

Anhang 3: Technisch-organisatorische Maßnahmen zur IT-Sicherheit nach Art. 32 DSGVO

der Organisation

Stand:

Verantwortlicher

Datum des Auftragsverarbeitungsvertrags:

Sofern der Auftragsverarbeiter seine „technischen und organisatorischen Maßnahmen zur IT-Sicherheit“ nicht bereits selbst dokumentiert hat, ist es erforderlich, dass er die nachfolgenden Fragen so umfassend und detailliert wie möglich beantwortet (vgl. § 3 des Vertrages), andernfalls ist die Dokumentation der technisch organisatorischen Maßnahmen als Anlage beizufügen und nur die Ziffern 1 und 6 auszufüllen.

1. Vorhandene Dokumentation

Die oben genannte Organisation setzt die erforderlichen technischen und organisatorischen Maßnahmen um, die erforderlich sind, um die Ausführungen der Vorschriften der Datenschutzgesetze zu gewährleisten. Die Maßnahmen sind bereits dokumentiert und als Anlage zu diesem Anhang beigefügt.

☐

ja

☐

nein

Wenn die Frage mit „nein“ beantwortet ist, sind die nachfolgenden Fragen auszufüllen, andernfalls sind nur die Anlagen unter Ziffer **6** zu benennen und das Dokumente zu signieren.

2. Maßnahmen zu Gewährleistung der Vertraulichkeit

2.1 Zutrittskontrolle Soll verhindern, dass Unbefugte räumlich Zugang zu Datenverarbeitungsanlagen erhalten. Maßnahmen zur Gebäude- und Raumsicherung.	Zutreffend (falls ja, bitte ankreuzen)
Schließsystem/ Schließanlage	☐
Spezialverglasung	☐
Sorgfältige Auswahl externer Wachdienst	☐
Alarmanlage	☐
Verbindung Alarmanlage zu Wachdienst/ Polizei	☐
Lichtschraken/ Bewegungsmelder	☐
Verbindung Bewegungsmelder zu Wachdienst/ Polizei	☐
Videoüberwachung	☐
Biometrische Zutrittskontrolle	☐
Wachdienst vor Ort/ Sicherung außerhalb der Arbeitszeiten	☐
Personenüberprüfung bei Pförtner /Empfang	☐
Berechtigungsausweise	☐
Besucherausweise	☐
Protokollierung von Besucherzutritten / Besucherbuch	☐
Begleitung von Besucherzutritten durch eigene Mitarbeiter	☐
Elektronische Zutrittscodekarten/ Zutrittstransponder	☐
Schlüsselregelung	☐

Zutrittsbegrüßungskonzept	☐
Abgestufte Sicherheitsbereiche und kontrollierter Zutritt	☐
Gesicherter Eingang für An und Ablieferungen	☐
Gesondert gesicherter Zutritt zum Serverraum	☐
Gesondert gesicherter Zutritt zum Rechenzentrum	☐
Arbeitsanweisungen /Richtlinien bzgl. des Verschließens von Räumlichkeiten bei Verlassen/Arbeitsende	☐
Sorgfältige Auswahl von Reinigungspersonal	☐
Sonstiges:	☐

2.2 Zutrittskontrolle Soll den Zugang Unbefugter zu Datenverarbeitungssystemen und deren unbefugte Nutzung verhindern. Systemabsicherung.	Zutreffend (falls ja, bitte ankreuzen)
Zuordnung von Benutzerrechten	☐
Erstellen von Benutzerprofilen	☐
Berechtigungsmanagement	☐
Dokumentierter Prozess zur Rechtevergabe bei Neueintritt von Mitarbeitern	☐
Dokumentierter Prozess zum Rechteentzug bei Abteilungswechseln von Mitarbeitern	☐
Dokumentierter Prozess zum Rechteentzug bei Austritt von Mitarbeitern	☐
Funktionelle und/oder zeitlich limitierte Vergabe von Benutzerberechtigungen	☐
Verwendung von individuellen Passwörtern	☐

Login mit Benutzername und Passwort	☐
Login mit biometrischen Daten	☐
Separates BIOS-Passwort	☐
Automatische passwortgesicherte Sperrung des Bildschirms nach Inaktivität (Bildschirmschoner)	☐
Passwortrichtlinie mit Mindestvorgaben zur Passwortkomplexität:	☐
• Mindestens 8 Ziffern	☐
• Groß- und Kleinschreibung, Sonderzeichen, Zahl (davon mind. 3 Kriterien)	☐
• Verhinderung von Trivialpasswörtern (z.B. Passwort1, Passwort2, 123456, qwertz)	☐
• Passworthistorie (keine erneute Verwendung der letzten 10 Passwörter)	☐
• Verhinderung von PW nach positivem Abgleich mit Wörterbüchern	☐
• Eingabebeschränkung bestimmter Sonderzeichen zur Verhinderung von SQL-Injections	☐
• Automatische Sperrung von Nutzeraccounts nach mehrfacher Fehleingabe von Passwörtern	☐
• Angemessen sicheres Verfahren zum Zurücksetzen von Passwörtern	☐
Sonstiges: (z.B. Nutzung von Fido2)	☐
Hashing von gespeicherten Passwörtern mittels	☐
• SHA3	☐
• RIPEMD320	☐
• bcrypt	☐

Anderes Hashverfahren:	☐
Hashes werden „gesalzen“ (Salt) oder „gepfeffert“ (Pepper)	☐
Verschlüsselung von Netzwerken	☐
Verwendete Verschlüsselungsalgorithmen:	☐
Verschluss von Datenverarbeitungsanlagen (z.B. verschlossener Cage für Server)	☐
Sperrung von externen Schnittstellen (z.B. USB)	☐
Verwendete Verschlüsselungsalgorithmen:	☐
Programmprüfungs- und Freigabeverfahren bei Neuinstallationen	☐
Verwendung von Intrusion-Prevention-Systemen	☐
Nutzung von VPN-Technologie	☐
Einsatz von Anti-Viren-Software: Server	☐
Einsatz von Anti-Viren-Software: Clients	☐
Einsatz einer Software-Firewall	☐
Einsatz einer Hardware-Firewall	☐
Mobile-Device-Management	☐
Aufbewahrung personenbezogener Daten/Datenträgern in verschließbaren Sicherheitsschränken oder in gesondert gesicherten Räumen	☐
Regelung zum Homeoffice / zur Telearbeit	☐
Sonstige Maßnahmen:	☐

2.3 Zugriffskontrolle	Zutreffend
Soll unerlaubte Tätigkeiten in Datenverarbeitungssystemen außerhalb eingeräumter Berechtigungen verhindern.	(falls ja, bitte ankreuzen)
Nutzung eines Berechtigungskonzepts	☐
Minimaler Einsatz von Administratoren-Konten	☐
Trennung von Berechtigungsbewilligung (organisatorisch) und Berechtigungsvergabe (technisch)	☐
Regelung zur Wiederherstellung von Daten aus Backups (wer, wann, auf wessen Anforderung)	☐
Aufbewahrung von Datensicherungen (z.B. Bänder, CDs) im zutrittsgeschützten Safe	☐
Regelmäßige Überprüfung von Berechtigungen	☐
Beschränkung der freien und unkontrollierten Abfragemöglichkeit von Datenbanken	☐
Regelmäßige Auswertung von Protokollen (Logfiles)	☐
Zeitliche Begrenzung von Zugriffsmöglichkeiten	☐
Teilzugriffsmöglichkeiten auf Datenbestände und Funktionen (Read, Write, Execute)	☐
Protokollierung von Dateizugriffen	☐
Protokollierung von Dateilöschungen	☐
Protokollierung von Dateiveränderungen	☐
• SPAM-Filter	☐
Intrusiondetection (IDS)	☐
• Software für das Security Information and Event Management (SIEM)	☐
Beschränkter Zugriff auf LogFiles (nur Log-Admin)	☐

Speicherung von Log-Files auf dedizierten LogFile-Server(n)	☐
Verschlüsselte Speicherung der Daten	☐
verwendete Verschlüsselungsalgorithmen:	☐
- AES (128/256 bit)	☐
3DES	☐
- RSA (1024/2048 bit)	☐
- Sonstiges:	☐
Verwendete Hash-Funktion:	☐
- SHA2 (256, 384, 512 bit)	☐
- SHA3	☐
- bcrypt	☐
- Andere Verfahren:	☐
- Hashes werden „gesalzen“ (Salt) oder „gepfeffert“(Pepper)	☐
Kontrollierte Vernichtung von Daten:	☐
Shredder (Cross-Cut, mindestens Stufe 3, DIN 66399)	☐
Verschlossene Behältnisse aus Metall (sog. Datenschutztonnen), Entsorgung durch Dienstleister	☐
Datenträgerentsorgung - Sichere Löschung von Datenträgern (DIN 66399):	☐
Peter-Gutmann-Algorithmus – 35-faches Überschreiben	☐
Physikalische Zerstörung (z.B. Shredder bei Partikelgrößen bis max. 1000 Quadrat-Millimeter)	☐

Entmagnetisierung durch thermische Zerstörung (Erhitzung der Magnetplattenoberfläche über die Curie-Temperatur der verwendeten Beschichtung hinaus)	☐
Entmagnetisierung mittels eines Degaussers	☐
Sonstiges Vernichtungsverfahren:	☐
Richtlinie zur Datenvernichtung	☐
Clean Desk-Policy	☐
Sonstige Maßnahmen:	☐

2.4 Auftragskontrolle Soll sicherstellen, dass Daten, die im Auftrag durch Dienstleister (Unterauftragsverarbeiter) verarbeitet werden, nur gemäß der Weisung des Verantwortlichen verarbeitet werden.	Zutreffend (falls ja, bitte ankreuzen)
Vertragsgestaltung gem. gesetzlichen Vorgaben (Art. 28 DSGVO)	☐
Zentrale Erfassung vorhandener Dienstleister (einheitliches Vertragsmanagement)	☐
Vorabkontrollen beim Auftragsverarbeiter vor Vertragsbeginn	☐
Regelmäßige Kontrollen beim Auftragsverarbeiter nach Vertragsbeginn (Während der Vertragsdauer)	☐
Vor-Ort-Kontrollen beim Auftragsverarbeiter	☐
Überprüfung des Datensicherheitskonzepts beim Auftragsverarbeiter	☐
Sichtung vorhandener IT-Sicherheitszertifikate der Auftragsverarbeiter	☐
Auftragsverarbeiter hat Datenschutzbeauftragten benannt	☐
Erteilung von Weisungen zur Verbesserung des Datenschutzes ggü. Auftragsverarbeitern	☐
Sonstige Maßnahmen:	☐

2.5 Trennungskontrolle Daten, die zu unterschiedlichen Zwecken erhoben wurden, sind auch getrennt voneinander zu verarbeiten.	Zutreffend (falls ja, bitte ankreuzen)
Trennung von Kunden (Mandantenfähigkeit des verwendeten Systems)	☐
Physikalische Datentrennung (z.B. unterschiedliche Systeme oder Datenträger)	☐
Logische Datentrennung (z.B. auf Basis von Kunden- oder Mandantennummern)	☐
Datensicherungen der Daten auf separaten Datenträgern (ohne Daten anderer Betroffenen)	☐
Berechtigungskonzept, getrennte Verarbeitung der Daten	☐
Trennung von Entwicklungs-, Test- und Produktivsystemen	☐
Zuordnung von Datensätzen zu Zweckattributen	☐
Bei pseudonymisierten Daten: Trennung der Zuordnungsdatei & Speicherung auf einem anderen System	☐
Sonstige Maßnahmen:	☐

3. Maßnahmen zur Gewährleistung der Integrität

3.1 Weitergabekontrolle Soll die Sicherheit der Daten bei elektronischer Übertragung und Datentransport und die Nachvollziehbarkeit der Weitergabe gewährleisten.	Zutreffend (falls ja, bitte ankreuzen)
Wie werden Daten zwischen Verantwortlichem und Auftragsverarbeitern übermittelt?	☐
VPN-Verbindung	☐
Secure File Transfer Protocol (sftp)	☐
Citrix-Verbindung	☐

E-Mail-Verschlüsselung	☐
• SMIME	☐
• OpenPGP	☐
• E-Mail Versand mit verschlüsselten ZIP-Dateien	☐
Datenaustausch über https-Verbindung	☐
- verwendetes Verschlüsselungsprotokoll:	☐
○ TLS 1.2	☐
○ TLS 1.3	☐
Sonstige Versendungsart:	☐
• verwendete Verschlüsselungsalgorithmen	☐
○ AES (128/256 bit)	☐
○ 3DES	☐
○ RSA (1024/2048 bit)	☐
○ Diffie-Hellmann	☐
• Sonstiges:	☐
Nutzung von Signaturverfahren	☐
Verwendetes Signaturverfahren: ○ RSA	☐
○ ElGamal	☐

○ DAS	☐
- Sonstige:	☐
Digitales Signieren von Makros	☐
Dokumentierte Verwaltung von Datenträgern, Bestandskontrolle	☐
Verschlüsselung vertraulicher Datensätze	☐
Verschlüsselung mobiler Datenträger (z.B. Laptop-Festplatten, externe Festplatten, USB-Sticks)	☐
Verbot der Mitnahme von Taschen und sonstigen Gepäckstücken sowie Mobiltelefonen in Sicherheitsbereiche	☐
Regelung zur Anfertigung von Datensatz-Kopien	☐
Erstellen von Sicherungskopien von Datenträgern, die transportiert werden müssen	☐
Dokumentation der Stellen, an die eine Übermittlung vorgesehen ist, sowie der Übermittlungswege	☐
Direktabholung, Kurierdienst, Transportbegleitung	☐
Vollständigkeits- und Richtigkeitsprüfung	☐
Sonstige Maßnahmen:	☐

3.2 Eingabekontrolle Soll gewährleisten, dass nachvollzogen werden kann, ob, wer, wann personenbezogene Daten in Datenverarbeitungssysteme eingeben, geändert oder gelöscht hat.	Zutreffend (falls ja, bitte ankreuzen)
Technische Protokollierung der Eingabe, Änderung und Löschung von Daten	☐
Manuelle oder automatisierte Auswertung der Protokolle	☐
Differenzierte Benutzerberechtigungen:	☐

- Einzelne Benutzernamen, keine Benutzergruppen	☐
- Vergabe von Rechten zur Eingabe, Änderung und Löschung von Daten auf Basis eines Berechtigungskonzepts	☐
- Feldzugriff bei Datenbanken	☐
Organisatorische Festlegung von Eingabezuständigkeiten	☐
Verpflichtung auf das Datengeheimnis	☐
Über OS-Standard hinausgehendes Log-Konzept	☐
Dezidiert Logserver	☐
Regelung der Zugriffsberechtigungen für Logserver (LogAdmin)	☐
Regelung zu Aufbewahrungsfristen für Revision/Nachweiszwecke	☐
Sonstige Maßnahmen:	☐

4. Maßnahmen zur Gewährleistung der Verfügbarkeit und Belastbarkeit

4.1 Verfügbarkeitskontrolle	Zutreffend
Soll Daten gegen zufällige Zerstörung oder Verlust schützen.	(falls ja, bitte ankreuzen)
Brandmeldeanlagen in Serverräumen	☐
Rauchmelder in Serverräumen	☐
Brandschutztüren	☐
Wasserlose Brandbekämpfungssysteme in Serverräumen	☐
Wassersensoren in Serverräumen	☐
Blitz-/ Überspannungsschutz	☐

Klimatisierte Serverräume	☐
Serverräumlichkeiten in separaten Brandabschnitt	☐
Unterbringung von Backupsystemen in separaten Räumlichkeiten und in separatem Brandabschnitt	☐
Serverräume nicht unter oder neben sanitären Anlagen	☐
Zutrittsbegrenzung bei Serverräumen auf notwendiges Personal	☐
Alarmmeldung bei unberechtigttem Zutritt zu Serverräumen	☐
Lagerung von Archiv-Speichermedien unter notwendigen Lagerbedingungen (Klimatisierung, Schutzbedarf etc.)	☐
CO2-Feuerlöscher in unmittelbarer Nähe der Serverräume	☐
USV-Anlage (Unterbrechungsfreie Stromversorgung)	☐
Stromgenerator	☐
Feuerfeste Schränke	☐
Datenschutztresor	☐
Dokumentiertes Datensicherungs- und Backupkonzept	☐
Durchführung von Datensicherungen und Erstellen von Backups	☐
Regelmäßige Tests zur Datenwiederherstellung	☐
Spiegeln der Festplatten (z.B. RAID)	☐
Getrennte Partitionen für Betriebssystem und Daten	☐
Havariearchiv (Auslagerung von Daten)	☐
Notfallplan vorhanden (BSI-Standard 100-4)	☐

Gewährleistung der langfristigen technischen Lesbarkeit von Backupspeicherm Medien	☐
Sonstige Maßnahmen:	☐

4.2 Belastbarkeit (Widerstandsfähigkeit und Ausfallkontrolle) Soll Systeme befähigen, mit risikobedingten Veränderungen umgehen zu können und Toleranz und Ausgleichsfähigkeit gegenüber Störungen aufzuweisen.	Zutreffend (falls ja, bitte ankreuzen)
Redundante Stromversorgung	☐
Redundante Datenanbindung	☐
Redundante Klimatisierung	☐
Ausweich-Rechenzentren vorhanden (Hot- bzw. Cold-Stand-by?):	☐
sonstige redundante Systeme/Verfahren:	☐
Einsatz einer hochverfügbaren SAN-Lösung (Storage Area Network)	☐
Computer Emergency Response Team (CERT)	☐
Einsatz von Lastenverteilung (Load Balancing)	☐
Abgrenzung kritischer Komponenten	☐
Durchführung von Penetrationstests	☐
Systemhärtung (Deaktivierung nicht erforderlicher Komponenten)	☐
Unverzögliche und regelmäßige Aktivierung von verfügbaren Soft- und Firmwareupdates	☐
Regelmäßige Sensibilisierung der Mitarbeiter (mind. jährlich)	☐

Prozess zur unverzüglichen Meldung von Vorkommnissen an die IT ist allen Mitarbeitern bekannt	☐
Abschluss einer Cyber-Versicherung	☐
Sonstige Maßnahmen:	☐

5. Maßnahmen zur regelmäßigen Überprüfung, Bewertung und Evaluierung

5.1 Kontrollverfahren	Zutreffend
Soll die Wirksamkeit der Datensicherheitsmaßnahmen gewährleisten.	(falls ja, bitte ankreuzen)
Verarbeitungsverzeichnisse (Art. 30 I und II DSGVO) werden jährlich aktualisiert	☐
Meldung neuer/veränderter Datenverarbeitungsverfahren an den Datenschutzbeauftragten	☐
Meldung neuer/veränderter Datenverarbeitungsverfahren an den IT-Sicherheitsbeauftragten	☐
Prozesse zur Meldung neuer/veränderter Verfahren sind dokumentiert	☐
Prüfung der Wirksamkeit getroffener Sicherheitsmaßnahmen mind. jährlich	☐
Bei negativen Feststellungen im Rahmen der zuvor gen. Überprüfung werden die Sicherheitsmaßnahmen risikobezogen angepasst	☐
Prozess zur Reaktion auf Sicherheitsverletzungen (Angriffe) und Systemstörungen existiert (Incident-Response-Management)	☐
Dokumentation von Sicherheitsvorfällen	☐
Einsatz Security Intelligence	☐
Sicherheitszertifizierungen (ISO 27001, BSI IT-Grundschutz etc.)	☐
Sonstige Maßnahmen:	☐

5.2 Sonstiges Datenschutzmanagement	Zutreffend
--	------------

	(falls ja, bitte ankreuzen)
Verwenden datenschutzfreundlicher Softwareeinstellungen	☐
Einsatz einer Datenschutzmanagement-Software	☐
Datenschutzbeauftragter benannt	☐
IT-Sicherheitsbeauftragter benannt	☐
Dokumentierter Prozess zum Umgang mit Datenschutzvorfällen	☐
Klare Verantwortlichkeiten bei der Handhabung von Datenschutz- und Sicherheitsvorfällen	☐
Dokumentierter Prozess zur Sicherstellung von Betroffenenrechten	☐
Zentrale, für alle Mitarbeiter zugängliche Ablage von Richtlinien/Verfahrensanweisungen	☐
Sonstige Maßnahmen:	☐

6. Anlagen

☐	Eigendokumentation der technischen und organisatorischen Maßnahmen (TOMs)
☐	Verzeichnis zu den Kategorien von im Auftrag durchgeführten Verarbeitungstätigkeiten (Art.30 Abs. 2 DSGVO) – soweit abweichend / ergänzend zum Anhang 1
☐	Richtlinie Datenschutz
☐	Richtlinie Umgang mit Datenpannen
☐	Übersicht der Sensibilisierungs- und Schulungsmaßnahmen der letzten 24 Monate
☐	
☐	
☐	
☐	
☐	

Bitte fügen Sie nichts bei, was bei unberechtigter Kenntnisnahme ein Sicherheitsrisiko für Ihre Organisation darstellen kann.

Ausgefüllt für die Organisation durch

Name:

Funktion:

Rufnummer:

E-Mail:

Ort, Datum

Unterschrift/Signatur