

Technische und organisatorische Maßnahmen

Anlage I: Art und Umfang der Datenverarbeitung

Art und Zweck der Verarbeitung

	Art und Zweck der Verarbeitung
SP_Data Cloud	Hosting, Wartung, Fehlerbehebung und Betrieb der beauftragten Softwareprodukte
SP_Data Payroll Outsourcing	Durchführung von Entgeltabrechnungen und der damit verbundenen Folgeprozesse im Auftrag
SP_Data Meldeserver	Hosting, Wartung, Fehlerbehebung und Betrieb
Softwarepflege	Support, Wartung, Fehlerbehebung und Qualitätssicherung

Art der personenbezogenen Daten

- Personenstammdaten (Name, Kontaktdaten, Kontoverbindung, Angaben zu Sozialversicherung, Besteuerungsmerkmale etc.)
- Daten zur Gehaltsabrechnung, Berechnung von Rente
- Daten aus der Zeiterfassung und der Zutrittskontrolle
- Personalverwaltung (Kommunikationsdaten, Bewertungen, Abmahnungen, Fehlzeiträume, etc.)

Kategorien betroffener Personen

- Beschäftigte und Bewerber des Auftraggebers und seiner verbundenen Unternehmen
- Ansprechpartner des Auftraggebers und seiner verbundenen Unternehmen

Anlage II

Nach Art. 32 DSGVO verabreden der Auftraggeber und der Auftragnehmer technische und organisatorische Maßnahmen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten:

1. Pseudonymisierung, Verschlüsselung und Anonymisierung personenbezogener Daten (Art. 32 Abs. 1 lit. a DSGVO)

Im Payroll Outsourcing sind die personenbezogenen Daten der Beschäftigten des Auftraggebers zur Durchführung von Entgeltabrechnungen im Auftrag des Kunden notwendig.

In der Cloud stellt der Auftragsverarbeiter lediglich die technische Infrastruktur für das Hosting der vertragsgegenständlichen Softwareprodukte und die Speicherung der Daten des Auftraggebers zur Verfügung und übernimmt die Wartung der technischen Infrastruktur (Wartung der Server-Hardware und der Kommunikationseinrichtungen, Installation von Software-Updates). Eine darüberhinausgehende Datenverarbeitung obliegt dem Auftraggeber, davon ausgenommen ist der SP_Data Meldeserver.

Im Hinblick auf die technisch und organisatorisch undurchführbaren Maßnahmen wird eine Pseudonymisierung und Anonymisierung der Daten nicht durchgeführt.

Die verschlüsselte Speicherung im Allgemeinen, das Verschlüsseln von Datenträgern, die Nutzung verschlüsselter Container, die Verschlüsselung einzelner Dateien oder Verzeichnisse einschließlich der verschlüsselten Datenübertragung ist dem Sachzusammenhang nach unter den nachfolgenden Punkten geregelt.

2. Vertraulichkeit (Art. 32 Abs. 1 lit. b DSGVO)

Die Vertraulichkeit von Systemen und Diensten verlangt ein Zugriffskonzept, das einschließlich Maßnahmen der Zugangs- und Zugriffskontrolle umfasst. Maßnahmen zum Schutz gegen einen unbefugten Zutritt zu den Datenverarbeitungsanlagen werden auch durch die genehmigten Unterauftragsverarbeiter umgesetzt.

- Die Zugangskontrolle im Rechenzentrum und in der Betriebsstätte des Auftragnehmers verhindert eine unbefugte Systembenutzung. Dazu zählt auch, dass Besucher begleitet werden und der Zugang auf befugte Personen durch technische Maßnahmen beschränkt wird.
- Auf der Datenverarbeitungsanlage im Rechenzentrum ist ein Virenschutzprogramm installiert. Die Signaturdatenbank wird mindestens alle 5 Minuten aktualisiert. Das Netzwerk ist gegen externe Zugriffe durch eine Firewall abgeschirmt und erlaubt nur autorisierte Zugriffe.
- Die Anmeldung an den Arbeitsplätzen erfolgt für die registrierten Benutzer über die Eingabe eines persönlichen Passworts. Sie wird protokolliert. Administratoren oder Dritte können das Passwort nicht einsehen. Es ist verboten, Passwörter anderen Personen weiterzugeben. Beim Verlassen des Arbeitsplatzes müssen sich die Mitarbeiter am System abmelden. Eine Sperre greift automatisch nach 10-minütiger Inaktivität am Arbeitsplatz und erfordert eine Neuanmeldung.
- Anhand der Benutzererkennung werden dem Benutzer spezielle und persönliche Nutzungsrechte für bestimmte Programme und Netzwerkverzeichnisse erteilt. Über die Berechtigungsbewilligung

entscheidet der jeweilige Vorgesetzte; der Administrator setzt sie im Verzeichnisdienst um. Zugriffe werden protokolliert und können durch berechtigte Personen ausgewertet werden.

- Für unterschiedliche Anwendungen gibt es separate Verzeichnisstrukturen, deren Verwaltung sicherstellt, dass nur berechtigte Benutzer zugreifen können.
- Eine Fernwartung der Systeme ist nur nach vorheriger Gestattung (Freigabe) möglich.
- Der Zugriff über einen VPN-Tunnel ist personalisiert.

3. Integrität (Art. 32 Abs. 1 lit. b DSGVO)

Die Integrität der personenbezogenen Daten erfordert Maßnahmen zur Sicherstellung ihrer Korrektheit sowie eine korrekte Funktionsweise der Systeme, einschließlich Maßnahmen zum Erkennen von Datenmodifikationen und zum Schutz vor Datenmanipulation.

- In den eingesetzten Programmen zur Entgeltabrechnung ist implementiert, dass jederzeit überprüft werden kann, ob und von wem personenbezogene Daten eingegeben, verändert oder gelöscht wurden. Ebenfalls erfolgt bei der Dateneingabe eine Plausibilitätskontrolle. Ein versehentliches Löschen von Datensätzen ist technisch ausgeschlossen. Im Falle der Fernwartung geschieht Vorstehendes auf dem System des Auftraggebers.
- Der online-Datenaustausch und der Fernwartungszugang erfolgt über sichere SSL-VPN-Verbindungen, über VPNsecure, SSH oder FTPS. Herkunft und Empfänger der Datenverbindung werden vom System erfasst.
- Geräte, die außerhalb der Betriebsstätte verbracht werden dürfen (z.B. Notebooks), erhalten einen verschlüsselten Datenträger. Sofern nicht online, werden personenbezogene Daten komprimiert und verschlüsselt auf diese übertragen.
- Defekte oder ausgesonderte Speichermedien werden durch ein zertifiziertes Entsorgungsunternehmen datenschutzgerecht vernichtet.
- Daten, die aufgrund gesetzlicher Vorgaben an die entsprechenden Stellen zu übertragen sind, wie zum Beispiel Steuer- und Sozialversicherungsdaten werden auf dem durch den Gesetzgeber vorgeschriebenen Weg und mit der dort vorgegebenen Verschlüsselung übertragen.
- Alle Mitarbeiter, die Umgang mit personenbezogenen Daten haben, sind schriftlich zur Verschwiegenheit verpflichtet. Interne Anweisungen und Richtlinien regeln verbindlich die Nutzung von Hard- und Software.

4. Verfügbarkeit und Belastbarkeit (Art. 32 Abs. 1 lit. b DSGVO)

Gefordert werden Maßnahmen, um nach einem physischen oder technischen Zwischenfall die Daten rasch wiederherstellen zu können.

- Die Datenspeicherung erfolgt auf Serverfestplatten im Rechenzentrum. Diese sind im RAID verbunden. Entsprechende Ersatzmedien werden bevorratet.
- Die Sicherheit und Verfügbarkeit der Daten werden durch ein Backup- und Recovery-Konzept gewährleistet. Einmal täglich erfolgt eine inkrementelle Datensicherung, einmal wöchentlich eine Vollsicherung.

- Mitarbeiter des Rechenzentrums haben keinen Zugriff auf die Daten. Sämtliche Kommunikation ist verschlüsselt einschließlich aller Backups.
- Das redundant ausgelegte System ist durch intelligente USV gegen Stromausfall und Überspannung geschützt.
- Der Zugriff auf die Server im Rechenzentrum ist über redundante Leitungen sichergestellt. Ebenfalls verfügen die Server über eine Serviceschnittstelle.
- Die Serverräume im Rechenzentrum sind mit einer Klimaanlage und einer Feuerschutz-einrichtung ausgestattet.
- Es erfolgt regelmäßig eine Überprüfung der Anlage durch ein externes Unternehmen.
- Durch die Dienstzeitenregelung und Urlaubsplanung ist sichergestellt, dass immer ein Administrator zugegen ist.

5. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der technischen und organisatorischen Maßnahmen (Art. 32 Abs. 1 lit. d DSGVO; Art. 25 Abs. 1 DSGVO)

Die ergriffenen technischen und organisatorischen Maßnahmen werden regelmäßig systematisch überprüft und in Bezug auf ihre Wirksamkeit zur Gewährleistung der Sicherheit der Verarbeitung bewertet und evaluiert.

- Risikobewertung (Sicherheitsaudit)
- Durchführen und Dokumentation von Kontrollen und Belastungstests
- Interne Richtlinien, Handlungsanweisungen und Prozesse zum Datenschutz werden bei Bedarf oder sich ändernden Voraussetzungen angepasst bzw. ergänzt.
- Kontrolle der Dokumentationen, Betriebsvereinbarungen, Dienstanweisungen und/oder Unternehmensrichtlinien
- Durchführung und Dokumentation von Rücksicherungstests der erzeugten Sicherungs-kopien
- Automatische Erkennung von Anomalien im Netzwerkverkehr
- Automatische Überprüfung auf Schadsoftware
- Weisungen der Auftraggeber werden auftragsbezogen dokumentiert.
- Strenge Auswahl von Unterauftragsverarbeitern sowie Einholung von Referenzen und Nachkontrollen
- Regelmäßige Kontrolle durch den betrieblichen Datenschutzbeauftragten

6. Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen (Art. 25 DSGVO)

Zur Umsetzung des Art. 25 DSGVO hat der Auftragnehmer geeignete technische und organisatorische Maßnahmen veranlasst. Durch Voreinstellungen können nur personenbezogene Daten, deren Verarbeitung für den jeweiligen bestimmten Verarbeitungszweck erforderlich ist, verarbeitet werden. Dieses gilt namentlich für die Menge der erhobenen Daten, den Umfang ihrer Verarbeitung, ihre Speicherfrist und ihre Zugänglichkeit. Insbesondere hat der Auftragnehmer Vorkehrungen getroffen, dass personenbezogene Daten durch Voreinstellungen nicht ohne Eingreifen der Person einer unbestimmten Zahl von natürlichen Personen zugänglich gemacht werden.



- Die Rechtevergabe folgt dem Need-to-Know-Prinzip. Ein neu angelegter Benutzer hat zunächst keine Rechte. Diese müssen ihm ausdrücklich zugeordnet werden. Jeder Mitarbeiter erhält nur ein Minimum an Rechten, die er zur Erledigung der eigenen Aufgaben benötigt. Durch diese Benutzerverwaltung ist sichergestellt, dass jeder Mitarbeiter nur im Umfang der ihm übertragenen Aufgaben Daten verarbeiten kann. Die Rechteverwaltung unterscheidet ferner nach der Qualität der anstehenden Arbeiten. So werden je nach Erforderlichkeit die Rechte beschränkt auf das Lesen, Lesen/Schreiben bzw. Lesen/Schreiben und Speichern.
- Mit Hilfe unseres CRM verwalten wir die Speicherfristen auftrags- und kundenbezogen. Es gibt keine Voreinstellungen, die es erlauben, ohne Eingreifen der Betroffenen deren persönlichen Daten einer unbestimmten Zahl von natürlichen Personen zugänglich zu machen.

Anlage III: Genehmigte Unterauftragsverarbeiter

Firmierung und ladungsfähige Anschrift des Unterauftrags- verarbeiters	centron GmbH Heganger 29 96103 Hallstadt	in-Reach UG (haftungsbeschränkt) & Co. KG Tiergartenstr. 26 96123 Litzendorf
Beschreibung der Leistung des Unterauftragsverarbeiters	Hosting, Wartung, Fehlerbehebung und Betrieb der Infrastruktur des SP_Data Meldeservers	Hosting, Wartung, Fehlerbehebung und Betrieb der Infrastruktur der SP_Data Cloud. Entwicklung, Wartung und Fehlerbehebung der Produkte SP_Data Studio, my_spdata und Mitarbeiterportal
Aufzählung der vom Unter- auftragsverarbeiter im Rahmen der Leistungserbringung für den Auftraggeber eingesetzten weiteren Unterunter- auftragsverarbeiter mit Firmierung, ladungsfähiger Anschrift und Beschreibung der Leistungen	keine	Hetzner Online GmbH Industriestr. 25 91710 Gunzenhausen Bereitstellung des Rechenzentrums/der Hosting Infrastruktur
Länder, in denen Daten im Auftrag des Auftraggebers durch Unterauftragsverarbeiter und Unterunterauftragsverarbeiter verarbeitet werden oder aus denen auf diese Daten zugegriffen werden kann	Deutschland	Deutschland (Produktivsystem) Finnland (verschlüsselte Datensicherungen)
Für die folgenden Drittländer liegt ein Angemessenheitsbeschluss der EU-Kommission vor. Für jedes Drittland ist das Aktenzeichen des Beschlusses anzugeben.	keine	keine
Für die folgenden Drittländer werden mit den dort tätigen Unterauftragsverarbeitern die Standarddatenschutzklauseln i.S.d. Art. 46 Abs. 2 lit. c) DS-GVO geschlossen.	keine	keine

Für die folgenden Drittländer sind die dort tätigen und zum Konzern des Auftragsverarbeiters gehörenden Unterauftragsverarbeiter Binding Corporate Rules beigetreten. Die Genehmigung durch die Datenschutzaufsichtsbehörde wird in Kopie beigefügt oder auf die Fundstelle im Internet verlinkt.	keine	keine
---	-------	-------

Informationen über die von den Unterauftragsverarbeitern getroffenen Sicherheitsmaßnahmen finden Sie unter www.spdata.de/vertraege.

Stand: 01.12.2025