HR factory GmbH

TECHNISCHE UND ORGANISATORISCHE MASSNAHMEN

Stand: 15.09.2025

Inhalt

Vorwort

Das Dokument beschreibt die verbindlichen technischen und organisatorischen Maßnahmen, die im Zusammenhang mit den von der Organisation durchgeführten Datenverarbeitungsvorgängen festgelegt wurden. Die beschriebenen Maßnahmen spiegeln somit das Datenschutz- und Datensicherheitskonzept in der Praxis der Organisation wider.

Datenschutz- und Datensicherheitskonzept

Der folgende Maßnahmenkatalog beschreibt die zu treffenden technischen und organisatorischen Einzelmaßnahmen gemäß den einschlägigen gesetzlichen Bestimmungen. Diese Bestimmungen verpflichten Unternehmen die Datenverarbeitung personenbezogener Daten durch angemessene, technische und organisatorische Maßnahmen abzusichern und personenbezogene Daten nach Möglichkeit zu pseudonymisieren. Die getroffenen Maßnahmen müssen dabei dem Risiko des jeweiligen Datenverarbeitungsvorgangs Rechnung tragen und dem derzeitigen Stand der Technik entsprechen. Diese Anforderungen erfüllt der HR factory GmbH durch ein wirksames Zusammenspiel aus Datenschutzmanagement und Informationssicherheitsmanagement und hat angemessene Maßnahmen zur Absicherung der Datenverarbeitungsvorgänge getroffen. Insbesondere die Schutzwerte: Verfügbarkeit, Vertraulichkeit, Integrität und Belastbarkeit. Den Schutzwerten werden dabei folgende informationssicherheitsrelevanten Definitionen zugrunde gelegt:

- Vertraulichkeit: Daten, Informationen und Programme sind vor unberechtigten Zugriffen und unbefugter Preisgabe zu schützen.
- Integrität: Der Begriff „Integrität“ bezieht sich auf die Korrektheit der verarbeiteten Informationen und Daten.
- Verfügbarkeit: Der Begriff der „Verfügbarkeit“ bezieht sich auf Informationen, Daten, Applikationen sowie Systeme und betrifft deren Funktionsfähigkeit bzw. Abrufbarkeit.
- Belastbarkeit: Die Belastbarkeit stellt als besonderen Aspekt der Verfügbarkeit die Anforderung, dass Systeme auch im Störfall, Fehlerfall oder bei hoher Belastung möglichst widerstandsfähig ausgestaltet sein müssen.

Physische Sicherheit der Infrastruktur

„Physische Sicherheit“ beschreibt Maßnahmen zur Verhinderung eines unbefugten Zutrittes, einer Beschädigung oder Beeinträchtigung von Informationswerten, personenbezogenen Daten und informationsverarbeitenden Einrichtungen eines Unternehmens.

Standort / Unternehmensräumlichkeiten

Die Unternehmensräumlichkeiten sind vom öffentlichen Bereich abgegrenzt durch:

- abschließbare Tür
- abgetrennte Räumlichkeiten in Gebäudekomplex

Es befinden sich keine weiteren Parteien im Gebäude, die Zutritt zu den Unternehmensräumlichkeiten haben.
Im Unternehmen wird ein Zutrittskontrollsystem eingesetzt, um den Zutritt zu Räumen, in denen personenbezogene Daten verarbeitet werden, zu schützen.
Das Unternehmensgelände bzw. Teile davon werden durch einen Pförtner oder Wachschutz bewacht.
Das Unternehmensgebäude wird mit einer Alarmanlage gesichert.
Im Unternehmen erfolgt die Besucheranmeldung durch:

- Besucherausweise
- Begleitung durch Mitarbeitende
- Klingel

Im Unternehmen sind Räume abschließbar, in denen Zugriff auf personenbezogene Daten möglich ist.
Im Unternehmen sind personenbezogene Daten in Bereichen mit Publikumsverkehr nicht frei zugänglich.
Im Unternehmen werden Arbeitsplätze zur Verarbeitung besonderer Kategorien personenbezogener Daten (z. B. Bewerber-/Gesundheitsdaten) räumlich von anderen Arbeitsplätzen getrennt.
Im Unternehmen existieren besondere Sicherheitsbereiche. Für den Zutritt zu den Sicherheitsbereichen existiert ein Berechtigungskonzept.
Im Unternehmen ist die Zutrittsberechtigungsstruktur für die Sicherheitsbereiche auf das Notwendigste beschränkt.
Im Unternehmen existiert eine unternehmensweite Richtlinie bzw. Handlungsanweisungen in schriftlicher Form zur Gebäudesicherheit.

Netzwerkstruktur

„Netzwerkstruktur“ beschreibt den Aufbau und Zusammenschluss von informationsverarbeitenden Einrichtungen im Unternehmen, sowie die Maßnahmen zum Schutz von Information in Netzwerken.

Netzwerkarchitektur

Das WLAN ist wie folgt verschlüsselt: WPA 2

Es gibt eine Trennung "Internet/öffentliches Netz".

Nicht interne Geräte können keinen Zugang zum internen Netzwerk/Sicherheitszonen erhalten.

Im Unternehmen wird ein dediziertes Netzwerk bzw. ein speziell abgetrennter Bereich für besondere Kategorien personenbezogener Daten eingesetzt.

Netzwerkfernzugriff

Im Unternehmen werden zum Schutz des Netzwerks Firewalls eingesetzt.

Folgende Arten von Firewalls werden eingesetzt:

- Software-Firewall(s)
- Hardware-Firewall(s)

Im Unternehmen werden moderne Netzwerkgeräte (Hubs, Switches) eingesetzt.

Im Unternehmen werden Mitarbeitende, die von außerhalb auf das Netzwerk zugreifen, auf die Einhaltung einschlägiger Datenschutzvorschriften an ihrem Arbeitsplatz hingewiesen.

Im Unternehmen werden Fernwartungen auf den IT-Systemen durch externer IT-Dienstleister durchgeführt. Ein Auftragsverarbeitungsvertrag mit dem externen IT-Dienstleister ist abgeschlossen.

Im Unternehmen wird jeder Fernwartungszugriff individuell freigegeben.

Durch Regelungen und Kontrollen wird sichergestellt, dass Fernwartungen nur durchgeführt werden, wenn angemessene Sicherheitsmaßnahmen durchgeführt werden. Diese Regelungen wurden schriftlich definiert.

Im Unternehmen werden individuelle Fernwartungszugriffe protokolliert.

Netzwerküberwachung

Im Unternehmen wird eine Software zur Überwachung des Netzwerks und der Anwendungen verwendet.

Business Continuity

„Business Continuity“ beschreibt die organisatorischen, technischen und personellen Maßnahmen, die zur Absicherung und Fortführung des Kerngeschäfts eines Unternehmens nach Eintritt eines Notfalls bzw. eines Sicherheitsvorfalls notwendig sind.

Wiederherstellbarkeit

Im Unternehmen werden (regelmäßig) Datensicherungen der relevanten Systeme durchgeführt.

Im Unternehmen ist die unternehmensinterne IT für die Durchführung von Sicherungen verantwortlich.

Die Wiederherstellungsmöglichkeiten umfassen folgende Bereiche:

- Benutzerkonten
- Daten
- Konfigurationen (Einstellungen und Freigaben)

Im Unternehmen wird folgende Art der Datensicherung durchgeführt:

- Inkrementelle Sicherung
- Komplett-/Vollsicherung

Im Unternehmen werden Sicherungen in einem separaten Brandabschnitt gelagert.

Im Unternehmen werden Datensicherungsverfahren regelmäßig getestet und bei Bedarf angepasst.

Im Unternehmen werden Datensicherungen verschlüsselt gespeichert.

Notfallvorsorge

Im Unternehmen wurde ein schriftlicher Notfallplan (Disaster Recovery Plan) definiert.

Im Unternehmen wurde der Notfallplan auch in ausgedruckter Form sicher abgelegt. Verantwortliche Personen wurden definiert und sensibilisiert.

Im Unternehmen existiert ein schriftliches Berechtigungskonzept für Notfallsituationen einschließlich Vertretungsregelungen.

Im Unternehmen wurde für den Notfall ein Administratorenzugang hinterlegt.

Im Unternehmen wird der Zugriff auf die hinterlegten Administratorenzugänge protokolliert.

Endgeräte

„Endgeräte“ umfassen die für die tägliche Arbeit genutzten Clients und Datenträger im Unternehmen. Bei der Handhabung dieser Endgeräte soll die unerlaubte Offenlegung, Veränderung, Entfernung oder Zerstörung von Information und personenbezogenen Daten verhindert werden.

Client-Struktur und Client-Management

Im Unternehmen wird zur Verwaltung mobiler Endgeräte ein Mobile-Device-Management-System verwendet.

Im Unternehmen wird ein zentrales Endpoint Management für Computer verwendet.

Im Unternehmen werden Sicherheits- und Softwareupdates der mobilen Endgeräte regelmäßig durchgeführt.

Im Unternehmen existiert ein Freigabeprozess für die Installation und Verwendung von Software.

Im Unternehmen dürfen nur vorab festgelegte Cloud- und Online-Dienste verwendet werden.

Im Unternehmen wird ein Bestandsverzeichnis der verwendeten Endgeräte geführt.
Im Unternehmen existiert ein dokumentierter Prozess zur Ausgabe von unternehmenseigenen Gegenständen an Mitarbeitende.
Im Unternehmen wird sichergestellt, dass sämtliche unternehmenseigene Gegenstände mit Bezug zu personenbezogenen Daten von einer ausscheidenden Person zurückgefordert werden.
Geräte werden über ein geregeltes Wiedereingliederungsmanagement wieder dem IT-Inventar zur Weiterverwendung zugeführt.

Datenträgermanagement

Im Unternehmen sind Richtlinien in schriftlicher Form zum Umgang mit mobilen Datenträgern definiert.
Im Unternehmen existiert eine Sicherheitsrichtlinie für mobile Endgeräte.
Im Unternehmen existiert eine Richtlinie für die Entsorgung von Datenträgern.
Im Unternehmen existiert ein Test- und Freigabeverfahren für Mobiltelefon-/Tabletcomputer-Applikationen.
Im Unternehmen ist ein Prozess definiert, wie sich Beschäftigte verhalten sollen, falls ein Datenträger abhandenkommt.
Im Unternehmen werden Datenträger vor der Benutzung auf Schadsoftware geprüft.
Im Unternehmen werden Dateien nur auf Wechseldatenträger übertragen, wenn diese Dateien zuvor auf Schadsoftware geprüft worden sind.
Im Unternehmen werden die in IT-Systemen verbauten Datenträger verschlüsselt.
Im Unternehmen besteht die Möglichkeit zur Fernlöschung von Daten auf mobilen Endgeräten. Im Unternehmen existieren komplexe Zugriffssperren für die eingesetzten mobilen Endgeräte.
Beschäftigte sind dazu angehalten personenbezogene Daten fachgerecht zu entsorgen.

- Daten elektronischer Datenträger werden sicher gelöscht, um eine sichere Wiederverwendung zu gewährleisten.

Im Unternehmen werden elektronische Datenträger sicher gelöscht.
Im Unternehmen werden Datenträger (auch Papierakten) regelmäßig entsorgt.
Im Unternehmen werden zur Entsorgung gesammelte schutzbedürftige Datenträger vor unberechtigtem Zugriff geschützt.
Der externe Dienstleister verfügt über folgende Zertifizierungen:

- Im Unternehmen wird zur Entsorgung von Datenträgern ein nach der DIN 66399 zertifizierter Dienstleister eingesetzt.

Ein Auftragsverarbeitungsvertrag mit diesem wurde geschlossen.

Datentransfers

Dieses Verfahren bezieht sich auf Datenübermittlungen innerhalb Ihrer Organisation und unter Einbeziehung Dritter.

Dies ist insbesondere im Zusammenhang mit der Übermittlung personenbezogener Daten relevant.

Datenübertragung & Kommunikation

Im Unternehmen werden zum Versand von E-Mails digitale Signaturen eingesetzt.

Folgende Verschlüsselungsverfahren werden beim E-Mail-Versand benutzt: Im Unternehmen werden E-Mails bei der Übertragung mit entsprechenden Verfahren/Protokollen (S/MIME) verschlüsselt.

Im Unternehmen werden langfristig archivierte E-Mails verschlüsselt gespeichert.

Im Unternehmen werden sichere Sofortnachrichtendienste verwendet bzw. diese sicher konfiguriert.

Einzelne Daten-Objekte, wie z.B. Container, Ordner oder einzelne Dateien (File & Folder Encryption), werden vor dem Datentransfer verschlüsselt.

Personal

„Personal“ umfasst die Sensibilisierung der Mitarbeitenden zu informationssicherheits- und datenschutzrelevanten Themen, sowie die Berechtigungen und Maßnahmen zur Authentifizierung der Mitarbeitenden beim Zugriff auf unternehmensintern IT-Systeme und Dienste.

Mitarbeitende Awareness & Sensibilisierung

Im Unternehmen werden Beschäftigte auf die Einhaltung von Verhaltensregeln gemäß den Grundsätzen der DSGVO verpflichtet.

Im Unternehmen werden die Beschäftigen zu datenschutzrechtlichen Themen geschult.

Im Unternehmen werden Schulungen der Beschäftigten zur Sensibilisierung zum Datenschutz regelmäßig durchgeführt.

Im Unternehmen werden die Beschäftigten regelmäßig über Neuigkeiten zum Datenschutz und IT-Sicherheit informiert.

Im Unternehmen erfolgt eine Sensibilisierung des Personals zum Umgang mit externen Personen/Unternehmen/Parteien.

Im Unternehmen sind Beschäftigten verpflichtet, personenbezogene Daten bei Verlassen des Arbeitsplatzes vor unbefugtem Zugriff zu schützen (sog. Clean-Desk-Policy).

Im Unternehmen sind relevante Informationen, Richtlinien und Handlungsempfehlungen für die Mitarbeitende leicht auffindbar.

IT-Personal und Administratoren werden im Unternehmen ausreichend sensibilisiert und geschult.

Berechtigungsmanagement

Im Unternehmen existiert ein geregelter Prozess zur zentralen Verwaltung von Benutzeridentitäten, insbesondere zur Anlage (z. B. neuer Mitarbeitende), Änderung (z. B. Namenswechsel nach Heirat) und Löschung (z. B. Ausscheiden

Mitarbeitende).
Im Unternehmen existiert ein formalisiertes Berechtigungskonzept, welches die Rollen und Rechte der Mitarbeitende dokumentiert.
Im Unternehmen wird die Vergabe sowie der Entzug von Zugangs- und Zugriffsberechtigungen für IT-Systeme dokumentiert.
Im Unternehmen wird ein zentraler Verzeichnisdienst (LDAP, AD, etc.) für die Berechtigungsattestierung eingesetzt.
Im Unternehmen wird die Dokumentation der zugelassenen Benutzer, Benutzergruppen und Rechteprofile in das Datensicherungsverfahren miteinbezogen.
Im Unternehmen werden regelmäßig die zugelassenen Benutzer, angelegte Benutzergruppen sowie die Rechteprofile geprüft.
Im Unternehmen ist die Dokumentation der zugelassenen Benutzer, Benutzergruppen und Rechteprofile vor unbefugtem Zugriff geschützt.
Im Unternehmen erfolgt die Vergabe von Zugangs- und Zugriffsberechtigungen anhand der Funktion der Zugangs- bzw. Zugriffsberechtigten.
Im Unternehmen existiert ein Funktionstrennungsprozess, um Berechtigungen zu vermeiden, die miteinander in Konflikt stehen.
Im Unternehmen wird sichergestellt, dass sämtliche Zugangsberechtigungen und Zugriffsberechtigungen einer ausscheidenden Person zeitnah gesperrt und ggf. gelöscht werden.
Im Unternehmen erfolgt eine vorübergehende Sperrung von Zugangs- bzw. Zugriffsberechtigungen bei längeren Abwesenheiten.
Im Unternehmen wurde für alle IT-Systeme und IT-Netze Administratoren sowie deren Stellvertreter bestimmt.
Im Unternehmen werden spezielle Administratorenkonten eingesetzt.

Authentifizierungsverfahren

Im Unternehmen wird ein Passwort-Manager eingesetzt.
Der eingesetzte Passwort-Manager bietet eine ausreichende Zugriffskontrolle und eine verschlüsselte Speicherung.
Im Unternehmen wird eine Multi-Faktor-Authentifizierung eingesetzt.
Im Unternehmen werden Benutzeraccounts nach Inaktivität automatische gesperrt (Bildschirmsperre).
Bildschirme werden nach weniger als 10 Minuten gesperrt.
Im Unternehmen werden die Benutzerkonten der IT-Systeme, auf denen personenbezogene Daten verarbeitet werden, durch Passwörter geschützt.
Im Unternehmen müssen Initialpasswörter bei der ersten Anmeldung geändert werden.
Im Unternehmen werden Benutzerkonten nach einer definierten Anzahl von Falschanmeldungen gesperrt.

Im Unternehmen erfolgt eine Vergabe von eindeutigen Kennungen für individuelle Nutzer von IT-Systemen, durch die personenbezogene Daten verarbeitet werden.
Im Unternehmen existieren konkrete Richtlinien für die Festlegung von Passwörtern oder systemseitige Forderung von Passwortanforderungen.
Im Unternehmen gibt es eine Vorgabe für die Passwortlänge.
Im Unternehmen dürfen Passwörter, welche in der Vergangenheit bereits verwendet wurden, nicht erneut verwendet werden.
Im Unternehmen werden Mitarbeitende und Admins direkt über kompromittierte, abgelaufene und schwache Passwörter informiert. Mitarbeitende sind zur sofortigen Änderung aufgefordert.

Organisation

„Organisation“ umfasst die unternehmensinternen Regelungen und Richtlinien zur Auswahl und dem Einsatz von externen Dienstleistern und Drittanbietertechnologien sowie zur Softwareentwicklung.

Auftragskontrolle

Mit allen Dienstleistern, die einen Teilbereich der Verarbeitung personenbezogener Daten auf die Weisung des Unternehmens übernehmen, wurde ein Auftragsverarbeitungsvertrag abgeschlossen.
Mit allen Dienstleistern, deren Datenverarbeitungsprozesse in Drittländern außerhalb der EU stattfinden, wurden zusätzliche geeignete Garantien geschlossen, um den Datentransfer zusätzlich abzusichern.
Externe Dienstleister, die Zugriff auf personenbezogene Daten haben könnten, werden regelmäßig auf Einhaltung der DSGVO auditiert.
Weisungen zur Verarbeitung personenbezogener Daten werden ausschließlich schriftlich an Auftragsverarbeitende erteilt.
Vor Auftragsvergabe erfolgt eine Prüfung von externen Dienstleistern.
Im Unternehmen wurden Kriterien (z. B. Referenzen, Zertifizierungen, o. Ä.) zur Auswahl von externen Dienstleistern schriftlich definiert. Die Prüfung vor Auftragsvergabe wird schriftlich dokumentiert.

Entwicklung und Auswahl von Software

Im Unternehmen wird Software regelmäßig aktualisiert und etwaige Schwachstellen geschlossen.
Im Unternehmen werden Standardsoftware und entsprechende Updates nur aus vertrauenswürdigen Quellen bezogen.

Sonstige organisatorische Maßnahmen

Im Unternehmen existiert ein IT-Sicherheitskonzept, welches die grundlegenden technischen und organisatorischen Maßnahmen darstellt, die im Unternehmen zur Gewährleistung von Datenschutz und Datensicherheit getroffen werden.

Im Unternehmen existiert ein Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen.

Im Unternehmen existiert ein Verfahren zur regelmäßigen Überprüfung und Aktualisierung der Konzepte und Dokumentationen zum Datenschutz.

Im Unternehmen besteht die Möglichkeit, auf Antrag personenbezogene Daten zu sperren und zu löschen.

Im Unternehmen wird jede Verarbeitung von personenbezogenen Daten protokolliert.

- Es gibt im Unternehmen eine unternehmensweite Richtlinie zur Protokollierung.
- Im Unternehmen wird jede Löschung von personenbezogenen Daten protokolliert.
- Im Unternehmen werden die Protokolle über die Verarbeitung personenbezogener Daten spätestens am Ende des auf deren Generierung folgenden Jahres gelöscht.

Im Unternehmen existieren Anweisungen und Eskalationsprozesse bei Sicherheitsverletzungen.

Im Unternehmen erfolgt eine konsequente Einbindung des Datenschutzbeauftragten bei Sicherheitsfragen und -vorfällen.

Im Unternehmen wird eine ausreichende fachliche Qualifikation des Datenschutzbeauftragten sichergestellt.