zugänge bleiben bis zur manuellen Aufhebung der Sperre gesperrt <input type="checkbox"/> Die Zugänge bleiben für bitte Anzahl angeben Minuten gesperrt.	A		
		C	Zugänge müssen bis zur manuellen Aufhebung gesperrt bleiben.	
3.15	Werden Firewalls eingesetzt?  <input type="checkbox"/> ja <input type="checkbox"/> 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?  <input type="checkbox"/> eigene IT <input type="checkbox"/> Externer Dienstleister	A		
3.17	<b>Wenn ein externer DL zum Einsatz kommt:</b> Kann sich dieser ohne Aufsicht durch Ihre IT auf ein System aufschalten?  <input type="checkbox"/> ja <input type="checkbox"/> 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?  <input type="checkbox"/> ja, über eine Security Information and Event Management-Lösung (SIEM) <input type="checkbox"/> nein, eine Auswertung wäre aber im Bedarfsfall möglich	B		
	<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</b>		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
<p><b>und Freiheiten der Betroffenen geeignet, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten?</b></p> <p><input type="checkbox"/> geeignet</p> <p><input type="checkbox"/> begrenzt geeignet</p> <p><input type="checkbox"/> ungeeignet</p> <p>Begründung: bitte angeben</p>			

## 4 MAßNAHMEN ZUM UMGANG MIT DATENTRÄGERN (ANALOG & DIGITAL)

FRAGE	SCHUTZ-STUFE	MINDESTANFORDERUNG	ERLÄUTERUNGEN ODER DARSTELLUNG GLEICHWERTIGER MAßNAHMEN DES AUFTRAGNEHMERS
<b>4.1</b> Erfolgt eine Klassifizierung und ggf. Kennzeichnung sensibler Informationen? <input type="checkbox"/> ja <input type="checkbox"/> nein	B	Sensible Informationen müssen klassifiziert und ggf. gekennzeichnet um den korrekten Umgang mit ihnen zu gewährleisten.	
<b>4.2</b> Wie werden nicht mehr benötigte Papier-Unterlagen mit personenbezogenen Daten (bspw. Ausdrucke / Akten / Schriftwechsel) entsorgt? <input type="checkbox"/> Altpapier / Restmüll <input type="checkbox"/> Es stehen hierfür Schredder zur Verfügung, deren Nutzung angewiesen ist. <input type="checkbox"/> Es sind verschlossene Datentonnen aufgestellt, die von einem Entsorgungsdienstleister zur datenschutzkonformen Vernichtung abgeholt werden. <input type="checkbox"/> Sonstiges: bitte angeben	A	Es ist eine datenschutzkonforme sichere Vernichtungsart zu wählen.	
<b>4.3</b> 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
	<input type="checkbox"/> Physische Zerstörung durch eigene IT. <input type="checkbox"/> Physische Zerstörung durch externen Dienstleister. <input type="checkbox"/> Löschen der Daten durch <i>bitte Anzahl angeben</i> Überschreibungen <input type="checkbox"/> Sonstiges: <i>bitte angeben</i>			
4.4	Dürfen im Unternehmen mobile Datenträger verwendet werden (z.B. USB-Sticks)  <input type="checkbox"/> ja <input type="checkbox"/> nein	A		
4.5	Dürfen die Mitarbeitenden private Datenträger (z.B. USB Sticks) verwenden?  <input type="checkbox"/> ja, aber Mitarbeitende sind angehalten, vorher einen Virencheck durchführen zu lassen. <input type="checkbox"/> ja, aber nur nach Genehmigung und Überprüfung des Speichermediums durch die IT. <input type="checkbox"/> 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
<p><b>4.6</b> Werden personenbezogene Daten auf mobilen Endgeräten verschlüsselt?</p> <p><input type="checkbox"/> Verschlüsselung der Festplatte/des Speichers</p> <p><input type="checkbox"/> Verschlüsselung einzelner Verzeichnisse</p> <p><input type="checkbox"/> keine Maßnahmen</p>	B	Die Daten sind zu verschlüsseln.	
<p><b>4.7</b> Verarbeiten Mitarbeitende personenbezogene Daten auch auf eigenen privaten Geräten (bring your own device)?</p> <p><input type="checkbox"/> ja</p> <p><input type="checkbox"/> nein</p>	A	Das Halten personenbezogener Daten des Auftraggebers auf privaten Geräten des Auftragnehmers ist untersagt.	
<p><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 und Freiheiten der Betroffenen geeignet, um ein dem Risiko</b></p>		<p>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.</p>	



FRAGE	SCHUTZ- STUFE	MINDESTANFORDERUNG	ERLÄUTERUNGEN ODER DARSTELLUNG GLEICHWERTIGER MAßNAHMEN DES AUFTRAGNEHMERS
<p><b>angemessenes Schutzniveau zu gewährleisten?</b></p> <p><input type="checkbox"/> geeignet</p> <p><input type="checkbox"/> begrenzt geeignet</p> <p><input type="checkbox"/> ungeeignet</p> <p>Begründung: bitte angeben</p>			

## 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 <u>nicht beantwortet werden</u> .			
5.1	<p>Erfolgt der Transfer personenbezogener Daten durchgängig verschlüsselt?</p> <p><input type="checkbox"/> ja:</p> <ul style="list-style-type: none"> <li><input type="checkbox"/> per verschlüsselter Datei als Mailanhang</li> <li><input type="checkbox"/> per PGP / SMime</li> <li><input type="checkbox"/> per verschlüsseltem Datenträger</li> <li><input type="checkbox"/> per VPN</li> <li><input type="checkbox"/> per https / TLS</li> <li><input type="checkbox"/> per SFTP</li> <li><input type="checkbox"/> Sonstiges: bitte angeben</li> </ul> <p><input type="checkbox"/> nein</p>	A	Beim Transfer personenbezogener Daten muss durch Verschlüsselung sichergestellt werden, dass keine unberechtigte Einsichtnahme Dritter möglich ist.	
5.2	<p>Wer verwaltet die Schlüssel bzw. die Zertifikate?</p> <ul style="list-style-type: none"> <li><input type="checkbox"/> Anwender selbst</li> <li><input type="checkbox"/> eigene IT</li> <li><input type="checkbox"/> Externer Dienstleister</li> </ul>	A		
5.3	Werden die Übertragungsvorgänge protokolliert?	A		

FRAGE		SCHUTZ-STUFE	MINDESTANFORDERUNG	ERLÄUTERUNGEN ODER DARSTELLUNG GLEICHWERTIGER MAßNAHMEN DES AUFTRAGNEHMERS
	<input type="checkbox"/> ja <input type="checkbox"/> nein			
5.4	<b>Wenn 5.3 ja:</b> Wie lange werden diese Protokolldaten aufbewahrt? bitte angeben	A		
5.5	<b>Wenn 5.3 ja:</b> Werden die Protokolle regelmäßig ausgewertet? <input type="checkbox"/> ja, über eine Security Information and Event Management-Lösung (SIEM) <input type="checkbox"/> nein, eine Auswertung wäre aber im Bedarfsfall möglich	A		
	<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 und Freiheiten der Betroffenen geeignet, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten?</b> <input type="checkbox"/> geeignet <input type="checkbox"/> 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
<input type="checkbox"/> 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?  <input type="checkbox"/> ja <input type="checkbox"/> nein	B	Zugangstüren müssen feuerhemmend bzw. feuerfest sein.	
6.2	Sind die Serverräume / RZ mit Rauchmeldern ausgestattet?  <input type="checkbox"/> ja <input type="checkbox"/> nein	B	Es müssen Rauchmelder vorhanden sein.	
6.3	Sind die Serverräume / RZ an eine Brandmeldezentrale angeschlossen?  <input type="checkbox"/> ja <input type="checkbox"/> nein	B	Der Anschluss an eine Brandmeldezentrale ist Pflicht.	
6.4	Sind die Serverräume / RZ mit Löschsystemen ausgestattet?  <input type="checkbox"/> ja <input type="checkbox"/> 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? <input type="checkbox"/> ja <input type="checkbox"/> nein	B	Die Klimatisierung ist zwingend erforderlich.	
6.7	Verfügen die Serverräume / RZ über eine unterbrechungsfreie Stromversorgung (USV)? <input type="checkbox"/> ja <input type="checkbox"/> nein	B	Der Einsatz einer USV ist zwingend erforderlich.	
6.8	Wird die Stromversorgung der Serverräume / RZ zusätzlich über ein Dieselaggregat abgesichert? <input type="checkbox"/> ja <input type="checkbox"/> nein	B		
6.9	Werden die Funktionalität 6.2, 6.3, 6.4, 6.6, 6.7 und 6.8, sofern vorhanden, regelmäßig getestet? <input type="checkbox"/> ja <input type="checkbox"/> 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
<input type="checkbox"/> ja, bitte angeben <input type="checkbox"/> nein		Rechtmanagement ist zu gewährleisten.	
<p><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 und Freiheiten der Betroffenen geeignet, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten?</b></p> <input type="checkbox"/> geeignet <input type="checkbox"/> begrenzt geeignet <input type="checkbox"/> 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?	A		
	<input type="checkbox"/> ja <input type="checkbox"/> nein	B	Ein Backupkonzept muss vorhanden sein.	
7.2	<b>Wenn 7.1 nein:</b> fortfahren mit 8.1			
7.3	Wird die Funktionalität der Backup / Wiederherstellung regelmäßig getestet?  <input type="checkbox"/> ja <input type="checkbox"/> nein	A		
7.4	In welchem Rhythmus werden Backups von Systemen angefertigt, auf denen personenbezogene Daten gespeichert werden?  bitte angeben	A		
7.5	<b>Im Falle eines Transports der Backups:</b> 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	<input type="checkbox"/> ja <input type="checkbox"/> nein	C	Backups müssen verschlüsselt sein.	
7.7	<p>Befindet sich der Aufbewahrungsort der Backups in einem (von den Serverräumen aus betrachtet) getrennten Brandabschnitt bzw. Gebäudeteil?</p> <input type="checkbox"/> ja <input type="checkbox"/> nein	B	Backups müssen in einem getrennten Brandabschnitt bzw. Gebäudeteil aufbewahrt werden.	
	<p><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 und Freiheiten der Betroffenen geeignet, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten?</b></p> <input type="checkbox"/> geeignet <input type="checkbox"/> begrenzt geeignet <input type="checkbox"/> 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	<p>Sind die IT Systeme technisch vor Angriffen geschützt?</p> <p><input type="checkbox"/> ja</p> <p><input type="checkbox"/> nein</p>	A		
8.2	<p><b>Wenn 8.1 ja:</b> Wer ist für die Aktualisierung von Virenschutz, Anti-Spyware und Spamfilter zuständig?</p> <p>bitte angeben</p>	A		
8.3	<p>Erfolgt eine Separierung von Netzen unterschiedlichen Schutzbedarfs (z. B. DMZ und Intern)?</p> <p><input type="checkbox"/> ja</p> <p><input type="checkbox"/> nein</p>	A	Eine Netztrennung ist zwingend erforderlich.	
8.4	<p>Werden Systeme gehärtet?</p> <p><input type="checkbox"/> ja:</p> <ul style="list-style-type: none"> <li><input type="checkbox"/> Patchmanagement</li> <li><input type="checkbox"/> Deaktivierung unnötiger Komponenten</li> <li><input type="checkbox"/> Aktivierung hardwarenaher Schutzfunktionen</li> <li><input type="checkbox"/> Sicherheitskonfiguration</li> </ul>	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
<input type="checkbox"/> Minimale Vergabe von Berechtigungen (z. B. Role Based Access Control) <input type="checkbox"/> Konten und Kennwörter <input type="checkbox"/> Einschränkung der Netzwerkkommunikation <input type="checkbox"/> Protokollierung <input type="checkbox"/> Sonstiges: <i>bitte angeben</i> <input type="checkbox"/> nein			
<b>8.5</b> Werden im Falle eines Angriffes Betroffene zeitnah informiert? <input type="checkbox"/> ja: <input type="checkbox"/> durch ein ungeregeltes Vorgehen <input type="checkbox"/> durch ein geregeltes Vorgehen <input type="checkbox"/> durch ein geregeltes Vorgehen inklusive Rollen- und Kommunikationsvorgaben <input type="checkbox"/> 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.	
<b>8.6</b> 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
<p>Angriffsdetails und Maßnahmen informiert?</p> <p><input type="checkbox"/> ja:</p> <p><input type="checkbox"/> durch ein ungeregeltes Vorgehen</p> <p><input type="checkbox"/> durch ein geregeltes Vorgehen</p> <p><input type="checkbox"/> durch ein geregeltes Vorgehen inklusive Rollen- und Kommunikationsvorgaben</p> <p><input type="checkbox"/> nein</p>	<p>B</p> <p>C</p>	<p>Details zu Informationssicherheitsvorfällen müssen geregelt kommuniziert werden..</p> <p>Details zu Informationssicherheitsvorfällen müssen, geregelt durch Verantwortlichkeiten im Prozess, kommuniziert werden.</p>	
<p><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 und Freiheiten der Betroffenen geeignet, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten?</b></p> <p><input type="checkbox"/> geeignet</p> <p><input type="checkbox"/> begrenzt geeignet</p> <p><input type="checkbox"/> ungeeignet</p> <p>Begründung:</p>		<p>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.</p>	

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? <input type="checkbox"/> ja <input type="checkbox"/> nein	B	Ein Update der Systeme ist regelmäßig erforderlich.	
9.2	<b>Wenn 9.1 ja:</b> Wer ist für die Installation von Updates bzw. Patches zuständig? bitte angeben	B		
9.3	Existiert ein Prozess zum Assetmanagement? <input type="checkbox"/> ja, dieser wird gelebt <input type="checkbox"/> ja, dieser ist dokumentiert und wird gelebt <input type="checkbox"/> nein	B	Ein Assetmanagementprozess ist vorhanden.	
		C	Der Assetmanagementprozess ist vorhanden und dokumentiert.	
9.4	Werden regelmäßige Schwachstellenprüfungen durchgeführt? <input type="checkbox"/> ja <input type="checkbox"/> 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.)? <input type="checkbox"/> ja <input type="checkbox"/> nein			
9.6	Verfügt das Unternehmen über eine redundante Internetanbindung? <input type="checkbox"/> ja <input type="checkbox"/> nein	A		
9.7	Sind die einzelnen Standorte des Unternehmens redundant miteinander verbunden? <input type="checkbox"/> ja <input type="checkbox"/> nein	A		
9.8	Wer ist für die Netzanbindung des Unternehmens verantwortlich? <input type="checkbox"/> eigene IT <input type="checkbox"/> Externer Dienstleister	A		
9.9	Es werden nur zuverlässige Personen zur Leistungserbringung eingesetzt, die über entsprechende Kenntnisse und Fähigkeiten für ihre Aufgaben verfügen: <input type="checkbox"/> ja <input type="checkbox"/> nein	A		



FRAGE	SCHUTZ- STUFE	MINDESTANFORDERUNG	ERLÄUTERUNGEN ODER DARSTELLUNG GLEICHWERTIGER MAßNAHMEN DES AUFTRAGNEHMERS
<p><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 und Freiheiten der Betroffenen geeignet, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten?</b></p> <p><input type="checkbox"/> geeignet</p> <p><input type="checkbox"/> begrenzt geeignet</p> <p><input type="checkbox"/> ungeeignet</p> <p>Begründung: bitte angeben</p>		<p>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.</p>	

## 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	<b>Wenn 8.4 ja:</b> Werden die Maßnahmen zur Härtung von Servern regelmäßig bei in Betrieb befindlichen Systemen überprüft? <input type="checkbox"/> ja <input type="checkbox"/> nein	B		
10.2	Findet eine unabhängige Überprüfung der IT-Systeme oder des Netzwerkes statt? <input type="checkbox"/> ja: <input type="checkbox"/> Penetrationstests <input type="checkbox"/> Sonstiges: bitte angeben <input type="checkbox"/> nein	B		



FRAGE	SCHUTZ- STUFE	MINDESTANFORDERUNG	ERLÄUTERUNGEN ODER DARSTELLUNG GLEICHWERTIGER MAßNAHMEN DES AUFTRAGNEHMERS
<p><b>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?</b></p> <p><input type="checkbox"/> geeignet</p> <p><input type="checkbox"/> begrenzt geeignet</p> <p><input type="checkbox"/> ungeeignet</p> <p>Begründung: bitte angeben</p>		<p>der Angabe „begrenzt geeignet“ muss eine Begründung erfolgen.</p>	