Technische und organisatorische Massnahmen Worldline Schweiz AG

(CHE DE)

1 Zweck dieses Dokuments

Dieses Dokument enthält eine Liste der technischen und betrieblichen Massnahmen, die standardmässig anzuwenden sind. Die konkreten Massnahmen hängen von der jeweiligen Dienstleistung und dem Ort der Verarbeitung ab, da nicht alle Massnahmen für alle Dienstleistungen und Standorte relevant sind. Worldline garantiert, dass sie für alle Dienstleistungen und Standorte über die notwendigen angemessenen technischen und betrieblichen Massnahmen verfügt, die in der untenstehenden Liste nach einer Folgenabschätzung zum Datenschutz aufgeführt sind. Die Massnahmen sollen:

- die Sicherheit und Vertraulichkeit der personenbezogenen Daten gewährleisten
- gegen jegliche zu erwartenden Bedrohungen oder Gefahren für die Sicherheit und Integrität der personenbezogenen Daten schützen
- vor tatsächlicher unbefugter Verarbeitung, Verlust, Verwendung, Offenlegung oder Erwerb von oder Zugriff auf personenbezogenen Daten schützen

Die Seite enthält auch eine Liste von Unterauftragnehmern, die Worldline zur Erbringung ihrer Dienstleistungen einsetzt. Worldline stellt sicher, dass alle ihre Unterauftragsverarbeiter durch die Verpflichtung zur Kontrolle der Unterauftragsverarbeitung angemessene Garantien für den Schutz personenbezogener Daten, die sie in unserem Auftrag verarbeiten, gegeben haben: Es sollte keine Auftragsdatenverarbeitung im Sinne von Art. 28 DSGVO ohne entsprechende Weisungen des Auftraggebers geben, z B. klare Vertragsgestaltung, formalisiertes Unterauftragsmanagement und eine strenge Auswahl der Auftragsverarbeiter (ISO-Zertifizierung, ISMS), vorheriger Kompetenznachweis, Nachkontrolle.

Worldline verpflichtet sich zu einer kontinuierlichen Überwachung der Wirksamkeit ihrer Informationsschutzmassnahmen und zu einem jährlichen Compliance-Audit durch einen Dritten, um eine Gewähr hinsichtlich der getroffenen Massnahmen und Kontrollen zu bieten.

2 Technische und organisatorische Massnahmen

A Menschen, Bewusstsein und HR:

- Alle Einstellungen von Mitarbeitern folgen einem Screening-Prozess nach den Grundsätzen der Worldline-Bestimmungen zur Hintergrundprüfung (Background Check Policy)
- In jedem Vertrag eines Mitarbeiters sind Bestimmungen zur Vereinbarung von Vertraulichkeit enthalten
- Die Schulung zur Sensibilisierung für den Ethikkodex (einschliesslich eines Tests) ist eine jährliche Verpflichtung für alle Mitarbeiter und soll über ein spezielles E-Learning-Modul durchgeführt werden
- Die Gruppenrichtlinie zur akzeptablen IT-Nutzung (bzw. die lokale Version) wird an alle Mitarbeitern weitergegeben
- Die von der Unternehmensleitung unterzeichnete Erklärung zu den Sicherheitsbestimmungen wird an alle Mitarbeiter weitergegeben
- Die Mitarbeiter von Worldline sind verpflichtet, jährlich an der Schulung zur Datenschutzrichtlinie und zur Informationssicherheit (inkl. Test) von Worldline teilzunehmen
- Regelmässige Sensibilisierungsschulungen zur DSGVO für alle Mitarbeiter (zusätzlich zur Schulung zur Datenschutzrichtlinie und zur Informationssicherheit)
- Der Zugang zu den Systemen wird auf einer «Need-to-have-Basis» unter Berücksichtigung der Aufgabentrennung gewährt
- Zur Überprüfung der Sicherheitspraktiken werden regelmässig interne Sicherheitsaudits durchgeführt

B Physische Sicherheit und Papieraufzeichnungen:

Einhaltung der Worldline-Gruppenrichtlinie zur physischen und ökologischen Sicherheit:

- Zugangskontroll- und Besuchermanagementsysteme für alle Besucher/Gäste implementiert
- Physische Zugangskontrolle (Schutz vor unbefugtem Zugriff auf Datenverarbeitung oder Lagereinrichtungen): insbesondere durch Magnet- oder Chipkarten, elektrische Türöffner, einen Pförtner, Sicherheitspersonal, Alarmanlagen, Videoanlagen
- Physikalische Zugriffsüberprüfungen in festgelegten zeitlichen Abständen
- Clean-Desk-, Clean-Screen- und Follow-me-Printing-Prozess implementiert
- Informationen, zu denen auch Papierdokumente gehören, die vom Datenimporteur bearbeitet werden, werden gemäss der Worldline-Richtlinie zur Informationsklassifizierung klassifiziert, gekennzeichnet, geschützt und bearbeitet
- Desktops dürfen nur mit vorheriger besonderer Genehmigung vom Standort entfernt werden
- CCTV-Überwachung zum Schutz von Sperrbereichen
- Feueralarm- und Feuerlöschsysteme für die Sicherheit der Mitarbeiter implementiert
- Evakuierungsübungen im Brandfall werden in angegebenen Intervallen durchgeführt

C Remote-Endgeräte sind geschützt:

Die Remote-Benutzer arbeiten mit Laptop und Desktop im gesicherten Worldline-Netzwerk, das von Global IT für die Worldline-Gruppe betreut wird. Folgende Sicherheitsmassnahmen sind zusätzlich eingebaut:

- Verschlüsselung der Festplatte auf firmeneigenen Laptops
- 2-Faktoren-Authentifizierung (PKI/Alternative)
- Zentrale Verwaltung und Virenschutz
- Verwaltung und Überwachung der Software zur Kontrolle einer autorisierten Softwareinstallation
- Für den Zugriff auf Informationen sind Login-ID- und Passwort-Kontrollen implementiert
- Eine regelmässige Zugriffsüberprüfung ist implementiert
- E-Mails werden automatisch von einer Antiviren- und Antispam-Software gescannt

D Sicherheit beim Remote-Zugriff

Für den Remote-Zugriff auf die kritischen Worldline-Zielsysteme wird generell eine 2-Faktor-Authentifizierung verwendet. Wenn die Quelle der Remote-Verbindung ein von Worldline kontrolliertes System ist, wird eine Geräteauthentifizierung auf Basis eines Zertifikats auf dem Gerät implementiert. Jede andere Einrichtung von Verbindungen muss im Vorfeld von der Sicherheitsabteilung genehmigt werden.

E Zu den allgemeinen Sicherheitsmassnahmen gehört Folgendes:

- Die Daten werden in den EU- und CH-Rechenzentren oder im Falle von Laptops verschlüsselt auf dem lokalen Gerät gespeichert
- Beendigung der Zugangsverbindung in der entmilitarisierten Zone
- Alle Verbindungen bis zum gesicherten Bereich (PCI-Zone) sind verschlüsselt
- Zugriff auf PCI-Zone nur über starke Authentifizierung über mitgelieferten Security-Client möglich
- Mehrere Schichten von Firewalls & Angriffserkennung müssen passiert werden
- Der Zugriff wird nach den Grundsätzen der rollenbasierten Zugriffskontrolle verwaltet
- Datenschutzmanagement, einschliesslich regelmässiger Mitarbeiterschulungen
- Vorfallsreaktionsmanagement
- Datenschutzfreundliche Standardeinstellungen

F Zugriffskontrolle auf personenbezogene Daten

Mitarbeiter mit Zugang zu personenbezogenen Daten können nur auf die Daten zugreifen, die für den Zweck der Tätigkeiten in ihrer Zuständigkeit notwendig sind. Die Zugriffsberechtigung wird auf der «Need-to-know» und «Need-to-access»-Basis erteilt und ist entweder rollen- oder namensbasiert. Zugangsprotokolle sind vorhanden und die Verantwortung für die Zugangskontrolle ist zugewiesen.

Folgende Massnahmen sind vorhanden:

- Verpflichtung der Mitarbeiter zur Einhaltung der geltenden Worldline- und der lokalen Sicherheits- und Datenschutzrichtlinien
- Arbeitsanweisung zum Umgang mit privaten Daten
- Elektronische Zugriffskontrolle (Schutz vor unbefugter Nutzung von Datenverarbeitungs- oder Speichersystemen): insbesondere durch Passwörter (einschliesslich der entsprechenden Richtlinie), automatische Sperrmechanismen, Zwei-Faktor-Authentifizierung, Verschlüsselung von Datenträgern

110.0789.01 CHE_DE/12.2021

- Interne Zugriffskontrolle (Verhinderung des unbefugten Lesens, Kopierens, Änderns oder Entfernens von Daten innerhalb von Worldline), und zwar durch die Verwendung von Standard-Autorisierungsprofilen auf «Need-to-know»-Basis, einen Standardprozess für die Vergabe von Benutzerrechten, Zugriffsprotokollierung, regelmässige Überprüfung der vergebenen Rechte, insbesondere von Administrator-Accounts
- Kontrollierte Zerstörung von Datenträgern
- Verfahren zur Überprüfung der Einhaltung von Verfahren und Arbeitsanweisungen sind vorhanden

G Sicherheit und Vertraulichkeit personenbezogener Daten

Auf der Grundlage einer Risikobewertung (und ggf. einer zusätzlichen DPIA) stellt Worldline ein dem Risiko angemessenes Sicherheitsniveau sicher, das u. a. Folgendes umfasst:

- Klassifizierungsschema für Daten: Kategorisierung personenbezogener Daten nach dem Grad der Vertraulichkeit auf Basis gesetzlicher Verpflichtungen oder Selbsteinschätzung
- Kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen während der elektronischen Übertragung oder des Transports: insbesondere durch Verschlüsselung und Virtual Private Networks (VPN)
- die Fähigkeit, die kontinuierliche Vertraulichkeit, Integrität, Verfügbarkeit und Ausfallsicherheit von Verarbeitungssystemen und -diensten zu gewährleisten
- Schutz vor versehentlicher oder absichtlicher Zerstörung oder Verlust, wie z. B. Backup-Strategie (online/offline; on-site/off-site), unterbrechungsfreie Stromversorgung (UPS, Dieselaggregat), Antivirus, Firewall, Alarmkanäle und Notfallpläne; Sicherheitskontrollen auf Infrastruktur- und Anwendungsebene, mehrstufiger Sicherheitsplan mit Auslagerung von Backups in Datensicherungszentren, Standardprozesse bei Wechsel/Entlassung von Mitarbeitern
- die Fähigkeit, die Verfügbarkeit und den Zugang zu personenbezogenen Daten im Falle eines physischen oder technischen Vorfalls zeitnah wiederherzustellen
- ein Verfahren zur regelmässigen Prüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Massnahmen zur Gewährleistung der Sicherheit der Verarbeitung (Interne Revision, PCI-DSS, ISO27001,nationale Überwachungsinstitutionen)
- Prozessregister gemäss DSGVO-Anforderungen
- Verwendung von Access-Log-Systemen mit Relevanz, um unberechtigte Zugriffsversuche erkennen zu können
- Für den Hauptkunden werden Daten und Metadaten (einschliesslich Backups, Archive, Logfiles usw.) nur so lange gespeichert, wie es den Zwecken dient, für die die Daten erhoben wurden, es sei denn, es besteht eine gesetzliche oder vertragliche Verpflichtung, die Daten länger zu speichern

H Organisationskontrolle

Der Auftragsverarbeiter ist verpflichtet, seine interne Organisation so zu gestalten, dass sie den Anforderungen der geltenden Gesetzgebung und den Anforderungen des Verantwortlichen an die Datensicherheit entspricht. Dies soll erreicht werden durch:

Interne Datenverarbeitungsrichtlinien und -verfahren, Richtlinien, Arbeitsanweisungen, Prozessbeschreibungen und Vorschriften für die Programmierung, Prüfung und Freigabe, soweit sie sich auf die vom Verantwortlichen übermittelten personenbezogenen Daten beziehen;

Implementierung eines Kontrollrahmens für den Datenschutz, der jährlich auf seine Einhaltung geprüft wird;

Vorhandensein eines Notfallplans mit Verfahren und Zuweisung von Verantwortlichkeiten (Backup-Notfallplan).