

Dokumentation
der technischen und organisatorischen Maßnahmen
zur Umsetzung und Einhaltung der Vorgaben nach Art. 32 der EU-DSGVO
(Sicherstellung der Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit)

Verantwortliche Stelle/ Unternehmen: SUSI & James GmbH

Datum: 25.09.2023

1. Zutrittskontrolle/Zugangskontrolle

Verwehrung des Zugangs zu Verarbeitungsanlagen, mit denen die Verarbeitung durchgeführt wird, für Unbefugte.
Vorhandene Maßnahmen:

Vorh.	Maßnahme	Kommentar
<input checked="" type="checkbox"/>	1. Gebäude, Alarmanlage/Wachpersonal/- Videoüberwachung/Lage der Serverräume	Für die Gebäudeeingänge werden einbruchhemmende Türen nach DIN EN 1627 verwendet, welche mit Sicherheitsschlössern nach DIN 18252 ausgestattet sind. Bei den eingesetzten Fenstern handelt es sich um einbruchhemmende Fenster nach DIN EN 1627.
<input checked="" type="checkbox"/>	2. Festlegung befugter Personen (Betriebsangehörige und Betriebsfremde)	Zutrittskontrolle wird nach Zonensystem geregelt. In eingeschränkte Zonen haben nur bestimmte Susi & James Mitarbeitende freien Zutritt. In kontrollierten Zonen haben Susi & James Angestellte uneingeschränkten Zutritt. Gäste und andere externe Personen haben nur unter Begleitung Zutritt zu diesen Bereichen. Gäste müssen sich schriftlich in den Geschäftsräumen anmelden und in eine Besucherliste eintragen. Die für die Gäste zuständigen Mitarbeitenden sind von SUSI&James im Umgang mit den Gästen eingewiesen. In öffentliche Zonen haben alle Personen freien Zutritt (z.B. Lieferanten, Gäste oder Bewerber), müssen sich allerdings registrieren.
<input type="checkbox"/>	3. Berechtigungsausweise	Berechtigungsausweise finden keine Anwendung. Zugänge zu vertraulichen und geheimen Bereichen werden durch das Zonenkonzept und das Besuchermanagement des ISMS organisatorisch und/oder physisch

		gesichert. Mitarbeitende werden regelmäßig geschult.
<input checked="" type="checkbox"/>	4. Schlüsselregelung	Die Ausgabe, Rücknahme und ein evtl. Verlust von Schlüsseln werden schriftlich dokumentiert. Schlüsselausgaben erfolgen entsprechend Zonensystem des ISMS.
<input checked="" type="checkbox"/>	5. Regelung für Firmenfremde	Besuche von externen Dienstleistern, Kunden etc. müssen angemeldet werden. Anwesenheiten werden dokumentiert. Richtlinien für, und regelmäßige Schulungen der Mitarbeitenden zum Umgang mit Besuchern sind im ISMS definiert und etabliert.
<input checked="" type="checkbox"/>	6. Anwesenheitsaufzeichnungen	Anwesenheiten von Betriebsfremden werden entsprechend des Besuchermanagementsystems erfasst.
<input type="checkbox"/>	7. Besucherausweise	Besucherausweise finden derzeit keine Anwendung. Zugänge zu vertraulichen und geheimen Bereichen werden durch das Zonenkonzept und das Besuchermanagement des ISMS organisatorisch und/oder physisch gesichert. Mitarbeitende werden regelmäßig geschult.
<input checked="" type="checkbox"/>	8. Sicherung auch außerhalb der Arbeitszeit durch Alarmanlage und/oder Werkschutz	Für die Gebäudeeingänge werden einbruchhemmende Türen nach DIN EN 1627 verwendet, welche mit Sicherheitsschlössern nach DIN 18252 ausgestattet sind. Bei den eingesetzten Fenstern handelt es sich um einbruchhemmende Fenster nach DIN EN 1627.
<input checked="" type="checkbox"/>	9. Gesicherter Eingang für An- und Ablieferung	Die Räumlichkeiten sind stets geschlossen. An- und Ablieferungen werden stets durch einen Mitarbeitenden getätigt, der den Prozess begleitet. Zonenkonzept umfasst einen expliziten Liefer-/Versandbereich.
<input checked="" type="checkbox"/>	10. Türsicherung (elektrischer Türschließer, Ausweisleser, Fernsehmonitor, Pfortner)	Selbstschließende Türen mit elektrischem Türschließer.
<input type="checkbox"/>	11. Closed-Shop-Betrieb	
<input checked="" type="checkbox"/>	12. Gegenseitige Überwachung (4-Augen-Prinzip)	Anwesenheiten sind durch ein Transpondersystem dokumentiert.
<input checked="" type="checkbox"/>	13. Entsprechende Ausgestaltung der Maßnahmen zur Objektsicherung (z. B. Spezialverglasung, Einbruchmeldesystem, Absicherung von Schächten, Geländebewachung)	
<input checked="" type="checkbox"/>	14. Verschießbarkeit von Datenstationen	Ist möglich. Technisch sind Datenstationen im Verlustfall wirksam durch Verschlüsselung geschützt.

<input checked="" type="checkbox"/>	15. Identifizierung eines Terminals und/oder eines Terminalbenutzers gegenüber dem DV-System (z. B. durch Ausweisleser)	Nutzerbasierte Zugänge sind eindeutig nachvollziehbar.
<input type="checkbox"/>	16. Vergabe und Sicherung von Identifizierungsschlüsseln	
<input type="checkbox"/>	17. Zuordnung einzelner Terminals und Identifizierungsmerkmale ausschließlich für bestimmte Funktionen	
<input type="checkbox"/>	18. Funktionelle und/oder zeitlich beschränkte Nutzung von Terminals und Identifizierungsmerkmale	
<input checked="" type="checkbox"/>	19. Regelung der Benutzerberechtigung	Need-to-know-Prinzip mit zyklischen Kontrollen entsprechend ISMS.
<input checked="" type="checkbox"/>	20. Verpflichtung der Mitarbeitenden nach BDSG-neu	Wird durchgeführt
<input checked="" type="checkbox"/>	21. Einsatz von Benutzercodes für Daten und Programme	Authentifizierung mittels single-sign-on oder Benutzernamen und Passwort
<input checked="" type="checkbox"/>	22. Einsatz von Verschlüsselungsroutinen für Dateien	Wird nach Bedarf eingesetzt
<input checked="" type="checkbox"/>	23. Differenzierte Zugriffsregelung (z. B. durch Segmentzugriffssperren)	Zugriffsrollen werden angewandt
<input type="checkbox"/>	24. Zeitliche Begrenzung der Zutrittsmöglichkeiten	Zutritte (auch außerhalb der Geschäftszeiten) können eindeutig nachvollzogen werden.
<input checked="" type="checkbox"/>	25. Richtlinien für die Dateioorganisation	Richtlinie zur Dokumentenlenkung ist etabliert.
<input checked="" type="checkbox"/>	26. Protokollierung und Auswertung der Dateibenutzung	Protokollierung findet statt. Auswertungen finden nur bei Bedarf statt.
<input type="checkbox"/>	27. Besondere Kontrolle des Einsatzes von Hilfsprogrammen, soweit diese geeignet sind, die Sicherungsmaßnahmen zu umgehen	
<input checked="" type="checkbox"/>	28. Kontrollierte Vernichtung von Datenträgern	Durch externen, zertifizierten Dienstleister
<input type="checkbox"/>	29. Arbeitsanweisung und Bearbeitungsverfahren für Datenerfassungsvorlagen	
<input checked="" type="checkbox"/>	30. Prüf-, Abstimm- und Kontrollsysteme	Anwendung des ISMS unter Aufsicht des externen ISB. Regelmäßige Schulungen aller Mitarbeitenden finden statt.
<input type="checkbox"/>	31. Programmprüfungs- und Freigabeverfahren	
<input checked="" type="checkbox"/>	32. Firewall	MS Enterprise – Security Suite

2. Zugriffskontrolle

Es ist zu gewährleisten, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können.

Vorhandene Maßnahmen:

Vorh.	Maßnahme	Kommentar
<input checked="" type="checkbox"/>	1. Datenträgerverwaltung/-entsorgung	Zentrale Erfassung und Verwaltung im Assetmanagement und MDM-.
<input type="checkbox"/>	2. Datenstation mit Funktionsberechtigungsschlüssel	
<input checked="" type="checkbox"/>	3. Regelung der Zugriffsberechtigung	Rechte werden nach dem need-to-know-Prinzip vergeben. Regelmäßige Prüfung von Freigaben findet statt.
<input type="checkbox"/>	4. Überprüfung der Berechtigung, maschinell z.B. durch Identifizierungsschlüssel	
<input checked="" type="checkbox"/>	5. Auswertung von Protokollen	Im Bedarfsfall
<input type="checkbox"/>	6. Ausweisleser am Terminal	
<input checked="" type="checkbox"/>	7. Zeitliche Begrenzung der Zugriffsmöglichkeiten	Zugriffsmöglichkeiten werden regelmäßig durch ISB überprüft.
<input type="checkbox"/>	8. Teilzugriffsmöglichkeiten auf Datenbestände und Funktionen	

3. Datenträgerkontrolle

Verhinderung des unbefugten Lesens, Kopierens, Veränderns oder Löschens von Datenträgern.

Vorhandene Maßnahmen:

Vorh.	Maßnahme	Kommentar
<input checked="" type="checkbox"/>	1. Sichere Aufbewahrung von Datenträgern	Datenträger sind generell verschlüsselt. Wenn vorhanden und nötig, werden Datenträger in Zugriffsbeschränkter Räumlichkeit aufbewahrt.
<input type="checkbox"/>	2. Einrichtungen von Standleitungen beziehungsweise VPN Tunneln	In Absprache möglich.
<input type="checkbox"/>	3. Weitergabe von Daten in anonymisierter oder pseudonymisierter Form	Nur bei Bedarf und wenn technisch möglich.
<input checked="" type="checkbox"/>	4. Verschlüsselung von (mobilen) Datenträgern	BitLocker Verschlüsselung.
<input checked="" type="checkbox"/>	5. Ordnungsgemäße Vernichtung von Datenträgern (DIN 66399)	Durch externen Dienstleister.

<input checked="" type="checkbox"/>	6.	Einsatz von Aktenvernichtern beziehungsweise Dienstleistern (nach Möglichkeit mit Datenschutz-Gütesiegel)	P4 Schredder im Großraumbüro P5 Schredder im HR und Controllingbüro
<input checked="" type="checkbox"/>	7.	Protokollierung der Vernichtung	Protokolle werden durch Dienstleister bei Vernichtung von Datenträgern bereitgestellt.

4. Speicherkontrolle

Die Verhinderung der unbefugten Eingabe von personenbezogenen Daten sowie der unbefugten Kenntnisnahme, Veränderung und Löschung von gespeicherten personenbezogenen Daten.

Vorhandene Maßnahmen:

Vorh.	Maßnahme	Kommentar
<input checked="" type="checkbox"/>	1. Bildschirm und Computersperre bei Verlassen des Arbeitsplatzes	Automatischer Logout durch Windows bei Inaktivität.
<input checked="" type="checkbox"/>	2. Benutzeridentifizierung	Zugriffe werden nutzerspezifisch protokolliert und können bei Bedarf ausgewertet werden.
<input checked="" type="checkbox"/>	3. Protokollierung des Verhaltens des Nutzers	Entsprechend Risikobewertung (z.B. bei generellen E-Mail-Weiterleitungen)
<input checked="" type="checkbox"/>	4. Verschlüsselte Speicherung der Daten	BitLocker Verschlüsselung
<input checked="" type="checkbox"/>	5. Trennung von Administration und Produktionsbereich	Dedizierte Administrationszugänge werden nach Need-To-Know-Prinzip vergeben
<input type="checkbox"/>	6. Protokollierung der Art und Weise des Zugriffes auf die Daten	

5. Benutzerkontrolle

Verhinderung der Nutzung automatisierter Verarbeitungssysteme mit Hilfe von Einrichtungen zur Datenübertragung durch Unbefugte.

Vorhandene Maßnahmen:

Vorh.	Maßnahme	Kommentar
<input checked="" type="checkbox"/>	1. Firewall, Intrusion Detection/Prevention	Automatisiertes Monitoring aller exponierten Systeme
<input checked="" type="checkbox"/>	2. Benutzeridentifizierung	Nutzerzugänge werden geloggt.
<input checked="" type="checkbox"/>	3. sichere technische Passwortvorgabe	Passwortrichtlinie ist in Abhängigkeit des Schutzbedarf etabliert und wird wo technisch möglich erzwungen.

<input checked="" type="checkbox"/>	4.	Passwort-Policy / Passwortrichtlinie	Passwortrichtlinie ist in Abhängigkeit des Schutzbedarf etabliert. Sie umfasst Mindestpasswortlänge von 10 Zeichen, wobei das Passwort auf Groß-/Kleinbuchstaben, Ziffern und Sonderzeichen bestehen muss. Es ist sichergestellt, dass Passwörter jährlich gewechselt werden. Passwörter werden verschlüsselt gespeichert.
<input checked="" type="checkbox"/>	5.	Absicherung der Geräte und Netzwerke (Verschlüsselung von Notebooks, Smartphones, Datenträger)	Bitlocker oder sonstige Deviceverschlüsselung bei Smartphones.
<input checked="" type="checkbox"/>	6.	Festlegung der Personen, die Nutzungsberechtigungen haben (Zuständigkeiten)	Nutzungsberechtigungen werden dokumentiert und zyklisch überprüft
<input checked="" type="checkbox"/>	7.	Protokollierung der Nutzer und Aktivitäten	Nutzerprotokollierung findet statt. Aktivitäten werden soweit möglich und nötig protokolliert.
<input checked="" type="checkbox"/>	8.	Clean-Desk-Policy	Ist etabliert.

6. Übertragungskontrolle

Gewährleistung, dass überprüft und festgestellt werden kann, an welche Stellen personenbezogene Daten mit Hilfe von Einrichtungen zur Datenübertragung übermittelt oder zur Verfügung gestellt wurden oder werden können.

Vorhandene Maßnahmen:

Vorh.	Maßnahme	Kommentar
<input checked="" type="checkbox"/>	1. Protokollierung von Datenübermittlungen	Entsprechende Konzepte und Prozessbeschreibungen sind von IT erarbeitet.
<input checked="" type="checkbox"/>	2. Auswertungsmöglichkeiten (Feststellung der Sender und Empfänger)	Entsprechende Konzepte und Prozessbeschreibungen sind von IT erarbeitet.
<input checked="" type="checkbox"/>	3. Festlegung von Übermittlungswegen (wie wird an welche Empfängerkategorie übermittelt)	Durch Richtlinie geregelt.

7. Eingabekontrolle

Es ist zu gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind.

Vorhandene Maßnahmen:

Vorh.	Maßnahme	Kommentar
-------	----------	-----------

<input type="checkbox"/>	1. Nachweis der organisatorisch festgelegten Zuständigkeiten für die Eingabe	Implizit durch Rechtevergabe geregelt.
<input checked="" type="checkbox"/>	2. Protokollierung von Eingaben	Zugriffe werden auf Datenbankebene geloggt.
<input type="checkbox"/>	3. Protokollierung der Dateibenutzung	Wo möglich, durch Datenbanklogs.

8. Transportkontrolle

Gewährleistung, dass bei der Übermittlung personenbezogener Daten sowie beim Transport von Datenträgern die Vertraulichkeit und Integrität der Daten geschützt werden.

Vorhandene Maßnahmen:

Vorh.	Maßnahme	Kommentar
<input checked="" type="checkbox"/>	1. Sicherheit der Datenübermittlung (VPN, FTPS etc.)	Entsprechende Richtlinien und Prozessbeschreibungen vorhanden.
<input checked="" type="checkbox"/>	2. Feststellung befugter Personen	Wird Projektbezogen durchgeführt.
<input type="checkbox"/>	3. Gegenseitige Überwachung (4-Augen-Prinzip)	
<input type="checkbox"/>	4. Gesicherter RZ-Eingang für An- und Ablieferung	
<input type="checkbox"/>	5. Ausgabe von Datenträgern nur an autorisierte Personen (z. B. Auftragsquittung, Begleitpapier)	
<input checked="" type="checkbox"/>	6. Datenträger-Verwaltung	
<input type="checkbox"/>	7. Festmontierte Plattenspeicher	
<input checked="" type="checkbox"/>	8. Bestandskontrolle	Überprüfungen über das Assetmanagement finden statt.
<input checked="" type="checkbox"/>	9. Gesonderter Verschluss vertraulicher Datenträger	Der Umgang mit vertraulichen und geheimen Informationen ist in einem entsprechenden Zonenplan geregelt.
<input type="checkbox"/>	10. Sicherheitsschranke	Keine spezifischen Sicherheitsschranke vorhanden. Je nach Schutzbedarf gibt es eine räumliche Trennung mit entsprechenden Zugangskontrollen.
<input type="checkbox"/>	11. Verbot der Mitnahme von Taschen und sonstigen Gepäckstücken in die Sicherheitsbereiche	Nein. Externe Personen sind in den Firmenräumlichkeiten entsprechend des Besuchermanagements immer in Begleitung eines Mitarbeitenden.
<input checked="" type="checkbox"/>	12. Kontrollierte Vernichtung von Datenträgern (z. B. Fehldrucke)	Dokumente werden entsprechend vernichtet (P4 und P5 Schutzklasse). Datenträger werden über zertifizierte Dienstleister vernichtet.
<input type="checkbox"/>	13. Regelung der Anfertigung von Kopien	

<input checked="" type="checkbox"/>	14. Dokumentation der Abruf- und Übermittlungsprogramme	Kommunikationskanäle und -medien werden zu Projektbeginn entsprechend der Klassifizierung bzgl. Vertraulichkeit festgelegt und dokumentiert.
<input type="checkbox"/>	15. Regelungen zur Fernwartung	
<input type="checkbox"/>	16. Dokumentation der Stellen, an die eine Übermittlung vorgesehen ist, sowie der Übermittlungswege (Konfiguration)	
<input type="checkbox"/>	17. Bestimmte autorisierte Benutzer	Zugangsberechtigung nach need-to-know Prinzip.
<input type="checkbox"/>	18. Verpackungs- und Versandvorschriften (Versandart z. B. in verschlossenen Behältnissen)	Kann in Absprache vereinbart werden.
<input type="checkbox"/>	19. Direktabholung, Kurierdienst, Transportbegleitung	Kann in Absprache vereinbart werden.
<input type="checkbox"/>	20. Plausibilitätsprüfung	Keine explizite Richtlinie etabliert, Mitarbeitende werden in diesen Belangen regelmäßig geschult und sind sensibilisiert.
<input type="checkbox"/>	21. Vollständigkeits- und Richtigkeitsprüfung	
<input type="checkbox"/>	22. Löschung von Datenresten vor Datenträgeraustausch	Austausch von Datenträger über Kunden hinweg findet nicht statt.

9. Wiederherstellbarkeit

Sie müssen gewährleisten, dass sie eingesetzte Systeme im Störfall wiederherstellen können.

Vorhandene Maßnahmen:

Vorh.	Maßnahme	Kommentar
<input checked="" type="checkbox"/>	1. Datensicherungen erfolgen in periodischen Abständen	Ein Datensicherungskonzept ist etabliert.
<input type="checkbox"/>	2. Regelmäßige Tests zur Datenwiederherstellung und Protokollierung der Ergebnisse	Wirksamkeit des Datensicherungskonzepts wird regelmäßig durch Restorettests überprüft und dokumentiert.

10. Zuverlässigkeit

Die Gewährleistung, dass alle Funktionen des Systems zur Verfügung stehen und auftretende Fehlfunktionen gemeldet werden.

Vorhandene Maßnahmen:

Vorh.	Maßnahme	Kommentar
<input checked="" type="checkbox"/>	1. Backup- und Recovery-Konzept mit täglicher Sicherung der Daten je nach gebuchten Leistungen des Hauptauftrages	Ist etabliert.
<input checked="" type="checkbox"/>	2. Einsatz von Festplattenspiegelung	Wenn nicht anders angegeben findet die Bereitstellung über den ISO27001 zertifizierten Hostler Hetzner Online GmbH

		statt. Entsprechende Mechanismen sind etabliert und finden Anwendung.
<input checked="" type="checkbox"/>	3. Sicherstellung der Stromversorgung bei Ausfall (USV)	Wenn nicht anders angegeben findet die Bereitstellung über den ISO27001 zertifizierten Hoster Hetzner Online GmbH statt. Entsprechende Mechanismen sind etabliert und finden Anwendung.
<input checked="" type="checkbox"/>	4. Einsatz von Portreglementierungen	Werden entsprechend interner Richtlinien umgesetzt. Die Defaultkonfiguration ist „Maximalrestriktiv“.
<input checked="" type="checkbox"/>	5. Vermeidung von Single-Point-of-Failures als Grundgedanke aller Infrastruktur im Rechenzentrumsbetrieb, d.h. Sicherstellen von Verfügbarkeit durch Redundanz von Systemen und Komponenten (z.B. 2. RZ-Standort)	Wenn nicht anders angegeben findet die Bereitstellung über den ISO27001 zertifizierten Hoster Hetzner Online GmbH statt. Entsprechende Mechanismen sind etabliert und finden Anwendung.
<input checked="" type="checkbox"/>	6. Systemüberwachung der relevanten Hard und Software (7x24h Monitoring aller Systeme der Rechenzentrumsinfrastruktur)	Alle Systeme werden automatisiert gemonitort und es ist ein proaktives Reporting/Alearting etabliert.
<input checked="" type="checkbox"/>	7. Verwendung von Firewalls und Load Balancern zur Zugangs- und Content-Filterung und horizontalen Lastverteilung auch bei Shared Services	Findet bei Bedarf Anwendung.
<input checked="" type="checkbox"/>	8. Klimaversorgung	Wenn nicht anders angegeben findet die Bereitstellung über den ISO27001 zertifizierten Hoster Hetzner Online GmbH statt. Entsprechende Mechanismen sind etabliert und finden Anwendung.

11. Datenintegrität

Die Gewährleistung, dass gespeicherte personenbezogene Daten nicht durch Fehlfunktionen des Systems beschädigt werden können.

Vorhandene Maßnahmen:

Vorh.	Maßnahme	Kommentar
<input checked="" type="checkbox"/>	1. Datensicherungen erfolgen in periodischen Abständen	Systeme sind alle entsprechend konfiguriert. Wirksamkeit wird regelmäßig überprüft
<input checked="" type="checkbox"/>	2. Einsatz von Virensclannern, Firewalls, Spam-Filter)	MS Enterprise – Security Suite
<input checked="" type="checkbox"/>	3. Sicherstellung der Stromversorgung bei Ausfall	Wenn nicht anders angegeben findet die Bereitstellung über den ISO27001 zertifizierten Hoster Hetzner Online GmbH statt. Entsprechende Mechanismen sind etabliert und finden Anwendung.
<input type="checkbox"/>	4. Einsatz von elektronischen Signaturen	
<input checked="" type="checkbox"/>	5. Datensicherungs- und Wiederherstellungskonzept	Ist etabliert und wird regelmäßig auf Wirksamkeit geprüft.

<input checked="" type="checkbox"/>	6. Systemüberwachung der relevanten Hard- und Software	Alle Systeme werden automatisiert gemonitort und es ist ein proaktives Reporting/Alerting etabliert.
-------------------------------------	--	--

12. Auftragskontrolle

Es ist zu gewährleisten, dass der Auftraggeber die entsprechenden Kontrollen durchführt.

Vorhandene Maßnahmen:

Vorh.	Maßnahmen	Kommentar
<input checked="" type="checkbox"/>	1. Sorgfältige Auswahl der Auftragnehmer	Auftragnehmer werden einer Risikobewertung unterzogen.
<input checked="" type="checkbox"/>	2. Vertragliche Vereinbarungen mit dem Auftragnehmer	ja
<input checked="" type="checkbox"/>	3. Beschreibung der technisch-organisatorischen Maßnahmen durch den Auftragnehmer	ja
<input type="checkbox"/>	4. Zertifizierung durch den Auftragnehmer	
<input type="checkbox"/>	5. Mitarbeitende werden in regelmäßigen Abständen im Datenschutzrecht unterwiesen auch im Hinblick auf das Weisungsrecht des Auftraggebers	

13. Verfügbarkeitskontrolle

Es ist zu gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind.

Vorhandene Maßnahmen:

Vorh.	Maßnahmen	Kommentar
<input checked="" type="checkbox"/>	1. Schutz der elektronischen Daten in IT-Systemen	Wenn nicht anders angegeben findet die Bereitstellung über den ISO27001 zertifizierten Hoster Hetzner Online GmbH statt. Entsprechende Mechanismen sind etabliert und finden Anwendung.
<input checked="" type="checkbox"/>	2. Schutz physischer Daten	Zugangsmöglichkeiten sind entsprechend Zonensystem geregelt. Wenn möglich und nötig werden physische Daten zusätzlich digitalisiert.
<input type="checkbox"/>	3. Räumlich getrennte Aufbewahrung von Sicherungsdatenträgern	Wenn nicht anders angegeben findet die Bereitstellung über den ISO27001 zertifizierten Hoster Hetzner Online GmbH statt. Entsprechende Mechanismen sind etabliert und finden Anwendung.
<input checked="" type="checkbox"/>	4. Brandschutzeinrichtungen	Feuerlöscher sind ausreichend vorhanden.
<input type="checkbox"/>	5. Unterbrechungsfreie Stromversorgung	
<input checked="" type="checkbox"/>	6. Backup-Verfahren	Vorhanden. Wird regelmäßig in Restoretests auf Wirksamkeit überprüft.

<input checked="" type="checkbox"/>	7. Notfallplan	Ein Notfallhandbuch ist vorhanden und Mitarbeitende sind geschult.
<input checked="" type="checkbox"/>	8. Spam-Filter	aktiv
<input checked="" type="checkbox"/>	9. Virenschutz	aktiv

14. Trennbarkeit

Maßnahmen, die gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können. Dieses kann beispielsweise durch logische und physikalische Trennung der Daten gewährleistet werden.

Vorhandene Maßnahmen:

Vorh.	Maßnahmen	Kommentar
<input checked="" type="checkbox"/>	1. Trennung von Produktiv- und Testumgebung	Ist gegeben.
<input checked="" type="checkbox"/>	2. Physikalische Trennung (Systeme / Datenbanken / Datenträger)	Wird, soweit möglich, angewandt. Falls nicht möglich, greifen Mechanismen zur Mandantentrennung.
<input checked="" type="checkbox"/>	3. Mandantenfähigkeit relevanter Anwendungen	Ist gegeben (wenn nötig).
<input type="checkbox"/>	4. Steuerung über Berechtigungskonzept	
<input checked="" type="checkbox"/>	5. Festlegung von Datenbankrechten	Verantwortlichkeiten und Rechte sind geregelt.
<input type="checkbox"/>	6. Datensätze sind mit Zweckattributen versehen	

15. Zweckbindungskontrolle

Es ist zu gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können.

Vorhandene Maßnahmen:

Vorh.	Maßnahmen	Kommentar
<input checked="" type="checkbox"/>	1. Mandantentrennung	Findet statt.
<input type="checkbox"/>	2. Funktionstrennungen	

16. Zugriffsberechtigungen

Die Zugriffsberechtigungen ergeben sich aus [Hier Anlage XY eingeben].

Vorh.	Maßnahmen	Kommentar
-------	-----------	-----------

<input type="checkbox"/>	1. Differenzierte Berechtigungsvergabe in den jeweiligen Applikationen	
--------------------------	--	--

17. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung

Durch Richtlinien und/oder Anweisungen an die Beschäftigten tragen wir dazu bei, dass eine Verarbeitung personenbezogener Daten in einer Weise gewährleistet ist, die den Anforderungen der DSGVO entspricht. Dies beinhaltet insbesondere eine regelmäßige Überprüfung der Wirksamkeit der getroffenen Maßnahmen zum Schutz personenbezogener Daten und ggf. der Anpassung. Es ist insbesondere sichergestellt, dass Datenschutzvorfälle von allen Beschäftigten erkannt und unverzüglich dem Auftraggeber gemeldet werden, wenn dies Daten betrifft, die im Rahmen der Auftragsverarbeitung für den Auftraggeber verarbeitet werden.

- Regelmäßige interne Audits
- Datenschutz-Managementsystem
- Externer Datenschutzbeauftragter
- Schulungen für Mitarbeitende
- Verpflichtung auf Vertraulichkeit
- Einhaltung der Informationspflichten nach Art. 13 und 14 DSGVO
- Prozessbeschreibung zu Betroffenenanfragen
- Managementsystem der Informationssicherheit
- Einsatz von Software mit datenschutzfreundlichen Voreinstellungen gem. (Art. 25 Abs. 2 DSGVO)