ALLGEMEINE VERTRAGSBEDINGUNGEN ÜBER DIE VERARBEITUNG VON PERSONENBEZOGENEN DATEN IM AUFTRAG

Die allgemeinen Vertragsbedingungen bilden die Grundlage für die Verarbeitung von personenbezogenen Daten im Auftrag des Kunden (Auftraggeber) durch die SP_Data GmbH & Co. KG (Auftragnehmer).

§ 1 Allgemeines

Im Rahmen von Softwarepflegeverträgen (Vertrag) führt der Auftragnehmer regelmäßig Arbeiten auf IT-Systemen seiner Auftraggeber durch. Die wesentlichen Arbeiten sind die Analyse von unerwünschtem Programmverhalten, Fehlerbehebung und Qualitätssicherung. Die Tätigkeit erfolgt vor Ort oder nach vorheriger Freigabe durch den Auftraggeber mittels einer Fernwartungsverbindung. Darüber hinaus verarbeitet der Auftragnehmer Daten zur Durchführung von Entgeltabrechnungen im Auftrag des Kunden (ebenfalls „Vertrag"). Es ist unumgänglich, dass dazu der Auftragnehmer und die ihr unterstellten Personen personenbezogene Daten verarbeiten. Zum Umfang der Datenverarbeitung wird auf Anlage I verwiesen. 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 Bundes-Datenschutzanpassungs- und Umsetzungsgesetz-EU (BDSG-EU) 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.

Art der Daten	Art und Zweck der Verarbeitung	Kategorie betroffener Personen
Personenstammdaten (Name, Kontaktdaten, Kontoverbindung, Krankenkasse, Steuerklasse, Kirchensteuermerkmal), die zur Gehaltsabrechnung, Berechnung von Rente, zur allg. Personalverwaltung (Kommunikationsdaten, Bewertungen, Abmahnungen, Gesundheitsdaten) und Verwaltung von Bewerberdaten aufgrund gesetzlicher Vorgaben und/oder vertraglichen Vereinbarungen benötigt werden.	Dienstleistungen in Zusammenhang mit einem Produkt des Auftragnehmers gemäß Vertrag. Analyse von unerwünschtem Programmverhalten und Fehlerbehebung. Die Tätigkeit erfolgt vor Ort oder per Remote-Support (Freischaltung des Auftragnehmers durch den Auftraggeber erforderlich).	Die Datenverarbeitung erfolgt für Zwecke des Beschäftigungsverhältnisses nach § 26 Abs. 1 BDSG-neu für die Beschäftigten des Auftraggebers und/oder mit diesem verbundenen Unternehmen im Sinne von § 26 Abs. 8 BDSG-neu.

§ 3 Pflichten des Auftragnehmers/Weisungen

1) Der Auftragnehmer verarbeitet personenbezogene Daten ausschließlich auf schriftliche oder elektronische (Textform) Weisung des Auftraggebers. 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 Auftragnehmer unterstellte Personen, die Zugang zu personenbezogenen Daten haben, verarbeiten diese nur auf Weisung des Auftraggebers, es sei denn, sie sind nach dem Recht der Union oder der Bundesrepublik Deutschland zur Verarbeitung verpflichtet. Jede dem Auftragnehmer unterstellte Person erhält vor Aufnahme ihrer Tätigkeit eine Abschrift sämtlicher Weisungen.
6) 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.
7) 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.
8) 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 Vertraulichkeit

1) Der Auftragnehmer gewährleistet, dass er die zur Verarbeitung der personenbezogenen Daten befugten Personen zur Vertraulichkeit verpflichtet hat bzw. diese einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen.
2) Der Auftragnehmer trägt Sorge dafür, dass die Verschwiegenheitsverpflichtung auch nach Beendigung des Auftrages fortbesteht.
3) 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.

§ 5 Datenschutzbeauftragter

Datenschutzbeauftragter des Auftragnehmers:
Dr. Niels Lepperhoff
Monschauer Straße 12
40549 Düsseldorf
Tel: 0211 960 823 80

§ 6 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 zu einem dem Risiko angemessenen Schutzniveau gewährleisten.
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.

§ 7 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) Der Auftragsnehmer darf Unterauftragsdatenverarbeiter nur nach vorheriger ausdrücklicher schriftlicher Zustimmung des Auftraggebers einschalten, wenn:
   - der Auftragnehmer die Auslagerung auf Unterauftragnehmer dem Auftraggeber mindestens 2 Wochen vorher schriftlich oder in Textform angezeigt hat;
   - der Auftraggeber bis zum Zeitpunkt der Übergabe der Daten gegenüber dem Auftragnehmer weder schriftlich noch in Textform Einspruch gegen die Auslagerung der Daten erhoben hat;
   - der Unterauftragsdatenverarbeitung eine Vereinbarung nach Maßgabe des Art. 28 Abs. 2-4 DSGVO zugrunde liegt.

§ 8 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) Der Auftragnehmer dokumentiert die Datenverarbeitung und protokolliert dazu mindestens die folgenden Datenverarbeitungsvorgänge, sofern sie im Rahmen des Auftrages erfolgen:

   - Erhebung
   - Veränderung
   - Abfrage
   - Offenlegung, einschl. Übermittlung
   - Kombination und
   - Löschung

3) Die Protokolle nach Abs. 2 werden ausschließlich für die Überprüfung der Rechtmäßigkeit der Datenverarbeitung durch die Datenschutzbeauftragte oder den Datenschutzbeauftragten, die Bundesbeauftragte oder den Bundesbeauftragten und die betroffene Person, die für die Eigenüberwachung, für die Gewährleistung der Integrität und Sicherheit der personenbezogenen Daten und für Strafverfahren zuständig sind, überlassen.
4) Die Protokolldaten sind am Ende des auf deren Generierung folgenden Jahres zu löschen.
5) 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 und §§ 64 bis 67 und 69 BDSG-EU genannten Pflichten.
6) 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.
7) Der Auftragnehmer meldet dem Auftraggeber unverzüglich eine ihm bekannte Verletzung des Schutzes personenbezogener Daten und dokumentiert die Verletzung einschließlich aller im Zusammenhang mit der Verletzung des Schutzes personenbezogener Daten stehenden Fakten von deren Auswirkungen und der ergriffenen Abhilfemaßnahmen.
8) Der Auftragnehmer stellt die von ihm gefertigte Dokumentation dem Auftraggeber so zur Verfügung, dass der Aufsichtsbehörde die Überprüfung der Einhaltung der Bestimmungen des Artikels 33 DSGVO möglich ist.
9) Der Auftragnehmer verwendet einen Report zur Information für den Fall der Verletzung des Schutzes personenbezogener Daten.
10) Hat die Verletzung des Schutzes personenbezogener Daten voraussichtlich ein hohes Risiko für die persönlichen Rechte und Freiheiten natürlicher Personen zur Folge, so unterstützt der Auftragnehmer den Auftraggeber bei der unverzüglichen Benachrichtigung der betroffenen Personen von der Verletzung.
11) Hat eine Form der Verarbeitung aufgrund der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung voraussichtlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen zur Folge, unterstützt der Auftragnehmer den Auftraggeber auch bei der vorab durchzuführenden Abschätzung der Folgen der vorgesehenen Verarbeitungsvorgänge für den Schutz personenbezogener Daten.
12) Für den Fall, dass infolge der Datenschutz-Folgenabschätzung aus der Verarbeitung ein hohes Risiko resultiert, unterstützt der Auftragnehmer den Auftraggeber insbesondere durch Zurverfügungstellung folgender Unterlagen:
    - Angaben zu den jeweiligen Zuständigkeiten des an der Verarbeitung beteiligten Auftragsverarbeiters,
    - Systematische Beschreibung der geplanten Verarbeitungsvorgänge,
    - Angaben zum Zweck und Mittel der beabsichtigten Verarbeitung,
    - Bewertung der Notwendigkeit und Verhältnismäßigkeit der Verarbeitungsvorgänge in Bezug auf deren Zweck,
    - Bewertung der Gefahren für die Rechtsgüter der betroffenen Personen,
    - Die zum Schutz der Rechte und Freiheiten der betroffenen Personen gemäß der DSGVO/BDSG vorgesehenen Maßnahmen und Garantien, Sicherheitsvorkehrungen und Verfahren, die den Schutz der persönlichen Daten sicherstellen,
    - Nachweis für die Einhaltung der gesetzlichen Vorgaben,
    - Kontaktdaten des Datenschutzbeauftragten,
    - Datenschutzfolgeabschätzung,
    - sonstige von der Aufsichtsbehörde angeforderte Informationen.
13) Der Auftragnehmer erhält für seine Unterstützungsleistung nach diesem Paragraphen eine Vergütung in Höhe des nachgewiesenen Aufwandes zu den vereinbarten Konditionen (Stundensätzen).

§ 9 Löschung/Rückgabe der personenbezogenen Daten

1) Der Auftragnehmer ist verpflichtet, nach Abschluss der Erbringung der Verarbeitungsleistungen alle personenbezogenen Daten nach Weisung des Auftraggebers entweder zu löschen oder zurückzugeben, sofern nicht nach dem Unionsrecht oder dem deutschen Datenschutzrecht eine Verpflichtung zur Speicherung der personenbezogenen Daten besteht. Entstehen zusätzliche Kosten durch abweichende Vorgaben des Auftraggebers bei der Herausgabe oder Löschung der Daten, so trägt diese der Auftraggeber.

§ 10 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 Auftraggeber den Auftragnehmer bei der Abwehr des Anspruchs im Rahmen seiner Möglichkeiten zu unterstützen.
3) Der Auftraggeber nennt dem Auftragnehmer den Ansprechpartner und dessen Kontaktdaten für im Rahmen des Vertrages anfallende Datenschutzfragen. Der Auftraggeber trägt Sorge für die Aktualität dieser Informationen.

§ 11 Informations- und Nachweispflicht

1) Der Auftragnehmer dokumentiert die Verzeichnisse und Unterlagen sowohl in schriftlicher als auch elektronischer Form.
2) Der Auftragnehmer ist verpflichtet, dem Auftraggeber alle erforderlichen Informationen zum Nachweis der Einhaltung der vorliegenden Vereinbarung zur Verfügung zu stellen.
3) Der Auftragnehmer ist verpflichtet, Überprüfungen, einschließlich Inspektionen, die vom Auftraggeber oder einem anderen von diesem beauftragten Prüfer durchgeführt werden, zu ermöglichen und dazu beizutragen.
4) Der Auftraggeber wird Sorge dafür tragen, dass die Kontrollen nur im erforderlichen Umfang durchgeführt werden. Auf die Betriebsabläufe des Auftragnehmers hat er Rücksicht zu nehmen. Sind die Prüfer nicht zur Amtsverschwiegenheit verpflichtet, hat der Auftraggeber deren Verschwiegenheit durch eine geeignete strafbewehrte Verpflichtungserklärung sicherzustellen.
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.

§ 12 Geheimhaltung

1) Auftraggeber und Auftragnehmer sind wechselseitig verpflichtet, alle Informationen, die sie im Zusammenhang mit der Durchführung des Vertrages erhalten, zeitlich unbegrenzt vertraulich zu behandeln und nur zur Durchführung des Vertrages zu verwenden.
2) Sie sind weiterhin verpflichtet, Informationen, die sie im Zusammenhang mit der Durchführung des Vertrages erhalten oder Teile davon nicht an Dritte weiterzugeben, auch nicht unter einem entsprechenden Geheimhaltungsvertrag.
3) Beiden ist es ferner untersagt, Informationen oder Teile davon ohne vorherige schriftliche Zustimmung des jeweils anderen in irgendeiner Form unmittelbar oder mittelbar zu verwerten.
4) Vorstehende Verpflichtung gilt nicht für solche Informationen, die eine der Parteien nachweisbar von Dritten erhalten hat, ohne zur Geheimhaltung verpflichtet zu sein oder die öffentlich bekannt bzw. allgemein zugänglich waren.
5) Die Beweislast für das Vorliegen eines Ausnahmetatbestandes trägt derjenige, der sich hierauf beruft.
6) Der Auftragnehmer hat alle Beschäftigten und beauftragten Personen, die Leistungen im Zusammenhang mit dem vorliegenden Auftrag erbringen, in schriftlicher Form verpflichtet, alle Daten des Auftraggebers, insbesondere die für den Auftraggeber verarbeiteten personenbezogenen Daten vertraulich zu behandeln.
7) Die Geheimhaltungsverpflichtungen bleiben von einer Beendigung des Vertrages, gleich aus welchem Grunde, unberührt.
8) Sollten die Daten des Auftraggebers beim Auftragnehmer durch Pfändung, Beschlagnahme, Insolvenz- oder Vergleichsverfahren oder durch sonstige Ereignisse Dritter gefährdet werden, so unterrichtet der Auftragnehmer den Auftraggeber darüber unverzüglich. Der Auftragnehmer unterrichtet alle in diesem Zusammenhang Verantwortlichen darüber, dass die Hoheit und das Eigentum an den Daten ausschließlich beim Auftraggeber als „Verantwortlicher" im Sinne des Datenschutzes liegen.
9) Nebenabreden wurden keine getroffen. Änderungen und Ergänzungen des Vertrages bedürfen zu ihrer Wirksamkeit der Schriftform. Das soll auch für das Abbedingen des Schriftformerfordernisses gelten.

§ 13 Anpassungsklausel

1) Sollten eine oder mehrere Bestimmungen des Vertrages, einschließlich 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

Umfang der Datenverarbeitung

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

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)

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.
- Änderungsprotokolle ermöglichen ein Zurücksetzen durch den Zugriff auf Daten zu einem konkreten Zeitpunkt bzw. Ereignis. Über Änderungsprotokolle lassen sich ebenfalls vorherige System- und Datenbankeinstellungen zurücksetzen.
- 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 zu evaluiert.

Im Unternehmen gelten folgende Grundsätze:

- Datenschutz ist Aufgabe des gesamten Unternehmens.
- Die IT-Sicherheit und der Schutz personenbezogener Daten hat oberste Priorität.
- Keine Auftragsdatenverarbeitung ohne entsprechende Weisung des Auftraggebers.

Durch folgende Maßnahmen wird den Grundsätzen Rechnung getragen:

- Zuweisung von Verantwortlichkeiten.
- Risikobewertung (Sicherheitsaudit) durch internen und externen Sicherheitsberater.
- 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: 26. Juni 2018