Anlage 1
Technische und organisatorische Maßnahmen

Stand: Januar 2026

1. Maßnahmen zur Gewährleistung der Vertraulichkeit

1.1 Zutrittskontrolle

Soll verhindern, dass Unbefugte räumlich Zugang zu Datenverarbeitungsanlagen erhalten. Maßnahmen zur Gebäude- und Raumsicherung.

Sicherung durch Wachdienst
Kontrolle des Unternehmensgebäudes außerhalb der Bürozeiten von außen durch einen Wachdienst.

Zutrittsbegrenzung
Der Zutritt zu den Unternehmensräumlichkeiten ist auf notwendiges Personal beschränkt. Es gibt spezielle Schutzvorkehrungen für Server- und Materialschränke.

Verschlossene Serverräume
Serversysteme im Unternehmensgebäude befinden sich in separaten verschlossenen Räumlichkeiten.

Schlüsselverwaltung
Es wird eine Schlüsselausgabeliste zur Nachvollziehbarkeit der Zutrittsmöglichkeiten zu den Unternehmensräumlichkeiten geführt.

Begleitung von Besucherzutritten
Ein unberechtigter Zutritt wird durch die Begleitung von Besuchern in den Räumlichkeiten des Unternehmens verhindert.

Rechenzentren
Die eingesetzten Rechenzentren verfügen über eine Videoüberwachung, Wach-/Sicherheitsdienst/Werksschutz/Empfang, Alarmanlage, Besucherregelungen und Berechtigungskonzepte/Zugangsregelungen durch Nutzung von personifizierte Magnet-, Chipkarten oder Ausweise, elektronische Zugangssicherungen.

1.2 Zugangskontrolle

Soll den Zugang Unbefugter zu Datenverarbeitungssystemen und deren unbefugte Nutzung verhindern. Systemabsicherung.

Diebstahlsicherung
Testgeräte werden über eine Ausleihliste ausgegeben und befinden sich ansonsten in einem Safe. Grundsätzlich verlassen diese aber nicht das Unternehmensgebäude.

Konzeptionelle Sicherheit
Schon während der Konzeption wird die Sicherheit der Schnittstellenkommunikation, des Berechtigungskonzepts und der Bereitstellung von Zugängen für externe Kräfte einbezogen und danach konzipiert.

Beschränkung Anmeldeversuche
Zur Verhinderung von unberechtigten Zugriffen ist die Anzahl der Anmeldeversuche beschränkt.

Zwei-Faktor Authentifizierung
Zur Nutzung der Systeme wird eine Zwei-Faktor-Authentifizierung eingesetzt.

Authentifizierung
Eine Herausgabe von Daten oder ein Zurücksetzen von Passwörtern findet nur nach vorheriger Authentifizierung mittels festgelegter Faktoren statt.

Berechtigungskonzept
Einsatz eines Berechtigungskonzepts, das regelmäßig überprüft und angepasst wird. Dieses ist darauf ausgelegt, dass Mitarbeiter nur diejenigen Daten bearbeiten oder einsehen, die für ihren Tätigkeitsbereich erforderlich sind.

Benutzerkonten
Es ist in einer Richtlinie festgelegt, wie Benutzerkonten eingerichtet, geändert, gesperrt und gelöscht werden. Für privilegierte Konten gelten besondere Vergabe-, Nutzungs- und Protokollierungsvorgaben.

Rechtevergabe neuer Mitarbeiter
Neue Mitarbeiter erhalten nur diejenigen Berechtigungen, die für die konkrete Tätigkeit benötigt werden.

Rechteanpassung Abteilungswechsel
Bei Wechsel des Arbeitsplatzes werden die Berechtigungen dem neuen Tätigkeitsbereich angepasst.

Rechteentzug Offboarding
Beim Austritt eines Mitarbeiters aus dem Unternehmen werden sämtliche Zugriffsmöglichkeiten gesperrt.

Zugriffsbeschränkung Datenbank
Ein direkter Zugriff auf die Systemdatenbanken ist nur durch ausgewählte Personen möglich.

Betrieb Firewall
Zur Absicherung der Systeme werden redundante Firewalls betrieben, welche mittels kontinuierlicher Updates das System gegen Bedrohungen schützen.

Betrieb End-Point-Protection
Eingesetzte Geräte sind mit einer End-Point-Protection ausgestattet.

IT-Inventarliste
Verwendete Soft- und Firmware, sowie die eingesetzte Hardware sind in einer Inventarliste aufgeführt.

Systemmonitoring
Die eingesetzten IT-Systeme werden zur Erkennung von Unregelmäßigkeiten und Einleitung von Entstörungsmaßnahmen einem Monitoring unterzogen.

Dokumentenverschlüsselung
Es werden Verschlüsselungstechniken für Daten, Datentransfer und die Kundenkommunikation eingesetzt.

Servergespeicherte Profile
Nutzerprofile der Mitarbeiter werden auf einem lokalen Server gespeichert.

Passwortvorgaben
Einsatz von Passwortvorgaben mit Mindestvorgaben hinsichtlich der Komplexität der Passwörter, sowie der Wechselhäufigkeit.

Automatische Bildschirmsperre
Zur Verhinderung von unberechtigten Zugriffen sind die elektronischen Arbeitsplätze mit einer automatischen Bildschirmsperre bei Inaktivität nach einem definierten Zeitraum ausgestattet.

Softwarefreigaberichtlinie
Es wird auf den Systemen nur freigegebene Software aus spezifizierten Quellen installiert, die zuvor eine Prüfung nach festgelegten Vorgaben einer Prüfung zur Softwarefreigabe durchlaufen hat.

Mitarbeiterauswahl
Mitarbeiter werden anhand ihrer Qualifikation sorgfältig ausgewählt.

Mobiles Arbeiten
Die Mitarbeiter werden bei Einsatz im Rahmen eines mobilen Arbeitens zuvor insbesondere hinsichtlich datenschutzrechtlicher als auch IT-sicherheitsrelevanter Aspekte unterrichtet und geschult.

1.3 Zugriffskontrolle
Soll unerlaubte Tätigkeiten in Datenverarbeitungssystemen außerhalb eingeräumter Berechtigungen verhindern.

Clean Desk Policy
Im Unternehmen existiert eine Clean Desk Policy.

Regelung zur Anfertigung von Kopien
Es existiert eine Regelung bezüglich der Anfertigung von Kopien, Ausdrucken und Papierkopien, welche auf das erforderliche Maß beschränkt sind.

Löschkonzept
Im Unternehmen ist ein Löschkonzept für sämtliche Daten aufgestellt, welches die gesetzlichen Aufbewahrungspflichten und den Grundsatz der Datenminimierung der DSGVO beachtet.

Verwaltung Datenträger
Datenträger werden in einer Inventarliste erfasst.

Lokalisierung Datenträger
Datenträger dürfen sich nur in einem definierten Bereich befinden und diesen nicht verlassen.

Datenträgervernichtung
Datenträger werden ordnungsgemäß unter Aufsicht durch einen externen Dienstleister gemäß DIN66399 Sicherheitsstufe 2 oder höher vernichtet.

Schutz gespeicherter Nutzer-Passwörter
Die gespeicherten Nutzerpasswörter sind verschlüsselt oder gehasht hinterlegt.

Anwenderschulung
Anwender werden im Umgang mit der jeweiligen Software geschult.

Verpflichtung zur Vertraulichkeit
Mitarbeiter werden durch eine Verpflichtungserklärung zur Vertraulichkeit unterrichtet und verpflichtet. Die Verpflichtungserklärung ist fester Bestandteil des Onboardingprozesses.

Berechtigungskonzept
Es besteht ein Konzept, das die Aufteilung und Vergabe von Berechtigungen sowie Rechten und Rollen regelt.

Rechte- und Rollenkonzept
Das Berechtigungskonzept wird ergänzt durch das Rechte- und Rollenkonzept. Darin sind Zugriffsberechtigungen genau festgelegt. Die Berechtigungen werden dadurch auf die notwendigen Personen beschränkt und bedarfsgerechte Zugriffsrechte geschaffen.

Eingabeprotokollierung/Login
Die Eingabe von persönlichen Daten in das Datensystem (z.B. Eingabe zur Anmeldung) wird technisch protokolliert.

Zugriffe auf Kundendaten
Zugriffe des Anbieters auf Kundendaten erfolgen nur bei dokumentiertem Bedarf und werden protokolliert.

1.4 Trennungskontrolle

Daten, die zu unterschiedlichen Zwecken erhoben wurden, werden getrennt voneinander verarbeitet.

Mandantenfähigkeit
Das System verfügt über eine Mandantenfähigkeit, sodass die Kundendaten getrennt voneinander verarbeitet werden. Kundendaten werden mandantenbezogen logisch getrennt; die eingesetzten Mechanismen sind beschrieben.

Zonenarchitektur
Produktiv-, Test- und Entwicklungsumgebungen sind technisch und organisatorisch getrennt und diese Trennung ist dokumentiert.

Zweckbindung
Daten werden nur zu einem bestimmten Zweck gemäß den Vorschriften der DSGVO verarbeitet und gespeichert.

2. Maßnahmen zur Gewährleistung der Integrität

2.1 Weitergabekontrolle

Soll die Sicherheit der Daten bei elektronischer Übertragung und Datentransport und die Nachvollziehbarkeit der Weitergabe gewährleisten.

Verpackungs- und Versandvorschriften
Datenträger werden entsprechend der Kategorie der enthaltenen Daten besonders versendet.

Verschlüsselter Emailversand/Verschlüsselte Emailanhänge
E-Mails werden ab einer bestimmten Schutzstufe verschlüsselt versandt. E-Mailanhänge werden ab einer Einstufung in die Schutzklasse "vertraulich" verschlüsselt versandt, dies gilt insbesondere für die Anhänge beim DTA-Versand.

Transportverschlüsselter Datenaustausch
Ein Datenaustausch findet grundsätzlich verschlüsselt nach dem TLS-Standard statt.

Verbindungen
Für alle externen Verbindungen ist ein Kommunikations- und Verschlüsselungskonzept dokumentiert, das zulässige Protokolle und Gegenstellen definiert. Verbindungen werden protokolliert und auf unzulässige oder ungewöhnliche Zugriffe überprüft.

Überwachung und Protokollierung
Ein zentrales Protokollierungs- und Überwachungskonzept legt Ereignisarten, Protokollquellen und Aufbewahrungsfristen fest. Protokolle werden zentral gesammelt, vor unbefugter Änderung geschützt und nur berechtigten Personen zugänglich gemacht. Die für Protokollierung und Überwachung eingesetzten Systeme werden auf Verfügbarkeit und Aktualität überwacht. Anwendungen protokollieren sicherheitsrelevante Ereignisse (z.B. Anmeldeversuche, Rechteänderungen) in ausreichender Detailtiefe.

2.2 Eingabekontrolle

Soll gewährleisten, dass nachvollzogen werden kann, ob, wer, wann personenbezogene Daten in Datenverarbeitungssysteme eingeben, geändert oder gelöscht hat.

Versionsverwaltung
Dokumente werden auf Grundlage zuvor festgelegter Versionierungsvorgaben angelegt und verwaltet.

Protokollauswertung
Systemprotokolle werden regelmäßig ausgewertet, um Fehler und Sicherheitsprobleme zu identifizieren und zu beheben.

Rechte- und Rollenkonzept
Ein umfassendes Rechte- und Rollenkonzept regelt die Zugriffe und die Rechte zur Datenverarbeitung zur Beschränkung der Eingabe, der Veränderung und der Löschung von Daten.

3. Maßnahmen zur Gewährleistung der Verfügbarkeit und Belastbarkeit

3.1 Verfügbarkeitskontrolle

Soll Daten gegen zufällige Zerstörung oder Verlust schützen.

Brandmeldeanlage Serverraum
Die Serverräume sind mit einer Brandmeldeanlage ausgestattet.

Klimatisierte Serverräume
Die Serverräume sind zum Schutz vor Überhitzung klimatisiert.

Brandschutz
Produktiv- und Backupserver befinden sich in verschiedenen Brandzonen. Es werden redundante Backups an verschiedenen Standorten vorgehalten.

Überspannungsschutz
Es ist ein Überspannungsschutz vorhanden.

USV-Anlage
Die Server sind mit einer Unterbrechungsfreien Stromversorgung ausgestattet.

Stromgenerator
Eingesetzte Rechenzentren verfügen über redundante Notstromaggregate.

Wartungszeiträume
Wartungen am System werden in definierten Zeiträumen durchgeführt, die eine geringe Auslastung haben.

RAID Datenspeicherung
Die Systeme sind mit einer RAID-Datensicherung ausgestattet.

Backup
Zur Absicherung der Daten werden inkrementelle sowie volle Backups nach einem Backupkonzept erstellt.

Backupwiederherstellung
Regelung bezüglich der Wiederherstellung von Backups, die entsprechend die Befugnisse und die Zeitpunkte eines Zugriffs festlegt.

Vertretungsregeln
Aufgrund von Vertretungsregelungen werden Lücken in Prozessen oder Wissen bei Abwesenheit oder Austritt von Personal reduziert oder verhindert.

Speicher- und Verarbeitungsorte
Speicher- und Verarbeitungsorte der Kundendaten werden dokumentiert und auf Anfrage bereitgestellt.

Sicherungs- und Wiederherstellungskonzept
Es ist ein Sicherungs- und Wiederherstellungskonzept dokumentiert, dass Sicherungshäufigkeiten, Aufbewahrungsorte und Verantwortlichkeiten enthält. Sicherungsläufe werden automatisiert überwacht; fehlerhafte Läufe werden ausgewertet und behoben. Wiederherstellungstests werden in festgelegten Abständen durchgeführt und protokolliert. Sicherungsdaten werden nach definierten Fristen und – sofern erforderlich – geographisch getrennt aufbewahrt.

Kritische Infrastruktur
Kritische Infrastruktur (Energie, Klima, Brandmeldung) wird überwacht; Störungen werden zeitnah bearbeitet.

Kapazitätsüberwachung
Kapazitäten der Produktivumgebungen werden geplant, überwacht und bei Bedarf erweitert.

3.2 Belastbarkeit

Soll Systeme befähigen, mit risikobedingten Veränderungen umgehen zu können und Toleranz und Ausgleichsfähigkeit gegenüber Störungen aufzuweisen. Dadurch soll die Belastbarkeit der Systeme sichergestellt werden, so dass eine Sicherung der Daten ermöglicht wird.

Verfügbarkeit
Die Systeme werden redundant bereitgestellt.

Ausweichmaßnahmen
Ausfälle können durch gleichwertige Alternativen ausgeglichen oder abgemildert werden.

Standard-Hard- und -Software
Es wird, soweit möglich, auf Standard-Hard- und -Software zurückgegriffen, sodass Komponenten schnellstmöglich ersetzt werden können.

Soft- und Firmwareupdates
Soft- und Firmwareupdates werden regelmäßig aktualisiert.

Informationskanäle zu Herstellern
Es werden Informationskanäle zu den Herstellern genutzt, wie Emailregistrierungen und Informations-Abonnements.

Cyber-Versicherung
Das Unternehmen ist gegen IT bezogene Fälle versichert.

Redundante Speicherung
Datenbanktransaktionen werden redundant gespeichert.

Geo-Redundante Architektur
Zur Minimierung von Umwelteinflüssen ist die IT-Architektur geo-redundant, also örtlich verteilt, aufgebaut.

Ersatzstromversorgung
Die Server verfügen über eine Ersatzstromversorgung sowie USV-Anlagen.

Umgang mit technischen Schwachstellen, Störungen und Patches
Für den Umgang mit technischen Schwachstellen, Störungen und Patches besteht ein dokumentierter Prozess; Ergebnisse werden nachverfolgt.

Notfallmanagement

Notfall- und Wiederanlaufpläne werden erstellt, aktuell gehalten und auf Wirksamkeit geprüft.

4. Löschung und Verschlüsselung personenbezogener Daten

4.1 Löschung

Nach dem Prinzip der Datensparsamkeit sollen nur solche Daten gespeichert werden, die auch tatsächlich erforderlich sind. Nicht mehr benötigte Daten sollen gelöscht werden.

Löschkonzept

Im Unternehmen ist ein Löschkonzept für sämtliche Daten aufgestellt, welches die gesetzlichen Aufbewahrungspflichten und den Grundsatz der Datenminimierung der DSGVO beachtet. Es erfolgt somit eine regelmäßige Löschung nicht mehr benötigter Daten nach dem Prinzip der Datensparsamkeit. Löschvorgänge an personenbezogenen bzw. kundenspezifischen Daten werden protokolliert.

4.2 Verschlüsselung

Um die Sicherheit von personenbezogenen Daten umfassend zu gewährleisten sollen die Daten so verschlüsselt werden, dass diese ohne den entsprechenden Schlüssel keiner spezifischen Person zugeordnet werden können und kein Zugriff auf die Daten erfolgt.

Dokumentenverschlüsselung

Dokumente, die vom Kunden hochgeladen werden, werden zum Schutz verschlüsselt gespeichert.

Verschlüsselter Emailversand/Verschlüsselte Emailanhänge

E-Mails werden ab einer bestimmten Schutzstufe verschlüsselt versandt. E-Mailanhänge werden ab einer Einstufung in die Schutzklasse "vertraulich" verschlüsselt versandt, dies gilt insbesondere für die Anhänge beim DTA-Versand.

Transportverschlüsselter Datenaustausch

Ein Datenaustausch findet grundsätzlich verschlüsselt nach dem TLS-Standard statt. Daten werden bei Übertragung über öffentliche oder unsichere Netze verschlüsselt.

Richtlinie Kryptografie und Schlüsselverwaltung

Es ist eine Richtlinie zur Nutzung von Kryptografie und zur Schlüsselverwaltung vorhanden, die Rollen, Verfahren und Aufbewahrung regelt. Kryptografische Schlüssel werden sicher erzeugt, verteilt, rotiert, gesichert und bei Widerruf gesperrt.

5. Maßnahmen zur regelmäßigen Überprüfung, Bewertung und Evaluierung

5.1 Kontrollverfahren

Soll die Wirksamkeit der Datensicherheitsmaßnahmen gewährleisten.

Funktionstrennung
Zur Vermeidung von Interessenskonflikten sind operative und kontrollierende Aufgabe getrennt.

Automatisches Deployment
Der Deploymentprozess ist weitestgehend automatisiert und dadurch optimiert.

Vier-Augen-Prinzip
Zur Reduzierung von Benutzerfehlern, Missbrauch und Ähnlichem wird bei Systemänderungen zur Minimierung von Risiken im Vier-Augen-Prinzip gearbeitet.

Verarbeitungsverzeichnis
Ein Verarbeitungsverzeichnis nach den Vorgaben der DSGVO wird geführt und regelmäßig aktualisiert.

Regelmäßige Überprüfung
Prozesse, Daten, Verträge, Zugänge sowie Richtlinien und Verfahren werden regelmäßig auf Aktualität, Korrektheit und Einhaltung nach Vorgaben eines festgelegten PDCA-Zyklus überprüft. Durchführung interner Datenschutz-Audits.

Qualitätssicherung
Software, die erstellt oder eingesetzt wird, wird einem Freigabeprozess nach festgelegten Vorgaben unterzogen.

Lizenzmanagement
Produktlizenzen werden zentral verwaltet.

Sicherheitsüberprüfungen
Sicherheitsüberprüfungen (z.B. Penetrationstests, Messungen) werden risikoorientiert durchgeführt und die Ergebnisse werden in Maßnahmen überführt.

Sicherheitsvorfälle
Sicherheitsvorfälle werden nach einem festgelegten Verfahren erfasst, klassifiziert, behandelt und nachverfolgt.

Eigenes geistiges Eigentum
Soweit möglich und sinnvoll wird eigenes geistiges Eigentum verwendet oder erzeugt, um Lizenzvereinbarungen zu vermeiden.

Datenschutzfreundliche Voreinstellung
Es werden so wenig Daten wie möglich erhoben und nach Möglichkeit nicht geteilt (privacy by default).

Datenschutzmanagementsystem
Es wird ein zentrales Datenschutzmanagementsystem geführt.

5.2 Auftragskontrolle

Soll sicherstellen, dass Daten, die im Auftrag durch Dienstleister (Subauftragnehmer) verarbeitet werden, nur gemäß der Weisung des Auftraggebers verarbeitet werden. Zudem soll sichergestellt werden, dass auch bei den Auftragnehmern eine ordnungsgemäße Datenverarbeitung erfolgt.

Auftragskontrolle Sub-Unternehmer
Bei der Einbindung von externen Dienstleistern oder Dritten wird entsprechend den Vorgaben des jeweils anzuwendenden Datenschutzrechts ein Auftragsverarbeitungsvertrag abgeschlossen. Auftragnehmer werden auch während des Vertragsverhältnisses regelmäßig nach Vorgaben eines festgelegten PDCA-Zyklus kontrolliert.

Auswahl
Dienstleister werden ausgewählt, risikobewertet, vertraglich verpflichtet und regelmäßig überwacht; eine Ausstiegsstrategie ist, abhängig von der Risikoklassifizierung, definiert.

ISO/TÜV Zertifizierung
Es werden bevorzugt ISO/TÜV zertifizierte Dienstleister ausgewählt.

Service-Level-Agreements
Mit Dienstleistern sind Service-Level-Agreements vereinbart, welche den Betrieb und die Verfügbarkeit sicherstellen.

Vertragsstrafen
Soweit gesetzlich möglich werden Vertragsstrafen zur Verhinderung von Vertragsbrüchen vereinbart.

6. Sonstiges Datenschutzmanagement

Datenschutzbeauftragter
Das Unternehmen hat einen Datenschutzbeauftragten benannt und wird von diesem in datenschutzrechtlichen Angelegenheiten beraten.

Informationssicherheitsbeauftragte
Zur Beratung in Fragen der Informationssicherheit wird auf die Expertise eines Informationssicherheitsbeauftragen zurückgegriffen.

Sensibilisierung
Mitarbeiter werden regelmäßig in datenschutzrechtlichen und informationssicherheitstechnischen Themen geschult. Im Bereich des Datenschutzes wird ein Schwerpunkt auf den Schutz von Sozial- und Gesundheitsdaten gelegt.

PDCA-Zyklus
Regelmäßige Überprüfungen auf Grundlage eines festgelegten PDCA-Zyklus.

Vertraulichkeitsverpflichtung
Alle Mitarbeiter werden auf die Einhaltung des Datenschutzes, Sozialgeheimnis und zur Verschwiegenheit verpflichtet.

7. Allgemeine Maßnahmen

Informationssicherheits-Managementsystem (ISMS)
Es wird ein zentrales Informationssicherheits-Managementsystem (ISMS) betrieben.

Informationssicherheits-, IT-Nutzungs- und Datenschutzrichtlinien
Die Informationssicherheits-, IT-Nutzungs- und Datenschutzrichtlinien sind für alle Mitarbeiter im Zugriff und werden regelmäßig oder bei Bedarf aktualisiert. Sicherheits- und Datenschutzrichtlinien werden dokumentiert, regelmäßig geprüft, freigegeben und Ausnahmen werden nachvollziehbar genehmigt.

Anfragen von staatlichen Stellen
Anfragen von staatlichen Stellen oder sonstigen Dritten werden nach einem dokumentierten Verfahren geprüft, rechtlich bewertet, dokumentiert und – soweit zulässig – dem Kunden angezeigt.

Export- und Bereitstellungswege
Vereinbarte Export- bzw. Bereitstellungswege für Kundendaten sind beschrieben und werden auf Anforderung bereitgestellt.

IT-Sicherheit
Ein Risikomanagement ist etabliert und berichtet an die Geschäftsführung. Eine Notfallplanung und ein Wiederanlaufplan ist etabliert. Ein Incidentmanagement-System ist etabliert.

Audits
Regelmäßige interne Informationssicherheits- und Datenschutz Audits. Interne Audits, Managementbewertungen und die Ermittlung anwendbarer Anforderungen werden geplant, durchgeführt und dokumentiert.