Umfang der Datenverarbeitung

	Fernwartung auf dem Kundensystem	Analyse mit zur Verfügung gestellten Kundendaten	Verwendung von zur Verfügung gestellten Kundendaten im Rahmen der Qualitätssicherung
1. Umfang der Datenverarbeitung			
Erheben			
Erfassen			
Organisieren			
Ordnen			
Speichern		X	X
Anpassen			
Verändern			
Auslesen	X	X	X
Verwendung			X
Offenlegung			
Verbreitung/Bereitstellung			
Abgleich/Verknüpfung			
Löschen			
Vernichten		X	X
2. Risikoabschätzung			
unbeabsichtigte oder unrechtmäßige Vernichtung	geringes Risiko	kein Risiko	kein Risiko
unbeabsichtigter oder unrechtmäßiger Verlust	geringes Risiko	kein Risiko	kein Risiko
unbeabsichtigte oder unrechtmäßige Veränderung	Risiko	kein Risiko	kein Risiko
unbefugte Offenlegung von personenbezogenen Daten	geringes Risiko	geringes Risiko	geringes Risiko
unbefugter Zugang zu personenbezogenen Daten	Risiko	Risiko	Risiko

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)

Ein Verzicht auf die Verarbeitung von personenbezogenen Daten in der Weise, dass die Daten ohne Hinzuziehung zusätzlicher Informationen keiner Person zugeordnet werden können, sofern diese zusätzlichen Informationen gesondert aufbewahrt werden und technischen und organisatorischen Maßnahmen unterliegen, die gewährleisten, dass die personenbezogenen Daten nicht einer identifizierten oder identifizierbaren natürlichen Person zugewiesen werden können, ist unter Berücksichtigung des Stands der Technik im Falle unserer Auftragsdatenverarbeitung nicht möglich. Die Zuordnung der Daten zu den betroffenen Personen ist für die beauftragte Datenverarbeitung unumgänglich. Ein unerwünschtes Programmverhalten sowie eine Fehlerbehebung und Qualitätssicherung lassen sich nur anhand von Originaldatenbanken analysieren bzw. durchführen, wobei eine Zuordnung der personenbezogenen Daten zu den betroffenen Personen entscheidend ist. Das Gleiche gilt bei der Verarbeitung von Daten zur Durchführung von Entgeltabrechnungen im Auftrag des Kunden (Abrechnungsservice). Im Hinblick auf die technisch und organisatorisch undurchführbaren Maßnahmen wird eine Pseudonymisierung, Verschlüsselung 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 Zutritts- und Zugangskontrolle umfasst.

2.1 Zutrittskontrolle

Mit der Zutrittskontrolle wird Schutz gegen einen unbefugten Zutritt zu den Datenverarbeitungsanlagen erreicht:

- Der Zutritt zum Gebäude ist elektronisch gesichert. Die Anwesenheit von Personen im Gebäude wird elektronisch protokolliert. Besucher müssen sich am Empfang melden und werden registriert. Die Flure sind videoüberwacht. Im Erdgeschoss sind die Fenster gegen Einbruch gesichert. Eingangsbereich und Fenster sind nach Dienstschluss stets verschlossen.
- Der Serverraum ist fensterlos. Die Tür zum Raum entspricht der geforderten Schutzklasse. Der Zutritt wird protokolliert und ist durch ein Sicherheitsschloss (Transponder) nur autorisierten Mitarbeitern möglich. Wartungsarbeiten an den Servern werden von einem Systemadministrator überwacht.

2.2 Zugangskontrolle

Die Zugangskontrolle verhindert eine unbefugte Systembenutzung.

- Auf der Datenverarbeitungsanlage 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. Das Passwort wird vom Benutzer erstellt. Es ist alle 6 Wochen durch ein neues zu ersetzen und darf mit den letzten drei vorangegangenen Passwörtern nicht übereinstimmen. Administratoren oder Dritte können das Passwort nicht einsehen. Es ist verboten, Passwörter anderen Personen weiter zu geben. 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.

2.3 Zugriffskontrolle

Mit der Zugriffskontrolle werden den Benutzern Rechte an der Datenverarbeitungsanlage eingeräumt, wie zum Beispiel das Lesen, Kopieren, Verändern oder Entfernen von Daten.

- 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 (Vertragsprodukten) 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 oder FTPS. Dem Auftraggeber steht es frei, Daten anonymisiert zu übermitteln. Herkunft und Empfänger der Datenverbindung werden vom System erfasst.
- Datenträger in Geräten, 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. Sie haben sich auf die IT-Richtlinie verpflichtet.

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

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

- Die Datenspeicherung erfolgt auf den Serverfestplatten. Diese sind im RAID verbunden. Entsprechende Ersatzmedien werden bevorratet.
- Die Sicherheit und Verfügbarkeit der Daten wird durch ein mehrstufiges Backup- und Recovery-Konzept gewährleistet. Mindestens einmal täglich erfolgt eine inkrementelle Bandsicherung; einmal wöchentlich eine Vollsicherung. Bandsicherungen der Vorwoche werden montags von einem Mitarbeiter im Bankschließfach deponiert. Insgesamt gibt es 4x7 Bänder.
- Das redundant ausgelegte System ist durch intelligente USV gegen Stromausfall und Überspannung geschützt.
- Der Zugriff auf die Server ist über eine redundante Leitung sichergestellt. Ebenfalls verfügen die Server über eine Serviceschnittstelle.
- Der Serverraum ist mit einer Klimaanlage und einer Feuerschutzeinrichtung (Kohlendioxid-Automatiklöscher) ausgestattet, die bei Schwellenwertüberschreitung die Systemadministratoren per SMS benachrichtigen.
- 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.
- Sensibilisierung und Schulung von Mitarbeitern.
- Dokumentation der Verarbeitungstätigkeit.
- Weisungen der Auftraggeber werden auftragsbezogen dokumentiert.
- Beim Einsatz von Auftragsdatenverarbeitern gelten die gleichen Maßstäbe, wie für die eigene Verarbeitung.
- Eindeutige Vertragsgestaltung mit dem Auftraggeber.
- Ein formalisiertes Auftragsmanagement einschl. CRM.

- Strenge Auswahl des Dienstleisters sowie Einholung von Referenzen und Nachkontrollen.
- Verantwortliche Auswahl eines hinreichend qualifizierten Datenschutzbeauftragten sowie regelmäßige Prüfung.
- Jeder Mitarbeiter erhält bei seiner Einstellung eine spezifische Einweisung in die von ihm verwendeten Systeme.
- Neben der von jedem Mitarbeiter zu beachtenden IT-Richtlinie finden Schulungen zum Datenschutz und zur Datensicherheit statt.
- Soweit erforderlich, werden eingesetzte Verfahren einer dokumentierten Datenschutz-Folgenabschätzung unterzogen, bestehend aus Schutzbedarfsfeststellung, Risikoanalyse, Sicherheitskonzept.

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

Unter Beachtung von Art. 25 garantieren wir die Anforderungen der DSGVO durch geeignete technische und organisatorische Maßnahmen, insbesondere die Umsetzung und Einhaltung der Datenschutzgrundsätze. Dazu haben wir auch 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 haben wir Vorkehrungen getroffen, dass personenbezogene Daten durch Voreinstellungen nicht ohne Eingreifen der Person einer unbestimmten Zahl von natürlichen Personen zugänglich gemacht werden.

- Wir verwenden stets die höchste Sicherheitsstufe. 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.
- Voreinstellungen dergestalt, dass ohne Eingreifen der Betroffenen, deren persönlichen Daten einer unbestimmten Zahl von natürlichen Personen zugänglich gemacht werden können, gibt es nicht.

Stand: 24.04.2023