Technische und organisatorische Maßnahmen (TOM) nach Art. 32 Abs. 3 lit. e DSGVO

Folgend sind die technischen und organisatorischen Maßnahmen (TOM) aufgelistet, die beim Auftragsverarbeiter (Lecos) standardmäßig für ein Verfahren mit dem Schutzbedarf „hoch“ (erhöhte Sicherheit – ES) BSI-IT-Grundschutz-Kompendium (Edition 2023) umgesetzt werden.

Weitere Maßnahmen für besondere Kategorien personenbezogener Daten (Art. 9 DSGVO) oder für einen anderen Schutzbedarf können erforderlich sein. Eine Regelung dazu muss im Leistungsvertrag enthalten sein.

Die folgend aufgelisteten Dokumente zu den TOM beim Auftragsverarbeiter (Lecos) sind vertraulich und können durch den Auftraggeber eingesehen werden.

☒ Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der TOM

Maßnahme	Beschreibung / Bemerkung
Richtlinien und Handlungsanleitungen zum Datenschutz und zur IT-Sicherheit	ständiger Prozess; im Organisationshandbuch (OHB) festgeschrieben; verbindliche Regelung für alle Mitarbeiter des Auftragsverarbeiters Leitlinie Informationssicherheitsmanagement V.: 10.0 Arbeitsanweisung Informationssicherheit V.: 9.0 Führung des Verzeichnisses der Verarbeitungstätigkeiten nach Art.30 Abs.1 DSGVO für eigene Zwecke und nach Art. 30 Abs. 2 DSGVO in der Funktion als Auftragsverarbeiter
schriftl. bestellter Datenschutzbeauftragter	Mitarbeiter des Auftragsverarbeiters Kommunikationsdaten in Regelungsvereinbarung nach Art. 28 DSGVO Anlage 1
bestellter Informationssicherheitsbeauftragter	Mitarbeiter des Auftragsverarbeiters Kommunikationsdaten in Regelungsvereinbarung nach Art. 28 DSGVO Anlage 1
Datenschutzmanagement	Maßnahmen vollständig umgesetzt Datenschutzrichtlinie Lecos V.: 2.0 Datenschutzordnung Lecos V.: 2.1 Verpflichtungserklärung MA (aktuell / Erstbelehrung) Verpflichtung auf das Datengeheimnis MA (aktuell / mit Arbeitsvertragsunterzeichnung) Geheimhaltungsvereinbarung Geschäftspartner vom 04.09.2019 (wird 2023 überarbeitet)
Verpflichtung aller Mitarbeiter zur Vertraulichkeit	mit Einstellung; Bestandteil der Personalunterlagen (siehe Verpflichtung auf das Datengeheimnis) (Online-)Schulung und Belehrung zum Datenschutz Verpflichtungserklärung bei Arbeitsbeginn
regelmäßige Sensibilisierungs-/Schulungsmaßnahmen zur Informationssicherheit und zum Datenschutz	Schulung und Belehrung zum Datenschutz für alle Mitarbeiter und Auftragsverarbeiter Auswertung aktueller Ereignisse und Rechtsprechung

Maßnahme	Beschreibung / Bemerkung
	Online-Schulungen mit individuellen Zertifikaten zur Informationssicherheit (zuletzt mit individuellen Prüfungszertifikat pro MA in 2022 durchgeführt)
regelmäßige Auditierung, Prüfungen (auch durch Externe) der Umsetzung der TOMs	Zertifizierung Grundschutz nach BSI für Informationssicherheit Eigenaudit für Datenschutz nach Kundenanforderung bei Umsetzbarkeit nach Art. 42 Abs. 1 DSGVO Fremdaudit / Zertifizierung interne Audits für bestimmte Verfahren und Technologien bei Bedarf
ISO 27001 Zertifizierung auf Basis von IT-Grundschutz	für den Informationsverbund (Zertifikatsnummer BSI-IGZ-0444-2021), gültig bis 24.02.2024 für den Service Scannen (Zertifikatsnummer BSI-K-TR-0350-2019), gültig bis 21.08.2022
Richtlinien und Handlungsanleitungen zum Datenschutz und zur IT-Sicherheit	Regelungen zur Auftragsdatenverarbeitung nach Art. 28 DSGVO Kontrolle der Wirksamkeit

☒ Zutrittskontrolle

Maßnahmen zur Regelung des Zutritts regelt der Auftragsverarbeiter, wenn die Verarbeitung in seinen Räumen stattfindet; der Auftraggeber ist für Zutrittsregelungen verantwortlich, wenn die Verarbeitung (oder Teile davon) in seinen Räumlichkeiten durchzuführen ist; im Unterauftragsverhältnis gilt dieser Grundsatz analog

Maßnahme	Beschreibung / Bemerkung
geregelter Zutritt	Zutrittskonzept V.: 6.0
Dokumentation der Vergabe und Rückgabe von Schließmitteln	Zutritt von Dienstleistern zu sensiblen Bereichen des AG grundsätzlich nur in Begleitung von Mitarbeitern Keine Ausgabe von Schlüsseln oder Zutrittsberechtigungen (Karten) für Schließanlagen Unterteilung in Zutrittsbereiche (3 Stufen) Dokumentiertes Verfahren zur Zutrittserteilung
Überwachung des Gebäudes durch Alarmanlage (außerhalb der Geschäftszeiten und dauerhaft für einzelne Bereiche)	Zutrittskonzept V.: 6.0 Bei Auftragsverarbeitung in Räumen des AG nach dessen Regelung Vertrauliche Angaben
Einsatz eines Zutrittskontrollsystems unter Verwendung von Zutrittskarte mit Protokollierung und Maßnahmen bei Verlust	Zutrittskonzept V.: 6.0 Zusätzlich durch Eingabe von personalisierten PIN außerhalb der Regelarbeitszeiten Verfahren zur Aufhebung von Zutrittsberechtigungen (u.a. bei Verlust)
Videoüberwachung von kritischen Bereichen	Handbuch Gebäudemanagement (OHB) – Mitarbeitern sind Kamerastandorte durch BV bekannt; Auftraggeber nur bei notwendigen Zutritt in die überwachten Bereiche auf Anfrage Gebäude- und Geländeüberwachung mit Kennzeichnung nach §4 Abs.1 BDSG (neu) im Eingangsbereich
Unterteilung in Sicherheitsbereiche	Zutrittskonzept V.: 6.0 Trennung zw. öffentlichen, unternehmensfremden und eigenen Bereichen Regelungen für Sicherheits- und Hochsicherheitsbereich (RZ)
Verwendung von Mitarbeiterausweisen mit Foto gegenüber Kunden	Mitarbeiterausweis mit Lichtbild und Name keine weiteren Hinweise auf Lokationen (Anschriften) Zutrittsberechtigungskarten mit Lichtbild und in CD-Farben des Auftragsverarbeiters zum Firmenstandort (kein Mitarbeiterausweis im herkömmlichen Sinne)
Einsatz eines Schließsystems für Gebäude und Geschäftsräume	für alle Gebäuden des Auftragsverarbeiters organisiert Datenschränke mit eigenem Schließsystem des Auftragsverarbeiters in Gebäuden des Auftraggebers möglich Schließsystem am Hauptstandort des Auftragsverarbeiters

Maßnahme	Beschreibung / Bemerkung
Zentrale Schlüsselverzeichnisse je Standort mit Maßnahmen bei Verlust des Schlüssels	Maßnahme in allen Gebäuden des Auftragsverarbeiters vollständig umgesetzt in Räumen des Auftraggebers wird Regelung in dessen Verantwortung angestrebt, wenn Zutritt vereinbart wird
Nutzung eines zentralen Empfangsbereichs mit Besetzung während der Geschäftszeiten, weitere Zu- und Ausgänge über alarmgesicherte Notausgänge	Maßnahme am Standort des Auftragsverarbeiter vollständig umgesetzt Zutritt zum internen Bereich mit Gästegarte nur unter Begleitung von MA des Auftragsverarbeiters Zutritt in Hochsicherheitsbereich nur bei Beauftragung oder Vorfällen entsprechend vertraglicher Regelungen im Beisein des Auftragsverarbeiters
Bewegungsmelder im RZ-Bereich, Serverraum und teilweise vor Fluchttüren	Alarmanlage zur Zutrittsüberwachung am Standort des Auftragsverarbeiters für alle relevanten Bereiche umgesetzt (vertrauliche Angaben – nähere Informationen nur nach Prüfung der Notwendigkeit an den AG) - vertraulich
Besucherkontrolle durch Begleitung von Mitarbeitern, Besucherausweise (sichtbar tragend) und Führen eines Besucherbuchs	Maßnahme für Zutritt zum Gebäude am Standort des Auftragsverarbeiter umgesetzt Regelung mit Empfangsbereich
Wartung der Geräte durch externe Techniker erfolgt in Begleitung autorisierten Personals und nur nach vorhergehender Anmeldung	Zutrittskonzept V.: 6.0 Maßnahme für Zutritt zur Technik m Gebäude am Standort des Auftragsverarbeiter umgesetzt Bei Auslieferung oder Wartung / Service von Geräten kann auch autorisiertes Personal eines Unterauftragnehmer (siehe Anlage 2) zum Einsatz kommen – in Abstimmung auch ohne Begleitung durch den Auftragsverarbeiter
überwachte Reinigung der Räume durch externe Dienstleister während der Arbeitszeit	Reinigungsplan Einweisung und Belehrung der MA des Dienstleisters In Technikräumen nur in Begleitung von MA des Auftragsverarbeiters

☒ Zugangskontrolle

Die folgenden Angaben betreffen den Zugang zu IT-Geräten und IT-Systemen durch Mitarbeiter des Auftragsverarbeiters (Lecos); der Zugang von Mitarbeitern des Auftraggebers wird/kann im Rahmen nach dessen Vorgaben durch den Auftragsverarbeiter (Lecos) eingerichtet, betrieben und überwacht werden.

Maßnahme	Beschreibung / Bemerkung
Berechtigungsmanagement Erstellung von Benutzerprofilen/-rollen auf Rollenebene mit Zuordnung von Benutzerrechten Prozess zur Vergabe und zum Entzug von Berechtigungen, bei Einstellung, Aufgabenänderung, Ausscheiden von Mitarbeitern	grundsätzlich im OHB geregelt Konzept Identitäts- und Berechtigungsmanagement V.: 2.0 wird entsprechend der Vorgaben des Auftraggebers auf Anwendungsebene umgesetzt – bei keiner Vorgabe ausschließlich in Verantwortung des Auftraggebers bei Auftragsverarbeitung mit Reglungsvereinbarung nach Art. 28 DSGVO als Bestandteil der zu vereinbarenden Leistungen auf allen zentralen Komponenten in Verantwortung und Eigentum des Auftragsverarbeiters nach OHB bzw. nach Weisung des Auftraggebers Sperrung und Löschung der Zugangsberechtigungen bei Notwendigkeit (bei anderer Aufgabenzuordnung oder Ausscheiden von Mitarbeitern) oder Weisung durch den Auftraggeber
Passwortrichtlinie mit Mindestanforderungen zu Länge, Komplexität, Gültigkeit, Vorgaben zum Umgang mit Passwörtern	Richtlinie Informationssicherheit für Mitarbeiter V.: 9.0 (Abschnitt 2.1 Nutzung von Passwörtern) Bei Aufgabenteilung mit AG eigenständige Abstimmungen notwendig
Änderung Standardkennwörter und Deaktivierung/Änderung Standardbenutzern	Richtlinie Informationssicherheit für Mitarbeiter V.: 9.0 (Abschnitt 2.1 Nutzung von Passwörtern)
personengebundene Ausgabe von Zugangsmitteln (Token)	Konzept IT-Betrieb V.: 9.0 Richtlinie Informationssicherheit für Mitarbeiter V.: 9.0 (Abschnitt 4.1.2 Allgemeine Reglungen – IT-Infrastruktur)
Identifikation per User-ID und Passwort auf Clients und Servern	Konzept IT-Betrieb V.: 9.0 (diverse Abschnitte)
VPN-Anbindung für externen Zugang (2-Faktor-Authentifizierung)	Konzept IT-Betrieb V.: 9.0 (Abschnitt 4.1.Virtualisierungskomponenten)
automatische Sperrmechanismen, u.a. passwortgeschützte Bildschirmsperre	Richtlinie Informationssicherheit für Mitarbeiter - (Abschnitt 3.7 Maßnahmen am Arbeitsplatz) Arbeitsanweisung Nutzung und Betrieb von Endgeräten V.: 3.0 (Abschnitt 2 Arbeiten mit den Endgeräten)
verfahrensabhängiges Session-Timeout nach einem festgelegten Zeitraum	Bildschirmpasswortschutz bei 10minütiger Inaktivität Session-Timeout (Option kann durch Auftragsverarbeiter für die einzelnen Anwendungen nach Vorgabe des Auftraggebers für das jeweilige Verfahren geprüft werden)

Maßnahme	Beschreibung / Bemerkung
Sperrung des Zugangs bei Nichteinhaltung der Passwortregeln	Richtlinie Informationssicherheit für Mitarbeiter V.: 9.0 (Abschnitt 2.1 Nutzung von Passwörtern)
Protokollierung und Auswertung fehlerhafter Anmeldeversuche	Konzeption IT-Management V.: 7.0 (Abschnitt 5 Protokollierung und Abschnitt 6 Monitoring) wenn das Verfahren in das ADS (Active Directory System) des Auftragsverarbeiters eingebunden wird – anderenfalls Administration nach Vorgaben des Auftraggebers Richtlinie Informationssicherheit für Mitarbeiter V.: 9.0 (Abschnitt 2.1 Nutzung von Passwörtern)
Zugang zu IT-Systemen von extern (Internet) über gesicherte Verbindungen	SSL bzw. TLS (end to end); https Freigabe nur über Firewallantrag / Information an den AG zu beauftragten Art und des Umfangs

☒ Auftragskontrolle

Maßnahme	Beschreibung / Bemerkung
Einsatz von Unterauftragnehmern nach den Vorgaben zur Auftragsverarbeitung gem. Betriebsleistungsvertrag, DSGVO, fachgesetzlicher Regelungen	in der Anlage 2 dieser Regelung für den jeweiligen Auftrag gelistet Anzeige des beabsichtigten Einsatzes eines Unterauftragnehmers während der Regelungslaufzeit
Dokumentation der Auftragsverhältnisse	Im Bereich Auftragsmanagement des Auftragsverarbeiters wird in das Verzeichnis der Verarbeitungstätigkeiten nach Art. 30 Abs. 2 beim Auftragsverarbeiter aufgenommen Regelung mit AG nach Art. 28 DSGVO wird vorgeschlagen
Regelmäßige Kontrollen von Unterauftragnehmern	auf Anforderung des Auftraggebers bei Datenschutzvorfällen aktive Einbindung zur Sachstandsklärung bei Vermutung von Unregelmäßigkeiten bzw. wirtschaftlichen Schwierigkeiten
Angepasste Verträge zur Datenverarbeitung im Auftrag	auf Anforderung des Auftraggeber
Angepasste Verträge zur Fernwartung	auf Anforderung des Auftraggebers besondere Regelungen bei Unterauftragnehmer Richtlinie Informationssicherheit für Mitarbeiter V.: 9.0 (Abschnitt 3.9 Regelungen zum Einsatz von Dienstleistern / Abschnitt 4.5.7 Fernwartung) Fernwartung erfolgt weisungsgebunden, ggf. nur im Beisein des Auftraggebers (UHD-Prozess) Vereinbarung im Leistungsvertrag

☒ Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste

Maßnahme	Beschreibung / Bemerkung
Konzepte (Berechtigungskonzept, Protokollierung, soziale Netzwerke, Fernwartung)	Arbeitsanweisung Informationssicherheit für Mitarbeiter V.: 9.0 (Abschnitt 3.9 Regelungen zum Einsatz von Dienstleistern / Abschnitt 4.5.7 Fernwartung / 4.2 soziale Netze) Konzept Schutz vor Schadprogrammen V.: 9.1 (Abschnitt 1.3 Geltungsbereich und Abgrenzungen) Rollenmatrix Lecos Datenschutzordnung V.: 2.1 Konzept IT-Management V.: 8.0
Aufgaben-/Funktionsbezogene Festlegung von Zugriffsrechten nach Erforderlichkeit	Konzept Berechtigungsmanagement V.: 2.0 (Abschnitt 5.2 Vergabe, Verwaltung und Entzug von Berechtigungen)
Dokumentierte Zuweisung von Zugriffsberechtigungen	Konzept Berechtigungsmanagement V.: 2.0 (Abschnitt 2.5 Allgemeiner Berechtigungsprozess für IAM)
Entzug von Zugriffsrechten bei Aufgabenänderung, Ausscheiden von Mitarbeitern	Konzept Berechtigungsmanagement V.: 2.0 (Abschnitt 5.2 Vergabe, Verwaltung und Entzug von Berechtigungen)
Protokollierung von Administrationstätigkeiten Protokollierung von Zugriffen, bei hohem und sehr hohem Schutzbedarf Protokollierung und Auswertung gem. Vorgaben des Auftraggeber Protokollierung und Auswertung zum Erkennen von systematischen Unregelmäßigkeiten	Konzept IT-Management V.: 8.0 (Abschnitt 6 Monitoring) Applikationen mit besonderen Schutzbedarf müssen durch den Verantwortlichen dem Auftragsverarbeiter in der Regelungsvereinbarung benannt werden bei konkreter Beauftragung möglich, im Falle eines Vorfalles, soweit standardmäßig eingerichtet (keine automatische Protokollierung und Auswertung ohne vorherige Bestimmung der Zweckbindung) für nicht personenbezogene Daten in Verantwortung des Administrators für Servicezwecke und vorbeugenden Erkennen von Sicherheitsvorfällen
System- und Datenbankadministrationskonzept mit abgestuften Administrationsrechten	Konzept Berechtigungsmanagement V.: 2.0 (Abschnitt 7.4 Prozesse zur Passwortverwaltung)
Vier-Augen-Prinzip für besondere Administratoren (Firewall, Core Switche)	bei Auftragsverarbeitung in Abstimmung möglich (z.B. durch geteiltes Passwort) Protokollierung der Administratortätigkeiten für Auftraggeber, soweit vereinbart und durch BV geregelt bei Datenschutzvorfällen grundsätzlich zur Ermittlung der Ursache, wenn Verantwortung beim Auftragsverarbeiter anzunehmen ist; eventuell Einsatz von Experten bzw. Forensiker (nachträglich) bei meldepflichtigen Datenschutzvorfällen auf Verlangen des Auftraggebers wenn im Leistungsvertrag so vereinbart

Maßnahme	Beschreibung / Bemerkung
Verfahrensspezifisches Berechtigungskonzepte	Konzept Berechtigungsmanagement V.: 2.0 (Abschnitt 6.1 Administrative Konten) Konzept IT-Betrieb V.: 8.0 (Kapitel 3 und 4 komplett (inkl. Telekommunikation))
Schriftliche Regelungen zum Einsatz von Datenträgern und Datenträgerkopien	vorhanden, je nach Art der Anwendung und des IT-Systems Richtlinie Nutzung und Betrieb von Endgeräten V.: 3.0 vom 04.12.2021 (Kapitel 4 Umgang mit mobilen Speichermedien / Kapitel 3 Umgang mit Daten und Programmen)
Aufbewahrung von Datenträgern im Robotersystem und in Sicherheitsbereichen	Konzept IT-Betrieb V.: 8.0 (Abschnitt 4.2 Speicherkomponenten und Netze)
Verschlossene Aufbewahrung von mobilen und sonstigen Datenträgern	Konzept Festlegungen zum Einsatz von Endgeräten V.: 5.0 (Abschnitt 3.5 Definition eines Standardarbeitsplatzes / Abschnitt 3.6 Daten sind zu verschlüsseln (bei lokaler Ablage))
Regelungen zur Datenträgerentsorgung und deren Protokollierung, einschließlich sichere Löschung oder Vernichtung nicht mehr benötigter Datenträger	Konzept Festlegungen zum Einsatz von Endgeräten V.: 5.0 (Abschnitt 10 Löschen und Vernichten) Beschreibung des Prozesses gemäß BSI-Grundschutzkompendium – CON. 6
Dokumentation der Datenträger und Bestandskontrolle (Robotersystem)	Konzept IT-Betrieb V.: 8.0 (Abschnitt 4.2.4 Administration)
Regelungen für den Versand von Datenträgern, Transport durch Bote/Kurier/fester Taxifahrer gesichert in einem Transportkoffer, Dokumentation durch Rückgabeschein und Begleitschein	Regelung Informationssicherheit für Mitarbeiter + Scancenter Arbeitsanweisung Informationssicherheit V.: 9.0 (Kapitel 3 Regelungen zum Arbeitsablauf und zur Informationssicherheit) Zertifikat: Digitalisierungsprozess beim Ersetzenden Scannen technisch und organisatorisch dem Standard „BSI TR-03138 Technische Richtlinie Ersetzendes Scannen (TR-RESISCAN)“ Auftragsverarbeiter erhalten (2021)
Mobile Datenträger (Nachweis, Vorgaben zum Umgang, Löschung etc.)	Konzept Festlegungen zum Einsatz von Endgeräten V.: 5.0 (Abschnitt 4.2. Mobile Endgeräte / Abschnitt 10 Löschen und Vernichten von Daten) Ausgabe über UHD; Freigabe durch SB EG

☒ Weitergabe-, Übertragungs- und Transportkontrolle

Maßnahme	Beschreibung / Bemerkung
Festlegung von Übermittlungskanälen und berechtigten Personen	Bestandteil der vorliegenden „Auftragsvereinbarung gemäß Art. 28 DSGVO“ – Pkt. 5“ Weitergabe grundsätzlich nicht an Dritte, es sei denn, der Auftraggeber erteilt eine Weisung Gesetzliche Regelungen können den Grundsatz widersprechen und müssen durch den Auftragsverarbeiter erfüllt werden der Auftraggeber wird informiert, wenn gesetzliche Bestimmungen den Auftragsverarbeiter daran nicht hindern und er dem Auftragsverarbeiter dazu auffordert
Dokumentation berechtigter Empfänger	
Protokollierung von Datenweitergaben	
Datenweitergabe an Dritte nur mit Zustimmung des Verantwortlichen	

☒ Pseudonymisierung und Verschlüsselung von pb Daten soweit möglich

Maßnahme	Beschreibung / Bemerkung
Verwendung anonymer oder pseudonymer Daten für Testumgebungen	Maßnahme grundsätzlich umgesetzt, wenn Auftraggeber den Test mit dieser Art von Daten anfordert; Auftraggeber informiert grundsätzlich den Auftragsverarbeiter, mit welchen Daten er den Test durchführen wird – Auftraggeber muss zustimmen, wenn keine anonymen oder pseudonymen Daten verwendet werden sollen; soll der Test mit den originalen Daten durchgeführt werden, müssen alle TOM, die auch den Betriebsdienst absichern, bereits in der Testphase implementiert sein; Datenschutzordnung V.: 2.1 (Kap. 5.2 Kundendaten) alle Ausnahmen müssen durch Auftragsverarbeiter dokumentiert und durch Auftraggeber bewertet und genehmigt werden
Definition von Maßnahmen zur Pseudonymisierung erfolgen abhängig von der Verarbeitungstätigkeit	wenn im Leistungsvertrag so vereinbart sichergestellt werden muss, dass nur der Auftraggeber den Schlüssel zur Wiederzuordnung der originären Daten kennt
zulässige Verschlüsselungsverfahren/-technologien	Maßnahme muss im Leistungsvertrag vereinbart werden Auftragsverarbeiter verschlüsselt Daten des Auftraggebers nicht eigenverantwortlich Kryptokonzept V.: 7.0 (Kapitel 4.1 Kryptografische Softwareprodukte) Kontrolle / interne Audits
Transportverschlüsselung	Kryptokonzept V.: 7.0 (Kapitel 4.1.1 Auswahl – z.B. SSH 2.0) Kontrolle / interne Audits im Regelfall, soweit möglich (z.B. VPN) oder mit Auftrag
Verschlüsselung gespeicherter Daten auf Servern	Kryptokonzept (Auftragsverarbeiter) V.: 7.0 (Kapitel 4.1 Kryptografische Softwareprodukte) Kontrolle / interne Audits nur wenn Auftraggeber entsprechende Weisung erteilt hat bzw. die Verschlüsslung dem Stand der Technik entspricht Daten, die der Auftraggeber explizit nicht beim Auftraggeber verschlüsseln möchte, werden von ihm auch nicht verschlüsselt (weisungsgebundene Auftragsverarbeitung)
Verschlüsselung der Daten auf mobilen Client-PCs und mobilen Datenträgern (USB-Sticks, CD-ROMs, externe Festplatten usw.)	Auflage aus Re-Zertifizierung - Umsetzung erfolgt organisatorische Kontrolle wenn im Leistungsvertrag vereinbart
verfahrensabhängige Inhaltsverschlüsselung auf Datenbankebene	wenn im Leistungsvertrag vereinbart oder dem Stand der Technik entspricht nicht in eigener Entscheidung durch den Auftragsverarbeiter

☒ Infrastrukturmaßnahmen und Wiederherstellung der Daten und Zugänge nach einem Zwischenfall

Maßnahme	Beschreibung / Bemerkung
Brandschutzeinrichtungen Einhaltung von Brandschutzvorschriften Brandschutzkonzept Rauch- oder Brandmelder Automatische Löschanlage Benennung eines Brandschutzbeauftragten	vorhanden bzw. umgesetzt Betrieb in Verantwortung des Auftragsverarbeiters an sonstigen Standorten teilweise in Verantwortung des Auftraggebers Löschanlage (Gas) im Rechenzentrum; regelmäßige Wartung Benennung Brandschutz-Beauftragter erfolgt, regelmäßige Schulungen aller Mitarbeiter
Wasserschutzeinrichtungen Keine wasserführenden Leitungen im Rechenzentrum Leckagesensoren zur Erkennung von Wassereinbrüchen	im Rechenzentrum am Standort des Auftragsverarbeiters befinden sich keine wasserführenden Leitungen. Der Serverraum ist mit Feuchtigkeitssensoren ausgestattet. Es werden regelmäßige Sichtprüfungen durchgeführt. Weiterhin liegen Reaktionspläne bei Wasserleckage vor, die bei Notfall genutzt werden können.
Stromversorgung Einsatz von USVs und Netzersatzanlage Monatliche Tests der Netzersatzanlage Überspannungsschutz Durchführung von Black Building Tests	am Standort des Auftragsverarbeiters für das Rechenzentrum Erdung aller Datenverteiler(-schränke) Benennung Brandschutzbeauftragten erfolgt, regelmäßige Schulungen aller Mitarbeiter
Klimaversorgung von Serverräumen	realisiert, inklusive Überwachung der Systeme online-Alarmierung des Bereitschaftsdienstes des Auftragsverarbeiters bei Regelabweichungen
Datensicherungsverfahren Datensicherungskonzept	Konzept IT-Betrieb V.: 8.0 (Abschnitt 4.1.7 Datensicherung) Konzept IT-Anwendungen V.: 5.0 (Kapitel 3 Datenbanken)
Notfallmanagement Notfallhandbuch (inkl. Wiederanlaufpläne für Anwendungen, Dienste, Netze, Server und Datenbanken) Jährliche Notfalltests im Bereich IT-Betrieb im Rahmen des Notfallmanagements	Konzept IT-Betrieb V.: 8.0 (Abschnitt 4.1.9 Notbetrieb) Konzept IT-Anwendungen V.: 5.0 (Abschnitt 6.4.2 Notfallvorsorge / Abschnitt 6.4.3 Sicherheitsvorfälle) Notfallplan IT-Serviceinfrastruktur vom V.: 3.0 (Abschnitt 2 Notbetrieb) Tests nach Regelungen Notfallplan (Pkt. 6) Leitfaden Sicherheitsvorfall V.: 1.0 (Checkliste – Vorgehen bei einem Sicherheitsvorfall)
System-Monitoring inkl. Eskalationsprozess	Notfallplan IT-Serviceinfrastruktur vom V.: 3.0 (Kapitel 3 Wiederherstellung / Abschnitt 1.4 Servicespezifische Sofortmaßnahmen (Kunden))
Incident-Response-Management	Prozessbeschreibung Change-Management V.: 4.0 (Abschnitt 1.6.3 Ablauf Emergency Change) Notfallplan IT-Serviceinfrastruktur vom V.: 3.0

Maßnahme	Beschreibung / Bemerkung
	(Abschnitt 1.3 Verantwortlichkeiten)
Redundanz von Hard- und Software sowie der Infrastruktur gemäß der verfahrensspezifischen technischen und organisatorischen Maßnahmen	je nach Anwendung ist im Leistungsvertrag als wesentlicher Punkt zu regeln
Automatisierte Schwachstellenscans für IT-Infrastruktur und Verfahren	2023 / wird umgesetzt als Einmalmaßnahme wird im Leistungsvertrag geregelt Durchführung im Auftrag Auswertung gemeinsam mit Auftraggeber, Abstimmung zu weiteren TOM
Penetrationstest für ausgewählte Verfahren	
Richtlinie Change- Management	Prozessbeschreibung Change-Management V.: 4.0 (Kapitel 1 Prozessgestaltung nach ITiL) ITIL-Rollenbeschreibung beim Auftraggeber nach Rollenmatrix
Mandantentrennung	mindestens logische Trennung Daten von Mandanten so getrennt, dass kein Lesen oder Schreiben untereinander möglich ist weitergehende Trennung kann im Leistungsvertrag vereinbart werden

☒ Mandantentrennung

Maßnahme	Beschreibung / Bemerkung
Infrastruktur (Hardware)	auf Vereinbarungsbasis im Leistungsvertrag zu regeln logische oder physische Trennung möglich mindestens logische Trennung durch Login/Passwort zu Datenbeständen der Mandanten
Verfahren	mindestens logische Trennung durch Login/Passwort zur Anwendung und der jeweiligen Datenbestände der einzelnen Mandanten Anwendungslizenzen mandantenbezogen im Leistungsvertrag können mandantenbezogene Servicelevel und Verfügbarkeiten vereinbart werden