Technische und organisatorische Maßnahmen

1 Vertraulichkeit (Art. 32 Abs. 1 lit. b DS-GVO)

Zutrittskontrolle

Zutrittskontrolle **Ein unbefugter Zutritt ist zu verhindern, wobei der Begriff räumlich zu verstehen ist.**	**vorhanden** **ja**
Berechtigungsausweise	
Elektronische Zutrittscodekarten/ Zutrittstransponder	☐
Zutrittsberechtigungskonzept	☒
Videoüberwachung	☐
Alarmanlage	☐
Schlüsselregelung	☒
Besucherausweise	☐
Begleitung von Besucherzutritten durch eigene Mitarbeiter	☒
Anwesenheitsaufzeichnungen von Besucherzutritten	☐
Sicherung auch außerhalb der Arbeitszeit durch Werkschutz	☐
Abgestufte Sicherheitsbereiche und kontrollierter Zutritt	☐
Spezialverglasung	☐
Gesondert gesicherter Zutritt zum Rechenzentrum	☒
Aufbewahrung der Server in verschlossenen Räumen	☒
Aufbewahrung der Datenträger unter Verschluss bzw. in abgeschlossenen Räumen	☒
Aufbewahrung von Datensicherungen (z.B. Bänder, CDs) im zutrittsgeschützten Safe	☒
Anweisung zur Ausgabe von Schlüsseln	☒
Sonstiges: Klicken Sie hier, um Text einzugeben.	☐

Zugangskontrolle

Zugangskontrolle **Das Eindringen Unbefugter in die DV-Systeme bzw. deren unbefugte Nutzung ist zu verhindern.**	**vorhanden** **ja**
Verschlüsselung von Netzwerken	☒
▪ Verwendete Verschlüsselungsalgorithmen:	
Verschluss von Datenverarbeitungsanlagen (z.B. verschlossener Cage für Server)	☒
Passwortsicherung von Bildschirmarbeitsplätzen	☒

Funktionelle und/oder zeitlich limitierte Vergabe von Benutzerberechtigungen	☒
Verwendung von individuellen Passwörtern	☒
Automatische Sperrung von Nutzeraccounts nach mehrfacher Fehleingabe von Passwörtern	☒
Automatische passwortgesicherte Sperrung des Bildschirms nach Inaktivität (Bildschirmschoner)	☒
Passwortpolicy mit Mindestvorgaben zur Passwortkomplexität:	
▪ Mindestens 8 Ziffern / Groß- und Kleinschreibung, Sonderzeichen, Zahl (davon mind. 3 Kriterien)	☒
▪ Verhinderung von Trivialpasswörtern (z.B. Hund1, Hund2, Hund3)	☒
▪ Passworthistorie (kein erneute Verwendung der letzten 5 Passwörter)	☒
▪ Sonstiges:	☐
Hashing von gespeicherten Passwörtern	☐
▪ Hashes werden „gesalzen“ (Salt) oder „gepfeffert“(Pepper)	☒
Prozess zur Rechtevergabe bei Neueintritt von Mitarbeitern	☒
Prozess zum Rechteentzug bei Abteilungswechseln von Mitarbeitern	☒
Prozess zum Rechteentzug bei Austritt von Mitarbeitern	☒
Verpflichtung zur Vertraulichkeit	☒
Protokollierung und Auswertung der Systembenutzung	☒
Kontrollierte Vernichtung von Datenträgern	☒
Sonstiges: Klicken Sie hier, um Text einzugeben.	☐

Zugriffskontrolle

Zugriffskontrolle **Unerlaubte Tätigkeiten in DV-Systemen außerhalb eingeräumter Berechtigungen sind zu verhindern.**	**vorhanden** **ja**
Festlegung der Zugriffsberechtigung, Berechtigungskonzept	☒
Regelung zur Wiederherstellung von Daten aus Backups (wer, wann, auf wessen Anforderung)	☒
Regelmäßige Überprüfung von Berechtigungen	☒
Beschränkung der freien und unkontrollierten Abfragemöglichkeit von Datenbanken	☒
Regelmäßige Auswertung von Protokollen (Logfiles)	☒
Teilzugriffsmöglichkeiten auf Datenbestände und Funktionen (Read, Write, Execute)	☒
Protokollierung von Dateizugriffen	☒

Protokollierung von Dateilöschungen	☒
Werden entsprechende Sicherheitssysteme (Software/Hardware) eingesetzt?	
▪ Virenscanner	☒
▪ Firewalls	☐
▪ SPAM-Filter	☒
▪ Intrusionprevention (IPS)	☒
▪ Intrusiondetection (IDS)	☐
▪ Software für das Security Information and Event Management (SIEM)	☐
Verschlüsselte Speicherung der Daten	
▪ verwendete Verschlüsselungsalgorithmen:	☒
▫ z.B. AES, RSA:	☐
▪ Verwendete Hash-Funktion:	☒
▫ SHA2 (256, 384, 512 bit)	☐
▫ SHA3	☐
▫ Hashes werden „gesalzen“ (Salt) oder „gepfeffert“ (Pepper)	☒
Sonstiges: Klicken Sie hier, um Text einzugeben.	☐

Trennungskontrolle

Trennungskontrolle **Daten, die zu unterschiedlichen Zwecken erhoben wurden, sind auch getrennt zu verarbeiten.**	vorhanden ja
Trennung von Kunden (Mandantenfähigkeit des verwendeten Systems)	☒
Dateiseparierung bei Datenbanken	☒
Logische Datentrennung (z.B. auf Basis von Kunden- oder Mandantennummern)	☒
Verarbeitung der Daten des Auftraggebers und anderer Kunden von unterschiedlichen Mitarbeitern des Auftragnehmers	☒
Datensicherungen der Auftraggeber-Daten auf separaten Datenträgern (ohne Daten anderer Kunden)	☒
Berechtigungskonzept, das der getrennten Verarbeitung der Auftraggeber-Daten von Daten anderer Kunden Rechnung trägt	☒
Funktionstrennung	☒
Trennung von Entwicklungs-, Test- und Produktivsystem	☒
Sonstiges: dediziertes System	☒

Pseudonymisierung

(Art. 32 Abs. 1 lit. a DS-GVO; Art. 25 Abs. 1 DS-GVO) **Die Verarbeitung personenbezogener Daten in einer Weise, dass die Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden können, sofern diese zusätzlichen Informationen gesondert aufbewahrt werden und entsprechende technischen und organisatorischen Maßnahmen unterliegen;**	vorhanden ja
Maßnahmen:	☐

2 Integrität (Art. 32 Abs. 1 lit. b DS-GVO)

Weitergabekontrolle

Weitergabekontrolle **Aspekte der Weitergabe (Übermittlung) personenbezogener Daten sind zu regeln: Elektronische Übertragung, Datentransport, sowie deren Kontrolle.**	**vorhanden** **ja**
Welche Versendungsart der Daten besteht zwischen Auftraggeber und Dritten?	
▪ Citrix-Verbindung (128 Bit verschlüsselt)	☐
▪ VPN-Verbindung (IP-Sec)	☐
▪ E-Mail Versand mit verschlüsselten ZIP-Dateien	☐
▪ Datenaustausch über https-Verbindung	☒
▪ Sonstige Versendungsart:	☒
▫ verwendete Verschlüsselungsalgorithmen:	☐
▫ Verwendete Hash-Funktion:	☒
- Hashes werden „gesalzen“ (Salt) oder „gepfeffert“(Pepper)	☒
Gesicherter Eingang für An- und Ablieferung	☒
Dokumentierte Verwaltung von Datenträgern, Bestandskontrolle	☒
Festlegung der Bereiche, in dem sich Datenträger befinden müssen	☒
Verschlüsselung vertraulicher Datenträger	☐
Verschlüsselung von Laptopfestplatten	☐
Verschlüsselung mobiler Datenträger	☐
Kontrollierte Vernichtung von Daten:	☒
Datenträgerentsorgung - Sichere Löschung von Datenträgern:	
▪ Physikalische Zerstörung (z.B. Shredder bei Partikelgrößen bis max. 1000 Quadrat-Millimeter)	☒

▪ Sonstiges: Überschreibung bei Bändern und Festplatten	☐
Papierentsorgung: Sicheres Vernichten von Papierdokumenten:	
▪ Verschlossene Behältnisse aus Metall (sog. Datenschutztonnen), Entsorgung durch Dienstleister	☒
▪ Shredder gem. DIN 66399	☐
▫ Sicherheitsstufe:	☐
Regelung zur Anfertigung von Kopien	☐
Sicherungskopien von Datenträgern, die transportiert werden müssen	☐
Dokumentation der Stellen, an die eine Übermittlung vorgesehen ist, sowie der Übermittlungswege	☐
Verpackungs- und Versandvorschriften, verschlüsselter E-Mail-Versand	☐
Vollständigkeits- und Richtigkeitsprüfung	☐
Sonstiges: Klicken Sie hier, um Text einzugeben.	☐

Eingabekontrolle

Eingabekontrolle **Die Nachvollziehbarkeit bzw. Dokumentation der Datenverwaltung und -pflege ist zu gewährleisten**	**vorhanden** **ja**
Kennzeichnung erfasster Daten	☒
Festlegung von Benutzerberechtigungen (Profile)	☒
Differenzierte Benutzerberechtigungen:	☒
Lesen, Ändern, Löschen	☒
Teilzugriff auf Daten bzw. Funktionen	☒
Feldzugriff bei Datenbanken	☒
Organisatorische Festlegung von Eingabezuständigkeiten	☒
Protokollierung von Eingaben/Löschungen	☒
Protokollauswertungssystem	☒
Verpflichtung auf das Datengeheimnis	☒
Über OS-Standard hinausgehendes Log-Konzept	☒
Dezidierter Logserver	☒
Regelung der Zugriffsberechtigungen für Logserver (LogAdmin)	☒
Regelung zu Aufbewahrungsfristen für Revision/Nachweiszwecke	☒
Sonstiges: Klicken Sie hier, um Text einzugeben.	☐

3 Verfügbarkeit und Belastbarkeit (Art. 32 Abs. 1 lit. b DS-GVO)

Verfügbarkeitskontrolle

Verfügbarkeitskontrolle **Die Daten sind gegen zufällige Zerstörung oder Verlust zu schützen.**	**vorhanden** **ja**
Datensicherungs- und Backupkonzepte	☒
Durchführung der Datensicherungs- und Backupkonzepte	☒
Zutrittsbegrenzung in Serverräumlichkeiten auf notwendiges Personal	☒
Brandmeldeanlagen in Serverräumlichkeiten	☒
Rauchmelder in Serverräumlichkeiten	☒
Wasserlose Brandbekämpfungssysteme in Serverräumlichkeiten	☒
Klimatisierte Serverräumlichkeiten	☒
Blitz-/ Überspannungsschutz	☒
Wassersensoren in Serverräumlichkeiten	☒
Serverräumlichkeiten in separaten Brandabschnitt	☒
Unterbringung von Backupsystemen in separaten Räumlichkeiten und Brandabschnitt	☒
Gewährleistung der technischen Lesbarkeit von Backupspeichermedien für die Zukunft	☒
Lagerung von Archiv-Speichermedien unter notwendigen Lagerbedingungen (Klimatisierung, Schutzbedarf etc.)	☒
CO2 Feuerlöscher in unmittelbarer Nähe der Serverräumlichkeiten	☒
Vereinbarung bzgl. Übergabe der (Daten-) Sicherungen	☒
Katastrophen- oder Notfallplan (z.B. Wasser, Feuer, Explosion, Androhung von Anschlägen, Absturz, Erdbeben)	☒
Einbeziehung des Einflusses angrenzender baulicher Einrichtungen	☒
Schwachstellenanalyse (Geländeschutz, Gebäudeschutz, Eindringen in Rechner, Rechnernetze)	☒
Aufbewahrung der Daten in Datensicherungsschränken, Tresoren	☒
USV-Anlage (Unterbrechungsfreie Stromversorgung)	☒
Stromgenerator	☒
Sonstiges: Klicken Sie hier, um Text einzugeben.	☐

Widerstandsfähigkeit- und Ausfallsicherheitskontrolle

Widerstandsfähigkeit- und Ausfallsicherheitskontrolle **Systeme müssen die Fähigkeit besitzen mit risikobedingten Veränderungen umgehen zu können und eine Toleranz und Ausgleichsfähigkeit gegenüber Störungen aufweisen.**	**vorhanden** **ja**
Ausweich-Rechenzentren vorhanden (Hot- bzw. Cold-Stand-by?): Hot	☒
Redundante Stromversorgung	☒
Redundante USV-Anlage	☒

Redundante Stromgeneratoren	☒
Redundante Klimatisierung	☒
Redundante Brandbekämpfung	☒
sonstige redundante Systeme/Verfahren:	☒
Festplattenspiegelung	☒
Computer Emergency Response Team (CERT)	☒
Loadbalancer	☐
Datenspeicherung auf RAID-Systemen (RAID 1 und höher)	☐
Abgrenzung kritischer Komponenten	☐
Durchführung von Penetrationstests	☒
Systemhärtung (Deaktivierung nicht erforderlicher Komponenten)	☐
Unverzügliche und regelmäßige Aktivierung von verfügbaren Soft- und Firmwareupdates	
▪ Identifikation der verschiedenen Geräte, aus denen sich das Netzwerk zusammensetzt, und Bestimmung ihrer Hardware-Version sowie ihrer aktuellen Software- und Firmware-Versionen.	☒
▪ Kommunikationskanal mit den Herstellern, um sich über neue Updates und Patches zu informieren, die für die im Besitz befindlichen Geräte freigegeben wurden.	☒
▪ Definition von Zeiträumen, in denen die Updates implementiert werden sollen (z. B. Perioden niedrigerer Operationen, Wartungszeiten usw.).	☒
▪ Verwendung redundanter Systeme, um den Betrieb aufrecht zu erhalten, während die Hauptgeräte aktualisiert werden.	☒
▪ Progressive Bereitstellung von Updates / Patches, um Probleme frühzeitig zu erkennen, ohne mehrere Geräte zu beeinträchtigen.	☒
▪ Festlegung einer Testperiode, um die korrekte Implementierung des Updates zu überprüfen und sicherzustellen, dass die Operationen mit den neuen Updates weiterhin reibungslos ablaufen.	☒
Sicherheit wird während der Entwurfsphase der Systeme als Hauptbetrachtung mit umfasst.	
▪ Definition von Sicherheitsmaßnahmen zum Schutz und zur Validierung der Kommunikation zwischen Systemkomponenten	☒
▪ Begrenzung von Berechtigungen auf Bedarfsnotwendigkeit.	☒
▪ Externe Auftragnehmer und Wartungspersonal erhalten einen spezifischen Zugang, der nur während des Eingriffs aktiv und den Rest der Zeit deaktiviert ist.	☒
Periodische Sicherheitstrainings und Sensibilisierungskampagnen innerhalb der Organisation.	
▪ Sensibilisierungskampagnen, um die Benutzer über die Sicherheitskonzepte zu informieren, die sowohl für konkrete Systeme als auch für traditionelle IT-Systeme spezifisch sind.	☒
▪ Spezielles Sicherheitstraining, um zu lehren, wie man Sicherheitsmaßnahmen und Verhaltensweisen auf die täglichen Prozesse mit möglichst geringem Aufwand anwendet.	☒
Abschluss einer Cyber-Versicherung	

▪ Identifikation der IT-Geräte, Assets und Netzwerksysteme in der Infrastruktur der Organisation.	☒
▪ Durchführung einer Risikoanalyse unter Berücksichtigung all dieser Systeme, Geräte und Vermögenswerte, die identifiziert wurden, zur Ermittlung der Bedrohungen, inklusive ihrer Wahrscheinlichkeit und ihrer Auswirkungen.	☒
Sonstiges: Klicken Sie hier, um Text einzugeben.	☐

4 Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung (Art. 32 Abs. 1 lit. d DS-GVO; Art. 25 Abs. 1 DS-GVO)

Kontrollverfahren

Kontrollverfahren **Ein Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der Datensicherheitsmaßnahmen ist zu implementieren**	**vorhanden** **ja**
Interne Verfahrensverzeichnisse werden mind. 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	☒
Es werden datenschutzfreundliche Voreinstellungen gewählt	☒
Getroffene Sicherheitsmaßnahmen werden einer regelmäßigen internen Kontrolle unterzogen	☒
Bei negativem Verlauf der zuvor genannten Überprüfung werden die Sicherheitsmaßnahmen risikobezogen angepasst, erneuert und umgesetzt	☒
Es besteht ein Prozess zur Vorbereitung auf Sicherheitsverletzungen (Angriffen) und Systemstörungen sowie zur Identifizierung, Eingrenzung, Beseitigung und Erholung von selbigen (Incident-Response-Prozess).	☒
Sonstiges: Klicken Sie hier, um Text einzugeben.	☐

Auftragskontrolle

Auftragskontrolle **Es ist sicherzustellen, dass Daten die im Auftrag durch Dienstleister (Subauftragnehmer) verarbeitet werden, nur gemäß der Weisung des Auftragnehmers verarbeitet werden.**	**vorhanden** **ja**
Vertragsgestaltung gem. gesetzlichen Vorgaben (Art. 28 DSGVO)	☒
Zentrale Erfassung vorhandener Dienstleister (einheitliches Vertragsmanagement)	☒
Regelmäßige Kontrollen beim Auftragnehmer nach Vertragsbeginn (Während Vertragsdauer)	☒
Vor-Ort-Kontrollen beim Auftragnehmer	☒
Überprüfung des Datensicherheitskonzepts beim Auftragnehmer	☒

Sichtung vorhandener IT-Sicherheitszertifikate der Auftragnehmer	☒
Sonstiges: Klicken Sie hier, um Text einzugeben.	☐