Vertrag zur Auftragsverarbeitung gemäß Art. 28 DS-GVO

[Basis: Mustervertrag GDD, Stand: Mai 2017]

Vereinbarung

zwischen dem/der

.....

- Verantwortlicher - nachstehend Auftraggeber genannt -

und dem/der

PCS GmbH

Boschetsrieder Straße 67-69

81379 München

Deutschland

- Auftragsverarbeiter - nachstehend Auftragnehmer genannt

[ggf.: Vertreter gemäß Art. 27 DS-GVO]

1. Gegenstand und Dauer des Auftrags

(1) Gegenstand

Der Gegenstand des Auftrags ergibt sich aus dem Telekommunikationsvertrag, auf den hier verwiesen wird (im Folgenden Leistungsvereinbarung).

(2) Dauer

Die Dauer dieses Auftrags (Laufzeit) entspricht der Laufzeit der Leistungsvereinbarung.

2. Konkretisierung des Auftragsinhalts

(1) Art und Zweck der vorgesehenen Verarbeitung von Daten

Art und Zweck der Verarbeitung personenbezogener Daten durch den Auftragnehmer für den Auftraggeber sind konkret beschrieben in der o.g. Leistungsvereinbarung.

Die Erbringung der vertraglich vereinbarten Datenverarbeitung findet ausschließlich in einem Mitgliedsstaat der Europäischen Union oder in einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum statt.

(2) Art der Daten

Gegenstand der Verarbeitung personenbezogener Daten sind folgende Datenarten/-kategorien (Aufzählung/Beschreibung der Datenkategorien)

- Kommunikationsdaten (z.B. Telefon, E-Mail)
- Vertragsstammdaten (Vertragsbeziehung, Produkt- bzw. Vertragsinteresse)
- Kundenhistorie
- Vertragsabrechnungs- und Zahlungsdaten

(3) Kategorien betroffener Personen

Die Kategorien der durch die Verarbeitung betroffenen Personen umfassen Kunden, Interessenten, Mitarbeiter und Lieferanten des Auftraggebers.

3. Technisch-organisatorische Maßnahmen

(1) 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 zur Prüfung zu übergeben. Bei Akzeptanz durch den Auftraggeber werden die dokumentierten Maßnahmen Grundlage des Auftrags. Soweit die Prüfung/ein Audit des Auftraggebers einen Anpassungsbedarf ergibt, ist dieser einvernehmlich umzusetzen.

(2) Der Auftragnehmer hat die Sicherheit gem. Art. 28 Abs. 3 lit. c, 32 DS-GVO insbesondere in Verbindung mit Art. 5 Abs. 1, Abs. 2 DS-GVO herzustellen. Insgesamt handelt es sich bei den zu treffenden Maßnahmen um Maßnahmen der Datensicherheit und zur Gewährleistung eines dem Risiko angemessenen Schutzniveaus hinsichtlich der Vertraulichkeit, der Integrität, der Verfügbarkeit sowie der Belastbarkeit der Systeme. Dabei sind der Stand der Technik, die Implementierungskosten und die Art, der Umfang und die Zwecke der Verarbeitung sowie die unterschiedliche Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen im Sinne von Art. 32 Abs. 1 DS-GVO zu berücksichtigen [Einzelheiten in Anlage 1].

(3) Die technischen und organisatorischen Maßnahmen unterliegen dem technischen Fortschritt und der Weiterentwicklung. Insoweit ist es dem Auftragnehmer gestattet, alternative adäquate Maßnahmen umzusetzen. Dabei darf das Sicherheitsniveau der festgelegten Maßnahmen nicht unterschritten werden. Wesentliche Änderungen sind zu dokumentieren.

4. Berichtigung, Einschränkung und Löschung von Daten

(1) Der Auftragnehmer darf die Daten, die im Auftrag verarbeitet werden, nicht eigenmächtig, sondern nur nach dokumentierter Weisung des Auftraggebers berichtigen, löschen oder deren Verarbeitung

einschränken. Soweit eine betroffene Person sich diesbezüglich unmittelbar an den Auftragnehmer wendet, wird der Auftragnehmer dieses Ersuchen unverzüglich an den Auftraggeber weiterleiten.

(2) Soweit vom Leistungsumfang umfasst, sind Löschkonzept, Recht auf Vergessenwerden, Berichtigung, Datenportabilität und Auskunft nach dokumentierter Weisung des Auftraggebers unmittelbar durch den Auftragnehmer sicherzustellen.

5. Qualitätssicherung und sonstige Pflichten des Auftragnehmers

Der Auftragnehmer hat zusätzlich zu der Einhaltung der Regelungen dieses Auftrags gesetzliche Pflichten gemäß Art. 28 bis 33 DS-GVO; insofern gewährleistet er insbesondere die Einhaltung folgender Vorgaben:

a) Schriftliche Bestellung eines Datenschutzbeauftragten, der seine Tätigkeit gemäß Art. 38 und 39 DS-GVO ausübt. Dessen jeweils aktuelle Kontaktdaten sind auf der Homepage des Auftragnehmers leicht zugänglich hinterlegt.
b) Die Wahrung der Vertraulichkeit gemäß Art. 28 Abs. 3 S. 2 lit. b, 29, 32 Abs. 4 DS-GVO. Der Auftragnehmer setzt bei der Durchführung der Arbeiten nur Beschäftigte ein, die auf die Vertraulichkeit verpflichtet und zuvor mit den für sie relevanten Bestimmungen zum Datenschutz vertraut gemacht wurden. Der Auftragnehmer und jede dem Auftragnehmer unterstellte Person, die Zugang zu personenbezogenen Daten hat, dürfen diese Daten ausschließlich entsprechend der Weisung des Auftraggebers verarbeiten einschließlich der in diesem Vertrag eingeräumten Befugnisse, es sei denn, dass sie gesetzlich zur Verarbeitung verpflichtet sind.
c) Die Umsetzung und Einhaltung aller für diesen Auftrag erforderlichen technischen und organisatorischen Maßnahmen gemäß Art. 28 Abs. 3 S. 2 lit. c, 32 DS-GVO [Einzelheiten in Anlage 1].
d) Der Auftraggeber und der Auftragnehmer arbeiten auf Anfrage mit der Aufsichtsbehörde bei der Erfüllung ihrer Aufgaben zusammen.
e) Die unverzügliche Information des Auftraggebers über Kontrollhandlungen und Maßnahmen der Aufsichtsbehörde, soweit sie sich auf diesen Auftrag beziehen. Dies gilt auch, soweit eine zuständige Behörde im Rahmen eines Ordnungswidrigkeits- oder Strafverfahrens in Bezug auf die Verarbeitung personenbezogener Daten bei der Auftragsverarbeitung beim Auftragnehmer ermittelt.
f) Soweit der Auftraggeber seinerseits einer Kontrolle der Aufsichtsbehörde, einem Ordnungswidrigkeits- oder Strafverfahren, dem Haftungsanspruch einer betroffenen Person oder eines Dritten oder einem anderen Anspruch im Zusammenhang mit der Auftragsverarbeitung beim Auftragnehmer ausgesetzt ist, hat ihn der Auftragnehmer nach besten Kräften zu unterstützen.
g) Der Auftragnehmer kontrolliert regelmäßig die internen Prozesse sowie die technischen und organisatorischen Maßnahmen, um zu gewährleisten, dass die Verarbeitung in seinem Verantwortungsbereich im Einklang mit den Anforderungen des geltenden Datenschutzrechts erfolgt und der Schutz der Rechte der betroffenen Person gewährleistet wird.
h) Nachweisbarkeit der getroffenen technischen und organisatorischen Maßnahmen gegenüber dem Auftraggeber im Rahmen seiner Kontrollbefugnisse nach Ziffer 7 dieses Vertrages.

6. Unterauftragsverhältnisse

(1) Als Unterauftragsverhältnisse 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 Telekommunikationsleistungen, Post-/ Transportdienstleistungen, Wartung und Benutzerservice 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 Auftragnehmer darf Unterauftragnehmer (weitere Auftragsverarbeiter) nur nach vorheriger ausdrücklicher schriftlicher bzw. dokumentierter Zustimmung des Auftraggebers beauftragen.
Die Auslagerung auf Unterauftragnehmer oder der Wechsel des bestehenden Unterauftragnehmers sind zulässig, soweit:

- der Auftragnehmer eine solche Auslagerung auf Unterauftragnehmer dem Auftraggeber eine angemessene Zeit vorab schriftlich oder in Textform anzeigt und
- der Auftraggeber nicht bis zum Zeitpunkt der Übergabe der Daten gegenüber dem Auftragnehmer schriftlich oder in Textform Einspruch gegen die geplante Auslagerung erhebt und
- eine vertragliche Vereinbarung nach Maßgabe des Art. 28 Abs. 2-4 DS-GVO zugrunde gelegt wird.

(3) Die Weitergabe von personenbezogenen Daten des Auftraggebers an den Unterauftragnehmer und dessen erstmaliges Tätigwerden sind erst mit Vorliegen aller Voraussetzungen für eine Unterbeauftragung gestattet.

(4) Erbringt der Unterauftragnehmer die vereinbarte Leistung außerhalb der EU/des EWR stellt der Auftragnehmer die datenschutzrechtliche Zulässigkeit durch entsprechende Maßnahmen sicher. Gleiches gilt, wenn Dienstleister im Sinne von Abs. 1 Satz 2 eingesetzt werden sollen.

(5) Eine weitere Auslagerung durch den Unterauftragnehmer bedarf der ausdrücklichen Zustimmung des Hauptauftragnehmers (mind. Textform); sämtliche vertraglichen Regelungen in der Vertragskette sind auch dem weiteren Unterauftragnehmer aufzuerlegen.

7. Kontrollrechte des Auftraggebers

(1) Der Auftraggeber hat das Recht, im Benehmen mit dem Auftragnehmer Überprüfungen durchzuführen oder durch im Einzelfall zu benennende Prüfer durchführen zu lassen. Er hat das Recht, sich durch Stichprobenkontrollen, die in der Regel rechtzeitig anzumelden sind, von der Einhaltung dieser Vereinbarung durch den Auftragnehmer in dessen Geschäftsbetrieb zu überzeugen.

(2) Der Auftragnehmer stellt sicher, dass sich der Auftraggeber von der Einhaltung der Pflichten des Auftragnehmers nach Art. 28 DS-GVO überzeugen kann. Der Auftragnehmer verpflichtet sich, dem Auftraggeber auf Anforderung die erforderlichen Auskünfte zu erteilen und insbesondere die Umsetzung der technischen und organisatorischen Maßnahmen nachzuweisen.

(3) Der Nachweis solcher Maßnahmen, die nicht nur den konkreten Auftrag betreffen, kann erfolgen durch aktuelle Testate, Berichte oder Berichtsauszüge unabhängiger Instanzen (z.B. Wirtschaftsprüfer, Revision, Datenschutzbeauftragte, IT-Sicherheitsabteilung, Datenschutz- oder Qualitätsauditoren) oder durch seitens der Aufsichtsbehörden zugelassene Datenschutzzertifikate.

(4) Für die Ermöglichung von Kontrollen durch den Auftraggeber kann der Auftragnehmer einen Vergütungsanspruch geltend machen.

8. Mitteilung bei Verstößen des Auftragnehmers

(1) Der Auftragnehmer unterstützt den Auftraggeber bei der Einhaltung der in den Artikeln 32 bis 36 der DS-GVO genannten Pflichten zur Sicherheit personenbezogener Daten, Meldepflichten bei Datenpannen, Datenschutz-Folgeabschätzungen und vorherige Konsultationen. Hierzu gehören u.a.

a) die Sicherstellung eines angemessenen Schutzniveaus durch technische und organisatorische Maßnahmen, die die Umstände und Zwecke der Verarbeitung sowie die prognostizierte Wahrscheinlichkeit und Schwere einer möglichen Rechtsverletzung durch Sicherheitslücken berücksichtigen und eine sofortige Feststellung von relevanten Verletzungsereignissen ermöglichen
b) die Verpflichtung, Verletzungen personenbezogener Daten unverzüglich an den Auftraggeber zu melden
c) die Verpflichtung, dem Auftraggeber im Rahmen seiner Informationspflicht gegenüber dem Betroffenen zu unterstützen und ihm in diesem Zusammenhang sämtliche relevante Informationen unverzüglich zur Verfügung zu stellen
d) die Unterstützung des Auftraggebers für dessen Datenschutz-Folgenabschätzung
e) die Unterstützung des Auftraggebers im Rahmen vorheriger Konsultationen mit der Aufsichtsbehörde

(2) Für Unterstützungsleistungen, die nicht in der Leistungsbeschreibung enthalten oder nicht auf ein Fehlverhalten des Auftragnehmers zurückzuführen sind, kann der Auftragnehmer eine Vergütung beanspruchen.

9. Weisungsbefugnis des Auftraggebers

(1) Mündliche Weisungen bestätigt der Auftraggeber unverzüglich (mind. Textform).

(2) Der Auftragnehmer hat den Auftraggeber unverzüglich zu informieren, wenn er der Meinung ist, eine Weisung verstoße gegen Datenschutzvorschriften. Der Auftragnehmer ist berechtigt, die Durchführung der entsprechenden Weisung solange auszusetzen, bis sie durch den Auftraggeber bestätigt oder geändert wird.

10. Löschung und Rückgabe von personenbezogenen Daten

(1) Kopien oder Duplikate der Daten werden ohne Wissen des Auftraggebers nicht erstellt. Hiervon ausgenommen sind Sicherheitskopien, soweit sie zur Gewährleistung einer ordnungsgemäßen Datenverarbeitung erforderlich sind, sowie Daten, die im Hinblick auf die Einhaltung gesetzlicher Aufbewahrungspflichten erforderlich sind.

(2) Nach Abschluss der vertraglich vereinbarten Arbeiten oder früher nach Aufforderung durch den Auftraggeber – spätestens mit Beendigung der Leistungsvereinbarung – hat der Auftragnehmer sämtliche in seinen Besitz gelangten Unterlagen, erstellte Verarbeitungs- und Nutzungsergebnisse sowie Datenbestände, die im Zusammenhang mit dem Auftragsverhältnis stehen, dem Auftraggeber auszuhändigen oder nach vorheriger Zustimmung datenschutzgerecht zu vernichten. Gleiches gilt für Test- und Ausschussmaterial. Das Protokoll der Löschung ist auf Anforderung vorzulegen.

(3) Dokumentationen, die dem Nachweis der auftrags- und ordnungsgemäßen Datenverarbeitung dienen, sind durch den Auftragnehmer entsprechend der jeweiligen Aufbewahrungsfristen über das Vertragsende hinaus aufzubewahren. Er kann sie zu seiner Entlastung bei Vertragsende dem Auftraggeber übergeben.

Akzeptiert durch Auftraggeber	Akzeptiert durch Auftragnehmer
Kunde	PCS München GmbH
Straße	Boschetsrieder Straße 67-69
D- PLZ-	81379 München
…….	…….
Unterschrift	Unterschrift
…….	Mario Zuppa
Name in Druckbuchstaben	Name in Druckbuchstaben
…….	GF
Position	Position
…….	…….
Datum	Datum

Anlage- Technische und organisatorische Maßnahmen (TOM)

Nr.	Gebiet	Beschreibung
1	Organisation	
1.1	Wie ist die Umsetzung des Datenschutzes organisiert?	Ein externer Datenschutzbeauftragter wird zur Wahrnehmung der Kontrollfunktion aus dem DSGVO eingesetzt.
1.2	Wenn Sie einen Datenschutzbeauftragten bestellt haben, geben Sie uns bitte den Namen und die Kontaktdaten an.	Philip Essinger, Essinger Consulting, Telefonnummer Tel: 089-461389-13, E-Mail: datenschutz@essinger.consulting.de
1.3	Welche organisatorischen Maßnahmen wurden getroffen, damit die Verarbeitung personenbezogener Daten gesetzeskonform erfolgt?	Mitarbeiter Verpflichtungen wurden schriftlich, zur Wahrnehmung des Datenschutz, vereinbart. Die Mitarbeiter werden regelmäßig zum Datenschutz geschult.
1.4	Wie stellen Sie sicher, dass die internen Prozesse gemäß den aktuellen Datenschutzbestimmungen ablaufen und regelmäßig geprüft werden?	Eine konstante monatliche Sensibilisierung der Mitarbeiter und regemäßige Prüfungen der Abläufe im Unternehmen wird durchgeführt.
1.5	In welcher Form werden die Mitarbeiter auf die Umsetzung der vereinbarten technischen und organisatorischen Maßnahmen geschult, die für diese Verarbeitung in Anwendung kommen?	Mitarbeiter erhalten eine Datenschutzunterweisung.
1.6	Sind die Verarbeitungen hinsichtlich datenschutzrechtlicher Zulässigkeit dokumentiert?	Ja
2	Zutrittskontrolle	
2.1	Wie werden die Gebäude, in denen die Verarbeitung stattfindet, vor unbefugtem Zutritt gesichert?	Das Gebäude ist mit einer Sicherheits-Schließanlage ausgestattet. Verschlossener Eingang mit Klingel. Empfang mit Gästebuch und Portiere.
2.2	Wie werden die Räume/Büros, in denen die Verarbeitung stattfindet, vor unbefugtem Zutritt gesichert?	Alarmanlage im Gebäudeanteil der Firma. Die Räume werden ebenfalls durch das Sicherheitsschließsystem gesichert. Videoüberwachungssystem überwacht die Zugänge.
2.3	Wie werden die Verarbeitungsanlagen vor unbefugtem Zugriff geschützt?	Abschließbare, dezentrale Serverschränke, dokumentierte Zutrittskontrolle für Externe.
2.4	Wie werden die umgesetzten Zutrittskontrollen auf Tauglichkeit geprüft?	Im Rahmen der Kontrollen durch den Datenschutzbeauftragten werden auch die Zutrittskontrollmaßnahmen überprüft.

Nr.	Gebiet	Beschreibung
3	Zugangskontrolle	
3.1	Wie erfolgt die Vergabe von Benutzerzugängen?	Benutzerzugänge werden nur sehr selektiv und nach Genehmigung durch die GF und Abteilungsleiter vergeben. Rechtevergabe und Änderungen sind dokumentiert. Zugriff auf kaufmännische Dokumente und Kommunikationsinformationen sind Passwort geschützt. Mitarbeiter erhalten bei Eintritt MS AD-Accounts, die Berechtigungen werden über AD-Gruppen geregelt.
3.2	Wie wird die Gültigkeit von Benutzerzugängen überprüft?	Eine regelmäßige Revision der vergebenen Rechte ist ein Teil der Prüfung und der Maßnahmen. Dieser Vorgang wird zusammen mit dem Datenschutzbeauftragten durchgeführt. Die Abteilungsleiter bzw. GF sind verpflichtet, relevante Änderungen in Beschäftigungsverhältnissen rechtzeitig der Administration anzuzeigen.
3.3	Wie werden Benutzerzugänge inkl. Antragstellung, Genehmigungsverfahren etc. dokumentiert?	Anforderungen zu Benutzerzugängen können nur von den Abteilungsleitern bzw. GF per Mail beantragt bzw. genehmigt werden. Dies wird von der Administration per Mail bestätigt. Der Verlauf wird über Mail-Archivierung festgehalten.
3.4	Wie wird sichergestellt, dass die Anzahl von Administrationszugängen ausschließlich auf die notwendige Anzahl reduziert ist und nur fachlich und persönlich geeignetes Personal hierfür eingesetzt wird?	Es wird streng auf Datensparsamkeit geachtet, um nach Art. 5 Abs. 1 lt. C dem Grundsatz "Datenminimierung" zu folgen. Der Systemadministrator arbeitet nach dem "Need-to-Know"-Prinzip und überprüft regelmäßig die Zugänge und deren Berechtigungen. Alle betreffenden und infrage kommenden Personen besitzen einen nachweislich fachlichen IT-Hintergrund. Sie sind weder temporär noch als externe Mitarbeiter beschäftigt, befinden sich nicht in der Probezeit, und wurden auf die "Verpflichtung auf das Datengeheimnis nach gesetzlichen Vorgaben der DSGVO" des Unternehmens verpflichtet.
3.5	Ist ein Zugriff auf die Systeme/Anwendungen von außerhalb des Unternehmens möglich (Heimarbeitsplätze, Dienstleister etc.)? Wie ist der Zugang gestaltet?	Der Zugriff ist über eine verschlüsselte VPN-Verbindung (L2TP) für explizit freigegebene Mitarbeiter möglich. Die Authentifizierung erfolgt über MS-AD Anmeldedaten.

Nr.	Gebiet	Beschreibung
4	Zugriffskontrolle	
4.1	Wie wird erreicht, dass Passwörter nur dem jeweiligen Benutzer bekannt sind?	Die PW werden vom jeweiligen Mitarbeiter selbst vergeben. Jeder Mitarbeiter hat einen eigenen Zugang. Es gibt für die Regelung der Passwörter eine Passwort-Policy.
4.2	Welche Anforderungen werden an die Komplexität von Passwörtern gestellt?	Das Passwort wird regelmäßig gewechselt. Das Passwort entspricht der Passwort-Policy und der darin festgelegten Sicherheitsmerkmale, wie Sonderzeichen, Groß u. Kleinschreibung, Zahlen. Mind. 8 Stellen, es müssen mind. 3 der erwähnten Regeln erfüllt sein.
4.3	Wie wird gewährleistet, dass der Benutzer sein Passwort regelmäßig ändern kann/muss?	Durch Gruppenrichtlinien wird ein Wechsel des Passwortes nach 60 Tagen erzwungen oder der Zugriff gesperrt. Das neue Passwort darf nicht einem der drei vorherigen entsprechen.
4.4	Welche organisatorischen Vorkehrungen werden zur Verhinderung von unberechtigten Zugriffen auf personenbezogene Daten am Arbeitsplatz getroffen?	Alle Zugänge sind kennwortgeschützt. Automatische Bildschirmsperre ist fest eingerichtet. Schulung und Sensibilisierung der Mitarbeiter. Die Mitarbeiter sind unterwiesen, bei verlassen des Arbeitsplatzes keine sichtbaren bzw. freizugängliche, personenbezogene Daten zu hinterlassen (Clean-Desk-Prinzip).
4.5	Wie wird sichergestellt, dass Zugriffsberechtigungen anforderungsgerecht und zeitlich beschränkt vergeben werden?	Der GF prüft in regelmäßigen Abständen die Rechte der Benutzerstruktur.
4.6	Wie erfolgt die Dokumentation von Zugriffsberechtigungen?	Regelmäßiger Report der IT-Verantwortlichen aus dem Berechtigungssystem der Access-Control-List.
4.7	Wie wird sichergestellt, dass Zugriffsberechtigungen nicht missbräuchlich verwendet werden?	Stichprobenartige Durchsicht der Systemprotokolle durch den GF.
4.8	Wie lange werden Protokolle aufbewahrt? Wer hat Zugriff auf die Protokolle? Wie oft werden sie ausgewertet?	Keine festgelegten Fristen, meist Systemparameter. Zugriff hat die Geschäftsführung.
5	Trennungskontrolle	
5.1	Wie wird sichergestellt, dass Daten, die zu unterschiedlichen Zwecken erhoben wurden, getrennt voneinander verarbeitet werden?	Zur Trennung der Daten wird ein dezidiertes Rechte-System eingesetzt.

Nr.	Gebiet	Beschreibung
6	Pseudonymisierung	
6.1	Welche organisatorischen Maßnahmen wurden getroffen, damit die Verarbeitung personenbezogener Daten gesetzeskonform erfolgt?	Alle, mit der Verarbeitung von personenbezogenen Daten betrauten Personen, wurden entsprechend verpflichtet. Ein Datenschutzkonzept wird im Unternehmen eingesetzt und ist allen Mitarbeitern bekannt und schriftlich fixiert. Datenschutzunterweisungen/ Sensibilisierungen finden regemäßig statt.
6.2	Wie werden personenbezogene Daten verarbeitet/ aufbewahrt, sodass diese nicht den betroffenen Personen zugeordnet werden können?	Die Verarbeitung personenbezogener Daten kann in den meisten Fällen einer betroffenen Person zugeordnet werden.
7	Weitergabekontrolle	
7.1	Wie gewährleisten Sie die Integrität und Vertraulichkeit bei der Weitergabe von personenbezogenen Daten?	Die Weitergabe erfolgt über verschlüsselte Kanäle und/ oder die Verschlüsselung der Daten selbst. Eine Zustellung oder Bekanntgabe erfolgt nur an den vorhergesehenen Empfänger.
7.2	Werden Verschlüsselungssysteme bei der Weitergabe von personenbezogenen Daten eingesetzt? Wenn ja, welche?	Verschlüsselte USB-Sticks, verschlüsselte ZIP-Archive (AES-256) und verschlüsselte E-Mail Übertragung. Ein Versenden per Mail oder die Bereitstellung per Internet erfolgt über Server mit Transportverschlüsselung (SSL/TLS).
7.3	Wie wird die Weitergabe personenbezogener Daten dokumentiert?	Ist vom jeweiligen Prozess (Personal, Kundendaten, etc.) abhängig und wird im Verfahrensverzeichnis individuell geregelt.
7.4	Wie wird der unberechtigte Abfluss von personenbezogenen Daten durch technische Maßnahmen beschränkt?	Eine strikte Rechtevergabe sichert die Daten vor unberechtigtem Zugriff.
7.5	Gibt es ein Kontrollsystem, das einen unberechtigten Abfluss von personenbezogenen Daten aufdecken kann?	Dies wird im Rahmen der Zugriffskontrolle mit geprüft.
8	Eingabekontrolle	
8.1	Welche Maßnahmen werden ergriffen, um nachvollziehen zu können, wer wann und wie lange auf Applikationen zugegriffen hat?	Zugriffs-Logs der Server und Systeme.
8.2	Wie ist nachvollziehbar, welche Aktivitäten auf den entsprechenden Applikationen durchgeführt wurden?	Zugriffs-Logs der einzelnen Applikationen.
8.3	Welche Maßnahmen werden ergriffen, damit die Verarbeitung durch die Mitarbeiter nur gemäß der Weisung des Auftraggebers erfolgen kann?	Stichproben zur Prüfung und Unterweisung der Mitarbeiter zur Einhaltung. Regelmäßige Datenschutz-Veranstaltungen bzw. Personalgespräche.

Nr.	Gebiet	Beschreibung
8.4	Welche Maßnahmen werden getroffen, damit auch Unterauftragnehmer ausschließlich im vereinbarten Umfang personenbezogene Daten des Auftraggebers verarbeiten?	Die Datenverarbeitung von Unterauftragnehmern erfolgt mit eindeutigen Auftragsdefinitionen und einer formalisierten Auftragserteilung (AV-Verträge nach Art. 28 DSGVO). Die Pflichten zur Überprüfung der Unterauftragnehmer übernimmt der Datenschutzbeauftragte des Unternehmens. Er ist auch bei der Wahl der beauftragten Firmen beteiligt.
8.5	Wie wird die Löschung/Sperrung von personenbezogenen Daten am Ende der Aufbewahrungsfrist bei Unterauftragnehmern sichergestellt?	Feststellung durch Vertragsbindung, bei Wegfall des Zwecks ist ebenfalls eine Löschung der Daten indiziert.
9	Verfügbarkeitskontrolle	
9.1	Welche organisatorischen und technischen Maßnahmen werden getroffen, um auch im Schadensfall die Verfügbarkeit von Daten und Systemen schnellstmöglich zu gewährleisten?	Eingerichtetes Backup-Verfahren (Restore-Konzept/Wiederanlaufkonzept).
9.2	Wie wird gewährleistet, dass die Datenträger vor elementaren Einflüssen (Feuer, Wasser, elektromagnetischer Abstrahlung etc.) geschützt sind?	Die Backup-Datenträger werden in einem Safe in einer anderen Räumlichkeit aufbewahrt.
9.3	Welche Schutzmaßnahmen werden zur Bekämpfung von Schadprogrammen eingesetzt? Wie werden deren Aktualität gewährleistet?	Firewall-Systeme mit Servicevertrag, Session Border Controller zur IT-Sicherheit für VoIP, diese werden zentral automatisiert ausgerollt und aktualisiert. Anti-Viren und Firewall-Lösungen werden auf den Client- und Server-Systemen eingesetzt. Eingehende Mails werden vor Zustellung durch den Exchange-Server auf Schadsoftware und SPAM geprüft.
9.4	Wie wird sichergestellt, dass nicht mehr benötigte bzw. defekte Datenträger ordnungsgemäß entsorgt werden?	Physische Löschung bei funktionsfähigen Datenträgern und mechanische Zerstörung defekter Datenträger werden zentral durch die IT-Abteilung gemeinsam mit einem ISO-zertifizierten Entsorgungsfachbetrieb entsorgt.
10	Wiederherstellbarkeit	
10.1	Welche organisatorischen und technischen Maßnahmen werden getroffen, um auch im Schadensfall die Verfügbarkeit von Daten und Systemen schnellstmöglich zu gewährleisten? (rasche Wiederherstellbarkeit nach Art. 32 Abs. 1 lit. C DS-GVO)	Streng konzipiertes Backup-system. Die Server und Stromversorgungssysteme der Verarbeitungsanlage sind redundant ausgelegt, um einem Ausfall vorzubeugen.

Nr.	Gebiet	Beschreibung
11	Auftragskontrolle	
11.1	Welche Verfahren gibt es zur regelmäßigen Bewertung/Überprüfung, um die Sicherheit der Datenverarbeitung zu gewährleisten (Datenschutz-Management)?	Der externe Datenschutzbeauftragte überprüft regelmäßig und stichprobenartig, die Einhaltung der technisch organisatorischen Maßnahmen.
11.2	Wie wird auf Anfragen bzw. Probleme reagiert (Incident-Response-Management)?	Einsatz eines eigenen Ticket-Systems. Zusätzlich Telefon-Hotline und automatisierte Systemüberwachung.
11.3	Welche datenschutzfreundlichen Voreinstellungen gibt es (Art. 25 Abs. 2 DS-GVO)?	Keine Vorbelegung, der Benutzer muss die Anmeldeinformationen jeweils eintragen.
11.4	Welche Vorgänge gibt es zur Weisung bzw. dem Umgang mit der Auftragsdatenvereinbarung (Datenschutz-Management)?	Das Vertragswerk wurde entsprechend den neuen Richtlinien zur Auftragsdatenverarbeitung gestaltet. Der externe Datenschutzbeauftragte nimmt entsprechende Beratungs- und Kontrollfunktionen wahr.