Technisch-Organisatorische Maßnahmen

Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung

Im Folgenden sind die technischen und organisatorischen Maßnahmen zu dokumentieren, die vom Auftragsverarbeiter für die Gewährleistung der Sicherheit der Datenverarbeitung umgesetzt werden. Die einzelnen technischen und organisatorischen Maßnahmen sind zur Übersichtlichkeit ihren primären Schutzzielen, der Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung der personenbezogenen Daten, zugeordnet. Organisatorische und prozessuale Schutzmaßnahmen unterstützen die primären Schutzziele.

Nicht alle im Folgenden aufgelisteten Maßnahmen sind umzusetzen; es ist jeweils ein in der Gesamtheit angemessener Schutz gemäß dem Stand der Technik durch den Auftragsverarbeiter zu gewährleisten.

1.1 Vertraulichkeit der Systeme und Dienste

Definition: Vertraulichkeit ist der Schutz vor unbefugter Preisgabe von Informationen; vertrauliche Daten und Informationen dürfen ausschließlich Befugten in der zulässigen Weise zugänglich sein.

1.1.1 Physischer Schutz der Vertraulichkeit

Festlegung und Dokumentation zutrittsberechtigter Personen, einschließlich des Umfanges der Berechtigung	☒
Existenz von Zutrittsregeln-Regelungen für Firmenfremde	☒
Umsetzung einer Schlüsselregelung	☒
Pforten- und Empfangspersonal während der Betriebszeiten	☒
Wach- und Schließdienst für Liegenschaften außerhalb der Betriebszeiten	☒
Physische Schutzmaßnahmen sind vorhanden und werden regelmäßig überprüft:	☒
gesicherter Eingang durch Ausweisleser	☒
Überwachungseinrichtung (z.B. Alarmanlage, Videoüberwachung)	☒
Unterteilung in verschiedene Sicherheitszonen	☒
Arbeitsplatzrechner sind in verschlossenen Räumen	☒
Räume mit Servern sind alarmüberwacht	☒
Maßnahmen gegen einfaches Mithören und Einsichtnahme	☒
Aktenvernichtung ausschließlich innerhalb definierter Zonen (z.B. durch Schredder)	☒

Unverzügliche Abarbeitung der Alarmmeldungen nach Alarmplan	☒	
Dauerhafte Überwachung von Fluchttüren	☒	

1.1.2 Schutz des Systemzugangs

Angemessener Passwortschutz (verbindliche dokumentierte Vorgaben)		☒
(System-)Passwörter werden nicht im Klartext gespeichert	☒	
(System-)Passwörter werden nach dem Stand der Technik gehashed gespeichert	☒	
Konzeption und Implementierung eines Berechtigungskonzepts		☒
Berechtigungskonzept für Endgeräte (Rechner)	☒	
Berechtigungskonzept für IT-Applikationen/IT-Systeme	☒	
Weitere Interaktionen mit dem IT-System sind nur nach einer erfolgreichen Authentifizierung möglich		☒
Zwei-Faktorauthentifizierung	☒	
Implementierung eines zentralen Systems zur Verwaltung von Benutzeridentitäten (Identity and Access Management System)		☒
Monitoring der Zugangsversuche mit Reaktion auf Sicherheitsvorfälle		☒
Spezielle Sicherheitssoftware (z.B. Anti-Malware-SW, VPN, Firewall)		☒
Eine Segmentierung der genutzten Netze ist definiert		☒
Regeln und Verfahren zur Netzwerksegmentierung sind definiert und umgesetzt		☒
Externer Aktenvernichter (DIN 66399)		☒

1.1.3 Berechtigungsmanagement

Anmerkung: Das Berechtigungsmanagement stützt auch das Schutzziel der Integrität.

Die Verwendung von eindeutigen und personalisierten Benutzerkonten ist festgelegt	☒
Es erfolgt eine sichere Zustellung der Anmeldeinformationen für Benutzer	☒
Berechtigungs- und Rollenkonzept für IT-Applikationen/IT-Systeme sind dokumentiert und umgesetzt	☒
Zugriffsberechtigungen und -beschränkungen gemäß „Need-to-Know“ und „Least Privilege“	☒
Regelmäßige Überprüfung der Berechtigungen	☒

Revisionssichere Dokumentation von Benutzerberechtigungen	☒
Implementierung eines zentralen Systems zur Verwaltung von Benutzeridentitäten (Identity and Access Management System)	☒
Benutzerbezogene Zugänge zu Daten des Verantwortlichen dürfen nicht von mehreren Benutzern verwendet werden	☒
Veränderungen der Zuständigkeiten von Mitarbeitern oder dem Arbeitsverhältnis mit diesen werden dem Systemadministrator umgehend mitgeteilt oder die Benutzerzugänge werden entsprechend angepasst	☒
Protokollierung von Events Protokollierung von unberechtigten Zugriffsversuchen ☒ Anlassbezogene Auswertung ☒	☒
Ein Management-Prozess (Vergabe/Änderung/Löschung) für privilegierte Benutzerkennungen ist dokumentiert und etabliert	☒
Die Vergabe von privilegierten Rechten erfolgt erst nach ausdrücklicher dokumentierter Genehmigung	☒
Benutzerkonten mit privilegierten Rechten sind dokumentiert und werden regelmäßig überprüft	☒

1.1.4 Verschlüsselung

Alle produktiv eingesetzten Verschlüsselungstechnologien entsprechen dem Stand der Technik	☒
Für die relevanten IT-Systeme ist die Verwaltung des Schlüsselmaterials definiert und dokumentiert	☒
Transportverschlüsselung wird ausschließlich Ende-zu-Ende implementiert	☒
Übermittlung von personenbezogenen Daten erfolgt ausschließlich verschlüsselt, unter Verwendung von Verschlüsselungsverfahren nach dem Stand der Technik	☒

1.2 Integrität der Systeme und Dienste

Definition: Eine unerlaubte oder unbeabsichtigte Veränderung stellt eine Verletzung der Integrität von Informationen dar; dies kann neben dem eigentlichen Inhalt auch Attribute wie den Urheber oder Absender sowie den Zeitpunkt der Erstellung betreffen. Integrität kann sich sowohl auf die Unversehrtheit von Daten als auch auf die korrekte Funktionsweise von Systemen beziehen.

1.2.1 Schutz der Datenübertragung

Anmerkung: Der Schutz der Datenübertragung stützt auch das Schutzziel der Vertraulichkeit.

Vollständige Dokumentation der Wege der Weitergabe von personenbezogenen Daten im Zuge dieser Auftragsverarbeitung (z.B. Ausdruck, Datenträger, automatisierte Übermittlung, WAN-Strecke, TLS)	☒
Definition und Dokumentation der Empfänger von personenbezogenen Daten im Kontext der hier vereinbarten Auftragsverarbeitung	☒
Sicherungen des Transports (z.B. sicheres Fahrzeug, Behälter, Verschlüsselung von Speichermedien, Übergabeprotokolle, TLS-verschlüsselte Übermittlung)	☒
Dokumentationen aller Schnittstellen und der Abruf- und Übermittlungsprogramme	☒
Maßnahmen zur Verhinderung von unkontrollierten Informationsabflüssen:	☒
Technische Beschränkung auf zulässige Empfänger	☒
Data Loss Prevention Lösungen werden eingesetzt	☒

Eine Weitergabe an Dritte erfolgt seitens des Auftragnehmers nicht oder nur auf dokumentierte Anweisung des Auftraggebers. Die oben gemachten Angaben beziehen sich daher auf innerhalb der Organisation des Auftragnehmers allgemein getroffenen Maßnahmen.

Falls Sie andere oder zusätzliche Maßnahmen umgesetzt haben oder die oben angegebenen Maßnahmen spezifizieren möchten, nutzen Sie bitte das folgende Freitextfeld:

1.2.2 Eingabekontrolle

Protokollierung der Eingaben von und Änderungen an personenbezogenen Daten	☒
Organisatorisch festgelegt Zuständigkeiten für die Eingabe	☒

1.2.3 Weitere Maßnahmen zur Gewährleistung der Integrität der Systeme und Dienste

Das Minimalprinzip wird eingehalten (z. B. Einschränkung der Berechtigungen, Ports, Protokolle, Software)	☒
Es erfolgt eine automatische Überprüfung der von zentralen Gateways transportierten Daten (z.B. E-Mail, Internet, Netze von Dritten) mittels einer Schutzsoftware (inkl. verschlüsselter Verbindungen)	☒
Es ist sichergestellt, dass durch eine wirksame Trennung unbefugte Nutzer von Organisationen nicht auf personenbezogene Daten anderer Organisationen zugreifen können	☒
Gemeinsam genutzte virtuelle Maschinen und/oder Applikationsinstanzen sind entsprechend gehärtet	☒
Eine Separierung von Daten, Applikationen, Betriebssystem, Storage und Netzwerk ist umgesetzt	☒
Eigene virtuelle Leitungen zur Datenübertragung	☒

Es erfolgt eine automatische Überprüfung von empfangenen Dateien und Programmen vor deren Ausführung auf Schadsoftware (On-Access-Scan)	☒
Es erfolgt eine regelmäßige Untersuchung des gesamten Datenbestandes aller Systeme auf Schadsoftware	☒
Es existiert ein Intrusion Detection System	☒
Es existiert ein Intrusion Prevention System	☒

1.3 Verfügbarkeit der Systeme und Dienste

Definition: Verfügbarkeit von [Daten,] Dienstleistungen, Funktionen eines IT-Systems, IT-Anwendungen oder IT-Netzen oder auch von Informationen bedeutet, dass diese von den Anwendern stets wie vorgesehen genutzt werden können.

1.3.1 Sicherung der Verfügbarkeit personenbezogener Daten

Anmerkung: Die Sicherung der Verfügbarkeit personenbezogener Daten stützt auch das Schutzziel der Integrität.

Vorhandensein von redundanten IT-Systemen (Endgeräte, Server, Speicher etc.)	☒
Unterbrechungsfreie Stromversorgung (USV)	☒
Funktionsfähige physische Schutzeinrichtungen für Brandschutz, Energieversorgung, Klimatisierung)	☒
Serverräume und Rechenzentren verfügen über Feuer- und Rauchmeldeanlagen	☒
Serverräume und Rechenzentren verfügen über Feuerlöscher bzw. Feuerlöschanlagen	☒
Serverräume und Rechenzentren verfügen über Anlagen zur Überwachung von Temperatur und Feuchtigkeit	☒

1.3.2 Löschung

Definition: Das Ergebnis der Löschung ist die (faktische) Unmöglichkeit die zuvor in den Daten verkörperte Information wahrzunehmen.

Definition und Dokumentation von Verfahren zur Entsorgung und Vernichtung von Datenträgen	☒
Umsetzung von Regelungen zum Umgang mit elektr. Speichermedien	☒
Umsetzung von Regelungen zur Entsorgung von Speichermedien	☒
Umgesetzte Löschung auf Entwicklungs-, Test- und Produktivumgebungen	☒

Daten werden nur auf ausdrückliche und dokumentierte Weisung des Verantwortlichen gelöscht

Falls Sie andere oder zusätzliche Maßnahmen zum Löschen umgesetzt haben oder die oben angegebenen Maßnahmen spezifizieren möchten, nutzen Sie bitte das folgende Freitextfeld:

1.4 Belastbarkeit der Systeme und Dienste

Definition: Belastbarkeit der Systeme u. Dienste beschreibt die Absicherung der Werte (hier: personenbezogene Daten) gegen ungewollten, zufälligen oder unrechtmäßigen Verlust oder Einschränkung (Störungen) von einem oder mehreren der klassischen Schutzziele (Vertraulichkeit, Integrität, Verfügbarkeit) sowie, dass Systeme und Dienste nach einer Störung in angemessener Zeit wieder in den Normalbetrieb überführt werden können. Im Falle einer Störung sollen deren Auswirkungen auf die drei vorherig beschriebenen klassischen Schutzziele möglichst gering sein.

1.4.1 Absicherung gegen Störungen (Kontinuitätssicherung)

Loadbalancer	☒
Virenscanner mit aktuellen Suchmustern	☒
Redundant ausgelegte IT-Systeme	☒
Maßnahmen zur Steigerung der Aufrechterhaltung der Funktionalität von Systemen	☒
Moderne Firewall Systeme	☒
Intrusion Detection Systeme	☒
Intrusion Prevention Systeme	☒

1.4.2 Wiederanlauf und Wiederherstellung der Verfügbarkeit

Backup- und Wiederanlaufkonzept (regelmäßige Datensicherungen)	☒
Dokumentiertes und getestetes Notfallkonzept	☒
Dokumentiertes und etabliertes Desaster Recovery Management	☒

1.5 Auftragskontrolle

Dokumentation aller Subunternehmer, die für die Verarbeitung der in diesem Vertrag beschriebenen personenbezogenen Daten eingesetzt werden	☒
Es erfolgen regelmäßige Subunternehmer-Audits	☒
Die regelmäßige Kontrolle der relevanten Subunternehmer erfolgt durch:	☒

Vorlage von Self-Assessments oder Zertifikaten	☒	