HINWEISE ZUR VEREINBARUNG ZUR AUFTRAGVERARBEITUNG

Füllen Sie die Felder auf folgenden Seiten der Vereinbarung aus:

SEITE 1 (in der PDF-Datei Seite 2)

SEITE 7 (in der PDF-Datei Seite 8)

SEITE 12 (in der PDF-Datei Seite 13)

Senden Sie uns dann die auf Seite 7 unterschriebene Vereinbarung zurück:

Per Fax an 05199-1294

oder

Eingescannt per E-Mail an mail@p-und-p.de

Das Dokument ist bereits von uns signiert, und somit gültig. Nehmen Sie Ihre Ausfertigung zu Ihren Datenschutz-Unterlagen.

Datenschutzvereinbarung

Vereinbarung zur Auftragsverarbeitung
gem. Verordnung (EU) 2016/679 (DSGVO)

Zwischen

	◄ Firma
	◄ Straße
	◄ Plz, Ort
	◄ Verantwortlicher (Geschäftsführer)
	◄ Datenschutzbeauftragter
	◄ Kontaktdaten Datenschutzbeauftragter

- nachstehend Auftraggeber genannt -

und

P&P Software GmbH
Scharrler Strasse 11
29640 Schneverdingen

- nachstehend Auftragnehmer genannt -

1 Präambel

(1) Der Auftragnehmer verarbeitet bzw. hat Zugriff auf personenbezogene Daten im Auftrag des Auftraggebers. Dieser Vertrag enthält nach dem Willen der Parteien und insbesondere des Auftraggebers den schriftlichen Auftrag zur Auftragsverarbeitung i.S.d. Artikel 28 der Verordnung (EU) 2016/679 – Datenschutz-Grundverordnung (DSGVO) und regelt die Rechte und Pflichten der Parteien im Zusammenhang mit der Datenverarbeitung.

(2) Sofern in diesem Vertrag der Begriff „Datenverarbeitung“ oder „Verarbeitung“ (von Daten) benutzt wird, wird die Definition der „Verarbeitung“ i.S.d. Art. 4 Nr. 2 DSGVO zugrunde gelegt.

(3) Diese Vereinbarung regelt ausschließlich und abschließend alle datenschutzrechtlich relevanten Vorgänge zwischen den Parteien. Sie gilt zusätzlich zu gegebenenfalls weiteren Vereinbarungen über die Leistungen und geht allen datenschutzrechtlichen Absprachen vor.

2 Beschreibung des Auftrages

(1) Gegenstand des Auftrags, sowie Dauer, Umfang, Art und Zweck der Daten sowie der betroffenen Personengruppen werden in **Anlage 4** beschrieben.

(2) Die in Anlage 4 beschriebenen Aufträge sind in jedem Fall Bedarfsaufträge, die nur im Bedarfsfall ausgeführt werden.

(3) Die Dauer des Auftrages besteht über die Zeit der Anwendung einer P&P Software beim Auftraggeber.

(4) 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.

(5) Der Auftraggeber kann diesen Vertrag jederzeit ohne Einhaltung einer Frist kündigen, wenn

a. ein schwerwiegender Verstoß des Auftragsverarbeiters gegen Datenschutzvorschriften oder die Bestimmungen dieser Vereinbarung vorliegt,

b. der Auftragsnehmer eine Weisung des Auftraggebers nicht ausführen kann oder will oder

c. der Auftragnehmer Kontrollrechte des Auftraggebers vertragswidrig verweigert.

(6) Insbesondere die Nichteinhaltung der in diesem Vertrag vereinbarten und aus Art. 28 DS-GVO abgeleiteten Pflichten stellt einen schweren Verstoß dar.

3 Rechte und Pflichten des Auftraggebers

(1) Der Auftraggeber ist Verantwortlicher i.S.d. Art. 4 Nr. 7 DSGVO für die Verarbeitung von Daten im Auftrag durch den Auftragnehmer. Die Beurteilung der Zulässigkeit der Datenverarbeitung obliegt allein dem Auftraggeber.

(2) Der Auftraggeber hat das Recht Überprüfungen beim Auftragnehmer 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 zu überzeugen. Der Auftraggeber wird dabei Sorge dafür tragen, dass die Kontrollen nur im erforderlichen Umfang durchgeführt werden, um die Betriebsabläufe durch die Kontrollen nicht unverhältnismäßig zu stören. Die Kontrollen erstrecken sich ausschließlich auf die in **Anlage 4** genannten Tätigkeiten und personenbezogene Daten des Auftraggebers.

(3) Der Nachweis solcher Maßnahmen, die nicht nur den konkreten Auftrag betreffen, kann auch erfolgen durch

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

(4) Der Auftraggeber unterstützt den Auftragnehmer nach besten Kräften bei Kontrollen der Aufsichtsbehörde, bei Ordnungswidrigkeits- oder Strafverfahren oder bei der Klärung von Haftungsansprüchen betroffenen Personen oder Dritten gegenüber dem Auftragnehmer.

4 Rechte und Pflichten des Auftragnehmers

(1) Der Auftragnehmer hat zusätzlich zu der Einhaltung der Regelungen dieses Auftrags gesetzliche Pflichten gemäß Art. 28 bis 33 DSGVO; insofern gewährleistet er insbesondere die Einhaltung folgender Vorgaben:

4.1 Weisungsgebundenheit und Kennzeichnung personenbezogener Daten

(1) Der Auftragnehmer führt die Tätigkeiten ausschließlich im Rahmen der getroffenen Leistungsvereinbarungen und nach Weisungen des Auftraggebers durch. Er verwendet Daten, die ihm im Rahmen der Erfüllung dieses Vertrags bekannt geworden sind, nur für die in **Anlage 4** genannten Zwecke.

(2) Soweit Weisungen des Auftraggebers Ermessensspielräume enthalten sollten, ist der Auftragnehmer verpflichtet, hierzu die Entscheidung des Auftraggebers einzuholen. Eine eigenständige Ermessensausübung oder Kulanzentscheidung steht dem Auftragnehmer nicht zu.

(3) Der Auftragnehmer wird die Daten, die er im Auftrag für den Auftraggeber verarbeitet, auf geeignete Weise kennzeichnen. Sofern die Daten für verschiedene Zwecke verarbeitet werden, wird der Auftragnehmer die Daten mit dem jeweiligen Zweck kennzeichnen und durch geeignete technisch-organisatorische Maßnahmen dafür sorgen, dass Daten ausschließlich für die vorhergesehenen Zwecke verarbeitet werden.

4.2 Organisation

(1) Der Auftragnehmer bestellt schriftlich einen Datenschutzbeauftragten, der seine Tätigkeit gemäß Art. 37 bis Art. 39 DSGVO nachweislich ausübt. Sofern der Auftragnehmer nicht zur Bestellung eines Datenschutzbeauftragten verpflichtet ist, wird ein „Ansprechpartner Datenschutz“ genannt. Die jeweiligen Kontaktdaten werden in **Anlage 3** hinterlegt. Ein Wechsel des Datenschutzbeauftragten bzw. „Ansprechpartner Datenschutz“ ist dem Auftraggeber unverzüglich mitzuteilen.

(2) Der Auftragnehmer verpflichtet sich gemäß Art. 28 Abs. 3 S. 2 lit. b, 29, 32 Abs. 4 DSGVO alle im Rahmen des Vertragsverhältnisses erlangten Kenntnisse von Geschäftsgeheimnissen und Datensicherheitsmaßnahmen des Auftraggebers geheim zu halten, in keinem Fall Dritten zur Kenntnis zu bringen und getrennt von sonstigen Datenbeständen zu halten.

(3) Der Auftragnehmer wird alle Beschäftigten, die Leistungen im Zusammenhang mit dem Auftrag des Auftraggebers erbringen, in schriftlicher Form verpflichten, alle Daten des Auftraggebers, insbesondere die für den Auftraggeber verarbeiteten personenbezogenen Daten vertraulich zu behandeln und nur zweck- und weisungsgebunden zur verarbeiten. Die Durchführung der Verpflichtung, sowie der Schulung der Beschäftigten ist auf Anfrage dem Auftraggeber nachzuweisen.

4.3 Technisch-organisatorische Maßnahmen

(1) Der Auftragnehmer etabliert für diesen Auftrag die erforderlichen technisch-organisatorischen Maßnahmen Art. 28 Abs. 3 S. 2 lit. c, sowie Art. 32 DSGVO. Diese werden in **Anlage 1** konkret aufgeführt. 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 DSGVO zu berücksichtigen.

(2) Bei Akzeptanz der technisch-organisatorischen Maßnahmen durch den Auftraggeber werden die dokumentierten Maßnahmen Grundlage des Auftrags.

(3) 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.

(4) Der Auftragnehmer kontrolliert regelmäßig und nachweislich die internen Prozesse sowie die technisch-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. Mängel in der Wirksamkeit der technisch-organisatorischen Maßnahmen sind durch den Auftragnehmer zu beseitigen.

(5) Die technisch-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.

4.4 Zusammenarbeit und Informationspflichten

(1) An der Erstellung der Verzeichnisse der Verarbeitungstätigkeiten gem. Art. 30 DSGVO durch den Auftraggeber hat der Auftragnehmer mitzuwirken. Er hat dem Auftraggeber die jeweils erforderlichen Angaben auf Antrag in geeigneter Weise mitzuteilen.

(2) Der Auftragnehmer arbeitet mit dem Auftraggeber auf Anfragen der Aufsichtsbehörde bei der Erfüllung ihrer Aufgaben zusammen. Er informiert unverzüglich den Auftraggeber 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.

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

a. die Sicherstellung eines angemessenen Schutzniveaus durch technisch-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 und in Abstimmung mit dem Auftraggeber angemessene Maßnahmen zur Minderung möglicher nachteiliger Folgen für Betroffene umzusetzen. Dies gilt auch bei schwerwiegenden Störungen des Betriebsablaufs, bei Verdacht auf sonstige Verletzungen gegen Vorschriften zum Schutz personenbezogener Daten oder anderen Unregelmäßigkeiten beim Umgang mit personenbezogenen Daten des Auftraggebers.

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.

(4) Soweit eine Mitwirkung des Auftragnehmers für die Wahrung von Betroffenenrechten - insbesondere auf Auskunft, Berichtigung, Sperrung oder Löschung - durch den Auftraggeber erforderlich ist, wird der Auftragnehmer die jeweils erforderlichen Maßnahmen nach Weisung des Auftraggebers treffen.

(5) Für Unterstützungsleistungen, die nicht in der Leistungsbeschreibung enthalten oder

nicht auf ein Fehlverhalten des Auftragnehmers zurückzuführen sind, kann der Auftragnehmer eine Vergütung beanspruchen.

(6) Sollte das Eigentum des Auftraggebers beim Auftragnehmer durch Maßnahmen Dritter (etwa durch Pfändung oder Beschlagnahme), durch ein Insolvenzverfahren oder durch sonstige Ereignisse gefährdet werden, so hat der Auftragnehmer den Auftraggeber unverzüglich zu informieren. Der Auftragnehmer wird die Gläubiger über die Tatsache, dass es sich um Daten handelt, die im Auftrag verarbeitet werden, unverzüglich informieren.

4.5 Weisungsbefugnisse

(1) Der Umgang mit den Daten erfolgt ausschließlich im Rahmen der getroffenen Vereinbarungen und nach Weisung des Auftraggebers. Der Auftraggeber hat ein umfassendes Weisungsrecht über Art, Umfang und Verfahren der Datenverarbeitung vor, das er durch Einzelweisungen konkretisieren kann.

(2) Mündliche Weisungen zwischen Auftragnehmer und Auftraggeber werden unverzüglich bestätigt (mind. Textform per E-Mail oder Fax oder Chat).

(3) 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.

(4) Weisungsberechtige bzw. weisungsempfangsberechtigte Personen sind in **Anlage 3** hinterlegt.

4.6 Berichtigung, Sperrung 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.

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

4.7 Unterauftragsverhältnisse

(1) Die Auslagerung auf Unterauftragnehmer bzw. der Wechsel des bestehenden Unterauftragnehmers sind zulässig, sofern

a. der Auftragnehmer eine solche Auslagerung auf Unterauftragnehmer dem Auftraggeber zwei Wochen vorab schriftlich oder in Textform anzeigt und

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

c. eine vertragliche Vereinbarung nach Maßgabe des Art. 28 Abs. 2-4 DSGVO und dieser Vereinbarung zugrunde gelegt wird.

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

(3) Erbringt der Unterauftragnehmer die vereinbarte Leistung außerhalb der EU/des EWR stellt der Auftragnehmer die datenschutzrechtliche Zulässigkeit durch entsprechende Maßnahmen nachweislich sicher.

(4) Die in **Anlage 2** aufgeführten Unterauftragnehmer gelten mit Unterschrift der

Vereinbarung als zulässig.

(5) Eine weitere Auslagerung durch den Unterauftragnehmer bedarf der ausdrücklichen Zustimmung des Hauptauftraggebers (mind. Textform). Sämtliche vertraglichen Regelungen in der Vertragskette sind auch weiteren Unterauftragnehmern aufzuerlegen.

(6) Dem Auftraggeber sind Auftragsvereinbarungen mit dem Unterauftragnehmer auf Anfrage zur Verfügung zu stellen.

(7) Nicht als Unterauftragsverhältnisse sind Dienstleistungen anzusehen, die der Auftragnehmer bei Dritten als reine Nebenleistung in Anspruch nimmt, um die geschäftliche Tätigkeit auszuüben. Dazu gehören beispielsweise

a. Reinigungsleistungen
b. reine Telekommunikationsleistungen ohne konkreten Bezug zu Leistungen, die der Auftragnehmer für den Auftraggeber erbringt,
c. Post- und Kurierdienste,
d. Transportleistungen oder
e. Bewachungsdienste.

Der Auftragnehmer ist gleichwohl verpflichtet, auch bei Nebenleistungen, die von Dritten erbracht werden, Sorge dafür zu tragen, dass angemessene Vorkehrungen und technisch-organisatorische Maßnahmen nachweislich getroffen wurden, um den Schutz personenbezogener Daten zu gewährleisten.

4.8 Beendigung der Leistungsvereinbarung

(1) 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.

(2) 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.

(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.

(4) Der Auftraggeber hat das Recht, die vollständige und vertragsgemäße Rückgabe und Löschung der Daten beim Auftragnehmer zu kontrollieren. Dies kann auch durch eine Einsicht der Datenverarbeitungsanlagen in der Betriebsstätte des Auftragnehmers erfolgen. Die Vor-Ort-Kontrolle soll mit angemessener Frist durch den Auftraggeber angekündigt werden.

(5) Der Auftraggeber kann diesen Vertrag jederzeit ohne Einhaltung einer Frist kündigen, wenn

a. ein Verstoß des Auftragsverarbeiters gegen die in Art. 28 DSGVO abgeleiteten Pflichten oder gegen die Bestimmungen dieser Vereinbarung vorliegt,

b. der Auftragsnehmer eine Weisung des Auftraggebers nicht ausführen kann oder will oder

c. der Auftragnehmer Kontrollrechte des Auftraggebers vertragswidrig verweigert.

5 Zurückbehaltungsrecht

(1) Sollten die personenbezogenen 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.

(2) Der Auftragnehmer wird alle in diesem Zusammenhang Verantwortlichen unverzüglich darüber informieren, dass die Hoheit an den personenbezogenen Daten des Auftraggebers bei dem Auftraggeber liegt.

(3) Auftraggeber und Auftragnehmer sind sich darüber einig, dass die Einrede des Zurückbehaltungsrechts durch den Auftragnehmer i.S.d. § 273 BGB hinsichtlich der verarbeiteten Daten und der zugehörigen Datenträger ausgeschlossen wird.

6 Wirksamkeit der Vereinbarung

(1) Für Nebenabreden ist die Schriftform erforderlich.

(2) Sollten einzelne Teile dieses Vertrages unwirksam sein, so berührt dies die Wirksamkeit der übrigen Regelungen des Vertrages nicht.

Auftraggeber:	**Auftragnehmer:**
	P&P Software GmbH Scharrler Strasse 11 29640 Schneverdingen
	
	Schneverdingen, den 30.04.2018
(Unterschrift, Ort, Datum)	(Unterschrift, Ort, Datum)
	Dipl.-Wi.-Inf. E. Petersen Geschäftsführer
(Name/Funktion in Blockschrift (Auftraggeber))	(Name/Funktion in Blockschrift (Auftragnehmer))

Datenschutzbeauftragter wenn vorhanden:

Anlage 1: Technisch-organisatorische Maßnahmen gem. Art. 32 Abs. 1 DSGVO

Die technisch-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.

Sicherheit der Datenverarbeitung

im Sinne des Art. 28 Abs. 3 Satz 2 lit. c), 32 DSGVO
P&P Software GmbH, Scharrler Str. 11, 29640 Schneverdingen

Vorwort

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, werden gem. Artikel 32 EU-Datenschutzgrundverordnung („DSGVO"), sowie als Auftragsarbeiter gem. Artikel 28 Abs. 3 Satz 2 lit. c) DSGVO die getroffenen technischen und organisatorischen Schutzmaßnahmen aufgelistet, um ein dem Risiko angemessenes Datenschutzniveau zu gewährleisten.

Diese Anlage findet Anwendung auf alle Tätigkeiten, bei denen Mitarbeiter des Auftragsverarbeiters (Auftragnehmer) mit personenbezogenen oder sonstigen Daten des Verantwortlichen (Auftraggeber) in Berührung kommen können. Für eingesetzte Unterauftragnehmer gelten dessen jeweiligen Maßnahmen zur Sicherheit der Datenverarbeitung.

Vertraulichkeit (Art. 32 Abs. 1 lit. b DSGVO)

Die hier aufgeführten Maßnahmen gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind. Diese Maßnahmen müssen so ausgelegt sein, dass sie die Verfügbarkeit auf Dauer gewährleisten.

2.1 Zutrittskontrolle (Verhinderung unbefugter Zutritt zu Datenverarbeitungsanlagen)

- Der Zugang zum Bürogebäude ist nur Beschäftigten vorbehalten. Es gibt keinen Publikumsverkehr.
- Das Gebäude ist mit manuellen Sicherheitsschlössern ausgestattet.
- Es gibt eine festgelegte Schlüsselregelung bzgl. der Ausgabe, Verwaltung, Zuordnung, des Verlustes und Rücknahme der Schlüssel.
- Alarmanlage

2.2 Zugangskontrolle (Verhinderung der unbefugten Systembenutzung)

- Die Authentifizierung zu den IT-Endgeräten erfolgt mit eine personenbezogenen Benutzernamen
- Jedes IT-Endgerät ist durch ein individuelles Passwort geschützt.
- Es gibt keine Gruppen-Accounts. Mitarbeiter und Administratoren nutzen eine personenbeziehbare Kennung
- Für den Tagesbetrieb erfolgt die Arbeit mit Standard-Benutzerrechten.
- Das Passwort ist mindestens 7 Stellen lang, enthält Klein- und Großbuchstaben, Sonderzeichen und Zahlen. Das Gerät sperrt sich nach 3 Fehlversuchen und muss durch den System-Administrator entsperrt werden.
- Die Verwaltung der Rechte der Mitarbeiter erfolgt durch den Systemadministrator
- Für spezielle Aufgaben werden zusätzlich separierte Rechner bzw. virtuelle Rechner verwendet.
- Der Zugang vom Internet her wird durch eine Firewall geschützt. Änderungen an der Firewall erfolgt ausschließlich durch eigenes Personal. Das dokumentierte Regelwerk der Firewall ist auf ein Minimum reduziert wird durch einen begrenzten Personenkreis regelmäßig überprüft.

- Der Zugang über das Internet auf die eigenen IT-Systeme erfolgt ausschließlich durch verschlüsselte Verbindungen (VPN-Technologie) und Schnittstellen (HTTPS, FTPS).
- Bildschirme werden bei Verlassen des Arbeitsplatzes gesperrt. Bei einem Vergessen der manuellen Sperrung des Bildschirms erfolgt dies automatisch nach 10 Minuten Inaktivität. Die Sperrung ist durch Eingabe des Passwortes notwendig.
- Beim Austritt oder längerfristigen Abwesenheiten werden die Accounts der Benutzer sofort gesperrt.
- Nach Feierabend werden die IT-Endgeräte heruntergefahren
- Verschlüsselung von Datenträgern
- Einsatz von Systemen gegen Schadsoftware auf Client- und Server-Systemen

2.3 Zugriffskontrolle (Verhinderung unbefugter Tätigkeiten in Datenverarbeitungsanlagen)

- Jeder Zugriff auf die Umgebung der Kunden im Rahmen eines Auftrages erfolgt protokolliert.
- Jeder Mitarbeiter wird regelmäßig vom Unternehmen im Bereich IT-Sicherheit und Datenschutz geschult und zur Vertraulichkeit gem. Artikel 28 Absatz 3 Buchstabe b DSGVO verpflichtet.
- Nach Beendigung des Auftrags werden die Daten nach einem vorgegebenen Verfahren fachgerecht gelöscht. Dies erfolgt bei Papier durch einen Schredder, bei der Löschung von Dateien mit der Methode ohne Papierkorb.
- Die Speicherung der Kundendaten erfolgt logisch getrennten auf gesonderten Systemen oder Datenträgern
- Produktiv- und Testsystem sind voneinander getrennt
- Für Auftrags - Aufgaben werden separate Rechner bzw. virtuelle Rechner genutzt.

Integrität (Art. 32 Abs. 1 lit. b DSGVO)

Die hier aufgeführten Maßnahmen gewährleisten eine angemessene Sicherheit der personenbezogenen Daten, einschließlich Schutz vor unbefugter oder unrechtmäßiger Verarbeitung und vor unbeabsichtigtem Verlust, unbeabsichtigter Zerstörung oder unbeabsichtigter Schädigung sowie unbefugter Änderung. Diese Maßnahmen müssen so ausgelegt sein, dass sie die Integrität auf Dauer gewährleisten.

3.1 Weitergabekontrolle (Maßnahmen bzgl. der Weitergabe personenbezogener Daten)

- Fest eingestellte Transportwege zwischen Auftraggeber und P&P
- Automatische Protokollierung von Up- und Downloads zum P&P Webserver
- Protokollierung jedes AuftragsVerfahrens
- Einsatz von VPN-Technologie (Verschlüsselter Zugang zu den jeweiligen Rechnern)
- Einsatz verschlüsselter Transportprotokolle (HTTPS, SFTP) für den sicheren Austausch von Dateien
- Einsatz von Firewalls

3.2 Eingabekontrolle (Maßnahmen zur Nachvollziehbarkeit bzw. Dokumentation der Datenverwaltung und –pflege)

- Protokollierung jedes Auftrags-Verfahrens bei P&P
- In den von P&P ausgeführten Aufträgen werden KEINE Veränderungen der Daten vorgenommen; dies gilt insbesondere bei Datenbankreparaturen.

3.3 Auftragskontrolle (Maßnahmen zur weisungsgemäßen Auftragsverarbeitung)

- Auswahl des Auftragnehmers unter Sorgfaltsgesichtspunkten (insbesondere hinsichtlich Datensicherheit)
- Abschluss einer Vereinbarung zur Auftragsdatenverarbeitung gem. Art 28 DSGVO einschl. Dokumentenprüfung der Unterauftragnehmer von P&P
- Regelmäßige Nachkontrolle der eingesetzten Unterauftragnehmer
- Protokollierung jeder weisungsbezogenen Auftragsarbeit bei P&P

- Verpflichtung der eigenen Mitarbeiter auf gem. Art. 28 Absatz Buchstabe b DSGVO
- Definition eines Schulungskonzeptes und Umsetzung regelmäßiger Schulungen der eigenen Beschäftigten.

Nichtverkettung

Die hier aufgeführten Maßnahmen gewährleisten, dass Daten nur für den Zweck verarbeitet und ausgewertet werden können, für den sie erhoben werden. Datenbestände sind prinzipiell dazu geeignet, für weitere Zwecke eingesetzt zu werden und mit anderen, unter Umständen öffentlich zugänglichen Daten kombiniert zu werden.

- Angemessene Funktionstrennungen zwischen oder auch innerhalb Organisationen
- Verarbeitung auf unterschiedlichen Systemen

4.1 Transparenz

Die hier aufgeführten Maßnahmen gewährleisten, dass sowohl Betroffene, als auch die Betreiber von Systemen sowie zuständige Kontrollinstanzen erkennen können, welche Daten für welchen Zweck in einem Verfahren erhoben und verarbeitet werden, welche Systeme und Prozesse dafür genutzt werden, wohin die Daten zu welchem Zweck fließen und wer die rechtliche Verantwortung für die Daten und Systeme in den verschiedenen Phasen einer Datenverarbeitung besitzt.

- Dokumentation der eingesetzten IT-Systeme und Software, der Daten und Datenflüsse einschl. Zuständigkeiten, Änderungsprozessen, administrativen Eingriffen, Tests und Freigaben gem. Art. 30 DSGVO (Verzeichnis der Verarbeitungstätigkeiten)
- Information und Unterrichtung von Betroffenen gem. Art. 13 DSGVO

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

Die hier aufgeführten Maßnahmen gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind. Diese Maßnahmen müssen so ausgelegt sein, dass sie die Verfügbarkeit auf Dauer gewährleisten. Hierzu gehören auch Maßnahmen, die schon in der Phase vor Durchführung der Datenverarbeitung durch die Beteiligten zu ergreifen sind, einschließlich einer kontinuierlichen Überwachung der Systeme.

- Einsatz hochwertiger und teilweise redundanter Hardware
- Regelmäßige Backups der Datenbestände
- Backup-Automatisierung mit Alarmfunktionen
- Unterbrechungsfreie Stromversorgung (USV) mit Selbsttests
- Aufbewahrung von Datensicherungen an einem sicheren, ausgelagerten Ort
- Einsatz einer Klimaanlage
- Feuer- und Rauchmeldeanlagen
- Einsatz von Feuerlöschern zur schnellen Brandbekämpfung

Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung (Art. 32 Abs. 1 lit. d DSGVO; Art. 25 Abs. 1 DSGVO)

Die hier erwähnten Maßnahmen gewährleisten eine laufende Aktualisierung der Maßnahmen zur Datensicherheit.

- Einsatz eines Datenschutz-Managements
- Kreative Mitgestaltung des aktiven Datenschutzes aller Mitarbeiter
- Datenschutzfreundliche Voreinstellungen (Art. 25 Abs. 2 DSGVO) der verwendeten IT-Systeme

Anlage 2: Unterauftragnehmer gem. Art. 28 DSGVO

☒	Im Rahmen der Leistungsvereinbarung werden folgende Unterauftragnehmer eingesetzt. Die Unterauftragnehmer erfüllen die in Kapitel 4.7 genannten Voraussetzungen.

Firmenname	**Anschrift**	**Funktion**
domainfactory GmbH	Oskar-Messter-Str. 33 85737 Ismaning	Hosting-Anbieter, Übergabeplattform der Kundendaten, Mail-Provider
Pcvisit Software AG	Manfred-von-Ardenne-Ring 20 01099 Dresden	Fernwartungs-Provider

Anlage 3: Ansprechpartner

Beim Auftraggeber:

Weisungsberechtigte Personen

Rolle / Funktion	Name	Kontakt (Tel. / E-Mail)
Der Verantwortliche und in seinem Namen handelnde Mitarbeiter.	Siehe Auftraggeber	Siehe Auftraggeber

Datenschutzbeauftragter bzw. Ansprechpartner

Rolle / Funktion	Name	Kontakt (Tel. / E-Mail)

Beim Auftragnehmer:

Weisungsempfangsberechtigte Personen

Rolle / Funktion	Name	Kontakt (Tel. / E-Mail)
Support-Mitarbeiter der P&P Software GmbH	./.	05199 – 464 mail@p-und-p.de

Rolle / Funktion	Name	Kontakt (Tel. / E-Mail)
Geschäftsführer	Edmund Petersen	05199 – 352 mail@p-und-p.de

Anlage 4: Gegenstand, Dauer, Art und Umfang des Auftrags

Die vom Auftragnehmer angebotenen Dienstleistungen werden gem. Art. 30 DSGVO nachfolgend aufgeführt.

Nr.	Dienstleistung / Zweck / Dauer	Kategorien von Betroffenen und Daten	Empfänger / Zugriffsberechtigte	Löschung der Daten	Prozessbeschreibung / Maßnahmen zur IT-Sicherheit
1.	Reparatur oder Auswertung der Kundendatenbank. Dauer: Bei Auswertungen bis zum Erreichen des Auftragszieles. (1 – x Tage) Bei Reparaturen bis zur Ablieferung der reparierten Daten. (1 – x Stunden)	Mitarbeiter Auftraggeber: ➢ Personenstammdaten, wie z.B. Name Ansprechpartner ➢ Adressdaten, wie z.B. Anschrift Auftraggeber ➢ Kommunikationsdaten, wie z.B. Telefonnummer, E-Mail-Adressen ➢ Auftragsbezogene Daten, wie z.B. Datum, Uhrzeit, Dauer, Kunde, Ansprechpartner, Auftragsinhalt	Intern: Zugriffsberechtigte Support-Mitarbeiter Extern: Unterauftragnehmer zum Dateiaustausch	Datenbank des Auftraggebers: Nach Erfüllung des Auftrages <u>Protokolldaten</u>: 10 Jahre Aufbewahrungsfrist gem. §257 HGB (Handelsgesetzbuch)	➢ Verschlüsselter Transport der zu bearbeitenden Datenbank mit einem in der beim Auftragnehmer installierten P&P Software integrierten FTPS-Upload-Tools auf den Webserver des Unterauftragnehmers in einen nur für diesen Kunden bestimmten Ordner. ➢ Download der DB vom Webserver des Unterauftragnehmers auf einen speziellen Arbeitsplatz des Auftragnehmers. Nach erfolgreichem Download zum Auftragnehemer wird die Datei vom Webserver des Unterauftragnehmers gelöscht. ➢ Ausführung des Auftrages beim Auftragnehmer ➢ FTPS-Upload zum Webserver des Unterauftragnehmers in den für diesen Auftraggeber bestimmten Ordner. ➢ FTPS Download der DB zurück auf das System des Auftraggebers und Erfolgskontrolle. ➢ Die Daten werden vom Webserver des Unterauftragnehmers gelöscht. ➢ Je nach Auftrag werden die Daten des Kunden beim Auftragnehmer sofort gelöscht (Reparaturfall) oder auf Weisung verschlüsselt zwischengelagert bis der Auftrag vollständig ausgeführt wurde.

		Kundendaten Auftraggeber: ➢ Kundenstammdaten, wie z.B. Personenstamm, Adressdaten, Kommunikationsdaten, Zahlungsdaten, … ➢ Auftragsbezogene Daten, wie z.B. Auftragsinhalt, Preise und Zahldaten.			➢ Der Mitarbeiter des Auftragnehmers führt ein Protokoll über diesen Vorgang.
2.	Fernwartung beim Kunden Für Hilfestellung, Schulung, Problemanalyse Dauer: Im Minuten bist Stundenbereich	Sämtliche Daten, die während der Supporttätigkeiten durch den Mitarbeiter des Auftragnehmers eingesehen werden können: Personenstammdaten, Adressdaten, Kommunikations-daten, … Protokolldaten der Fernwartung, wie z.B. Datum, Uhrzeit, Kunde, Name, durchgeführte Arbeiten, …	Intern: Zugriffsberechtigte Support-Mitarbeiter Extern: -	Protokolldaten 10 Jahres Aufbewahr-ungsfrist	Eine Fernwartung kann ausschließlich vom Arbeitsplatz eines autorisierten Mitarbeiters des Auftrag-nehmers durchgeführt werden und ist ausschließlich vom Auftraggeber aktiv startbar. Die komplette Sitzung kann vom Auftraggeber beobachtet und kann jederzeit vom ihm unter-brochen werden. Sicherheit: Pcvisit ist ein deutsches Produkt mit deutschen Servern. Der Verbindungsaufbau erfolgt verschlüsselt 256-Bit AES.
3.	Entiwcklung von Internet-	Alle Daten, die vom Auftraggeber zur Erstellung	Intern: Berechtigte	10 Jahres Aufbewahr-	Gestaltung der Homepage nach Auftraggeber-Weisung unter den heute gebotenen

	Auftritten	einer Webseite übergeben werden.	P&P Mitarbeiter Extern: Web-Hoster	ungsfrist	Sicherheitsaspekten.
4.	Service ‚Kollegenmail' Informationsaustausch unter P&P Kunden.	Absender-Name und Mailadresse des P&P Kunden.	Intern: Berechtigte P&P Mitarbeiter Extern: 1 - Alle per Mail erreichbaren P&P-Kunden, die diesen Service wünschen. 2 – Mail-Provider	10 Jahres Aufbewahr-ungsfrist	Eine Mailanfrage eines P&P-Kunden wird an alle an diesem Service teilnehmenden Kollegen (P&P Kunden) weitergeleitet. Die Teilnahme ist freiwillig und kann auf der P&P Homepage aktiviert oder deaktiviert werden. Sicherheit: Sicherer Mailversand.
1-4	<u>Rechtsgrundlage für alle Verarbeitungstätigkeiten:</u> Beschäftigtendaten des Auftragsgebers: Art. 6 Absatz 1 Buchstabe b DSGVO (Vertragserfüllung) Kundendaten des Auftragsgebers: Art. 28 DSGVO (Auftragsverarbeitung)				