Vereinbarung zur Verarbeitung von personenbezogenen Daten im Auftrag i.S.d. Art. 28 DSGVO

Stand: 01.11.2026

zwischen der

pco GmbH, Albert-Einstein-Straße 8, 49076 Osnabrück

– Auftragnehmer – nachstehend „pco“ oder „Auftragnehmer“ genannt –

und dem/der

– Auftraggeber – nachstehend „Kunde“ oder „Auftraggeber“ genannt.

1. Einleitung

Diese Vereinbarung zur Auftragsverarbeitung gemäß Art. 28 gilt für sämtliche zwischen den Parteien vereinbarten Leistungen und Dienstleistungen, soweit pco dabei personenbezogene Daten im Auftrag des Kunden als Verantwortlichem im Sinne der DSGVO verarbeitet. Die Vereinbarung regelt die gegenseitigen Rechte und Pflichten der Parteien hinsichtlich der Verarbeitung und des Schutzes dieser personenbezogenen Daten.

Diese Vereinbarung findet auf alle bestehenden und zukünftigen Leistungsvereinbarungen zwischen den Parteien Anwendung, soweit eine Auftragsverarbeitung im Sinne des Art. 28 DSGVO vorliegt. Sie geht abweichenden vertraglichen Regelungen hinsichtlich der Auftragsverarbeitung personenbezogener Daten vor, soweit in dieser Vereinbarung nichts anderes bestimmt ist.

Für Vertragspartner, die dem Gesetz über den Kirchlichen Datenschutz (KDG) oder dem Datenschutzgesetz der Evangelischen Kirche in Deutschland (DSG-EKD) unterliegen, gelten ergänzend die jeweils einschlägigen kirchlichen Datenschutzbestimmungen, soweit diese auf die betreffende Auftragsverarbeitung Anwendung finden.

2. Gegenstand, Dauer, Art und Zweck der Verarbeitung, Datenkategorien und Kategorien betroffener Personen

(1) Gegenstand dieser Vereinbarung ist die Verarbeitung personenbezogener Daten durch pco im Auftrag des Kunden im Rahmen der zwischen den Parteien vereinbarten Leistungen. Hierzu zählen insbesondere die Bereitstellung, Implementierung, Konfiguration, Administration, Wartung und Betreuung von IT-Infrastrukturen, Hardware, Softwaresystemen, Anwendungen und Cloudsystemen sowie die Erbringung damit verbundener IT-Dienstleistungen und Services.

Diese Vereinbarung gilt für sämtliche Leistungen, bei deren Erbringung pco personenbezogene Daten im Auftrag und auf Weisung des Kunden verarbeitet oder auf diese zugreifen kann, soweit eine Auftragsverarbeitung im Sinne des Art. 28 DSGVO vorliegt. Der konkrete Gegenstand der Verarbeitung ergibt sich aus den jeweils zwischen den Parteien geschlossenen Hauptverträgen einschließlich der zugehörigen Leistungsbeschreibungen, Angebote, Bestellungen und sonstigen vertraglichen Vereinbarungen (nachfolgend gemeinsam „Leistungsvereinbarungen“).

(2) Die Dauer der Verarbeitung richtet sich nach der Laufzeit der jeweiligen Leistungsvereinbarung

und umfasst den Zeitraum, in dem pco zur Erbringung der vereinbarten Leistungen personenbezogene Daten im Auftrag des Kunden verarbeitet.

(3) Art und Zweck der Verarbeitung richten sich nach den jeweils vereinbarten Leistungen und deren vertragsgemäßer Nutzung durch den Kunden.

Die Verarbeitung kann insbesondere folgende Tätigkeiten umfassen:

- Bereitstellung, Betrieb, Hosting und Verwaltung von IT-Systemen, Anwendungen, Plattformen und Cloudumgebungen;
- Installation, Konfiguration, Administration, Überwachung, Wartung und Aktualisierung von IT-Systemen und Anwendungen;
- Erbringung von IT-Support, Helpdesk-, Fernwartungs-, Beratungs- und sonstigen technischen Unterstützungsleistungen;
- Speicherung, Organisation, Strukturierung, Sicherung, Wiederherstellung, Übertragung, Bereitstellung, Auswertung im Rahmen der Leistungserbringung sowie Löschung personenbezogener Daten;
- Durchführung von Datensicherungen, Systemmigrationen, Fehleranalysen, Störungsbehebungen und Maßnahmen zur Gewährleistung der IT-Sicherheit;
- Verarbeitung von Protokoll-, Nutzungs- und Systemdaten, soweit dies für die Erbringung der vereinbarten Leistungen erforderlich ist.

Die vorstehende Aufzählung beschreibt mögliche Verarbeitungstätigkeiten und begründet für sich genommen weder eine Verpflichtung noch eine Berechtigung zur Durchführung sämtlicher genannter Tätigkeiten. Die jeweils tatsächlich durchgeführten Verarbeitungstätigkeiten und deren konkrete Zwecke ergeben sich aus den Leistungsvereinbarungen sowie den dokumentierten Weisungen des Kunden.

Eine Verarbeitung personenbezogener Daten zu eigenen Zwecken von pco ist im Rahmen dieser Vereinbarung ausgeschlossen, soweit nicht eine eigenständige gesetzliche Grundlage oder eine gesonderte datenschutzrechtliche Vereinbarung vorliegt.

(4) Art der personenbezogenen Daten: Die Verarbeitung kann sämtliche Kategorien personenbezogener Daten umfassen, die der Kunde im Rahmen der vereinbarten Leistungen bereitstellt, in die von pco betreuten Systeme einbringt oder die im Rahmen der vertragsgemäßen Leistungserbringung verarbeitet werden.

Hierzu können insbesondere die in Anlage 1 dieser Vereinbarung aufgeführten Datenkategorien gehören. Die in Anlage 1 enthaltene Aufzählung dient der Beschreibung der grundsätzlich möglichen Datenkategorien. Sie bedeutet nicht, dass im Rahmen jeder Leistungsvereinbarung sämtliche dort aufgeführten Datenkategorien tatsächlich verarbeitet werden.

Maßgeblich sind ausschließlich die Datenkategorien, deren Verarbeitung sich aus der jeweiligen Leistungsvereinbarung, deren vertragsgemäßer Durchführung und den dokumentierten Weisungen des Kunden ergibt.

(5) Kategorien betroffener Personen: Die Verarbeitung kann personenbezogene Daten insbesondere folgender Kategorien betroffener Personen umfassen:

- Beschäftigte, ehemalige Beschäftigte, Bewerber und sonstige für den Kunden tätige Personen;
- Kunden, Interessenten, Geschäftspartner und Lieferanten des Kunden sowie deren Beschäftigte und Ansprechpartner;
- Nutzer und Administratoren der vom Kunden eingesetzten oder durch pco betreuten IT-Systeme und Anwendungen;

- sonstige natürliche Personen, deren personenbezogene Daten im Rahmen der vertragsgemäßen Nutzung der vereinbarten Leistungen verarbeitet werden.

Weitere mögliche Kategorien betroffener Personen sind in Anlage 1 dieser Vereinbarung aufgeführt.

Die tatsächlich betroffenen Personenkategorien ergeben sich aus den jeweiligen Leistungsvereinbarungen sowie der vertragsgemäßen Nutzung der Leistungen durch den Kunden.

(6) Sofern besondere Kategorien personenbezogener Daten i.S.v. Art. 9 DSGVO verarbeitet werden, stellt pco sicher, dass hierfür angemessene, dem Risiko entsprechende zusätzliche Schutzmaßnahmen umgesetzt werden.

3. Leistungsort des Auftrags

Die Erbringung der vertraglich vereinbarten Datenverarbeitung findet grundsätzlich in einem Mitgliedsstaat der Europäischen Union oder in einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum statt. Der Kunde gestattet pco, unter Berücksichtigung der erforderlichen Sicherheitsmaßnahmen, auch eine Datenübermittlung in Drittländer, sofern die Unterauftragnehmer dort tätig sind. Punkt 10 Abs. 5 gilt entsprechend.

4. Technische und organisatorische Maßnahmen

(1) pco ergreift in seinem Verantwortungsbereich alle erforderlichen technischen und organisatorischen Maßnahmen gemäß Art. 32 DSGVO zum Schutz der personenbezogenen Daten des Kunden. Die jeweils aktuell geltenden technischen und organisatorischen Maßnahmen werden in der **Anlage TOM** beschrieben, welche in der aktuellen Version unter www.pco-online.de/docs bereitgestellt wird. Der Kunde informiert sich vor Abschluss der Vereinbarung zur Auftragsverarbeitung über die jeweils geltenden technischen und organisatorischen Maßnahmen der pco. Änderungen der technischen und organisatorischen Maßnahmen werden dem Kunden über die unter www.pco-online.de/docs bereitgestellten Informationen zugänglich gemacht. Der Kunde hat die Möglichkeit, sich dort für einen E-Mail-Benachrichtigungsservice zu registrieren, um über Änderungen informiert zu werden. Soweit die Prüfung/Audit des Kunden einen Anpassungsbedarf ergibt, ist dieser einvernehmlich umzusetzen.

(2) pco hat die Sicherheit gemäß Art. 28 Abs. 3 lit. c), 32 DSGVO, insbesondere i.V.m. Art. 5 Abs. 1, 2 DSGVO 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 DSGVO zu berücksichtigen.

(3) Die technischen und organisatorischen Maßnahmen unterliegen dem technischen Fortschritt und der Weiterentwicklung. pco gewährleistet, seinen Pflichten nach Art. 32 Abs. 1 Buchstabe d) DSGVO nachzukommen, ein Verfahren zur regelmäßigen Überprüfung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung einzusetzen. Insoweit ist es pco auch gestattet, alternative, adäquate Maßnahmen umzusetzen. Dabei darf das Sicherheitsniveau der festgelegten Maßnahmen nicht unterschritten werden. Wesentliche Änderungen sind zu dokumentieren.

5. Weisungsbefugnis des Kunden

(1) pco darf Daten von betroffenen Personen nur im Rahmen der Leistungsvereinbarung und der Weisungen des Kunden verarbeiten, außer es liegt ein Ausnahmefall im Sinne des Art. 28 Abs. 3 lit. a DSGVO vor. pco verwendet darüber hinaus die zur Verarbeitung überlassenen Daten für keine anderen, insbesondere nicht für eigene Zwecke.

(2) Die Weisungen werden anfänglich durch die Leistungsvereinbarung oder diese Bedingungen festgelegt und können vom Kunden danach in schriftlicher Form oder in einem elektronischen Format (Textform) an die von pco bezeichnete Stelle durch einzelne Weisungen geändert, ergänzt oder ersetzt werden (Einzelweisung). Mündliche Weisungen sind unverzüglich schriftlich oder in Textform zu bestätigen.

(3) pco hat den Kunden unverzüglich zu informieren, wenn eine Weisung gegen Datenschutzvorschriften verstößt. pco ist berechtigt, die Durchführung der entsprechenden Weisung so lange auszusetzen, bis sie durch den Kunden bestätigt oder geändert wird.

6. Auskunft, Berichtigung, Löschung und Einschränkung von Daten

(1) pco darf die Daten, die im Auftrag verarbeitet werden, nicht eigenmächtig, sondern nur nach dokumentierter Weisung des Kunden beauskunften, berichtigen, löschen oder deren Verarbeitung einschränken. Soweit eine betroffene Person sich diesbezüglich unmittelbar an pco wendet, wird pco dieses Ersuchen unverzüglich an den Kunden weiterleiten, sofern eine Zuordnung zum Kunden nach Angaben der betroffenen Person möglich ist. pco unterstützt den Kunden im Rahmen seiner Möglichkeiten auf Weisung, soweit vereinbart. pco haftet nicht, wenn das Ersuchen der betroffenen Person vom Kunden nicht, nicht richtig oder nicht fristgerecht beantwortet wird.

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

7. Qualitätssicherung und sonstige Pflichten von pco

(1) Der Kunde ist im Rahmen dieses Vertrages für die Einhaltung der gesetzlichen Bestimmungen der Datenschutzgesetze, insbesondere für die Rechtmäßigkeit der Datenweitergabe an pco, sowie für die Rechtmäßigkeit der Datenverarbeitung verantwortlich („Verantwortlicher“ im Sinne des Art. 4 Nummer 7 DSGVO).

(2) pco benennt einen Datenschutzbeauftragten, der seine Tätigkeit gemäß Art. 38 und 39 DSGVO ausübt. Dessen Kontaktdaten sind auf der Webseite von pco leicht zugänglich hinterlegt.

(3) pco setzt bei der Durchführung der Arbeiten nur Beschäftigte ein, die auf die Wahrung der Vertraulichkeit gemäß Art. 28 Abs. 3 S. 2 lit. b, 29, 32 Abs. 4 DSGVO verpflichtet und zuvor mit den für sie relevanten Bestimmungen zum Datenschutz vertraut gemacht wurden. pco und jede von pco unterstellte Person, die Zugang zu personenbezogenen Daten hat, darf diese Daten ausschließlich entsprechend der Weisung des Kunden verarbeiten einschließlich der in diesen Bedingungen eingeräumten Befugnisse, es sei denn, eine gesetzliche Verpflichtung steht dem entgegen. Diese Verpflichtungen bestehen auch nach Beendigung des Auftrages fort.

(4) Der Kunde und pco arbeiten auf Anfrage mit der Aufsichtsbehörde bei der Erfüllung ihrer Aufgaben zusammen.

(5) pco informiert unverzüglich den Kunden 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 Geschäftsbeziehung bei pco ermittelt.

(6) Soweit der Kunde 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 bei pco ausgesetzt ist, hat ihn pco nach besten Kräften zu unterstützen.

(7) pco 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.

(8) Im Falle einer Inanspruchnahme des Kunden durch eine betroffene Person hinsichtlich etwaiger Ansprüche nach Art. 82 DSGVO, verpflichtet sich pco, den Kunden bei der Abwehr des Anspruches im Rahmen seiner Möglichkeiten zu unterstützen.

8. Pflichten des Kunden

(1) Der Kunde ist verpflichtet, alle im Rahmen des Vertragsverhältnisses erlangten Kenntnisse von Geschäftsgeheimnissen und Datensicherheitsmaßnahmen von pco vertraulich zu behandeln. Diese Verpflichtung bleibt auch nach Beendigung dieses Vertrages bestehen.

(2) Der Kunde hat pco unverzüglich und vollständig zu informieren, wenn er in den Auftragsergebnissen Fehler oder Unregelmäßigkeiten bzgl. datenschutzrechtlicher Bestimmungen feststellt.

(3) Im Falle einer Inanspruchnahme von pco durch eine betroffene Person hinsichtlich etwaiger Ansprüche nach Art. 82 DSGVO verpflichtet sich der Kunde, pco bei der Abwehr des Anspruches im Rahmen seiner Möglichkeiten zu unterstützen.

(4) Der Kunde nennt pco den Ansprechpartner für im Rahmen des Vertrages anfallende Datenschutzfragen.

9. Vereinbarung zur Wahrung des Berufsgeheimnisses nach § 203 StGB

(1) Sollten im Rahmen dieses Auftrages auch Daten verarbeitet werden, die unter ein Berufsgeheimnis (im Sinne von § 203 StGB) fallen, verpflichtet sich pco, über diese Berufsgeheimnisse Stillschweigen zu bewahren und sich nur insoweit Kenntnis von diesen Daten zu verschaffen, wie dies zur Erfüllung der ihm zugewiesenen Aufgaben erforderlich ist. Es obliegt dem Kunden, die Bewertung vorzunehmen, welche der zu verarbeitenden Daten dem Schutz von § 203 StGB unterliegen und dies für pco kenntlich zu machen.

(2) pco stellt sicher, dass alle mit der Verarbeitung von dem Berufsgeheimnis unterliegenden Daten des Kunden befassten Beschäftigten und andere für pco tätigen Personen (z.B. Subunternehmer), die damit befasst sind, sich in Textform dazu verpflichtet haben, die ihnen bei der Ausübung oder bei Gelegenheit ihrer Tätigkeit bekannt gewordenen Berufsgeheimnisse nicht unbefugt zu offenbaren und sie über die mögliche Strafbarkeit nach § 203 Abs. 4 StGB belehrt wurden.

10. Unterauftragsverhältnisse

(1) Der Kunde erteilt pco die allgemeine Genehmigung Unterauftragnehmer i.S.d. Art. 28 DSGVO in Anspruch zu nehmen.

(2) Die jeweils aktuell eingesetzten Unterauftragnehmer kann der Kunde unter www.pco-online.de/docs abrufen. Sämtliche vertraglichen Regelungen dieses Vertrages werden auch jedem (weiteren) Unterauftragnehmer auferlegt.

(3) pco veröffentlicht Informationen über geplante Änderungen hinsichtlich der eingesetzten

Unterauftragnehmer auf www.pco-online.de/docs mit angemessener Vorlaufzeit, in der Regel mindestens 14 Tage vor deren erstmaligem Einsatz. Kunden haben dort die Möglichkeit, sich für einen E-Mail-Benachrichtigungsservice zu registrieren, um über Änderungen informiert zu werden.

(4) Der Kunde kann gegen den Einsatz eines Unterauftragnehmers aus wichtigem datenschutzrechtlichem Grund innerhalb angemessener Frist nach Veröffentlichung der Änderung Einspruch erheben. Erfolgt kein fristgerechter Einspruch, gilt die Änderung als genehmigt. Im Falle eines berechtigten Einspruchs wird pco nach eigener Wahl

a) die Leistung ohne den betreffenden Unterauftragnehmer erbringen oder
b) sofern dies pco wirtschaftlich oder technisch nicht zumutbar ist, die von der Änderung betroffene Leistung mit angemessener Frist kündigen.

(5) Erbringt der Unterauftragnehmer die vereinbarte Leistung außerhalb der EU/des EWR, stellt pco die datenschutzrechtliche Zulässigkeit durch entsprechende Maßnahmen unter den Voraussetzungen der Art. 44 ff. DSGVO sicher.

11. Kontrollrechte des Kunden

(1) Der Kunde hat das Recht, im Benehmen mit pco 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, zu den üblichen Geschäftszeiten ohne Störung des Betriebsablaufs von der Einhaltung dieses Vertrages durch pco in dessen Geschäftsbetrieb zu überzeugen. pco darf die Kontrollen von der vorherigen Anmeldung mit angemessener Vorlaufzeit und von der Unterzeichnung einer Verschwiegenheitserklärung und der eingerichteten technischen und organisatorischen Maßnahmen abhängig machen. Sollte der durch den Kunden beauftragte Prüfer in einem Wettbewerbsverhältnis zu pco stehen, hat pco gegen diesen ein Einspruchsrecht.

(2) Die Parteien gehen davon aus, dass eine Kontrolle höchstens einmal jährlich erforderlich ist. Weitere Prüfungen sind vom Kunden unter Angabe des Anlasses zu begründen. Im Falle von Vor-Ort-Kontrollen wird der Kunde pco die entstehenden Aufwände inkl. der Personalkosten für die Betreuung und Begleitung der Kontrollpersonen vor Ort in Höhe der vereinbarten Stundensätze, hilfsweise zu den jeweils aktuell gültigen Beraterkosten von pco ersetzen. Die Grundlagen der Kostenberechnung werden dem Kunden von pco vor Durchführung der Kontrolle mitgeteilt.

(3) pco stellt sicher, dass sich der Kunde von der Einhaltung der Pflichten nach Art. 28 DSGVO überzeugen kann. pco verpflichtet sich, dem Kunden auf Anforderung die erforderlichen Auskünfte zu erteilen und insbesondere die Umsetzung der technischen und organisatorischen Maßnahmen nachzuweisen.

(4) Der Nachweis solcher Maßnahmen, die nicht nur den konkreten Auftrag betreffen, kann z.B. erfolgen durch

- die Einhaltung genehmigter Verhaltensregeln gemäß Art. 40 DSGVO,
- 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 oder ISO 27001)

Die Vorlage solcher Nachweise ersetzt nicht die Pflicht von pco zur Dokumentation der technischen und organisatorischen Maßnahmen.

12. Mitteilung bei Verstößen von pco

(1) pco unterstützt den Kunden bei der Einhaltung der in den Artikeln 32 bis 36 der DSGVO 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 Kunden zu melden und hierbei zumindest folgende Informationen mitzuteilen:
   - eine Beschreibung der Art der Verletzung, der Kategorien und ungefähre Anzahl der betroffenen Personen und Datensätze,
   - Name und Kontaktdaten eines Ansprechpartners für weitere Informationen,
   - eine Beschreibung der wahrscheinlichen Folgen der Verletzung sowie
   - eine Beschreibung der ergriffenen Maßnahmen zur Behebung oder Abmilderung der Verletzung.
c) Die Verpflichtung, dem Kunden 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 Kunden bei dessen Datenschutzfolgenabschätzung.
e) Die Unterstützung des Kunden im Rahmen vorheriger Konsultationen mit der Aufsichtsbehörde.

(2) pco verpflichtet sich ferner, unverzüglich über relevante Änderungen von Überprüfungsergebnissen im Datenschutz mitzuteilen, wie z.B. den Ausschluss von genehmigten Verhaltensregeln nach Art. 41 Abs. 4 DSGVO oder den Widerruf einer Zertifizierung nach Art. 42 Abs. 7 DSGVO.

13. Löschung und Rückgabe von personenbezogenen Daten

(1) Nach Beendigung der jeweiligen Leistungsvereinbarung hat pco nach Wahl des Kunden sämtliche im Auftrag verarbeiteten personenbezogenen Daten entweder zurückzugeben oder datenschutzgerecht zu löschen, sofern keine gesetzliche Verpflichtung zur weiteren Speicherung besteht. Der Kunde teilt pco seine Wahl rechtzeitig vor Vertragsende in Textform mit. Erfolgt keine entsprechende Weisung, ist pco berechtigt, die Daten nach einer angemessenen Übergangsfrist datenschutzgerecht zu löschen. Gesetzliche Aufbewahrungspflichten bleiben unberührt.

(2) Die Löschung umfasst auch vorhandene Kopien und Sicherungsbestände. Soweit eine unmittelbare Löschung aus technischen Gründen nicht möglich ist, insbesondere bei Datensicherungen, erfolgt diese im Rahmen der dokumentierten Lösch- und Aufbewahrungszyklen. Bis zur endgültigen Löschung werden die betreffenden Daten angemessen geschützt und nicht mehr für andere Zwecke verarbeitet.

(3) Die Rückgabe und Löschung erfolgen im Rahmen der vertraglich vereinbarten Leistungen. Entstehen durch besondere Vorgaben des Kunden zusätzliche Aufwände, insbesondere hinsichtlich Datenformat, Übertragungsweg oder vorzeitiger Löschung, können diese nach den vereinbarten Vergütungssätzen berechnet werden. Die zur Erfüllung gesetzlicher Pflichten erforderliche Rückgabe oder Löschung bleibt hiervon unberührt. pco dokumentiert die Durchführung der Löschung in geeigneter Weise und bestätigt diese dem Kunden auf Anfrage.

14. Haftung

(1) Die Haftung der Parteien gegenüber betroffenen Personen sowie etwaige Ausgleichsansprüche zwischen den Parteien richten sich nach den gesetzlichen Bestimmungen, insbesondere Art. 82 DSGVO.

(2) Im Übrigen gelten für die Haftung der Parteien untereinander die Haftungsregelungen der jeweiligen Leistungsvereinbarung, soweit diese gesetzlich zulässig und wirksam sind. Zwingende gesetzliche Haftungsbestimmungen bleiben unberührt.

15. Sonstiges

(1) Änderungen und Ergänzungen dieser Vereinbarung und aller seiner Bestandteile – einschließlich etwaiger Zusicherungen von pco – bedürfen der Schriftform und des ausdrücklichen Hinweises darauf, dass es sich um eine Änderung bzw. Ergänzung dieser Vereinbarung handelt. Dies gilt auch für den Verzicht auf dieses Formerfordernis.

(2) Im Falle eines Widerspruchs zwischen einem Hauptvertrag oder einer anderweitigen getroffenen Regelung und dieser Vereinbarung, geht diese Vereinbarung in jedem Fall vor, soweit der Widerspruch die Verarbeitung personenbezogener Daten betrifft, selbst dann, wenn ein Hauptvertag oder eine anderweitig getroffene Regelung vorrangig sein soll.

(3) Sollten einzelne Teile dieser Vereinbarung unwirksam sein, so berührt dies die Wirksamkeit des Vertrages im Übrigen nicht. Anstelle der unwirksamen Bestimmungen haben die Parteien eine Regelung zu treffen, die dem Sinn und Zweck dieses Vertrages am nächsten kommt.

(4) Als ausschließlicher Gerichtsstand für Streitigkeiten aus und im Zusammenhang mit diesem Vertrag wird der Geschäftssitz von pco vereinbart. pco ist allerdings berechtigt, jedes ansonsten zuständige Gericht anzurufen.

(5) Es gilt deutsches Recht.

Für den Auftragnehmer	**Für den Auftraggeber**
Datum: 30.10.2026	Datum:
Name und Funktion: André Kramer, Geschäftsführer	Name und Funktion:
Unterschrift:	Unterschrift:
_____	_____

Anlage 1

Betroffene Personen, Kategorien von Daten

Allgemeines:

Diese Anlage beschreibt die Kategorien betroffener Personen und die Arten personenbezogener Daten, die im Rahmen der zwischen dem Kunden und pco vereinbarten Leistungen verarbeitet werden können.

Die nachfolgenden Aufzählungen sind nicht abschließend. Welche Kategorien im Einzelfall tatsächlich betroffen sind, ergibt sich aus den jeweiligen Leistungsvereinbarungen, der vertragsgemäßen Nutzung der Leistungen durch den Kunden sowie dessen dokumentierten Weisungen.

Die Aufzählungen begründen keine eigenständige Berechtigung zur Verarbeitung sämtlicher genannter Daten.

Kategorien betroffener Personen:

Im Rahmen der vereinbarten Leistungen können insbesondere personenbezogene Daten folgender Personengruppen verarbeitet werden:

- **Beschäftigte und Bewerber**: Mitarbeiter, ehemalige Mitarbeiter, Bewerber, Auszubildende, freie Mitarbeiter und sonstige für den Kunden tätige Personen.
- **Kunden und Geschäftspartner**: Kunden, Interessenten, Lieferanten, Dienstleister, Geschäftspartner und deren Ansprechpartner.
- **Nutzer von IT-Systemen**: Interne und externe Nutzer, Administratoren sowie Personen, die mit den IT-Systemen und Anwendungen des Kunden interagieren.
- **Weitere betroffene Personen**: Patienten, Mandanten, Mitglieder, Besucher, Angehörige, Minderjährige sowie sonstige Personen, deren Daten im Rahmen der vereinbarten Leistungen verarbeitet werden.

Kategorien personenbezogener Daten:

Abhängig von den vereinbarten Leistungen können insbesondere folgende Datenkategorien verarbeitet werden:

- **Stamm- und Kontaktdaten**: Namen, Anschriften, Kontaktdaten, Geburtsdaten und Identifikationsnummern.
- **Vertrags- und Geschäftsdaten**: Vertrags-, Bestell-, Rechnungs-, Kunden-, Lieferanten- und Kommunikationsdaten.
- **Benutzer- und Zugangsdaten**: Benutzerkennungen, Authentifizierungsdaten, Berechtigungen und Zugriffsrechte.
- **IT- und Nutzungsdaten**: IP-Adressen, Gerätekennungen, System-, Netzwerk-, Protokoll-, Nutzungs- und Standortdaten.
- **Finanz- und Beschäftigtendaten**: Zahlungs-, Bank-, Versicherungs-, Personal-, Bewerbungs-, Gehalts- und Ausbildungsdaten.
- **Inhalts- und Kommunikationsdaten**: E-Mails, Dokumente, Dateien, Datenbankinhalte, Bild-, Video- und Audiodaten.

- **Analyse- und Profildaten**: Nutzungsprofile, pseudonymisierte Kennungen, Auswertungen und sonstige abgeleitete personenbezogene Informationen.
- **Besondere Kategorien personenbezogener Daten gemäß Art. 9 DSGVO**: Insbesondere Gesundheitsdaten, biometrische und genetische Daten sowie Angaben zur ethnischen Herkunft, politischen Meinung, religiösen oder weltanschaulichen Überzeugung, Gewerkschaftszugehörigkeit oder zum Sexualleben und zur sexuellen Orientierung.
- **Daten gemäß Art. 10 DSGVO**: Personenbezogene Daten über strafrechtliche Verurteilungen, Straftaten und damit zusammenhängende Sicherungsmaßregeln.
- **Sonstige personenbezogene Daten**: Weitere personenbezogene Daten im Sinne des Art. 4 Nr. 1 DSGVO, soweit deren Verarbeitung vom vereinbarten Leistungsumfang umfasst und hinreichend bestimmbar ist.

Umfang der Verarbeitung:

Die tatsächliche Verarbeitung beschränkt sich auf die Datenkategorien und Personengruppen, die im Rahmen der jeweiligen Leistungsvereinbarungen und dokumentierten Weisungen des Kunden verarbeitet werden.

Die Aufnahme einer Datenkategorie oder Personengruppe in diese Anlage bedeutet nicht, dass diese im Rahmen jeder Leistung tatsächlich verarbeitet wird.

Die Verantwortung für die Rechtmäßigkeit der vom Kunden veranlassten Verarbeitung liegt beim Kunden. Die gesetzlichen Verpflichtungen von pco als Auftragsverarbeiter bleiben unberührt.