

## Anlage 3: Sicherheit der Verarbeitung (technisch-organisatorische Maßnahmen - TOM)

Kontaktdaten des Auftragnehmers	
Firmenname:	Firmenstempel
Anschrift:	
Telefon:	
Mail:	
Ansprechpartner:	
Stand der TOM:	
Name Hauptvertrag:	
Zusammenfassung:  (Zweck und Art der Datenverarbeitung für die Gesundheit Nord)	

### Definition

**Digitale Systeme** im Sinne dieses Dokuments sind jedliche Art elektronischer datenverarbeitender Systeme. Darunter fallen u.a. **IT-Systeme**, die der Informationsverarbeitung dienen und eine abgeschlossene Funktionseinheit bilden. Dazu gehören z.B. Computer, Großrechner, Serversysteme, Datenbanksysteme, Clients, Mobiltelefone, Smartphones, Tablets, IoT-Komponenten, Router, Switches, Firewalls, Informationssysteme, Prozessrechner, Digitale Messsysteme, Microcontroller-Systeme, Kompaktregler, eingebettete Systeme, Handhelds, digitale Anrufbeantworter, Videokonferenzsysteme und diverse Kommunikationssysteme. Ebenfalls sind im Sinne dieses Dokuments die **mobilen Datenträger**, wie z.B. externe Festplatten, CD-ROMs, DVDs, Speicherkarten, Magnetbänder, Wechselplatten, USB-Festplatten und USB-Sticks in der Definition der digitalen Systeme inbegriffen.

### Eingangsfragen

	Antwort	Bitte ausfüllen
Werden personenbezogene Daten auf <b>digitalen Systemen</b> verarbeitet, die von Ihnen betrieben werden?	<input type="checkbox"/> ja	A, B, E, H
	<input type="checkbox"/> nein	ab A2, <b>nicht</b> A1, B1, B2
Werden Cloud-Dienstleistungen in Anspruch genommen oder arbeiten Ihre Mitarbeiter im Home-Office?	<input type="checkbox"/> ja	zusätzlich C
	<input type="checkbox"/> nein	<b>nicht</b> C
Werden personenbezogene Daten/besondere personenbezogene Daten (z. B. Gesundheitsdaten, Mitarbeiterdaten, Sozialdaten, DICOM-Daten) auf dem System verarbeitet?		
Kann ein Dienstleister, z.B. im Rahmen der Fernwartung auf personenbezogene Daten zugreifen?	<input type="checkbox"/> ja	zusätzlich D
	<input type="checkbox"/> nein	<b>nicht</b> D
Findet eine allgemeine Risikobewertung zum Zugang Dritter (Unterauftragnehmer, Lieferanten, Dienstleister) zu personenbezogenen Daten (Gesundheitsdaten) statt?	<input type="checkbox"/> ja, bitte ausführen (letzte Seite) <input type="checkbox"/> nein <input type="checkbox"/> Sonstiges:	

### Hinweis

Sollte der Platz zum Ausfüllen bei einzelnen Fragen nicht ausreichend sein, können auf der letzten Seite zu jeder Frage Ergänzungen eingetragen werden.

Dokumentenstatus: Freigegeben	Wiedervorlagestatus: Gültig bis 25.11.2026
Erstellt von: Dr. Pukrop, Joerg	Gültig bis: 25.11.2026
Geprüft von: Knoke, Fabian	Dateiname: Checkliste technische und organisatorische Maßnahmen
Freigegeben von: Dr. Pukrop, Joerg	Seite: 1 von 14

## A Maßnahmen zur Sicherstellung der Vertraulichkeit und Integrität

A1

1	Zutrittskontrollmaßnahmen zu Serverräumen/ Rechenzentren	
1.1	Betreiben Sie das Rechenzentrum selbst?  Kann der Betreiber des Rechenzentrums auf die personenbezogenen Daten des Auftraggebers (GeNo) zugreifen?	<input type="checkbox"/> ja <input type="checkbox"/> nein, es wird durch folgenden Dienstleister betrieben (Name und Anschrift):  <input type="checkbox"/> ja, es wird jedoch protokolliert <input type="checkbox"/> ja, der Zugriff ist unbemerkt möglich <input type="checkbox"/> nein
1.2	Gelten die folgenden Angaben zu Zutrittskontrollmaßnahmen für <b>mehrere</b> im Einsatz befindlichen <b>digitalen Systemen</b> / RZ Standorte?	<input type="checkbox"/> ja <input type="checkbox"/> nein → <b>A und B für jeden Standort ausfüllen</b>
1.3	Sind die personenbezogenen Daten auf mehr als einen Serverstandort / Rechenzentrum verteilt (z. B. Backup Server)?	<input type="checkbox"/> ja, weitere Standorte: <input type="checkbox"/> nein
1.4	Standorte der Serverräume / Rechenzentren (RZ):	
1.5	Ist der Serverraum fensterlos?  Wie sind die Fenster vor Einbruch geschützt?	<input type="checkbox"/> ja <input type="checkbox"/> nein  <input type="checkbox"/> vergittert <input type="checkbox"/> alarmgesichert <input type="checkbox"/> abschließbar <input type="checkbox"/> gar nicht <input type="checkbox"/> Sonstiges:
1.6	Ist der Serverraum mittels einer Einbruchmeldeanlage (EMA) alarmgesichert?  Wer wird informiert, wenn die EMA auslöst? <b>Mehrfachantworten möglich!</b>	<input type="checkbox"/> ja <input type="checkbox"/> nein  <input type="checkbox"/> beauftragter Wachdienst <input type="checkbox"/> Administrator <input type="checkbox"/> Leiter IT <input type="checkbox"/> Sonstiger:
1.7	Ist der Serverraum videoüberwacht?	<input type="checkbox"/> ja, ohne Bildaufzeichnung <input type="checkbox"/> ja, mit Bildaufzeichnung für                      Tage <input type="checkbox"/> nein
1.8	Wie viele Personen haben Zutritt zum Serverraum und welche Funktionen haben diese inne?	Anzahl der Personen: Funktion im Unternehmen:

Dokumentenstatus: Freigegeben	Wiedervorlagestatus: Gültig bis 25.11.2026
Erstellt von: Dr. Pukrop, Joerg	Gültig bis: 25.11.2026
Geprüft von: Knoke, Fabian	Dateiname: Checkliste technische und organisatorische Maßnahmen
Freigegeben von: Dr. Pukrop, Joerg	Seite: 2 von 14

1.9	Ist der Serverraum mit einem elektronischen Schließsystem versehen?	<input type="checkbox"/> ja, mit <input type="checkbox"/> RFID, <input type="checkbox"/> PIN, <input type="checkbox"/> Biometrie <input type="checkbox"/> nein, mit mechanischem Schloss	
	Werden die Zutrittsrechte personalisiert vergeben?	<input type="checkbox"/> ja <input type="checkbox"/> nein	
	Gibt es einen definierten Freigabeprozess für die Vergabe des Zutrittsrechts?	<input type="checkbox"/> ja <input type="checkbox"/> nein	
	<b>Beim PIN-Verfahren:</b> Besitzt jeder eine eigene PIN oder wurde eine Standard PIN vergeben?	<input type="checkbox"/> personalisiert <input type="checkbox"/> Standard-PIN	
	Werden die Zutritte zum Raum im Zutrittssystem protokolliert?	<input type="checkbox"/> ja, erfolgreiche wie erfolglose Zutrittsversuche <input type="checkbox"/> ja, aber nur erfolgreiche Zutritte <input type="checkbox"/> ja, aber nur erfolglose Zutrittsversuche <input type="checkbox"/> nein	
	Wie lange werden die Zutrittsdaten gespeichert?	Tage	
1.10	Wie viele Schlüssel zum Serverraum existieren, wo werden diese aufbewahrt, wer gibt die Schlüssel aus?	<input type="checkbox"/> keine Schlüssel, da elektronischer Zugriff Anzahl Schlüssel: Aufbewahrungsort: Ausgabestelle:	
1.11	Aus welchem Material besteht die Zugangstür zum Serverraum?	<input type="checkbox"/> Stahl / Metall <input type="checkbox"/> sonstiges Material	
1.12	Für welche Zwecke wird der Serverraum neben seiner eigentlichen Funktion noch genutzt?	<input type="checkbox"/> keine <input type="checkbox"/> Telefonanlage <input type="checkbox"/> andere Firmen <input type="checkbox"/> Sonstiges:	
	Was wird in dem Serverraum noch aufbewahrt?	<input type="checkbox"/> Lagerung Büromaterial <input type="checkbox"/> Lagerung Akten/Archiv <input type="checkbox"/> Lagerung von IT Ausstattung <input type="checkbox"/> Sonstiges:	
<b>2</b>	<b>Zutrittskontrollmaßnahmen zu Büroräumen</b> (Homeoffice / Mobile Arbeit siehe Teil C)		
A2	2.1	Standort(e) der Clientarbeitsplätze, von denen auf personenbezogene Daten zugegriffen wird:	
	2.2	Existiert ein Pförtnerdienst / ständig besetzter Empfangsbereich zum Gebäude bzw. zu Ihren Büros?	<input type="checkbox"/> ja <input type="checkbox"/> nein
	2.3	Wird ein Besucherbuch geführt?	<input type="checkbox"/> ja <input type="checkbox"/> nein
	2.4	Ist das Gebäude oder sind die Büroräume mittels einer Einbruchmeldeanlage (EMA) alarmgesichert?	<input type="checkbox"/> ja <input type="checkbox"/> nein
		Wer wird informiert, wenn die EMA auslöst?	<input type="checkbox"/> beauftragter Wachdienst <input type="checkbox"/> Administrator <input type="checkbox"/> Leiter IT <input type="checkbox"/> Sonstige/r:
	2.5	Werden das Bürogebäude bzw. seine Zugänge videoüberwacht?	<input type="checkbox"/> ja, ohne Bildaufzeichnung <input type="checkbox"/> ja, mit Bildaufzeichnung für <span style="float: right;">Tage</span> <input type="checkbox"/> nein

Dokumentenstatus: Freigegeben	Wiedervorlagestatus: Gültig bis 25.11.2026
Erstellt von: Dr. Pukrop, Joerg	Gültig bis: 25.11.2026
Geprüft von: Knoke, Fabian	Dateiname: Checkliste technische und organisatorische Maßnahmen
Freigegeben von: Dr. Pukrop, Joerg	Seite: 3 von 14

2.6	Sind das Gebäude / die Büroräume mit einem elektronischen Schließsystem versehen?	<input type="checkbox"/> ja, insgesamt elektronisch verschlossen <input type="checkbox"/> nein, nur vereinzelt: <input type="checkbox"/> nein	
	Welche Zutrittstechnik kommt zum Einsatz? <b>Mehrfachantworten möglich!</b>	<input type="checkbox"/> RFID, <input type="checkbox"/> PIN, <input type="checkbox"/> Biometrie Sonstiges:	
	Werden die Zutrittsrechte personifiziert vergeben?	<input type="checkbox"/> ja <input type="checkbox"/> nein	
	Werden die Zutritte im Zutrittssystem protokolliert?	<input type="checkbox"/> ja, erfolgreiche wie erfolglose Zutrittsversuche <input type="checkbox"/> ja, aber nur erfolgreiche Zutritte <input type="checkbox"/> ja, aber nur erfolglose Zutrittsversuche <input type="checkbox"/> nein	
	Wie lange werden diese Protokolldaten aufbewahrt?	Tage	
	Werden die Protokolle regelmäßig ausgewertet?	<input type="checkbox"/> ja <input type="checkbox"/> nein, Auswertung im Bedarfsfall mögl.	
2.7	Existiert ein mechanisches Schloss für die Gebäude / Büroräume?	<input type="checkbox"/> ja <input type="checkbox"/> nein	
	Wird die Schlüsselausgabe protokolliert, wer gibt die Schlüssel aus?	<input type="checkbox"/> ja, Ausgabestelle: <input type="checkbox"/> nein	
2.8	Gibt es offizielle Zutrittsregelung für betriebsfremde Personen (bspw. Besucher) zu den Büroräumen?	<input type="checkbox"/> ja <input type="checkbox"/> nein Welche:	
<b>3 Zugangs- und Zugriffskontrollmaßnahmen</b>			
A3	3.1	Existiert ein Prozess zur Vergabe von Benutzerkennungen und Zugriffsberechtigungen bei der Neueinstellung, Funktions-/Aufgabenwechsel und beim Ausscheiden von Mitarbeitern bzw. bei organisatorischen Veränderungen?	<input type="checkbox"/> definierter Freigabeprozess <input type="checkbox"/> kein definierter Freigabeprozess, auf Zuruf <input type="checkbox"/> Sonstige Vergabeweise: <input type="text"/>
		3.2	Werden die Vergabe bzw. Änderungen von Zugriffsberechtigungen protokolliert?
	3.3	Erfolgt die Benutzerverwaltung zentral (z.B. durch Active Directory) oder dezentral (lokal auf dem Rechner)?	<input type="checkbox"/> zentraler Verzeichnisdienst. Welcher: <input type="text"/> <input type="checkbox"/> dezentrale Benutzerverwaltung. Anmeldung durch: <input type="checkbox"/> eigenen Account (personalisiert) <input type="checkbox"/> Gruppenaccount
	Existiert eine individuelle Kennung für die Softwareprodukte, die für die Verarbeitung personenbezogener Daten genutzt werden?	<input type="checkbox"/> ja <input type="checkbox"/> nein	

Dokumentenstatus: Freigegeben	Wiedervorlagestatus: Gültig bis 25.11.2026
Erstellt von: Dr. Pukrop, Joerg	Gültig bis: 25.11.2026
Geprüft von: Knoke, Fabian	Dateiname: Checkliste technische und organisatorische Maßnahmen
Freigegeben von: Dr. Pukrop, Joerg	Seite: 4 von 14

3.4	Existieren verbindliche Passwortparameter für alle verwendeten Softwareprodukte im Unternehmen?	<input type="checkbox"/> ja <input type="checkbox"/> nein
	Muss das Passwort Sonderzeichen und Groß- und Kleinschreibung enthalten?	<input type="checkbox"/> ja <input type="checkbox"/> nein Passwort-Zeichenlänge: <input type="text"/> Maximale Gültigkeitsdauer in Tagen: <input type="text"/>
	Wird die Passwort-Policy auf alle relevanten Softwareprodukte angewandt?	<input type="checkbox"/> ja <input type="checkbox"/> nein, weil: <input type="text"/>
3.5	Zwingt das IT-System den Nutzer zur Einhaltung der oben genannten Passwortvorgaben?	<input type="checkbox"/> ja <input type="checkbox"/> nein
3.6	Wird der Bildschirm bei Inaktivität des Benutzers gesperrt?	<input type="checkbox"/> ja, nach <input type="text"/> Minuten <input type="checkbox"/> nein
3.7	Welche Maßnahmen ergreifen Sie bei Verlust, Vergessen oder Ausspähen eines Passworts?	<input type="text"/>
3.8	Gibt es eine Begrenzung von erfolglosen Anmeldeversuchen?	Betriebssystem: <input type="checkbox"/> ja, maximal <input type="text"/> Versuche <input type="checkbox"/> nein Software: <input type="checkbox"/> ja, maximal <input type="text"/> Versuche <input type="checkbox"/> nein
	Wie lange bleiben Zugänge gesperrt?	<input type="checkbox"/> Bis zur manuellen Aufhebung der Sperre <input type="checkbox"/> Bis zum Ablauf von <input type="text"/> Minuten
3.9	Wie erfolgt die Authentisierung bei Fernzugängen?	<input type="checkbox"/> Token (2 Faktorauthentifizierung) <input type="checkbox"/> Zertifikate / VPN <input type="checkbox"/> Passwort <input type="checkbox"/> Sonstiges: <input type="text"/>
3.10	Gibt es eine Begrenzung von erfolglosen Anmeldeversuchen bei Fernzugängen?	<input type="checkbox"/> ja, maximal <input type="text"/> Versuche <input type="checkbox"/> nein
	Wie lange bleiben Zugänge gesperrt?	<input type="checkbox"/> Bis zur manuellen Aufhebung der Sperre <input type="checkbox"/> Bis zum Ablauf von <input type="text"/> Minuten
3.11	Wird der Fernzugang nach einer gewissen Zeit der Inaktivität automatisch getrennt?	<input type="checkbox"/> ja, nach <input type="text"/> Minuten <input type="checkbox"/> nein
3.12	Werden die Systeme, auf denen personenbezogene Daten verarbeitet werden, über eine Firewall abgesichert?	<input type="checkbox"/> ja <input type="checkbox"/> nein
	Wird die Firewall regelmäßig upgedatet?	<input type="checkbox"/> ja <input type="checkbox"/> nein
	Wer administriert Ihre Firewall?	<input type="checkbox"/> eigene IT-Abteilung <input type="checkbox"/> ext. Dienstleister: <input type="text"/>
	Kann sich der ext. Dienstleister ohne Aufsicht auf die Firewall aufschalten?	<input type="checkbox"/> ja <input type="checkbox"/> nein, nur im 4-Augenprinzip

Dokumentenstatus: Freigegeben	Wiedervorlagestatus: Gültig bis 25.11.2026
Erstellt von: Dr. Pukrop, Joerg	Gültig bis: 25.11.2026
Geprüft von: Knoke, Fabian	Dateiname: Checkliste technische und organisatorische Maßnahmen
Freigegeben von: Dr. Pukrop, Joerg	Seite: 5 von 14

A4

3.13	Ist ein Berechtigungskonzept vorhanden, welches die Anforderungen der gängigen Normen erfüllt, wie z.B. ISO 27001, Europäische Datenschutzverordnung?	<input type="checkbox"/> ja, welche: <input type="text"/> <input type="checkbox"/> nein
3.14	Sind Zugriffsbeschränkungen so geregelt und dokumentiert, dass nachvollziehbar ist, auf welche Daten jeder Mitarbeiter zugreifen darf?	<input type="checkbox"/> ja <input type="checkbox"/> nein
3.15	Ist es bei Bedarf nachvollziehbar, z.B. wer auf personenbezogene Daten zugegriffen hat?	<input type="checkbox"/> ja <input type="checkbox"/> nein
	Wird der Zugriff von Zugriffsberechtigten protokolliert?	<input type="checkbox"/> ja <input type="checkbox"/> nein
	Wie lange werden diese Protokolle aufbewahrt?	Tage <input type="checkbox"/> regelmäßig <input type="checkbox"/> anlass-/bedarfsbezogen
<b>4</b>	<b>Maßnahmen zur Sicherung von Unterlagen, mobilen Datenträgern und Endgeräten</b>	
4.1	Existieren Löschkonzepte für personenbezogene Daten in Ihrem Unternehmen?	<input type="checkbox"/> ja <input type="checkbox"/> nein
4.2	Wie werden nicht mehr benötigte Papier-Unterlagen mit personenbezogenen Daten (bspw. Ausdrücke / Akten / Schriftwechsel) entsorgt?	<input type="checkbox"/> Altpapier / Restmüll <input type="checkbox"/> Schredder, Nutzung ist angewiesen <input type="checkbox"/> Mit verschlossenen Datentonnen eines Entsorgungsdienstleisters (datenschutzkonform) <input type="checkbox"/> Sonstiges: <input type="text"/>
4.3	Wie werden nicht mehr benötigte <b>digitale Systeme</b> , auf denen personenbezogene Daten gespeichert sind, entsorgt?	<input type="checkbox"/> Physikalische Zerstörung eigene IT <input type="checkbox"/> Physikalische Zerstörung externer Dienstleister <input type="checkbox"/> Löschen der Daten <input type="checkbox"/> Überschreiben der Daten: Anzahl <input type="text"/> <input type="checkbox"/> gem. Löschkonzept Sonstiges: <input type="text"/>
4.4	Dürfen im Unternehmen mobile Datenträger verwendet werden (z.B. USB-Sticks)?	<input type="checkbox"/> ja, dienstliche <input type="checkbox"/> ja, private ohne Überprüfung <input type="checkbox"/> ja, private nur nach Genehmigung <input type="checkbox"/> nein
	Wie wird sichergestellt, dass keine privaten bzw. nur erlaubte mobilen Datenträger verwendet/angeschlossen werden können?	<input type="text"/>
4.5	Verarbeiten Mitarbeiter personenbezogene Daten auch auf eigenen privaten Geräten (bring your own device)?	<input type="checkbox"/> ja <input type="checkbox"/> nein
	Wie ist BYOD abgesichert (VPN, Zertifikate, etc.)?	<input type="text"/>

Dokumentenstatus: Freigegeben	Wiedervorlagestatus: Gültig bis 25.11.2026
Erstellt von: Dr. Pukrop, Joerg	Gültig bis: 25.11.2026
Geprüft von: Knoke, Fabian	Dateiname: Checkliste technische und organisatorische Maßnahmen
Freigegeben von: Dr. Pukrop, Joerg	Seite: 6 von 14

**A5**

4.6	Werden personenbezogene Daten auf mobilen Endgeräten verschlüsselt?  Art der Verschlüsselung (z.B. AES-128):	<input type="checkbox"/> Verschlüsselung der Festplatte <input type="checkbox"/> Verschlüsselung einzelner Verzeichnisse <input type="checkbox"/> keine Maßnahmen
<b>5 Maßnahmen zur sicheren Datenübertragung</b>		
5.1	Mit welchem Verschlüsselungsalgorithmus erfolgt der Transfer personenbezogener Daten?  Art der Verschlüsselung (z.B. AES-128, TLS 1.3)	<input type="checkbox"/> keinem <input type="checkbox"/> nur vereinzelt, Beispiele: <input type="checkbox"/> per verschlüsselter Datei als Mailanhang (.zip) <input type="checkbox"/> per PGP/Smime <input type="checkbox"/> per verschlüsseltem Datenträger <input type="checkbox"/> per VPN <input type="checkbox"/> per https/TLS <input type="checkbox"/> per SFTP <input type="checkbox"/> Sonstiges:
5.2	Wer verwaltet die Schlüssel bzw. die Zertifikate?	<input type="checkbox"/> Anwender selbst <input type="checkbox"/> eigene IT <input type="checkbox"/> externer Dienstleister
5.3	Werden die Übertragungsvorgänge protokolliert?  Wie lange werden diese Protokolldaten aufbewahrt?  Werden die Protokolle regelmäßig ausgewertet?	<input type="checkbox"/> ja <input type="checkbox"/> nein  Tage <input type="checkbox"/> ja <input type="checkbox"/> nein, Auswertung im Bedarfsfall möglich
<b>6 Datentransfer Drittland</b>		
6.1	Findet ein Datentransfer in ein Drittland (nicht EU) statt?  Welche Grundlage existiert für die Datenverarbeitung im Drittland (44 ff. DS-GVO)?	<input type="checkbox"/> ja, Länder: <input type="checkbox"/> nein  <input type="checkbox"/> Angemessenheitsbeschluss (beifügen) <input type="checkbox"/> Übermittlung vorbehaltlich geeigneter Garantien (beifügen) <input type="checkbox"/> Sonstiges:

**A6**

## B Maßnahmen zur Sicherstellung der Verfügbarkeit

**B1**

<b>1</b>	<b>Serverraum</b>	
1.1	Verfügt der Serverraum über eine feuerfeste bzw. feuerhemmende Zugangstür?	<input type="checkbox"/> ja <input type="checkbox"/> nein
1.2	Ist der Serverraum mit Rauchmeldern ausgestattet?	<input type="checkbox"/> ja <input type="checkbox"/> nein
1.3	Ist der Serverraum an eine Brandmeldezentrale angeschlossen?	<input type="checkbox"/> ja <input type="checkbox"/> nein

Dokumentenstatus: Freigegeben	Wiedervorlagestatus: Gültig bis 25.11.2026
Erstellt von: Dr. Pukrop, Joerg	Gültig bis: 25.11.2026
Geprüft von: Knoke, Fabian	Dateiname: Checkliste technische und organisatorische Maßnahmen
Freigegeben von: Dr. Pukrop, Joerg	Seite: 7 von 14

1.4	Ist der Serverraum mit Löschsystemen ausgestattet? <b>Mehrfachantworten möglich!</b>	<input type="checkbox"/> ja, CO2 Löscher <input type="checkbox"/> ja, Halon / Argon Löschanlage <input type="checkbox"/> Sonstiges:
1.5	Woraus bestehen die Außenwände des Serverraumes?	<input type="checkbox"/> Massivwand (bspw. Beton, Mauer) <input type="checkbox"/> Leichtbauweise <input type="checkbox"/> Brandschutzwand (bspw. F90)
1.6	Ist der Serverraum klimatisiert?	<input type="checkbox"/> ja <input type="checkbox"/> nein
1.7	Verfügt der Serverraum über eine unterbrechungsfreie Stromversorgung (USV)?	<input type="checkbox"/> ja <input type="checkbox"/> nein
1.8	Wird die Stromversorgung des Serverraums über ein zusätzliches Notstromaggregat abgesichert?	<input type="checkbox"/> ja <input type="checkbox"/> nein
1.9	Werden die Funktionalitäten von 1.2, 1.3, 1.4, 1.6, 1.7 und 1.8 regelmäßig getestet?	<input type="checkbox"/> ja <input type="checkbox"/> nein
1.10	Wenn die Anwendung über das Internet zur Verfügung gestellt wird, wie ist dies entsprechend abgesichert?	
1.11	Werden Schadsoftwareschutzprogramme (u.a. Virens Scanner) flächendeckend eingesetzt und ständig aktualisiert?	<input type="checkbox"/> ja <input type="checkbox"/> nein Aktualisierungsintervall: alle      Tage
1.12	Sind Firewall Lösungen vorhanden und werden diese eingesetzt, z.B. bei einem externen Hosting?	<input type="checkbox"/> ja <input type="checkbox"/> nein
1.13	Existieren redundante Rechenzentren  Wer betreibt dieses Rechenzentrum/ diese Rechenzentren?	<input type="checkbox"/> ja      Anzahl: <input type="checkbox"/> nein  <input type="checkbox"/> Auftragnehmer (Sie selbst) <input type="checkbox"/> Folgender Subunternehmer (Name, Anschrift):
<b>2</b>	<b>Backup- und Notfall-Konzept</b>	
2.1	Existiert ein Backupkonzept?	<input type="checkbox"/> ja <input type="checkbox"/> nein
2.2	Wird die Funktionalität der Backup-Wiederherstellung regelmäßig getestet?	<input type="checkbox"/> ja <input type="checkbox"/> nein
2.3	In welchem Rhythmus werden Backups von den Systemen angefertigt, auf denen personenbezogene Daten gespeichert werden?	<input type="checkbox"/> Echtzeitspiegelung <input type="checkbox"/> täglich <input type="checkbox"/> ein bis dreimal pro Woche <input type="checkbox"/> Sonstiges:
2.4	Auf was für Sicherungsmedien werden die Backups gespeichert?	<input type="checkbox"/> Zweiter redundanter Server; Standort: <input type="checkbox"/> Sicherungsbänder <input type="checkbox"/> Festplatten <input type="checkbox"/> Sonstiges:

B2

Dokumentenstatus: Freigegeben	Wiedervorlagestatus: Gültig bis 25.11.2026
Erstellt von: Dr. Pukrop, Joerg	Gültig bis: 25.11.2026
Geprüft von: Knoke, Fabian	Dateiname: Checkliste technische und organisatorische Maßnahmen
Freigegeben von: Dr. Pukrop, Joerg	Seite: 8 von 14

2.5	Wo werden die Backups aufbewahrt?	<input type="checkbox"/> Zweiter redundanter Server (anderen Ort) <input type="checkbox"/> Safe, feuerfest, dokumentensicher <input type="checkbox"/> einfacher Safe <input type="checkbox"/> Bankschließfach <input type="checkbox"/> abgeschlossener Aktenschrank / Schreibtisch <input type="checkbox"/> Im Serverraum <input type="checkbox"/> Privathaushalt <input type="checkbox"/> Sonstiges:
2.6	Im Falle eines Transports der Backups: Wie wird dieser durchgeführt?	<input type="checkbox"/> Mitnahme durch einen MA der IT / Geschäftsleitung / Sekretärin <input type="checkbox"/> Abholung durch Dritte (bspw. Bankmitarbeiter / Wachunternehmen) <input type="checkbox"/> Sonstiges:
2.7	Sind die Backups verschlüsselt?  Art der Verschlüsselung (z.B. AES-128, TLS 1.3)	<input type="checkbox"/> ja <input type="checkbox"/> nein
2.8	Befindet sich der Aufbewahrungsort der Backups in einem vom primären Server aus betrachtet getrennten Brandabschnitt bzw. Gebäudeteil?	<input type="checkbox"/> ja <input type="checkbox"/> nein
2.9	Existiert ein Notfallkonzept (bspw. Notfallmaßnahmen bei Hardwaredefekte / Brand / Totalverlust etc.)?	<input type="checkbox"/> ja <input type="checkbox"/> nein
2.10	Wie sind die IT Systeme technisch vor Datenverlusten / unbefugten Datenzugriffen geschützt?	
<b>3 Netzanbindung</b>		
3.1	Verfügt das Unternehmen über eine gleichwertige redundante Internetanbindung?	<input type="checkbox"/> ja <input type="checkbox"/> nein <input type="checkbox"/> Sonstiges:
	Sind interne Netzwerke (Verbindungen der Server/Switches) redundant ausgelegt?	<input type="checkbox"/> ja <input type="checkbox"/> nein <input type="checkbox"/> Sonstiges:
3.2	Sind die einzelnen Standorte des Unternehmens redundant miteinander verbunden?	<input type="checkbox"/> ja <input type="checkbox"/> nein
3.3	Wer ist für die Netzanbindung des Unternehmens verantwortlich?	<input type="checkbox"/> eigene IT <input type="checkbox"/> externer Dienstleister

B3

Dokumentenstatus: Freigegeben	Wiedervorlagestatus: Gültig bis 25.11.2026
Erstellt von: Dr. Pukrop, Joerg	Gültig bis: 25.11.2026
Geprüft von: Knoke, Fabian	Dateiname: Checkliste technische und organisatorische Maßnahmen
Freigegeben von: Dr. Pukrop, Joerg	Seite: 9 von 14

**B4**

4 Update/Patchmanagement, Virenschutz und Support		
4.1	<p>Existiert ein dokumentierter Prozess zum Software- bzw. Patchmanagement?</p> <p>Wer ist für das Software- bzw. Patchmanagement verantwortlich?</p>	<input type="checkbox"/> ja <input type="checkbox"/> nein <input type="checkbox"/> Prozess existiert, ist jedoch nicht dokumentiert  <input type="checkbox"/> Anwender selbst <input type="checkbox"/> eigene IT <input type="checkbox"/> externer Dienstleister
4.2	<p>Sind regelmäßig neue Updates für die Anwendung vorgesehen?</p> <p>Wie werden diese zur Verfügung gestellt, in welchen Zeiträumen und von wem werden sie installiert?</p>	<input type="checkbox"/> ja <input type="checkbox"/> nein
4.3	<p>Wer ist für den aktuellen Virenschutz, Anti-Spyware und Spamfilter für Endgeräte (z.B. Notebooks) verantwortlich?</p>	<input type="checkbox"/> Anwender selbst <input type="checkbox"/> eigene IT <input type="checkbox"/> externer Dienstleister
4.4	<p>Wie oft werden Sicherheitsupdates für die betriebenen Systeme (z.B. Betriebssysteme, Switche, etc.) eingespielt?</p>	
4.5	<p>Ist der angebotene Support in deutscher Sprache?</p>	<input type="checkbox"/> ja <input type="checkbox"/> nein
4.6	<p>Ist die Entwicklungsleitung des Anbieters in Europa angesiedelt?</p>	<input type="checkbox"/> ja <input type="checkbox"/> nein
4.7	<p>Aus welchem Land findet der First- und Second-Level Support statt?</p>	First: Second:

## C Cloud-Dienste und Home-Office-Regelungen

**C1**

1 Cloud		
1.1	<p>Werden Cloud-Dienste in Anspruch genommen?</p> <p>Betreiben Sie die Cloud selbst?</p> <p>Befinden sich die Anbieter (mindestens die Server) der Cloud-Dienste innerhalb der Europäischen Union?</p> <p>Gibt der Cloud-Betreiber Daten an ein Drittland weiter?</p> <p>In welchen Ländern werden personenbezogene Daten weitergegeben und welche Daten werden weitergegeben?</p>	<input type="checkbox"/> ja, folgende: <input type="checkbox"/> nein  <input type="checkbox"/> ja <input type="checkbox"/> nein  <input type="checkbox"/> ja <input type="checkbox"/> nein, Länder:  <input type="checkbox"/> ja <sup>1</sup> , <input type="checkbox"/> nein  Länder: Daten:

<sup>1</sup> Sollte der Platz nicht ausreichend sein, beschreiben Sie weitere Details bitte auf der letzten Seite.

Dokumentenstatus: Freigegeben	Wiedervorlagestatus: Gültig bis 25.11.2026
Erstellt von: Dr. Pukrop, Joerg	Gültig bis: 25.11.2026
Geprüft von: Knoke, Fabian	Dateiname: Checkliste technische und organisatorische Maßnahmen
Freigegeben von: Dr. Pukrop, Joerg	Seite: 10 von 14

C2

1.2	Wurden die technischen Dokumente zur Sicherstellung der Schutzziele Verfügbarkeit, Vertraulichkeit, und Integrität von Ihnen ausgewertet und werden diese in regelmäßigen Abständen überprüft?	<input type="checkbox"/> ja <input type="checkbox"/> nein <input type="checkbox"/> Überprüfung alle Monate
1.3	Wurden die Allgemeinen Geschäftsbedingungen des Cloud-Anbieters durch Sie ausgewertet und werden diese in regelmäßigen Abständen geprüft?	<input type="checkbox"/> ja <input type="checkbox"/> nein <input type="checkbox"/> Überprüfung alle Monate
<b>2 Home-Office</b>		
2.1	Existieren Vorgaben für die Einrichtung des Home-Office-Büros?	<input type="checkbox"/> ja <input type="checkbox"/> nein
	Können Ihre Mitarbeiter aus dem Home-Office auf personenbezogene Daten zugreifen?	<input type="checkbox"/> ja <input type="checkbox"/> nein
2.2	Wie wird sichergestellt, dass Mitarbeiter mit privaten Geräten (Notebook, Smartphone) auf die personenbezogenen Daten <b>sicher</b> zugreifen können?  Bsp.: Verhinderung von Kopien von personenbezogenen Daten durch virtuelle, gekapselte Umgebung.	
2.3	Welche Verschlüsselungstechnik und Software wird für die Verbindung vom Home-Office zum Unternehmen benutzt?	Technik: Software:
2.4	Sind USB-Ports an den dienstlichen Rechnern des Home-Office gesperrt?	<input type="checkbox"/> ja <input type="checkbox"/> nein <input type="checkbox"/> Sonstiges:
2.5	Können dienstliche Daten im Home-Office ausgedruckt oder anders aus dem Netzwerk auch auf den privaten Rechner übertragen und gespeichert werden?	<input type="checkbox"/> ja <input type="checkbox"/> nein <input type="checkbox"/> Sonstiges:

Dokumentenstatus: Freigegeben	Wiedervorlagestatus: Gültig bis 25.11.2026
Erstellt von: Dr. Pukrop, Joerg	Gültig bis: 25.11.2026
Geprüft von: Knoke, Fabian	Dateiname: Checkliste technische und organisatorische Maßnahmen
Freigegeben von: Dr. Pukrop, Joerg	Seite: 11 von 14

## D Fernwartung

D1

1	<b>Fernwartung</b>	
1.1	Wie viele Personen führen Fernwartung auf Systemen des Auftraggebers durch?	Personen
1.2	Sind diese Personen dem Auftraggeber namentlich bekannt?	<input type="checkbox"/> ja <input type="checkbox"/> nein
1.3	Erfolgt die Fernwartung über Individual- oder Sammelkennungen?	<input type="checkbox"/> Individualkennung <input type="checkbox"/> Sammelkennung
1.4	Werden neue bzw. ausgeschiedene Mitarbeiter, die über eine Fernwartungskennung verfügen, dem Auftraggeber gemeldet?	<input type="checkbox"/> ja <input type="checkbox"/> nein
1.5	Erfolgt die Fernwartung auch im Rahmen von Home-Office Tätigkeit?	<input type="checkbox"/> ja <input type="checkbox"/> nein
1.6	Wie erfolgt die Fernwartung?	<input type="checkbox"/> Remote-Tools z-B. Teamviewer <input type="checkbox"/> VPN <input type="checkbox"/> Terminal-Server
1.7	Werden im Rahmen der Fernwartung personenbezogene Daten aus dem Verantwortungsbereich des Auftraggebers auf Servern oder Client des Auftragnehmers oder von ihm beauftragter Subunternehmen gespeichert?	<input type="checkbox"/> ja <input type="checkbox"/> nein

## E Sonstige Maßnahmen nach Art. 32 Abs. 1 lit. b, c, d DSGVO

E1

1	<b>Belastbarkeit</b>	
E1	Es existieren Maßnahmen, die die Fähigkeit gewährleisten, die Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung auf Dauer sicherzustellen.	<input type="checkbox"/> ja, folgende: <input type="checkbox"/> nein

E2

2	<b>Wiederherstellbarkeit</b>	
E2	Es existieren Notfallkonzepte und Maßnahmen, die die Fähigkeit gewährleisten, die Verfügbarkeit der personenbezogenen Daten und den Zugang zu ihnen bei einem physischen oder technischen Zwischenfall rasch wiederherzustellen.	<input type="checkbox"/> ja, folgende: <input type="checkbox"/> nein

E3

3	<b>Verfahren zur Überprüfung, Bewertung und Evaluierung der getroffenen Maßnahmen</b>	
E3	Es existiert ein Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung.	<input type="checkbox"/> ja, folgendes: <input type="checkbox"/> nein

Dokumentenstatus: Freigegeben	Wiedervorlagestatus: Gültig bis 25.11.2026
Erstellt von: Dr. Pukrop, Joerg	Gültig bis: 25.11.2026
Geprüft von: Knoke, Fabian	Dateiname: Checkliste technische und organisatorische Maßnahmen
Freigegeben von: Dr. Pukrop, Joerg	Seite: 12 von 14

## F Zertifikate

F1

1 Vorhandene Nachweise/ Zertifikate	
Existieren Unterlagen, z.B. Zertifikate, die Auskunft über die Datensicherheit/Informationssicherheit geben können?	<input type="checkbox"/> ja, folgende:  <b>Hinweis:</b> Die genannten Zertifikate sind unaufgefordert mit einzureichen.  <input type="checkbox"/> nein

## G Unterauftragnehmer/Dienstleister

G1

1 Unterauftragnehmer/Dienstleister		
1.1	Sind Unterauftragnehmer vorhanden, die auf personenbezogene Daten des Verantwortlichen zugreifen können?	<input type="checkbox"/> ja <sup>2</sup> <input type="checkbox"/> nein
1.2	Existieren definierte Prozesse/Regeln, wie Unterauftragnehmer auf personenbezogene Daten zugreifen können?	<input type="checkbox"/> ja <input type="checkbox"/> nein
1.3	Können Unterauftragnehmer unbemerkt auf personenbezogene Daten zugreifen?	<input type="checkbox"/> ja <input type="checkbox"/> nein

## H Übergreifende Informationen

H1

1 Unterauftragnehmer/Dienstleister		
1.1	Ist beim Auftragnehmer ein Datenschutzbeauftragter bestellt?	<input type="checkbox"/> ja <input type="checkbox"/> nein
1.2	Ist beim Auftragnehmer ein Informationssicherheitsbeauftragter bestellt?	<input type="checkbox"/> ja <input type="checkbox"/> nein
1.3	Existiert beim Auftragnehmer ein Informationssicherheits-Management?	<input type="checkbox"/> ja <input type="checkbox"/> nein
1.4	Existieren beim Auftragnehmer eine Sicherheitsrichtlinie oder andere organisatorische Vorgaben zum Umgang mit personenbezogenen Daten?	<input type="checkbox"/> ja <input type="checkbox"/> nein

<sup>2</sup> Bitte fügen Sie eine Liste aller Unterauftragnehmer inkl. Beschreibung der beauftragten Dienstleistung (z.B. auf der letzten Seite) bei.

Dokumentenstatus: Freigegeben	Wiedervorlagestatus: Gültig bis 25.11.2026
Erstellt von: Dr. Pukrop, Joerg	Gültig bis: 25.11.2026
Geprüft von: Knoke, Fabian	Dateiname: Checkliste technische und organisatorische Maßnahmen
Freigegeben von: Dr. Pukrop, Joerg	Seite: 13 von 14

