Allgemeine Vertragsbedingungen über die Verarbeitung von personenbezogenen Daten im Auftrag

Diese Allgemeinen Vertragsbedingungen bilden die Grundlage für die Verarbeitung von personenbezogenen Daten im Auftrag des Kunden (Auftraggeber) durch die SP_Data GmbH & Co. KG (Auftragnehmer) nach Art 28 DSGVO.

Der Auftragnehmer bietet seinen Auftraggebern verschiedene Leistungen an, die einzeln oder in Kombination beauftragt werden können. Der Leistungsumfang ergibt sich aus der Beauftragung, der Leistungsbeschreibung und den Allgemeinen Geschäftsbedingungen des Auftragnehmers in der jeweils gültigen Fassung:

- SP_Data Cloud: Der Auftragnehmer hostet in externen Rechenzentren für den Auftraggeber verschiedene Softwareprodukte, die im Rahmen der Beauftragung festgelegt werden.
- SP_Data Payroll Outsourcing: Der Auftragnehmer erstellt Entgeltabrechnungen für die Beschäftigten des Auftraggebers. Dazu verwendet der Auftragnehmer die SP_Data Cloud.
- SP_Data Meldeserver: Hosting einer Plattform zur Durchführung der elektronischen Meldeverfahren in den Bereichen Sozialversicherung und Steuer.
- Softwarepflege: Der Auftragnehmer führt regelmäßig Wartungs- und Supportarbeiten in den von SP_Data angebotenen Softwareprodukten mit den Daten seiner Auftraggeber durch. Die Arbeiten bestehen im Wesentlichen aus der Analyse von unerwünschtem Programmverhalten, Fehlerbehebung und Qualitätssicherung. Die Tätigkeit erfolgt beim Auftragnehmer, in der SP_Data Cloud, vor Ort beim Auftraggeber oder nach vorheriger Freigabe durch den Auftraggeber mittels einer Fernwartungsverbindung.

§ 1 Allgemeines

Die Parteien stellen klar, dass die Datenverarbeitung ausschließlich im Auftrag des Auftraggebers erfolgt (Auftragsdatenverarbeitung). Zwingende datenschutzrechtliche Gesetze, Verordnungen, Richtlinien, insbesondere die Datenschutzgrundverordnung (DSGVO) und das Bundesdatenschutzgesetz (BDSG) werden nicht berührt und sind im Zweifel bei der Auslegung und Lückenausfüllung heranzuziehen.

§ 2 Gegenstand

Gegenstand und Dauer der Verarbeitung, Art und Zweck der Verarbeitung, die Art der personenbezogenen Daten und die Kategorien betroffener Personen ergeben sich aus dem Vertrag und Anlage I.

§ 3 Pflichten des Auftragnehmers/Weisungen

1) Der Auftragnehmer verarbeitet personenbezogene Daten ausschließlich auf Weisung des Auftraggebers in Schrift- oder Textform. Weisungen können bereits im Vertrag formuliert werden.
2) Der Auftragnehmer dokumentiert alle Weisungen des Auftraggebers.

3) Der Auftragnehmer übermittelt personenbezogene Daten an ein Drittland oder eine internationale Organisation ausschließlich auf schriftliche oder elektronische Weisung des Auftraggebers.
4) Ist der Auftragnehmer durch das Recht der Union oder dem Recht der Bundesrepublik Deutschland zur Verarbeitung oder Übermittlung verpflichtet, teilt er dem Auftraggeber die Anforderungen vor der Verarbeitung mit, sofern das betreffende Recht eine solche Mitteilung nicht wegen eines wichtigen öffentlichen Interesses verbietet.
5) Dem Auftraggeber ist bewusst, dass besondere Datenkonstellationen zu Fehlfunktionen und Fehlberechnungen in Softwareprodukten führen können. Der Auftragnehmer erklärt sich bereit, Softwareänderungen vor Bereitstellung in der SP_Data Cloud unter Verwendung der Daten des Auftraggebers auf Fehler in einem standardisierten Verfahren zu testen, sofern der Auftraggeber nicht widerspricht. Auftraggebern, die SP_Data Produkte selber hosten und betreiben (on-premises), bietet der Auftragnehmer an, Softwareänderungen vor Bereitstellung an den Auftraggeber unter Verwendung der Daten des Auftraggebers auf Fehler in einem standardisierten Verfahren zu testen. Um diesen Service nutzen zu können, müssen Auftraggeber eine Kopie der entsprechenden Datenbank zur Verfügung stellen.
6) Der Auftragnehmer gewährleistet, dass sich die zur Verarbeitung der personenbezogenen Daten befugten Personen zur Vertraulichkeit verpflichtet haben oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen (Art. 28 Abs. 3 S. 2 lit. b DS-GVO) und über die Pflicht zur Verarbeitung nur entsprechend der erteilten Weisungen belehrt worden sind (vgl. Art. 28 Abs. 3 S. 2 lit. b, Art. 29 DS-GVO). Der Auftragnehmer unternimmt Schritte, um sicherzustellen, dass ihm unterstellte natürliche Personen, die Zugang zu personenbezogenen Daten haben, diese nur entsprechend der Weisung des Auftraggebers nach Maßgabe dieser Vereinbarung verarbeiten, es sei denn, sie sind nach dem Recht der Union oder der Mitgliedstaaten zur Verarbeitung verpflichtet (vgl. Art. 32 Abs. 4 DS-GVO).
7) Der Auftragnehmer trägt Sorge dafür, dass die Verschwiegenheitsverpflichtung auch nach Beendigung des Auftrages fortbesteht.
8) Der Auftragnehmer unterrichtet den Auftraggeber unverzüglich, wenn ihm Verletzungen des Schutzes personenbezogener Daten des Auftraggebers bekannt werden. Der Auftragnehmer trifft die erforderlichen Maßnahmen zur Sicherung der Daten und zur Minderung möglicher nachteiliger Folgen für betroffene Personen und spricht sich hierzu unverzüglich mit dem Auftraggeber ab.
9) Der Auftragnehmer informiert den Auftraggeber unverzüglich, falls er der Auffassung ist, dass eine Weisung gegen die DSGVO oder ein anderes Datenschutzgesetz der Union oder der Bundesrepublik Deutschland verstößt.
10) Bis zur Klärung, ob die vom Auftragnehmer beanstandete Weisung gegen die DSGVO oder ein anderes Datenschutzgesetz der Union oder der Bundesrepublik Deutschland verstößt, ruht die Verpflichtung des Auftragsnehmers zur Auftragsdatenverarbeitung.
11) Hat der Auftraggeber das Ruhen zu verantworten, stehen dem Auftragnehmer Schadensersatzansprüche zu. Anstelle eines konkreten Schadens kann der Auftragnehmer für jeden Tag des Ruhens pauschal 5% des Auftragswertes als Schadensersatz verlangen. Dem Auftraggeber bleibt der Nachweis eines geringeren Schadens vorbehalten.

§ 4 Datenschutzbeauftragter

Kontaktdaten des Datenschutzbeauftragten des Auftragnehmers:

Xamit Bewertungsgesellschaft mBH
Monschauer Straße 12
40549 Düsseldorf
Email: info@xamit.de

§ 5 Sicherheit

1) Unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeiten und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen wird der Auftragnehmer die in Anlage II dargestellten technischen und organisatorischen Maßnahmen ergreifen.
2) Die in der Anlage II Abs. 1 beschriebenen organisatorischen und technischen Maßnahmen entwickeln sich stets weiter. Dem Auftragnehmer ist es gestattet, alternative Maßnahmen umzusetzen, wenn sie das Schutzniveau der festgelegten Maßnahme nicht unterschreitet. Wesentliche Änderungen werden vom Auftragnehmer dokumentiert.
3) Der Auftragnehmer gewährleistet ein Verfahren zur regelmäßigen Überprüfung der Wirksamkeit der organisatorischen und technischen Maßnahmen.

§ 6 Unterauftragsdatenverarbeitung

1) Als Unterauftragsdatenverarbeitung im Sinne dieser Regelung sind solche Dienstleistungen zu verstehen, die sich unmittelbar auf die Erbringung der Hauptleistung beziehen. Nicht hierzu gehören Nebenleistungen, die der Auftragnehmer z.B. als Telekommunikationsleistung, Post-/ Transportdienstleistung, Wartung und Benutzungsservice oder die Entsorgung von Datenträgern sowie sonstige Maßnahmen zur Sicherstellung der Vertraulichkeit, Verfügbarkeit, Integrität und Belastbarkeit der Hard- und Software von Datenverarbeitungsanlagen in Anspruch nimmt. Der Auftragnehmer ist jedoch verpflichtet, zur Gewährleistung des Datenschutzes und der Datensicherheit der Daten des Auftraggebers auch bei ausgelagerten Nebenleistungen angemessene und gesetzeskonforme vertragliche Vereinbarungen sowie Kontrollmaßnahmen zu ergreifen.
2) Zu den in Anlage III benannten Unternehmen mit den dort beschriebenen Leistungen an den dort bestimmten Standorten hat der Auftraggeber seine Zustimmung als Unterauftragsverarbeiter erteilt, wobei die Zustimmung nicht von der Einhaltung der Vorgaben dieser Vereinbarung zur Beauftragung von Unterauftragsverarbeiter befreit.
3) Der Auftragnehmer hat die in Anlage III aufgeführten Unterauftragsverarbeiter sorgfältig auf ihre Eignung geprüft und vertraglich sichergestellt, dass sie gegenüber dem Auftraggeber ausnahmslos die gleichen Verpflichtungen zu erfüllen haben wie er selbst.
4) Der Auftragsnehmer darf Unterauftragsverarbeiter, die nicht in Anlage III aufgeführt sind, nur einschalten, wenn:
   a) der Auftragnehmer die Auslagerung auf Unterauftragnehmer dem Weisungsempfänger des Auftraggebers mindestens 14 Tage vorher schriftlich oder in Textform angezeigt hat;
   b) die Anzeige mindestens die Angaben aus Anlage III umfasst;
   c) der Auftraggeber nicht innerhalb von 14 Tagen nach Zugang der Anzeige schriftlich oder in Textform widersprochen hat.

Vorstehende Ziffern a) und b) gelten analog auch für das Entfallen eines Unterauftragsverarbeiters.

5) In Fällen, in denen der Auftragsverarbeiter keinen Einfluss auf den Anlass für das Ersetzen eines Unterauftragsverarbeiters hat, bspw. Insolvenz des Unterauftragsverarbeiters oder eine länger anhaltende Leistungsstörung beim Unterauftragsverarbeiter, darf der Auftragsverarbeiter die in Abs. 4 genannten Fristen angemessenen verkürzen.
6) Der Auftragnehmer hat neue Unterauftragsverarbeiter vorab sorgfältig auf ihre Eignung zu prüfen und vertraglich sicherzustellen, dass sie gegenüber dem Auftraggeber ausnahmslos die gleichen Verpflichtungen zu erfüllen haben wie er selbst.
7) Widerspricht der Auftraggeber gemäß Abs. 4 so steht dem Auftragnehmer ein Sonderkündigungsrecht mit einer Frist von 14 Tagen zu.

§ 7 Unterstützungsleistungen des Auftragnehmers

1) Der Auftragnehmer unterstützt den Auftraggeber nach Möglichkeit mit geeigneten technischen und organisatorischen Maßnahmen bei dessen Pflichten zur Beantwortung von Anträgen auf Wahrnehmung der in Kapitel III DSGVO genannten Rechte der betroffenen Personen.
2) Unter Berücksichtigung der Art der Datenverarbeitung und der ihm zur Verfügung stehenden Informationen unterstützt der Auftragnehmer den Auftraggeber ferner bei Einhaltung der in den Artikeln 32- 36 DSGVO genannten Pflichten. Diese Pflicht umfasst insbesondere die Bereitstellung der Informationen, die sich im Einflussbereich des Auftragnehmers befinden und über die der Auftraggeber nicht selbst verfügen kann.
3) Wenn und soweit der Auftragnehmer die Informationen nicht zur gleichen Zeit bereitstellen kann, kann er diese Informationen ohne unangemessene weitere Verzögerung schrittweise zur Verfügung stellen.
4) Der Auftragnehmer meldet dem Auftraggeber an die vom Auftraggeber mitgeteilte Adresse zur Meldung von Verletzung des Schutzes personenbezogener Daten unverzüglich eine ihm bekannte Verletzung des Schutzes personenbezogener Daten.
5) Der Auftragnehmer stellt dem Auftraggeber - sofern und soweit dies möglich ist - die Informationen zur Verfügung, die dieser zur Erfüllung seiner Pflichten aus den Artt. 33 und 34 DS-GVO benötigt.

§ 8 Löschung/Rückgabe der personenbezogenen Daten

Der Auftragnehmer gibt grundsätzlich nach Abschluss der Erbringung der Verarbeitungsleistungen alle personenbezogenen Daten an den Auftraggeber zurück. Die Daten werden im MS-SQL-Backup-Format, als Exportdateien im Standardformat der genutzten Software sowie in Form der entschlüsselten Dokumente aus der digitalen Personalakte zur Verfügung gestellt. Der Auftraggeber ist für die Lesbarmachung der exportierten Daten verantwortlich. Der Auftragnehmer stellt dem Auftraggeber die Daten über einen gesicherten Weg zur Verfügung. Der Auftraggeber hat keinen Anspruch darauf, auch die zur Verwendung der Daten geeignete Software zu erhalten. Der Auftraggeber ist berechtigt anstelle einer Rückgabe die Löschung der Daten anzuweisen.

§ 9 Pflichten des Auftraggebers

1) Der Auftraggeber hat den Auftragnehmer unverzüglich und vollständig zu informieren, wenn er bei der Prüfung der Auftragsergebnisse Fehler oder Unregelmäßigkeiten bzgl. datenschutzrechtlicher Bestimmungen feststellt.
2) Im Falle einer Inanspruchnahme des Auftraggebers durch eine betroffene Person hinsichtlich etwaiger Ansprüche nach Art. 82 DSGVO verpflichtet sich der Auftragnehmer den Auftraggeber bei der Abwehr des Anspruchs im Rahmen seiner Möglichkeiten zu unterstützen.
3) Der Auftraggeber erteilt dem Auftragnehmer spätestens mit der Unterzeichnung des Vertrags unaufgefordert schriftlich oder in Textform die nachfolgenden Auskünfte und informiert den Auftragnehmer unverzüglich und unaufgefordert über Änderungen:
   - Kontaktdaten der weisungsberechtigten Personen sowie Angabe deren Namen und Funktionsbezeichnung,
   - Meldeadresse (Fax, E-Mail, Post) für Verletzungen des Schutzes personenbezogener Daten i.S.d. Art. 4 Nr. 12 DS-GVO einschließlich der Vorfälle nach Artt. 33 und 34 DS-GVO,
   - Kontaktdaten des Datenschutzbeauftragten oder – sofern kein Datenschutzbeauftragter bestellt ist - einen Ansprechpartner für den Datenschutz und
   - Kontaktdaten der Sachbearbeiter des Auftraggebers.

§ 10 Kontrollrechte des Auftraggebers

1) Der Auftraggeber hat das Recht, Überprüfungen durchzuführen oder durch im Einzelfall zu benennende Prüfer durchführen zu lassen, die sich auf die Einhaltung der vertraglichen Vereinbarung zwischen Auftraggeber und Auftragsverarbeiter, die vom Auftraggeber erteilten Weisungen sowie die Einhaltung der einschlägigen datenschutzrechtlichen Pflichten beziehen. Er hat das Recht, sich dazu in angemessenen Abständen oder bei Anzeichen für eine Nichteinhaltung in dem Geschäftsbetrieb des Auftragsverarbeiters zu überzeugen. Der Auftragsverarbeiter darf Prüfer ablehnen, sofern diese in einem Wettbewerbsverhältnis zu ihm stehen.
2) Der Auftragsverarbeiter verpflichtet sich, dem Auftraggeber oder dem benannten Prüfer auf Anforderung innerhalb einer angemessenen Frist alle Auskünfte zu erteilen, Nachweise (z.B. vorhandene Testate von Sachverständigen, Zertifizierungen oder interne Prüfungen) zur Verfügung zu stellen und insbesondere die Umsetzung der technischen und organisatorischen Maßnahmen nachzuweisen.
3) Der Auftragsverarbeiter hat vertraglich sicherzustellen, dass Unterauftragsverarbeiter gegenüber dem Auftraggeber ausnahmslos dieselben Verpflichtungen zu erfüllen haben wie er selbst. Dies gilt insbesondere für die in (1), (2) und (4) genannten Kontrollregelungen durch den Auftraggeber beim Unterauftragsverarbeiter.
4) Eine Verarbeitung der übermittelten Daten des Auftraggebers durch den Auftragsverarbeiter ist ausschließlich in der Betriebsstätte des Auftragnehmers und im Homeoffice der Mitarbeiter des Auftragnehmers gestattet. Der Auftragsverarbeiter stellt sicher und weist auf Anfrage dem Auftraggeber nach, dass die Anforderungen von Art. 32 DS-GVO an Orten außerhalb seiner Betriebsstätten vollumfänglich erfüllt werden, sowie dass der Auftraggeber und die zuständige Datenschutzaufsichtsbehörde ihre Kontrollrechte uneingeschränkt an diesen Orten ausüben können.

5) Wenn der Auftraggeber die Inspektion veranlasst hat, darf der Auftragnehmer eine angemessene Vergütung für die Unterstützung bei der Durchführung einer Inspektion verlangen, sofern nicht Anlass der Inspektion der dringende Verdacht eines Datenschutzvorfalls im Verantwortungsbereich des Auftragnehmers war. Der Auftraggeber hat entsprechende Verdachtsmomente mit der Ankündigung der Inspektion vorzutragen.

§ 11 Anpassungsklausel

1) Sollten eine oder mehrere Bestimmungen der vorliegenden allgemeinen Vertragsbedingungen gegen geltendes Recht oder künftig geltendes Recht verstoßen, bleibt hiervon die Gültigkeit der übrigen Bestimmungen unberührt. In diesem Fall werden die Parteien die ungültige Bestimmung durch eine gesetzlich statthafte Regelung ersetzen, die dem mit der unwirksamen Bestimmung verfolgten Zweck am nächsten kommt.
2) Diese Regelung gilt sinngemäß auch im Falle einer von beiden Parteien übereinstimmend festgestellten Vertragslücke.
3) Es gilt deutsches Recht.

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 Benutzerkennung 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 Feuerschutzeinrichtung 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 Sicherungskopien
- 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 Rah-men der Leistungserbringung für den Auftraggeber ein-gesetzten weiteren Unter-unterauftragsverarbeiter 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 Unterauftragsverarbei-ter und Unterunterauftrags-verarbeiter verarbeitet wer-den oder aus denen auf diese Daten zugegriffen werden kann	Deutschland	Deutschland (Produktivsystem) Finnland (verschlüsselte Datensicherungen)
Für die folgenden Drittländer liegt ein Angemessenheits-beschluss der EU-Kommission vor. Für jedes Drittland ist das Aktenzeichen des Be-schlusses 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	keine	keine

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.		

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

Stand: 16.01.2024