Vertrag zur Auftragsverarbeitung gemäß Art. 28 DS-GVO

zwischen dem/der

.....

– Verantwortlicher –nachstehend Auftraggeber genannt –

und dem/der

Prozeßsteuerung & Systementwicklung GmbH & Co. KG

– Auftragsverarbeiter – nachstehend Auftragsverarbeiter genannt –

Inhalt

Präambel

(1) Dieser Vertrag ergänzt und konkretisiert die Verpflichtungen der Vertragsparteien zum Datenschutz, die sich aus den zugrunde liegenden AGB ergeben. Sie findet Anwendung auf alle Tätigkeiten, die mit dem Hauptvertrag in Zusammenhang stehen und bei denen personenbezogene Daten („Daten“) des Auftraggebers durch Mitarbeiter des Auftragsverarbeiters oder durch vom Auftragsverarbeiter Beauftragte verarbeitet werden.

1 Einleitung, Geltungsbereich, Definitionen

1 Dieser Vertrag regelt die Rechte und Pflichten von Auftraggeber und Auftragsverarbeiter (im folgenden „Parteien“ genannt) im Rahmen einer Verarbeitung von personenbezogenen Daten im Auftrag.

Mit Abschluss dieses Vertrags werden zwischen den Parteien bereits bestehende bzw. anderslautende vertragliche Vereinbarungen zur Auftragsverarbeitung mit Bezug zu der Leistungsvereinbarung durch diese Vereinbarung ersetzt.

2 Dieser Vertrag findet auf alle Tätigkeiten Anwendung, bei denen Mitarbeiter des Auftragsverarbeiters oder durch ihn beauftragte Unterauftragsverarbeiter (Subunternehmer) personenbezogene Daten des Auftraggebers verarbeiten.

3 Die Inhalte dieses Vertrags gelten entsprechend, wenn die Prüfung oder Wartung automatisierter Verfahren oder von Datenverarbeitungsanlagen im Auftrag vorgenommen wird und dabei ein Zugriff auf Auftraggeber-Daten nicht ausgeschlossen werden kann.

4 In diesem Vertrag verwendete Begriffe sind entsprechend ihrer Definition in der EU-Datenschutz-Grundverordnung zu verstehen. Soweit Erklärungen im Folgenden „schriftlich“ zu erfolgen haben, ist die Schriftform nach § 126 BGB gemeint. Im Übrigen können Erklärungen auch in anderer Form erfolgen, soweit eine angemessene Nachweisbarkeit gewährleistet ist.

2 Gegenstand und Dauer des Auftrags

Aus dem Vertrag ergeben sich Gegenstand und Dauer des Auftrags sowie Art und Zweck der Verarbeitung.

Die Laufzeit dieser Anlage richtet sich nach der Laufzeit des Vertrages, sofern sich aus den Bestimmungen dieser Anlage nicht darüber hinaus gehende Verpflichtungen ergeben.

3 Konkretisierung des Auftragsinhaltes

1 Art und Zweck der vorgesehenen Verarbeitung von Daten

- Art und Zweck der Verarbeitung personenbezogener Daten durch den Auftragsverarbeiter für den Auftraggeber sind konkret beschrieben in der Leistungsvereinbarung.
- Die Erbringung der vertraglich vereinbarten Datenverarbeitung findet in der Bundesrepublik Deutschland statt. Jede Verlagerung in ein Drittland bedarf der vorherigen Zustimmung des Auftraggebers und darf nur erfolgen, wenn die besonderen Voraussetzungen der Art. 44 ff. DS-GVO erfüllt sind.

2 Art der Daten und Kategorien betroffener Personen

- Allgemeine Personendaten der Mitarbeiter des Auftraggebers im Zeiterfassungssystem sind mindestens Personalnummer, Name, Ausweisnummer (Zeiterfassungstoken) Sowie Eintrittsdatum
- In Eigenverantwortung kann der Auftraggeber weiter Daten erfassen

4 Technisch-organisatorische Maßnahmen

1 Der Auftragsverarbeiter hat die Umsetzung der im Vorfeld der Auftragsvergabe als Anlage zu diesem Vertrag 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 Auftragsverarbeiter 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.

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

5 Betroffenenrechte

1 Betroffenenrechte sind die Rechte der betroffenen Personen, deren personenbezogene Daten verarbeitet werden (vorrangig mit / durch unsere Zeiterfassungssoftware). Hierbei gilt es mehrere Rechte zu beachten.

2 Aufgrund der Tatsache das P&S ausschließlich als Dienstleister gemäß Art. 30 Absatz 2 DSGVO tätig ist, liegt die Verantwortung hinsichtlich aller Betroffenenrechte bei den Leitungsfunktionen des Auftraggebers.

3 Der einzige Ausschluss entfällt auf Prozesse in Verbindung mit dem Cloud-Service, und zwar lediglich für die Löschung personenbezogener Daten.

4 Ablaufskizze (Software ist auf Servern von P&S-installiert):

- Anfrage durch den Auftraggeber bei P&S zur Prüfung eines „Betroffenenrechtes“
- Prüfung, ob der Auftraggeber den Betroffenen im Live-System bereits gelöscht hat
- Ja, Cloud-Backups löschen, den Auftraggeber darüber informieren
- Nein, den Auftraggeber bitten, dies zu tun und darüber informieren. Anschließend Hinweis auf Löschung/ Überschreibung der Kundenseitigen Backups

6 Qualitätssicherung und allgemeine Pflichten des Auftragsverarbeiters

Der Auftragsverarbeiter 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:

1 Schriftliche Benennung eines Datenschutzbeauftragten, der seine Tätigkeit gemäß Art. 38 und 39 DS-GVO ausübt.

Als Ansprechpartner beim Auftragsverarbeiter wird

Herr Rinat Bär Tel +49365552060 E-Mail: service@ipus.de

benannt.

2 Die Wahrung der Vertraulichkeit gemäß Art. 28 Abs. 3 S. 2 lit. b, 29, 32 Abs. 4 DS-GVO. Der Auftragsverarbeiter setzt bei der Durchführung der Arbeiten nur Mitarbeiter ein, die auf die Vertraulichkeit verpflichtet und zuvor mit den für sie relevanten Bestimmungen zum Datenschutz vertraut gemacht wurden. Der Auftragsverarbeiter und jede dem Auftragsverarbeiter 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.

3 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, die konkret in der **Anlage** zu diesem Vertrag beschrieben sind.

4 Der Auftraggeber und der Auftragsverarbeiter arbeiten auf Anfrage der Aufsichtsbehörde bei der Erfüllung ihrer Aufgaben zusammen.

5 Der Auftragsverarbeiter informiert den Auftraggeber unverzüglich 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 Auftragsverarbeiter ermittelt.

6 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 Auftragsverarbeiter ausgesetzt ist, hat ihn der Auftragsverarbeiter nach besten Kräften zu unterstützen.

7 Nachweisbarkeit der getroffenen technischen und organisatorischen Maßnahmen gegenüber dem Auftraggeber im Rahmen seiner Kontrollbefugnisse nach Ziffer 9 dieses Vertrages.

7 Kontrollpflichten des Auftragsverarbeiters

1 Der Auftragsverarbeiter führt angemessene Kontrollen der Einhaltung der Vorgaben aus diesem Vertrag und der Weisungen des Auftraggebers, insbesondere bezüglich der Umsetzung und Wirksamkeit der technischen und organisatorischen Maßnahmen durch, die er zum Schutz der Auftraggeber-Daten getroffen hat, mindestens einmal pro Kalenderjahr. Insbesondere prüft er die Maßnahmen und Prozesse zur Realisierung einer wirksamen Zugriffs- und Zugangskontrolle.

2 Die Durchführung und die Ergebnisse der Selbstkontrolle sind zu dokumentieren und für die gesamte Vertragslaufzeit, mindestens jedoch für 24 Monate, zu archivieren und auf Anforderung des Auftraggebers binnen einem Werktag in Textform zur Verfügung zu stellen. Stellt der Auftragsverarbeiter Abweichungen oder Lücken zu den vertraglichen Vorgaben fest oder ist die Wirksamkeit einer Maßnahme nicht vorhanden, ist der Auftraggeber unverzüglich über die Art der Abweichung sowie die geplante Maßnahme zur Behebung der Abweichung und den geplanten Umsetzungszeitpunkt zu unterrichten.

3 Der Auftraggeber behält sich das Recht vor, dem Auftragsverarbeiter Vorgaben in Form von Prüflisten zur Durchführung der Selbstkontrolle zu geben. Diese sind durch den Auftragsverarbeiter bei der nächsten, turnusgemäßen Selbstkontrolle anzuwenden.

4 Sofern der Auftragsverarbeiter für wesentliche Teile des Auftrages (Hauptleistungspflichten) einen oder mehrere Subunternehmer verpflichtet, ist der jeweilige Subunternehmer ebenfalls zur Durchführung dieser Selbstkontrollen zu verpflichten. Über festgestellte Abweichungen im Rahmen der Unterbeauftragung ist der Auftraggeber ebenfalls zu unterrichten. § 8 (Subunternehmer) sowie die gesetzlichen Pflichten des Auftragsverarbeiters zur Durchführung von Kontrollen bei den Subdienstleistern bleiben unberührt.

8 Unterauftragsverhältnisse / Subunternehmer

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 Auftragsverarbeiter z.B. als Telekommunikationsleistungen, Post-/Transportdienstleistungen 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 Auftragsverarbeiter 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 Auftragsverarbeiter darf Unterauftragsverarbeiter (weitere Auftragsverarbeiter) nur nach vorheriger ausdrücklicher schriftlicher bzw. dokumentierter Zustimmung des Auftraggebers beauftragen.

a Der Auftraggeber stimmt der Beauftragung der nachfolgenden Unterauftragsverarbeiter zu unter der Bedingung einer vertraglichen Vereinbarung nach Maßgabe des Art. 28 Abs. 2-4 DS-GVO:

Firma Unterauftragsverarbeiter	Anschrift/Land	Leistung	Bemerkungen
TeamViewer GmbH	Jahnstr. 30 73037 Göppingen	Fernwartungs-software	Optional, wenn durch den Kunden gefordert, ansonsten wird die Nutzung kundenseitiger VPN-Verbindung bevorzugt
Hetzner Online GmbH	Industriestr. 25 91710 Gunzenhausen	Cloud-Dienste	
VEOLIA – GERAER UMWELTDIENSTE GMBH & CO. KG	Am Fuhrpark 1 07548 Gera	Aktenvernichtung	Zertifizierter Anbieter

b Die Auslagerung auf Unterauftragsverarbeiter oder der Wechsel des bestehenden Unterauftragsverarbeiters sind zulässig, soweit:

i der Auftragsverarbeiter eine solche Auslagerung auf Unterauftragsverarbeiter dem Auftraggeber eine angemessene Zeit vorab schriftlich oder in Textform anzeigt und

ii der Auftraggeber nicht bis zum Zeitpunkt der Übergabe der Daten gegenüber dem Auftragsverarbeiter schriftlich oder in Textform Einspruch gegen die geplante Auslagerung erhebt und

iii 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 Unterauftragsverarbeiter und dessen erstmaliges Tätigwerden sind erst mit Vorliegen aller Voraussetzungen für eine Unterbeauftragung gestattet.

4 Erbringt der Unterauftragsverarbeiter die vereinbarte Leistung außerhalb des Europäischen Wirtschaftsraumes, bedarf dies der vorherigen Zustimmung des Hauptauftragsverarbeiters (mind. Textform). Sämtliche vertraglichen Regelungen in der Vertragskette sind auch dem weiteren Unterauftragsverarbeiter aufzuerlegen.

9 Kontrollrechte des Auftraggebers

1 Der Auftraggeber hat das Recht, im Benehmen mit dem Auftragsverarbeiter 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 Auftragsverarbeiter in dessen Geschäftsbetrieb zu überzeugen.

2 Der Auftragsverarbeiter stellt sicher, dass sich der Auftraggeber von der Einhaltung der Pflichten des Auftragsverarbeiters nach Art. 28 DS-GVO überzeugen kann. Der Auftragsverarbeiter 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

- die Einhaltung genehmigter Verhaltensregeln gemäß Art. 40 DS-GVO
- die Zertifizierung nach einem genehmigten Zertifizierungsverfahren gemäß Art. 42 DSGVO
- aktuelle Testate, Berichte oder Berichtsauszüge unabhängiger Instanzen (z.B. Wirtschaftsprüfer, Revision, Datenschutzbeauftragter, IT-Sicherheitsabteilung, Datenschutzauditoren, Qualitätsauditoren);
- eine geeignete Zertifizierung durch IT-Sicherheits- oder Datenschutzaudit (z.B. nach BSI-Grundschutz).

10 Mitteilung bei Verstößen des Auftragsverarbeiters

1 Der Auftragsverarbeiter 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 oder deren Sicherheit unverzüglich an den Auftraggeber zu melden.

i Der Auftragsverarbeiter muss dem Auftraggeber eine Verletzung der Sicherheit, die nachteilige Auswirkungen für den Schutz der personenbezogenen Daten haben könnte, die er auf Weisung des Auftraggebers verarbeitet, innerhalb von 24 Stunden mitteilen. Die Benachrichtigung muss rechtzeitig an den Datenschutzbeauftragten und IT-Sicherheitsbeauftragten des Auftraggebers erfolgen, so dass der Auftraggeber in der Lage ist, eine Datenschutzverletzung an die zuständige Datenschutzbehörde innerhalb von 72 Stunden zu melden. Die Benachrichtigung muss auf jeden Fall enthalten, dass es eine Verletzung der Datensicherheit gegeben hat oder gibt und ist unverzüglich an den Datenschutzbeauftragten und IT-Sicherheitsbeauftragten des Auftraggebers mit mindestens folgenden Angaben zu richten:

- ♦ eine Zusammenfassung von dem Vorfall, in dem die Verletzung der Sicherheit der personenbezogenen Daten eingetreten ist
- ♦ wie viele Personen und Datensätze betroffen sind/waren, die minimale und maximale Anzahl
- ♦ Wann die Verletzung stattfand (Datum oder den Zeitraum), ob sie aktuell noch besteht und den Zeitpunkt der Feststellung
- ♦ Art des Verstoßes (lesen, kopieren, Änderung, Löschung/Zerstörung, Diebstahl)
- ♦ welche personenbezogenen Daten betroffen sind, wie z. B. (kein Anspruch auf Vollständigkeit):
  - ∗ Name und Anschrift (Details)
  - ∗ Telefon-Nummern
  - ∗ E-Mail-Adressen
  - ∗ Login-Daten
  - ∗ finanzielle Details (z. B. Bankverbindung, Bonität o. Ä.)
  - ∗ Identifikations- (IDD) oder Steuer- und Sozialversicherungsnummern

- Kopien der Ausweispapiere (z.B. Reisepass)
- Geschlecht, Geburtsdatum und/oder Alter
- spezielle persönliche Daten wie z. B. Rasse, Ethnizität, Vorstrafen, politische Überzeugungen, Mitgliedschaft in einer Gewerkschaft, Religion, Sexualleben oder Gesundheitsdaten
- weitere Details

♦ ob die personenbezogenen Daten verschlüsselt, gehashed oder anderweitig für unbefugte Benutzer unverständlich oder unzugänglich gemacht wurden und wie dies stattgefunden hat

♦ die (vermutete) Ursache der Verletzung

♦ Verhältnis zu früheren Verletzungen

♦ die zu erwartenden potenziellen Auswirkungen der Verletzung

♦ welche Maßnahmen bereits ergriffen wurden, die Auswirkungen zu begrenzen

♦ empfohlene Maßnahmen, um die negativen Auswirkungen des Verstoßes weiter einzuschränken. Der Auftragsverarbeiter sichert dem Auftraggeber seine uneingeschränkte Zusammenarbeit zu, ohne zusätzliche Kosten dafür zu berechnen, bei der Untersuchung der Ursachen und Wirkungen der Verletzung, die auch die Bereitstellung angemessener Informationen und die Unterstützung in Bezug auf Untersuchungen der Regulierungsbehörde sowie die für eventuelle Mitteilungen an die Regulierungsbehörde und die Betroffenen erforderlichen Informationen beinhalten. Der Auftragsverarbeiter hält auch einen aktuellen Überblick über alle Verstöße gegen die Sicherheit der personenbezogenen Daten, die er im Rahmen der Weisungen des Auftraggebers verarbeitet.

ii Der Auftragsverarbeiter muss auf eigene Kosten die Maßnahmen ergreifen, die vernünftigerweise erforderlich sind:

♦ um die Verletzung zu reparieren;

♦ um eine Wiederholung zu verhindern;

♦ um die Auswirkungen des Verstoßes auf die Privatsphäre der betroffenen

♦ Personen und/oder

♦ um den Schaden infolge der Verletzung zu begrenzen.

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.

11 Weisungsbefugnis des Auftraggebers

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

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

12 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 Auftragsverarbeiter 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 unter Einhaltung unserer TOM 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 Auftragsverarbeiter entsprechend den jeweiligen Aufbewahrungsfristen über das Vertragsende hinaus aufzubewahren. Er kann sie zu seiner Entlastung bei Vertragsende dem Auftraggeber übergeben.

13 Haftung und Freistellung

Der Auftragsverarbeiter haftet dem Auftraggeber für Schäden, die der Auftragsverarbeiter, seine Mitarbeiter bzw. die von ihm mit der Vertragsdurchführung Beauftragten bei der Erbringung der vertraglichen Leistung schuldhaft verursachen. Soweit der Auftraggeber von Dritten infolge von durch den Auftragsverarbeiter zu vertretenden Schäden in Anspruch genommen wird, stellt der Auftragsverarbeiter den Auftraggeber von den diesbezüglichen Ansprüchen vollumfänglich frei.

Verantwortlicher des Auftraggebers

(Ort, Datum)	(Name des Unterzeichnenden)	(Unterschrift und Stempel)

Verantwortlicher des Auftragsverarbeiters

Gera, den 08.03.2022	Nico Packroff	P&S GmbH & Co. KG Hainstraße 13 07545 Gera Tel. 0365/55206-0
(Ort, Datum)	(Name des Unterzeichnenden)	(Unterschrift und Stempel)

Datenschutzbeauftragter des Auftragsverarbeiters

Gera, den 08.03.2022	Rinat Bär	P&S GmbH & Co. KG Hainstraße 13 07545 Gera Tel. 0365/55206-0
(Ort, Datum)	(Name des Unterzeichnenden)	(Unterschrift und Stempel)

Die detaillierten Punkte finden Sie bequem auf unserer Homepage:

https://pus-gmbh.eu/tom-dsgvo/

Anlage zum Vertrag zur Auftragsverarbeitung
Technische und organisatorische Maßnahmen (TOM)
der P&S GmbH & Co. KG

Stand: 8.03.2022

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

1 Zugangskontrolle

- Besucher Begleitung durch P&S-Personal.
- Haupteingangstür mit Knauf auf der Außenseite
- Eingangsbereiche und Fenster sind außerhalb der Geschäftszeiten verschlossen.
- Elektronisches Zutrittssystem mit automatischem Verschließen an der Büro Eingangstür.
- Außerhalb der Bürozeiten ist der Eingangsbereich der Geschäftsräume videoüberwacht.
- Außerhalb der Bürozeiten sind die Gebäudeeingangstüren verschlossen.
- Bei Reinigungsdiensten setzen wir auf Kontinuität und langfristige Partnerschaft

2 Zugriffskontrolle

- Rechner- Login mit Benutzername und Passwort mit Protokoll
- Verwendung von Anti-Virus Software auf Servern und Clients
- Computersysteme werden ständig auf dem aktuellen Stand gehalten
- Verwendung von Firewall und Intrusion Detection System als Schutz für das P&S Netzwerk
- Einsatz von VPN bei Zugriffen von außen auf das P&S Netzwerk
- . Aktenvernichtung über zertifizierten Dienstleister

3 Organisatorische Maßnahmen:

- Nutzerrechte und Zugänge werden durch Administratoren verwaltet
- Berechtigung auf Netzwerkverzeichnisse nutzerbezogen rollenbasierend.
- Zertifizierter zentraler Passwortmanager zum Speichern der System- und Kundenpasswörter
- Einsatz von Passwortregelungen nach aktuell empfohlenem Standard.
- Zugänge werden nach einer entsprechenden Anzahl von Fehlversuchen gesperrt.
- Protokollierung von Zugriffen auf Anwendungen bei der Eingabe, Änderung und Löschung von Daten.
- Mindestens jährlich Schulungen und Unterweisungen zum Datenschutz und zur Datensicherheit.

4 Trennungskontrolle

- Trennung von Produktiv- und Testumgebung.
- Physikalische Trennung von System und Datenbank
- Für unterschiedliche Anwendungen werden getrennte Verzeichnisse/Datenbanken mit verschiedenen Rechten eingesetzt.

5 Pseudonymisierung (Art. 32 Abs. 1 lit. a DS-GVO; Art. 25 Abs. 1 DS-GVO)

- Die Übertragung zwischen den Systemkomponenten der P&S-Produkte erfolgt

  a Pseudonymisiert

b Verschlüsselt in der P&S-Cloud

c Bei Installation auf einem Kundensystem, obliegt die Verschlüsselung der Übertragung dem Auftraggeber

- Die verwendete Datenbank ist generell verschlüsselt.

2 Integrität (Art. 32 Abs. 1 lit. b DS-GVO)

1 Weitergabekontrolle

- Einsatz von VPN zur Online-Datenübertragung
- Daten, die über Datenträger weitergegeben werden, werden komprimiert und verschlüsselt gespeichert
- Nutzung von 2FA (Zwei-Faktor-Authentisierung) bei allen Subunternehmern, sofern die Möglichkeit dazu besteht.
- Daten, die aufgrund von gesetzlichen Vorgaben an die entsprechenden Stellen zu übertragen sind, wie zum Beispiel Steuer- und Sozialversicherungsdaten werden auf den durch den Gesetzgeber vorgeschrieben Wegen und mit den dort vorgegeben Verschlüsselungen übertragen.
- Alle Mitarbeiter, die mit personenbezogenen Daten Umgang haben, sind schriftlich zur Verschwiegenheit verpflichtet.

2 Eingabekontrolle

- In dem von der P&S eingesetzten Programme ist implementiert, dass jederzeit, insbesondere auch nachträglich überprüft werden kann, ob und von wem personenbezogene Daten in dem System eingegeben, verändert oder gelöscht wurden.
- Es gibt neben Berechtigungseinstellungen auch zusätzliche Sperrmechanismen, die eine Veränderung oder Löschung verhindern können.

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

1 Für Kunden der P&S-Cloud wird durch das Rechenzentrum gewährleistet:

- Die Sicherheit der Daten und deren Verfügbarkeit wird durch ein mehrstufiges Backup- und Recovery-Konzept gewährleistet, sowie die redundante Auslegung zentraler Systeme und ihrer Komponenten.
- Systeme und Datenbanken werden online gesichert, um eine größtmögliche Verfügbarkeit im Rahmen der vereinbarten Leistungserbringung zu gewährleisten.
- Im gesamten Gebäude existiert eine Brandmeldeanlage. Der Serverraum ist durch eine automatische Feuerlöschanlage gesichert.
- Im gesamten Gebäude besteht Rauchverbot.
- Das gesamte Gebäude ist durch eine Alarmanlage mit automatischer Benachrichtigung des Sicherheitsunternehmens geschützt.
- Es erfolgen regelmäßige Datensicherungen sowie permanente Datenspiegelung.
- Der Zugang zu den Servern ist durch mehrstufige Sicherheitskomponenten abgesichert.
- Die Zugriffe auf die zentrale Anwendung im Rechenzentrumsbetrieb erfolgen über redundante Leitungen.

2 Für die Installation auf dem Kundensystem, obliegen die Maßnahmen für die Verfügbarkeit dem Auftraggeber.

4 Rasche Wiederherstellbarkeit (Art. 32 Abs. 1 lit. c DS-GVO);

1 Für Kunden der P&S-Cloud wird durch das Rechenzentrum gewährleistet:

- Systeme und Datenbanken werden gesichert, um eine größtmögliche Verfügbarkeit zu gewährleisten.
- Für alle internen Systeme ist eine Eskalationskette definiert, die vorgibt, wer im Fehlerfall zu informieren ist, um das System schnellstmöglich wiederherzustellen.

2 Für die Installation auf dem Kundensystem:

- Die Datenbank wird für den Fall einer nötigen Wiederherstellung täglich in einen Ordner gesichert.
- Für die weitere Sicherung und Wiederherstellung der Kundensysteme, ist der Auftraggeber verantwortlich.

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

1 Quartalsweise Überprüfung durch das Datenschutzteam:

- Dokumentation der Verfahrensweisen und Regelungen auf notwendige Änderungen
- Wirksamkeit der Verfahrensweisen und Regelungen
- Aktuell zusätzlicher Schulungsbedarf der Mitarbeiter

2 Automatische Überprüfung der Systeme über Monitoring-Tools für:

- Auffälligkeiten im Netzwerk
- Auffälligkeiten auf den Serversystemen