Allgemeine Geschäftsbedingung zur Auftragsverarbeitung der 4SELLERS GmbH
(Stand: Oktober 2021)

Vorbemerkung

Diese Bedingung beschreibt die Verpflichtungen der Vertragsparteien zum Datenschutz, die sich aus den Verträgen der Parteien ergeben. Sie findet Anwendung auf alle Tätigkeiten, die mit einem Vertrag in Zusammenhang stehen und bei denen Beschäftigte des Auftragnehmers oder durch den Auftragnehmer Beauftragte personenbezogene Daten (»Daten«) des Auftraggebers verarbeiten.
Diese Bedingungen gelten in Bezug auf den Umgang mit personenbezogenen Daten vorrangig gegenüber anderen Regelungen der Vertragspartner. Etwaige Haftungsbeschränkungen insbesondere in Hauptverträgen gelten nicht.

§ 1 Anwendungsbereich, Verantwortlichkeit und Auftragsinhalt

1.1 Der Auftragnehmer verarbeitet personenbezogene Daten im Auftrag des Auftraggebers. Dies umfasst Tätigkeiten, die im jeweiligen Vertrag und ggf. in der Leistungsbeschreibung konkretisiert sind und kann Installation, Konfiguration und Wartung von Hard- und Software auf dem Datenverarbeitungssystem des Auftraggebers beinhalten. Der Auftraggeber ist im Rahmen jedes Vertrages für die Einhaltung der gesetzlichen Bestimmungen der Datenschutzgesetze, insbesondere für die Rechtmäßigkeit der Datenweitergabe an den Auftragnehmer sowie für die Rechtmäßigkeit der Datenverarbeitung allein verantwortlich (»Verantwortlicher« im Sinne des Art. 4 Nr. 7 DS-GVO).

Die datenschutzrechtlichen Pflichten des Auftragnehmers werden in diesen Vertragsbedingungen festgelegt und können vom Auftraggeber danach in schriftlicher Form oder in einem elektronischen Format (Textform) durch einzelne Weisungen geändert, ergänzt oder ersetzt werden (Einzelweisung). Mündliche Weisungen sind unverzüglich schriftlich oder in Textform zu bestätigen. Einzelweisungen, die von den Festlegungen dieses Vertrags abweichen oder zusätzliche Anforderungen aufstellen, bedürfen einer vorherigen Zustimmung des Auftragnehmers.

1.2 Der Vertrag beginnt mit der Inbetriebnahme der beauftragten Umgebungen und erfolgt auf unbestimmte Zeit bis zur Kündigung dieses Vertrags oder des Hauptvertrags durch eine Partei.

1.3 Die personenbezogenen Daten können im Rahmen von Projekt-Realisierungen und einer Störungsbeseitigung eingesehen werden. Für Wartungs- und Kontroll-Arbeiten ist nicht auszuschließen, dass die vom Auftraggeber gesicherten Daten eingesehen werden. Im Rahmen einer Fernwartung können auch die lokalen Daten beim Auftraggeber eingesehen werden. Die personenbezogenen Daten dürfen nur für diesen Zweck verwendet werden.

1.4 Die Art der personenbezogenen Daten ergeben sich aus den Modulen, die laut Hauptvertrag vom Kunden genutzt werden. Die Art der personenbezogenen Daten und deren Verwendungszweck sind für die jeweiligen Module unter https://www.4sellers.de/medien/handbuecher/ in den einzelnen Handbüchern im Abschnitt „Rechtliche Hinweise“ angegeben.

1.5 Kategorien betroffener Personen sind Beschäftigte, Kunden, Lieferanten und Endkunden des Auftraggebers.

§ 2 Pflichten des Auftragnehmers

2.1 Der Auftragnehmer darf Daten von betroffenen Personen nur im Rahmen des Auftrages und der Weisungen des Auftraggebers verarbeiten, außer es liegt ein Ausnahmefall im Sinne des Artikel 28 Abs. 3 a) DS-GVO vor. Der Auftragnehmer informiert den Auftraggeber unverzüglich, wenn er der Auffassung ist, dass eine Weisung gegen anwendbare Gesetze verstößt. Der Auftragnehmer darf die Umsetzung der Weisung solange aussetzen, bis sie vom Auftraggeber bestätigt oder abgeändert wurde.

2.2 Der Auftragnehmer wird in seinem Verantwortungsbereich die innerbetriebliche Organisation so gestalten, dass sie den besonderen Anforderungen des Datenschutzes gerecht wird. Er wird technische und organisatorische Maßnahmen zum angemessenen Schutz der Daten des Auftraggebers treffen, die den Anforderungen der Datenschutz- Grundverordnung (Art. 32 DS-GVO) genügen. Der Auftragnehmer

hat technische und organisatorische Maßnahmen zu treffen, die die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung auf Dauer sicherstellen. Dem Auftraggeber sind diese technischen und organisatorischen Maßnahmen bekannt und er trägt die Verantwortung dafür, dass diese für die Risiken der zu verarbeitenden Daten ein angemessenes Schutzniveau bieten.

Die Änderung der getroffenen Sicherheitsmaßnahmen bleibt dem Auftragnehmer vorbehalten, wobei jedoch sichergestellt sein muss, dass ein angemessenes oder vertraglich vereinbartes Schutzniveau nicht unterschritten wird.

2.3 Der Auftragnehmer unterstützt den Auftraggeber im Rahmen seiner Möglichkeiten bei der Erfüllung der Anfragen und Ansprüche betroffenen Personen gem. Kapitel III der DS-GVO sowie bei der Einhaltung der in Art. 33 bis 36 DS-GVO genannten Pflichten.

2.4 Der Auftragnehmer gewährleistet, dass es den mit der Verarbeitung der Daten des Auftraggebers befassten Mitarbeitern und anderen für den Auftragnehmer tätigen Personen untersagt ist, die Daten außerhalb der Weisungen zu verarbeiten. Ferner gewährleistet der Auftragnehmer, dass sich die zur Verarbeitung der personenbezogenen Daten befugten Personen zur Vertraulichkeit verpflichtet haben oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen. Die Vertraulichkeits-/ Verschwiegenheitspflicht besteht auch nach Beendigung des Auftrages fort.

2.5 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 der betroffenen Personen und spricht sich hierzu unverzüglich mit dem Auftraggeber ab.

2.6 Der Auftragnehmer nennt dem Auftraggeber den Ansprechpartner für im Rahmen des Vertrages anfallende Datenschutzfragen. Der Datenschutzbeauftragte des Auftragnehmers ist folgendermaßen zu kontaktieren:

Dipl.-Inform. Olaf Tenti
Gesellschaft für Datenschutz und Informationssicherheit mbH
Körnerstr. 45, 58095 Hagen

Tel: +49 (0) 2331 / 35 68 32 0
Fax: +49 (0) 2331 / 35 68 32 1
Mail: datenschutz@gdi-mbh.eu

2.7 Der Auftragnehmer gewährleistet, seinen Pflichten nach Art. 32 Abs. 1 lit. d) DS-GVO nachzukommen und ein Verfahren zur regelmäßigen Überprüfung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung einzusetzen.

2.8 Der Auftragnehmer berichtigt oder löscht die vertragsgegenständlichen Daten, wenn der Auftraggeber dies anweist. Ist eine datenschutzkonforme Löschung oder eine entsprechende Einschränkung der Datenverarbeitung nicht möglich, übernimmt der Auftragnehmer die datenschutzkonforme Vernichtung von Datenträgern und sonstigen Materialien auf Grund einer Einzelbeauftragung durch den Auftraggeber oder gibt diese Datenträger an den Auftraggeber zurück, sofern nicht im Vertrag bereits vereinbart.

In besonderen, vom Auftraggeber zu bestimmenden Fällen, erfolgt eine Aufbewahrung bzw. Übergabe, Vergütung und Schutzmaßnahmen hierzu sind gesondert zu vereinbaren, sofern nicht im Vertrag bereits vereinbart.

2.9 Daten, Datenträger sowie sämtliche sonstige Materialien sind nach Auftragsende auf Verlangen des Auftraggebers entweder herauszugeben oder zu löschen.

2.10 Im Falle einer Inanspruchnahme des Auftraggebers durch eine betroffene Person hinsichtlich

etwaiger Ansprüche nach Art. 82 DS-GVO, verpflichtet sich der Auftragnehmer den Auftraggeber bei der Abwehr des Anspruches im Rahmen seiner Möglichkeiten zu unterstützen.

§ 3 Pflichten des Auftraggebers

5.1 Der Auftraggeber hat den Auftragnehmer unverzüglich und vollständig zu informieren, wenn er in den Auftragsergebnissen Fehler oder Unregelmäßigkeiten bzgl. datenschutzrechtlicher Bestimmungen feststellt.

5.2 Im Falle einer Inanspruchnahme des Auftraggebers durch eine betroffene Person hinsichtlich etwaiger Ansprüche nach Art. 82 DS-GVO, gilt §2 Abs. 10 entsprechend.

5.3 Der Auftraggeber nennt dem Auftragnehmer den Ansprechpartner für im Rahmen des Vertrages anfallende Datenschutzfragen.

§ 4 Anfragen betroffener Personen

Wendet sich eine betroffene Person mit Forderungen zur Berichtigung Löschung oder Auskunft an den Auftragnehmer, wird der Auftragnehmer die betroffene Person an den Auftraggeber verweisen, sofern eine Zuordnung an den Auftraggeber nach Angaben der betroffenen Person möglich ist. Der Auftragnehmer leitet den Antrag der betroffenen Person unverzüglich an den Auftraggeber weiter. Der Auftragnehmer unterstützt den Auftraggeber im Rahmen seiner Möglichkeiten auf Weisung soweit vereinbart. Der Auftragnehmer haftet nicht, wenn das Ersuchen der betroffenen Person vom Auftraggeber nicht, nicht richtig oder nicht fristgerecht beantwortet wird.

§ 5 Nachweismöglichkeiten

5.4 Der Auftragnehmer hat die Umsetzung der im Vorfeld der Auftragsvergabe dargelegten und erforderlichen technischen und organisatorischen Maßnahmen vor Beginn der Verarbeitung, insbesondere hinsichtlich der konkreten Auftragsdurchführung zu dokumentieren und dem Auftraggeber auf Anforderung zur Prüfung zu übergeben. Bis zum Widerspruch durch den Auftraggeber werden die dokumentierten Maßnahmen Grundlage des Auftrages. Soweit die Prüfung/ein Audit des Auftraggebers ein Defizit in den dokumentierten technischen-organisatorischen Maßnahmen ergibt, das die Sicherheit der Verarbeitung nicht gewährleistet, werden nach Darlegung der Abweichung durch den Auftraggeber diese Maßnahmen einvernehmlich umgesetzt. Der Auftragnehmer kann die Kosten für die Umsetzung ersetzt verlangen, wenn er Maßnahmen umsetzt, welche über die üblichen Maßnahmen hinausgehen.

5.5 Der Auftragnehmer stellt sicher, dass sich der Auftraggeber von der Einhaltung der Pflichten des Auftragnehmers nach Art. 28 DS-GVO überzeugen kann, wenn der Auftraggeber konkret vorträgt, dass technisch-organisatorische Maßnahmen das Schutzniveau des Art. 32 DSGVO unterschreiten und insgesamt die Sicherheit der Verarbeitung nicht mehr gewährleistet wird. Der Auftraggeber hat dann das Recht, in Abstimmung mit dem Auftragnehmer Überprüfungen durchzuführen oder durch im Einzelfall zu benennende Prüfer durchführen zu lassen. Sollten im Einzelfall Inspektionen durch den Auftraggeber oder einen von diesem beauftragten Prüfer erforderlich sein, werden diese zu den üblichen Geschäftszeiten ohne Störung des Betriebsablaufs nach Anmeldung unter Berücksichtigung einer angemessenen Vorlaufzeit von vier Wochen durchgeführt. Der Auftragnehmer darf diese von der Unterzeichnung einer Verschwiegenheitserklärung hinsichtlich der Daten anderer Kunden und der eingerichteten technischen und organisatorischen Maßnahmen abhängig machen. Sollte der durch den Auftraggeber beauftragte Prüfer in einem Wettbewerbsverhältnis zu dem Auftragnehmer stehen, hat der Auftragnehmer gegen diesen ein Einspruchsrecht.

5.6 Nach Wahl des Auftragnehmers kann eine Inspektion der technischen und organisatorischen Maßnahmen gemäß Anlage 1 anstatt einer Vor-Ort-Kontrolle auch durch die Vorlage eines geeigneten, aktuellen Testats, von Berichten oder Berichtsauszügen unabhängiger Instanzen (z.B. Wirtschaftsprüfer, Revision, Datenschutzbeauftragter, IT-Sicherheitsabteilung, Datenschutzauditoren oder Qualitätsauditoren) oder einer geeigneten Zertifizierung durch IT-Sicherheits- oder Datenschutzaudit – z.B. nach BSI-Grundschutz – („Prüfungsberichts“) erbracht werden, wenn der Prüfungsbericht es dem

Auftraggeber in angemessener Weise ermöglicht, sich von der Einhaltung der technischen und organisatorischen Maßnahmen gemäß Anlage 1 zu diesem Vertrag zu überzeugen. Sofern der Auftraggeber auf Basis tatsächlicher Anhaltspunkte berechtigte Zweifel daran geltend macht, dass diese Prüfberichte bzw. Zertifizierungen unzureichend oder unzutreffend sind, oder besondere Vorfälle im Sinne von Art. 33 Abs. 1 DS-GVO im Zusammenhang mit der Durchführung der Auftragsverarbeitung des Auftraggebers dies rechtfertigen, kann er Vor-Ort-Kontrollen durchführen unter der Maßgabe der Ziffer. 5.2 Satz 3, 4 und 5.

5.7 Sollte eine Datenschutzaufsichtsbehörde oder eine sonstige hoheitliche Aufsichtsbehörde des Auftraggebers eine Inspektion vornehmen, gilt grundsätzlich Ziff. 5.2 Satz 3, 4 und 5 entsprechend. Eine Unterzeichnung einer Verschwiegenheitsverpflichtung ist nicht erforderlich, wenn diese Aufsichtsbehörde einer berufsrechtlichen oder gesetzlichen Verschwiegenheit unterliegt, bei der ein Verstoß nach dem Strafgesetzbuch strafbewehrt ist.

§ 6 Subunternehmer (weitere Auftragsverarbeiter)

6.1 Der Auftragnehmer ist berechtigt, die vertraglich vereinbarten Leistungen bzw. die nachfolgend beschriebenen Teilleistungen unter Einschaltung folgender Subunternehmer durchzuführen:

Hetzner Online GmbH Industriestr. 25, 91710 Gunzenhausen, Deutschland	Kontakt: data-protection@hetzner.com Leistungen: Colocation
CRM Solutions GmbH Kattrepel 2 (Montanhof), 20095 Hamburg, Deutschland	Kontakt: info@crm-solutions-gmbh.de Leistungen: Support, Vertrieb
Greyhound Software GmbH & Co. KG Segelfliegerweg 53, 49324 Melle, Deutschland	Kontakt: datenschutz@greyhound-software.com Leistungen: Kommunikation, Mailversand
Visiosoft GmbH Pöllau 210, 8311 Markt Hartmannsdorf, Österreich	Kontakt: hilfe@visiosoft.at Leistungen: Support, Dienstleistung
parcelLab GmbH Kapellenweg 6, 81371 München, Deutschland	Kontakt: dataprotection@parcellab.com Leistungen: Nachrichtenversand

6.2 Der Auftraggeber stimmt zu, dass der Auftragnehmer weitere Subunternehmer unter folgenden Bedingungen hinzuzieht: 6.2.1 Vor Hinzuziehung oder Ersetzung der Subunternehmer informiert der Auftragnehmer den Auftraggeber mit einer Frist von drei Wochen. 6.2.2 Bis zur geplanten Hinzuziehung oder Ersetzung erklärt der Auftraggeber keinen Widerspruch.

6.2.1 Der Einsatz von Subunternehmern als weiteren Auftragsverarbeiter ist auch dann zulässig, wenn der Auftraggeber vorher zugestimmt hat.

6.2.2 Ein Subunternehmerverhältnis liegt vor, wenn der Auftragnehmer weitere Auftragnehmer mit der ganzen oder einer Teilleistung der im Vertrag vereinbarten Leistung beauftragt. Der Auftragnehmer wird mit diesen Dritten im erforderlichen Umfang Vereinbarungen treffen, um angemessene Datenschutz- und Informationssicherheitsmaßnahmen zu gewährleisten.

6.3 Erteilt der Auftragnehmer Aufträge an Subunternehmer, so obliegt es dem Auftragnehmer, seine datenschutzrechtlichen Pflichten aus diesem Vertrag dem Subunternehmer zu übertragen.

§ 7 Informationspflichten, Schriftformklausel, Rechtswahl

7.1 Sollten die Daten des Auftraggebers beim Auftragnehmer durch Pfändung oder

Beschlagnahme, durch ein Insolvenz- oder Vergleichsverfahren oder durch sonstige Ereignisse oder Maßnahmen Dritter gefährdet werden, so hat der Auftragnehmer den Auftraggeber unverzüglich darüber zu informieren. Der Auftragnehmer wird alle in diesem Zusammenhang Verantwortlichen unverzüglich darüber informieren, dass die Hoheit und das Eigentum an den Daten ausschließlich beim Auftraggeber als »Verantwortlicher « im Sinne der Datenschutz-Grundverordnung liegen.

7.2 Änderungen und Ergänzungen dieser Bedingungen und aller ihrer Bestandteile – einschließlich etwaiger Zusicherungen des Auftragnehmers – bedürfen einer schriftlichen Vereinbarung, die auch in einem elektronischen Format (Textform) erfolgen kann, und des ausdrücklichen Hinweises darauf, dass es sich um eine Änderung bzw. Ergänzung dieser Bedingungen handelt. Dies gilt auch für den Verzicht auf dieses Formerfordernis.

7.3 Bei etwaigen Widersprüchen gehen Regelungen dieser Anlage zum Datenschutz den Regelungen des Vertrages vor. Sollten einzelne Teile dieser Bedingungen unwirksam sein, so berührt dies die Wirksamkeit der Anlage im Übrigen nicht.

7.4 Auftraggeber und Auftragnehmer vereinbaren, dass zeitgleich mit Beginn dieser Vertragsbedingungen die zwischen den Parteien bestehende Vereinbarung zur Auftragsdatenverarbeitung gemäß § 11 Bundesdatenschutzgesetz sowie etwaige weitere Vereinbarungen zur Auftragsdatenverarbeitung einvernehmlich aufgehoben und durch diese neue Vereinbarung zur Auftragsverarbeitung ersetzt werden.

7.5 Alle in diesen Bedingungen enthaltenen Verweise auf die DS-GVO gelten für die DS-GVO in ihrer jeweils aktuellen Fassung bzw. etwaige Nachfolgeregelungen.

7.6 Es gilt deutsches Recht.

Anhang 1

Technische und Organisatorische Maßnahmen (TOM)

gemäß Artikel 32 DSGVO

der

4SELLERS GmbH

Stand: Oktober 2021

Dieses Dokument beschreibt die technischen und organisatorischen Maßnahmen der 4SELLERS GmbH.

Gemäß Artikel 32 der europäischen Datenschutzgrundverordnung hat ein Verantwortlicher bei der Verarbeitung von personenbezogenen Daten für diese ein ausreichendes Schutzniveau durch die Wahl und Anwendung seiner Maßnahmen herzustellen.
Technische Maßnahmen beziehen sich auf den Datenverarbeitungsvorgang als solches. Sie bezeichnen alle Maßnahmen, die sich physisch umsetzen lassen, zum Beispiel durch das Installieren einer Alarmanlage oder Benutzerkonten, die passwortgeschützt sind.
Organisatorische Maßnahmen beziehen sich auf die Rahmenbedingungen des Datenverarbeitungsvorgangs. Sie umfassen Regeln, Vorgaben und Handlungsanweisungen, die dazu dienen, dass Mitarbeiter den Datenschutz gesetzestreu einhalten.
Diese Maßnahmen sind unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen durch den Verantwortliche zu treffen.
Die Angemessenheit einer Schutzmaßnahme richtet sich dabei nach dem immanenten Risiko.

Im Folgenden werden anhand der in Art. 32 Absatz 1 DSGVO abstrakt benannten Maßnahmen, die einzelnen spezifischen technischen und organisatorischen Umsetzungen der Verarbeitungsvorgänge der Verantwortlichen beschrieben. Diese beziehen sich auf die im Verzeichnis von Verarbeitungstätigkeiten dargestellten Prozesse. Das Dokument orientiert sich an den in Art. 32 DSGVO aufgelisteten Kategorien.
Der Stand der technischen und organisatorischen Maßnahmen obliegt dabei einem stetigen Entwicklungsprozess.

Technische und organisatorische Maßnahmen der 4SELLERS GmbH als Auftragnehmer

Im Folgenden werden die technischen und organisatorischen Maßnahmen zur Gewährleistung von Datenschutz und Datensicherheit festgelegt. Ziel ist die Gewährleistung insbesondere der **Vertraulichkeit, Integrität, Belastbarkeit und Verfügbarkeit** der verarbeiteten Informationen.

Die hier genannten Maßnahmen beziehen sich auf die Büroumgebung. Das Rechenzentrum ist nach ISO 27001 zertifiziert.

A. Vertraulichkeit (Art. 32 Abs. 1 lit. b DS-GVO)

(Technische und organisatorische Maßnahmen, welche die Vertraulichkeit der Systeme und Dienste schützen, sollen verhindern, dass es zu einer unbefugten Datenverarbeitung kommt)

1. Zutrittskontrolle

(kein unbefugter Zutritt zu Räumlichkeiten und Datenverarbeitungsanlagen)

In dem Bürogebäude:

- Verwendung von Gruppenkonzepten zur Festlegung zutrittsberechtigter Personen
- Abgrenzung sicherheitsrelevanter Bereiche
- Authentifikation über Transponder in einigen Bereichen
- Separate Zutrittsregelungen für Gebäude, Zonen, Räume und Serverracks.
- Minimierung von Zugriffsrechten
- Schlüsselvergabe und –einzug werden dokumentiert, Rechtevergabe wird protokolliert.
- Zugang für Dritte zum Gebäude nur mit Klingel, Tür ist immer verschlossen.
- Gäste werden in einem zentralen Bereich abgeholt und bewegen sich nur unter Aufsicht durch das Gebäude.

2. Zugangskontrolle

(Verhinderung der unbefugten Benutzung der Datenverarbeitungssysteme)

- Authentisierung am System

  Verwendung von Benutzername/Passwort
  - Forderung einer unterschiedlichen Zeichenzusammensetzung (Passwortkomplexität) entsprechend der Microsoft Active Directory-Richtlinie
  - Mindestlänge festgelegt (min. 8 Zeichen)
  - Verbot von Trivialpasswörtern
  - Frist zur Passwortänderung festgelegt (90 Tage)
  - Erstanmeldeprozedur festgelegt (der Mitarbeiter erhält das erste Passwort vom Administrator und wird dann aufgefordert, dieses zu ändern)
  - Zugangssperre bei wiederholten Fehlversuchen bei der Anmeldung

- Anmeldung nach Inaktivität erforderlich (automatische Zugangssperre)
- Zugangsprotokollierung
  - Zugangsversuche werden protokolliert (verwendete Kennung, Rechner, IMEI, IP- oder Macadresse) entsprechend der Microsoft Active Directory-Richtlinie
  - Zugriffsregelung auf Protokolle
  - Auf die Protokolle haben nur bestimmte Personen Zugriff
- Zugangsberechtigte Personen
  - Anmeldedaten sind einer bestimmten Person zuzuordnen
  - Zugangsberechtigte Personen(-gruppen) sinnvoll in Bezug auf Erforderlichkeit der Zugangsberechtigung eingeteilt (auf das notwendige Minimum beschränkt)
- Standardmäßig verschlüsselte Übertragung der Authentisierungsgeheimnisse oder per Telefon
- Firewall
  - Verwendung einer Firewall
  - Verantwortliche Personen für Wartung, Regeländerung, etc. festgelegt
  - Vorgaben für die Installation von Updates
- Der Remote Zugriff auf die Unternehmensserver erfolgt mit 2-Faktor-Authentifizierung (zB für Bereitschaftsdienst)

3. Zugriffskontrolle

(Verhinderung von unbefugtem Lesen, Kopieren, Verändern oder Entfernen innerhalb des Datenverarbeitungssystems)

- Zugriffsrechte
  - Umfang der Berechtigung wird auf das notwendige Minimum beschränkt
- Berechtigungskonzept
  - Definierte Vorgehensweise für das Anlegen, Ändern und Löschen von Berechtigungsprofilen/Benutzerrollen
  - Berechtigungen sind an eine Person, bzw. ein Account geknüpft
  - Entziehung von Zugriffsberechtigungen, wenn die Grundlage für diese Berechtigung entfällt
- Interne Anweisung über die Verwendung (Ausgabe, Nutzung, Vernichtung) von Datenträgern ist vorhanden
- Datentonne zur datenschutzkonformen Vernichtung von Festplatten/SSD über einen zertifizierten Anbieter mit Zertifikat über die Vernichtung
- Protokollierung
  - Protokollierung von Datenträgervernichtung (und 24-Monatige revisionssichere Aufbewahrung)
- Wenn Daten vom bzw. an den Kunden übertragen werden, ist technisch gewährleistet, dass die Übertragung verschlüsselt stattfindet (z.B. sftp)

4. Trennungskontrolle (Art. 32 Abs. 1 lit. a DS-GVO)

(Maßnahmen zur Trennungskontrolle die gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können. Dieses kann

beispielsweise durch logische und physikalische Trennung der Daten gewährleistet werden)

- Physikalische und logische Trennung der verarbeitenden Systeme
- Sparsamkeit bei der Datenerhebung
  - Nur zweckgemäße und notwendige Datenerhebung, -speicherung und -verarbeitung
- Es besteht eine Trennung von Test- und Produktionsbetrieb

B. Integrität, Weitergabekontrolle, Auftragskontrolle und Fernwartung (Art. 32 Abs. 1 b DSGVO)

1. Weitergabekontrolle

(Kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen bei elektronischer Übertragung oder Transport)

- Empfangs-/Weitergabeberechtigungen festgelegt (Berechtigungskonzept)
- Daten werden nicht außerhalb der EU verarbeitet oder erhoben die dem Telekommunikationsgesetz unterliegen
- Protokollierung findet statt (Übermittlung; Sender/Empfänger), soweit die technischen Voraussetzungen gegeben sind.
- Datenübertragung zwischen Client und Server erfolgt standardmäßig verschlüsselt
- Firewalls
  - Verwendung von Hardware-Firewalls
  - Firewalls stets aktiv und für Nutzer nicht deaktivierbar

2. Eingabekontrolle

(Feststellung, ob und von wem personenbezogene Daten in Datenverarbeitungssystemen eingegeben, verändert oder entfernt worden sind)

- Systeme zur Protokollierung und Protokollauswertung
  - Eingaben von personenbezogenen Daten werden protokolliert
  - Geregelte Zugriffsrechte auf Protokolle
  - Protokollauswertungsroutine
- Dokumentation der Eingabeverfahren
  - Befugte für das Vornehmen von Eingaben in der Datenverarbeitungsanlage sind festgelegt

3. Fernwartung

- Software für die Fernwartung ist selbstgehostet
- Verschlüsselter Zugang
- Fernwartung ist in den Leistungsverträgen mit abgedeckt

4. Auftragskontrolle

- Auftragsnehmerauswahl und Weisungserteilung und -entgegennahme
  - Festgelegte Personen für die Auswahl, Weisungserteilung, -entgegennahme
- Regelungen der Auftragsausführung sind in der Leistungsbeschreibung niedergelegt und ergänzen ggf. die Regelungen des Auftragsverarbeitungsvertrages nach Art. 28 DS-GVO
- Reinigungs-, Entsorgungspersonal und andere Dienstleister werden sorgfältig ausgewählt

C. Verfügbarkeit und Belastbarkeit (Art. 32 Abs. 1 lit. b DS-GVO)

(Technische und organisatorische Maßnahmen, welche die Verfügbarkeit und Belastbarkeit der Systeme absichern, sollen sicherstellen, dass das verantwortliche Unternehmen auch in Notfallsituationen noch agieren kann und die personenbezogenen Daten gegen eine zufällige Zerstörung oder Verlust geschützt sind.)

- Brandschutzeinrichtungen
  - Feuerlöscher vorhanden
- Geltendes Rauchverbot
- Stromversorgung
  - USV
  - Überspannungsschutzeinrichtung
- Notfalleinrichtungen werden regelmäßig geprüft
- Klimaversorgung Serverraum
- Datensicherungskonzept (und Einhaltung inkl. nötiger Maßnahmen)
- Festplattenspiegelung

D. Wiederherstellbarkeit der Daten und des Datenzugangs nach physischem oder technischem Zwischenfall und Kontrollverfahren

1. Datensicherung (Art. 32 Abs. 1 lit. c DS-GVO)

- Datensicherungskonzept ist vorhanden
  - Backups finden täglich statt
  - Verantwortliche Personen festgelegt
  - Regelmäßige Überprüfung auf Rückspiel-Möglichkeit eines Backups
  - Regelmäßige Sicherung der wichtigsten Datenbanken und Systeme
  - Standort der Backupserver in einem anderen Brandabschnitt als Produktivumgebung

2. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung (Art. 32 Abs. 1 lit. d DS-GVO)

- Die vorhandenen Dokumentationen der Datensicherheit werden regelmäßig auf Aktualität geprüft
- Jährliche Audits des externen Datenschutzbeauftragten

3. Organisatorische Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung (Art. 32 Abs. 1 lit. d DS-GVO)

- Ein externer Datenschutzbeauftragter ist bestellt und an die Behörde gemeldet
- Umsetzung von Schulungsmaßnahmen
  - Grundsätze Datenschutz und TOM
  - Die Mitarbeiter sind schriftlich auf die Vertraulichkeit verpflichtet
  - Schweigepflicht über Betriebs- und Geschäftsgeheimnisse
  - Ordnungsgemäßer Umgang mit Daten, Dateien, etc.
  - Fernmeldegeheimnis
  - Schulungen werden dokumentiert
- Vertreter für alle betriebsnotwendigen Aufgaben/Funktionen festgelegt
- Regelungen über Betrieb und Abläufe der Datenverarbeitung und Datensicherungsmaßnahmen
- Ein Prozess zur Risikoanalyse bzgl. neuer Verarbeitungen und einer u.U. notwendigen Datenschutzfolgenabschätzung ist vorhanden
- Die Prozesse für
  - den Umgang mit Datenschutzvorfällen und
  - die Wahrnehmung von Betroffenenrechten sind dokumentiert bekannt gegeben.
- Externe Dienstleister werden schriftlich auf die Vertraulichkeit verpflichtet
- Die private Nutzung der betrieblichen Kommunikationstechnik ist verboten