Anhang C

TECHNISCHE UND ORGANISATORISCHE MASSNAHMEN

1. Vertraulichkeit (Art. 32 Abs. 1 lit. b DSGVO)

1.1 Zugangskontrollen zu Räumlichkeiten und Einrichtungen (physische Zugangskontrolle)

Zugangskontrolle zu Räumlichkeiten und Einrichtungen Der unbefugte Zugang zu Räumlichkeiten und Einrichtungen muss verhindert werden, wobei der Begriff räumlich zu verstehen ist	**Vorhanden Ja**
Elektronische Zutrittscodekarte / Zutrittstransponder	X
Zutrittsberechtigungskonzept	X
Videoüberwachung	X
Schlüsselverwaltung	X
Besucherausweise	X
Begleitung des Besucherzugangs durch eigene Mitarbeiter	X
Anwesenheitsprotokollierung der Besucherzugänge	X
Gestaffelte Sicherheitsbereiche und kontrollierter Zugang	X
Separat gesicherter Zugang zum Rechenzentrum	X
Lagerung von Servern in abgeschlossenen Räumen	X
Anweisung zur Ausgabe von Schlüsseln	X

1.2 Zugangskontrolle zu Systemen (Hardware-Zugangskontrolle)

Zugangskontrolle zu Systemen Das Eindringen von Unbefugten in die Datenverarbeitungssysteme oder deren unbefugte Nutzung muss verhindert werden.	**Vorhanden Ja**
Passwortschutz der Bildschirme von Arbeitsplätzen	X
Funktionale und/oder zeitlich begrenzte Vergabe von Benutzerberechtigungen	X
Verwendung von individuellen Passwörtern	X
Automatisches Sperren von Benutzerkonten nach mehrfacher falscher Passworteingabe	X
Automatische passwortgeschützte Bildschirmsperrung nach Inaktivität (Bildschirmschoner)	X
Passwort-Richtlinie mit Mindestanforderungen an die Komplexität der Passwörter:	
▪ Mindestens 8 Zeichen / Groß- und Kleinschreibung, Sonderzeichen, Zahlen (davon mind. 3 Kriterien)	X
▪ Vermeidung von Trivialpasswörtern (z. B. Hund1, Hund2, Hund3)	X
▪ Passworthistorie (keine Wiederverwendung der letzten 5 Passwörter)	X
Verfahren für die Vergabe von Berechtigungen bei der Eingabe von Mitarbeitern	X
Verfahren zum Entzug von Berechtigungen bei Abteilungswechsel von Mitarbeitern	X
Verfahren zum Widerruf von Berechtigungen bei Austritt von Mitarbeitern	X
Verpflichtung zur Vertraulichkeit / Datengeheimnis	X

Protokollierung und regelmäßige Auswertung der Systemnutzung	X
Kontrollierte Vernichtung von Datenträgern	X

1.3 3 Zugriffskontrolle auf Daten (Software-Zugriffskontrolle)

Zugriffskontrolle auf Daten **Unbefugte Tätigkeiten in Datenverarbeitungssystemen außerhalb der zugewiesenen Berechtigungen müssen verhindert werden.**	**Vorhanden** **Ja**
Definition der Zugriffsberechtigung, Berechtigungskonzept	X
Einschränkung der freien und unkontrollierten Abfragemöglichkeiten von Datenbanken	X
Regelmäßige Auswertung von Protokollen (Logfiles)	X
Partieller Zugriff auf Datenbestände und Funktionen (Lesen, Schreiben, Ausführen)	X
Einsatz von geeigneten Sicherheitssystemen (Software/Hardware)?	
▪ Virenscanner	X
▪ Firewalls	X
▪ SPAM-Filter	X
Verschlüsselte Speicherung von Daten	
☐ z.B. AES, RSA:	X

1.4 Trennungskontrolle

Kontrolle der Trennung **Daten, die für unterschiedliche Zwecke erhoben werden, müssen auch getrennt verarbeitet werden.**	**Vorhanden** **Ja**
Trennung von Kundendaten (Mandantenfähigkeit von Systemen)	X
Berechtigungskonzept, das eine getrennte Verarbeitung von Daten verschiedener Kunden berücksichtigt	X
Trennung von Entwicklungs-, Test- und Produktionssystem	X

1.5 Pseudonymisierung

(Art. 32 Abs. 1 lit. a DSGVO; Art. 25 Abs. 1 DSGVO) **Die Verarbeitung personenbezogener Daten in einer Weise, dass die Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer bestimmten betroffenen Person zugeordnet werden können, sofern diese zusätzlichen Informationen gesondert aufbewahrt werden und geeigneten technischen und organisatorischen Maßnahmen unterliegen**	**Vorhanden** **Ja**
Maßnahmen:	X
PII-Tresor wird zur Aufbewahrung personenbezogener Daten verwendet	

2. Integrität (Art. 32 Abs. 1 lit. b DSGVO)

2.1 Kontrolle der Übermittlung

Kontrolle der Übermittlung **Aspekte der Übertragung (Übermittlung) personenbezogener Daten sind zu regeln: elektronische Übertragung, Datentransport sowie deren Kontrolle.**	**Vorhanden Ja**
Wie erfolgt die Übermittlung von Daten zwischen dem für die Verarbeitung Verantwortlichen und Dritten?	
▪ Datenaustausch über https-Verbindung	X
▪ Andere Art der Übertragung:	X
☐ Verschlüsselungsalgorithmus verwendet:	X
- Hashes werden mit einem "Salt" oder "Pepper" addiert	X
Gesicherter Eingang für Anlieferung und Auslieferung	X
Dokumentierte Verwaltung von Datenträgern, Bestandskontrolle	X
Definition der Bereiche, in denen Datenträger gelagert werden	X
Verschlüsselung von Datenträgern mit vertraulichen Daten	X
Verschlüsselung von Laptop-Festplatten	X
Verschlüsselung von mobilen Datenträgern	X
Kontrollierte Vernichtung von Daten:	X
Datenträgerentsorgung - Sicheres Löschen von Datenträgern:	
▪ Physikalische Vernichtung (z.B. Shredder mit Partikelschnitt - 1000 mm² max.)	X
▪ Sonstiges: z. B. Überschreiben von Bändern und Festplatten	X
Sicherungskopien von Datenträgern, die übertragen werden müssen	X
Dokumentation der Stellen, an die Übertragungen geplant sind, und der Übertragungswege	X
Verpackungs- und Versandanweisungen, verschlüsselter E-Mail-Versand	X
Kontrolle der Vollständigkeit und Korrektheit	X

2.2 Zugangskontrolle

Zugangskontrolle **Die Nachvollziehbarkeit und Dokumentation der Datenverwaltung und -pflege muss gewährleistet sein.**	**Vorhanden Ja**
Definition von Benutzerberechtigungen (Profile)	X
Differenzierte Benutzerberechtigungen:	X
Lesen, Ändern, Löschen	X
Teilweiser Zugriff auf Daten oder Funktionen	X
Protokollierung von Eingaben/Löschungen	X
Log-Analyse-System	X
Über den OS-Standard hinausgehendes Log-Konzept	X
Dedizierter Log-Server	X
Steuerung der Zugriffsberechtigungen auf Log-Server (Log-Admin)	X

3. Verfügbarkeit und Ausfallsicherheit (Art. 32 Abs. 1 lit. b DSGVO)

3.1 Verfügbarkeitskontrolle

Verfügbarkeitskontrolle **Die Daten müssen gegen zufällige Zerstörung oder Verlust geschützt werden.**	**Vorhanden** **Ja**
Datenschutz- und Sicherungskonzept	X
Durchführung eines Datenschutz- und Backup-Konzeptes.	X
Beschränkung des Zugangs zu Serverräumen auf autorisiertes Personal	X
Brandmeldeanlagen in Serverräumen	X
Rauchwarnmelder in Serverräumen	X
Klimatisierte Serverräume	X
Blitzschutz / Überspannungsschutz	X
Wassersensoren in Serverräumen	X
Backup-Systeme in separaten Räumen und Brandabschnitt unterbringen	X
Sicherstellung der technischen Lesbarkeit von Backup-Speichermedien für die Zukunft	X
Lagerung von Archivspeichermedien unter den erforderlichen Lagerbedingungen (Klimatisierung, Schutzanforderungen, etc.)	X
CO2-Feuerlöscher in unmittelbarer Nähe der Serverräume	X
Notfallplan (z.B. Wasser, Feuer, Explosion, Anschlagsdrohung, Absturz, Erdbeben)	X
Beobachtung des Einflusses von Nachbargebäuden	X
Schwachstellenanalyse (Geländeschutz, Gebäudeschutz, Eindringen in Computer, Computernetzwerke)	X
Speicherung von Daten in Datensicherungsschränken, Tresoren	X
USV-System (unterbrechungsfreie Stromversorgung)	X
Stromgenerator	X

3.2 Widerstands- und Zuverlässigkeitskontrolle

Widerstandsfähigkeit und Zuverlässigkeitskontrolle **Systeme müssen in der Lage sein, risikobedingte Veränderungen zu verkraften und müssen tolerant sein und Störungen kompensieren können.**	**Vorhanden** **Ja**
Alternative Rechenzentren verfügbar (Hot- oder Cold-Stand-by?): Kalt	X
Redundante Stromversorgung	X
Redundantes USV-System	X
Redundante Stromerzeuger	X
Redundante Klimatisierung	X
Redundante Brandbekämpfung	X
Festplattenspiegelung	X
Computer-Notfallteam (CERT)	X
Lastverteiler	X
Datenspeicherung auf RAID-Systemen (RAID 1 und höher)	X
Abgrenzung von kritischen Komponenten	X
Durchführung von Penetrationstests	X
Systemhärtung (Deaktivierung von nicht benötigten Komponenten)	X

Unverzügliche und regelmäßige Aktivierung von verfügbaren Software- und Firmware-Updates	
▪ Identifizierung der verschiedenen Geräte, aus denen sich das Netzwerk zusammensetzt, und Identifizierung ihrer Hardware-Version sowie ihrer aktuellen Software- und Firmware-Versionen.	X
▪ Kommunikationskanal mit den Herstellern, um über neue Updates und Patches für die eigenen Geräte auf dem Laufenden zu bleiben.	X
▪ Festlegung von Zeiträumen, in denen die Aktualisierungen durchgeführt werden sollen (z. B. Zeiten mit geringerem Betrieb, Wartungszeiten usw.)	X
▪ Einsatz von redundanten Systemen zur Aufrechterhaltung des Betriebs, während die Hauptgeräte aktualisiert werden.	X
▪ Schrittweiser Einsatz von Updates/Patches, um Probleme frühzeitig zu erkennen, ohne mehrere Geräte zu beeinträchtigen.	X
▪ Festlegung eines Testzeitraums, um die korrekte Implementierung des Updates zu überprüfen und sicherzustellen, dass der Betrieb mit den neuen Updates reibungslos weiterläuft.	X
Die Sicherheit wird in der Entwurfsphase der Systeme als Hauptüberlegung einbezogen.	
▪ Definition von Sicherheitsmaßnahmen zum Schutz und zur Validierung der Kommunikation zwischen Systemkomponenten.	X
▪ Begrenzung der Berechtigungen auf eine Need-to-know-Basis.	X
▪ Externe Auftragnehmer (Dienstleister) und Wartungspersonal müssen einen speziellen Zugang haben, der nur während des Eingriffs aktiv sein darf und in der übrigen Zeit deaktiviert bleibt.	X
Regelmäßige Sicherheitsschulungen und Sensibilisierungskampagnen innerhalb der Organisation	
▪ Sensibilisierungskampagnen, um die Nutzer über die Sicherheitskonzepte bestimmter Systeme und herkömmlicher IT-Systeme zu informieren	X
▪ Spezifische Sicherheitsschulungen, in denen vermittelt wird, wie Sicherheitsmaßnahmen und -verhaltensweisen mit möglichst geringen Auswirkungen auf die täglichen Prozesse anzuwenden sind.	X
Abschluss einer Cyber-Versicherung	
▪ Identifizierung der Geräte, Anlagen und Netzsysteme innerhalb der Infrastruktur der Organisation.	X
▪ Durchführung einer Risikoanalyse unter Berücksichtigung all dieser identifizierten Systeme, Geräte und Vermögenswerte, um die Bedrohungen, denen sie ausgesetzt sind, sowie deren Wahrscheinlichkeit und Auswirkungen zu ermitteln.	X

4. Verfahren für eine regelmäßige Prüfung, Bewertung und Evaluierung (Art. 32 Abs. 1 lit. d DSGVO; Art. 25 Abs. 1 DSGVO)

4.1 Kontrollverfahren

Kontrollverfahren	Vorhanden Ja

Es ist ein Verfahren zur regelmäßigen Prüfung, Bewertung und Evaluierung der Wirksamkeit der Datensicherheitsmaßnahmen zu implementieren.	
Die Aufzeichnungen über die Verarbeitungstätigkeiten werden überprüft und mindestens einmal jährlich aktualisiert (falls zutreffend)	X
Meldung von neuen/geänderten Datenverarbeitungsvorgängen an den Datenschutzbeauftragten.	X
Meldung neuer/geänderter Datenverarbeitungsvorgänge an den IT-Sicherheitsbeauftragten.	X
Prozesse zur Meldung neuer/geänderter Verfahren sind dokumentiert.	X
Sicherheitsmaßnahmen unterliegen regelmäßigen internen Audits.	X
Im Falle eines negativen Ergebnisses der o.g. Überprüfung werden die Sicherheitsmaßnahmen risikogerecht angepasst, erneuert und umgesetzt.	X

4.2 Kontrolle von Anweisungen

Kontrolle von Anweisungen **Es ist sicherzustellen, dass Auftragsdatenverarbeitungen durch Dienstleister (Subunternehmer) nur nach den Weisungen des Auftragsverarbeiters erfolgen.**	**Vorhanden** **Ja**
Verträge gemäß den Anforderungen des Art. 28 GDPR	X
Zentrale Erfassung von beauftragten Dienstleistern (Vertragsmanagement)	X