Vertrag über die Auftragsverarbeitung personenbezogener Daten

Zwischen	und
Auftraggeber gemäß Online-Beauftragung der pCDS-propdation® Cloud Data Services	**propdation Systems GmbH** Egerländer Str. 1 35510 Butzbach *vertreten durch* Dr. Raffaele M. Mattiello Mob.: +49 172 69 31 560 E-Mail: r.mattiello@propdation.com im Folgenden: **Auftragnehmer**

1 Einleitung, Geltungsbereich, Definitionen

(1) Dieser Vertrag regelt die Rechte und Pflichten von Auftraggeber und -nehmer (im Folgenden „Parteien“ genannt) im Rahmen einer Verarbeitung von personenbezogenen Daten im Auftrag.
(2) Dieser Vertrag findet auf alle Tätigkeiten Anwendung, bei denen Mitarbeiter des Auftragnehmers oder durch ihn beauftragte Unterauftragnehmer (Subunternehmer) personenbezogene Daten des Auftraggebers in dessen Auftrag verarbeiten.
(3) In diesem Vertrag verwendete Begriffe sind entsprechend ihrer Definition in der EU Datenschutz-Grundverordnung zu verstehen. In diesem Sinne ist der Auftraggeber der „Verantwortliche“, der Auftragnehmer der „Auftragsverarbeiter“. 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 der Verarbeitung

2.1 Gegenstand

(1) Der Auftragnehmer verarbeitet im Rahmen der pCDS-propdation® Cloud Data Services (im Folgenden pCDS) personenbezogene Daten für den Mandanten insbesondere im Zusammenhang mit der Beschaffung und Integration externer Daten über kommerzieller Drittdienstleister.
(2) Die Verarbeitung beruht auf den AGB der propdation Systems GmbH in der Version Stand 03/2023 inklusive Leistungsbeschreibung in der Version 1.02 20230415 (im folgenden **AGB**).

2.2 Dauer

(1) Die Verarbeitung beginnt mit der Online-Auftragsbestätigung und endet mit den vereinbarten Leistungen gemäß AGB.

2.3 Bestandteile

Bestandteile des Vertrages sind dieser Vertrag und **Anhänge 1-4**.

© propdation Systems März 2024, Version 2.3

3 Art, Zweck und Betroffene der Datenverarbeitung:

3.1 Art und Zweck der Verarbeitung

(1) Die Verarbeitung ist folgender Art: Erheben, Erfassen, Organisation, Ordnen, Speicherung, Anpassung oder Veränderung, Auslesen, Abfragen, Verwendung, Offenlegung durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung, Abgleich oder Verknüpfung, Einschränkung, Löschen oder Vernichtung von Daten.

(2) Die Verarbeitung dient folgendem Zweck: Integration von Dienstleistungen Dritter und digitale Datenverarbeitung anhand der pCDS.

3.2 Art der Daten

(1) Gegenstand der Verarbeitung personenbezogener Daten sind folgende Datenarten/-kategorien (Aufzählung/Beschreibung der Datenkategorien):
Personenstammdaten (u.a. Namen, Geschlecht, Adressen, Geburtsdatum, Geburtsort), Kommunikationsdaten (z.B. Telefon, E-Mail), Bonitätsdaten (u.a. Merkmale, Zahlungsverhalten, Scores), soziodemografische Kennzeichen, Vertragsstammdaten (Abonnements, Produkt- bzw. Vertragsinteressen), Kundenhistorien, Vertragsabrechnungs- und Zahlungsdaten, Planungs- und Steuerungsdaten, Aktivitätsdaten (z.B. Click-Verhalten, Bestell- und Teilnahmehistorien) , jegliche sonstige Auskunftsangaben von Dritten (z.B. Auskunfteien, oder öffentliche Verzeichnisse).

3.3 Kategorien der betroffenen Personen

Von der Verarbeitung betroffen sind:

- Kunden (inkl. Schuldner)
- Interessenten
- Beschäftigte
- Ansprechpartner
- Lieferanten
- Abonnenten
- Vermittler

4 Pflichten des Auftragnehmers

(1) Der Auftragnehmer verarbeitet personenbezogene Daten ausschließlich wie vertraglich vereinbart oder wie vom Auftraggeber angewiesen, es sei denn, der Auftragnehmer ist gesetzlich zu einer bestimmten Verarbeitung verpflichtet. Sofern solche Verpflichtungen für ihn bestehen, teilt der Auftragnehmer diese dem Auftraggeber vor der Verarbeitung mit, es sei denn, die Mitteilung ist ihm gesetzlich verboten. Der Auftragnehmer verwendet darüber hinaus die zur Verarbeitung überlassenen Daten für keine anderen, insbesondere nicht für eigene Zwecke.

(2) Der Auftragnehmer bestätigt, dass ihm die einschlägigen, allgemeinen datenschutzrechtlichen Vorschriften bekannt sind. Er beachtet die Grundsätze ordnungsgemäßer Datenverarbeitung.

(3) Der Auftragnehmer verpflichtet sich, bei der Verarbeitung die Vertraulichkeit streng zu wahren.

(4) Personen, die Kenntnis von den im Auftrag verarbeiteten Daten erhalten können, haben sich schriftlich zur Vertraulichkeit zu verpflichten, soweit sie nicht bereits gesetzlich einer einschlägigen Geheimhaltungspflicht unterliegen.

(5) Der Auftragnehmer sichert zu, dass die bei ihm zur Verarbeitung eingesetzten Personen vor Beginn der Verarbeitung mit den relevanten Bestimmungen des Datenschutzes und dieses Vertrags vertraut gemacht wurden. Entsprechende Schulungs- und Sensibilisierungsmaßnahmen sind angemessen regelmäßig zu wiederholen. Der Auftragnehmer trägt dafür Sorge, dass zur Auftragsverarbeitung eingesetzte Personen hinsichtlich der Erfüllung der Datenschutzanforderungen laufend angemessen angeleitet und überwacht werden.

(6) Im Zusammenhang mit der beauftragten Verarbeitung unterstützt der Auftragnehmer den Auftraggeber soweit erforderlich bei der Erfüllung seiner datenschutzrechtlichen Pflichten, insbesondere bei Erstellung und Fortschreibung des Verzeichnisses der Verarbeitungstätigkeiten, bei Durchführung der Datenschutzfolgeabschätzung und einer notwendigen Konsultation der Aufsichtsbehörde. Die erforderlichen Angaben und Dokumentationen sind vorzuhalten und dem Auftraggeber auf Anforderung unverzüglich zuzuleiten.

(7) Wird der Auftraggeber durch Aufsichtsbehörden oder andere Stellen einer Kontrolle unterzogen oder machen betroffene Personen ihm gegenüber Rechte geltend, verpflichtet sich der Auftragnehmer den Auftraggeber im erforderlichen Umfang zu unterstützen, soweit die Verarbeitung im Auftrag betroffen ist.

(8) Auskünfte an Dritte oder den Betroffenen darf der Auftragnehmer nur nach vorheriger Zustimmung durch den Auftraggeber erteilen. Direkt an ihn gerichtete Anfragen wird er unverzüglich an den Auftraggeber weiterleiten.
(9) Soweit gesetzlich verpflichtet, bestellt der Auftragnehmer eine fachkundige und zuverlässige Person als Beauftragten für den Datenschutz. Es ist sicherzustellen, dass für den Beauftragten keine Interessenskonflikte bestehen. In Zweifelsfällen kann sich der Auftraggeber direkt an den Datenschutzbeauftragten wenden. Der Auftragnehmer teilt dem Auftraggeber unverzüglich die Kontaktdaten des Datenschutzbeauftragten mit oder begründet, weshalb kein Beauftragter bestellt wurde. Änderungen in der Person oder den innerbetrieblichen Aufgaben des Beauftragten teilt der Auftragnehmer dem Auftraggeber unverzüglich mit. Der Datenschutzbeauftragte des Auftragnehmers ist in **Anhang 3** genannt.
(10) Die Auftragsverarbeitung erfolgt grundsätzlich innerhalb der EU oder des EWR. Jegliche Verlagerung in ein Drittland darf nur mit ausdrücklicher Zustimmung des Auftraggebers und unter den in Kapitel V der Datenschutz-Grundverordnung enthaltenen Bedingungen sowie bei Einhaltung der Bestimmungen dieses Vertrags erfolgen.
(11) Ist der Auftragnehmer nicht in der Europäischen Union niedergelassen, bestellt er, soweit verpflichtet, einen verantwortlichen Ansprechpartner in der Europäischen Union gem. Art. 27 Datenschutz-Grundverordnung. Die Kontaktdaten des Ansprechpartners sowie sämtliche Änderungen in der Person des Ansprechpartners sind dem Auftraggeber unverzüglich mitzuteilen.

5 Sicherheit der Verarbeitung

(1) Die im **Anhang 1** beschriebenen Datensicherheitsmaßnahmen werden als verbindlich festgelegt. Sie definieren das vom Auftragnehmer geschuldete Minimum. Die Beschreibung der Maßnahmen muss so detailliert erfolgen, dass für einen sachkundigen Dritten allein aufgrund der Beschreibung jederzeit zweifelsfrei erkennbar ist, was das geschuldete Minimum sein soll. Ein Verweis auf Informationen, die dieser Vereinbarung oder ihrem **Anhang** nicht unmittelbar entnommen werden können, ist nicht zulässig.
(2) Diese Maßnahmen im **Anhang 1** beziehen sich vornehmlich auf die Verarbeitung von Daten auf einem durch den Auftragnehmer gestellten, jedoch sowohl dem Auftraggeber als auch dem Auftragnehmer zugänglichen System zum Aufbau eines Systems mit Echtdaten. Für Arbeiten auf den Systemen des Auftraggebers ist der Auftraggeber für die Einhaltung von technischen und organisatorischen Maßnahmen verantwortlich.
(3) Die Datensicherheitsmaßnahmen können der technischen und organisatorischen Weiterentwicklung entsprechend angepasst werden, solange das hier vereinbarte Niveau nicht unterschritten wird. Zur Aufrechterhaltung der Informationssicherheit erforderliche Änderungen hat der Auftragnehmer unverzüglich umzusetzen. Änderungen sind dem Auftraggeber unverzüglich mitzuteilen. Wesentliche Änderungen sind zwischen den Parteien zu vereinbaren.
(4) Soweit die getroffenen Sicherheitsmaßnahmen den Anforderungen des Auftraggebers nicht oder nicht mehr genügen, benachrichtigt der Auftragnehmer den Auftraggeber unverzüglich.
(5) Der Auftragnehmer sichert zu, dass die im Auftrag verarbeiteten Daten von sonstigen Datenbeständen strikt logisch getrennt werden.
(6) Kopien oder Duplikate werden ohne Wissen des Auftraggebers nicht erstellt. Ausgenommen sind technisch notwendige, temporäre Vervielfältigungen, soweit eine Beeinträchtigung des hier vereinbarten Datenschutzniveaus ausgeschlossen ist.
(7) Die Verarbeitung von Daten zum Zweck der Analyse, Migration, Qualitätssicherung oder in Support-Fällen ist auf Mobilen Endgeräten (Laptops) unabhängig vom Einsatzort gestattet, soweit Zutritt- und Zugangskontrolle durch z.B. die jeweilige Nutzung nur durch eine dedizierte Person sowie die Daten des Auftraggebers durch passwortgeschützten Zugang und verschlüsselte Ablagen der dedizierten Person mit Zugriff auf das Gerät gesichert sind und Daten ausschließlich über verschlüsselte Verbindungen (VPN, SSH) ausgetauscht werden. Die Verarbeitung von Daten im Rahmen der zum Zweck der Analyse, Migration, Qualitätssicherung oder in Support-Fällen als Remote-Service ist ausdrücklich auch in Privatwohnungen gestattet, muss dort jedoch in einem dafür vorgesehenen abgetrennten Arbeitsbereich stattfinden.
(8) In allen anderen Fällen außer (7) ist die Verarbeitung von Daten in Privatwohnungen nur mit vorheriger schriftlicher Zustimmung des Auftraggebers im Einzelfall gestattet. Soweit eine solche Verarbeitung erfolgt, ist vom Auftragnehmer sicherzustellen, dass dabei ein diesem Vertrag entsprechendes Niveau an Datenschutz und Datensicherheit aufrechterhalten wird und die in diesem Vertrag bestimmten Kontrollrechte des Auftraggebers uneingeschränkt auch in den betroffenen Privatwohnungen ausgeübt werden können. Die Verarbeitung von Daten im Auftrag mit Privatgeräten ist unter keinen Umständen gestattet.

(9) Dedizierte Datenträger, die vom Auftraggeber stammen bzw. für den Auftraggeber genutzt werden, werden besonders gekennzeichnet und unterliegen der laufenden Verwaltung. Sie sind jederzeit angemessen aufzubewahren und dürfen unbefugten Personen nicht zugänglich sein. Ein- und Ausgänge werden dokumentiert.

(10) Der Auftragnehmer ist mit angemessener Vorankündigung dazu berechtigt, die Erfüllung der Pflichten des Auftragnehmers zu kontrollieren. Alternativ weist der Auftragnehmer in regelmäßigen Zeitabständen oder nach Aufforderung des Auftraggebers die Erfüllung seiner Pflichten nach, insbesondere der vollständigen Umsetzung der vereinbarten technischen und organisatorischen Maßnahmen sowie ihrer Wirksamkeit. Der Nachweis kann durch genehmigte Verhaltensregeln oder ein genehmigtes Zertifizierungsverfahren erbracht werden. Nachweise sind mindestens bis zum Ablauf drei Kalenderjahren nach Beendigung der Auftragsverarbeitung aufzubewahren und dem Auftraggeber jederzeit auf Verlangen vorzulegen.

6 Regelungen zur Berichtigung, Löschung und Sperrung von Daten

(1) Im Rahmen des Auftrags verarbeitete Daten wird der Auftragnehmer nur entsprechend der getroffenen vertraglichen Vereinbarung oder nach Weisung des Auftraggebers berichtigen, löschen oder sperren.

(2) Den entsprechenden Weisungen des Auftraggebers wird der Auftragnehmer jederzeit und auch über die Beendigung dieses Vertrages hinaus Folge leisten.

7 Unterauftragsverhältnisse

(1) Die Beauftragung von Subunternehmern ist nur mit schriftlicher Zustimmung des Auftraggebers im Einzelfall zugelassen.

(2) Die Zustimmung ist nur möglich, wenn dem Subunternehmer vertraglich mindestens Datenschutzpflichten auferlegt wurden, die den in diesem Vertrag vereinbarten vergleichbar sind.

(3) Die Verantwortlichkeiten des Auftragnehmers und des Subunternehmers sind eindeutig voneinander abzugrenzen.

(4) Eine weitere Subbeauftragung durch den Subunternehmer ist nur zulässig, sofern sämtliche Rechte und Pflichten dieser Vereinbarung mit Wirkung für den Auftraggeber auch auf Sub-Subunternehmer weiterübertragen werden.

(5) Der Auftragnehmer wählt den Subunternehmer unter besonderer Berücksichtigung der Eignung der vom Subunternehmer getroffenen technischen und organisatorischen Maßnahmen sorgfältig aus.

(6) Die Weiterleitung von im Auftrag verarbeiteten Daten an den Subunternehmer ist erst zulässig, wenn sich der Auftragnehmer dokumentiert davon überzeugt hat, dass der Subunternehmer seine Verpflichtungen vollständig erfüllt hat.

(7) Die Beauftragung von Subunternehmern, die Verarbeitungen im Auftrag nicht ausschließlich aus dem Gebiet der EU oder des EWR erbringen, ist nur bei Beachtung der in Kapitel 4 (10) und (11) dieses Vertrages genannten Bedingungen möglich. Sie ist insbesondere nur zulässig, soweit und solange der Subunternehmer angemessene Datenschutzgarantien bietet. Der Auftragnehmer teilt dem Auftraggeber mit, welche konkreten Datenschutzgarantien der Subunternehmer bietet und wie ein Nachweis hierüber zu erlangen ist. Soweit aktuell gültige Standardvertragsklauseln auf Basis einer Entscheidung der EU-Kommission (z.B. gemäß Kommissionsentscheidung 2010/87/EU) oder Standarddatenschutzklauseln gem. Art. 46 DSGVO als angemessene Garantien eingesetzt werden, bevollmächtigt der Auftraggeber den Auftragnehmer unter Befreiung vom Verbot der Doppelvertretung gemäß § 181 BGB, zur Vornahme aller hierfür erforderlichen Handlungen sowie zur Abgabe und Entgegennahme von Willenserklärungen gegenüber dem Subunternehmer. Ferner ist der Auftragnehmer berechtigt, die Rechte und Befugnisse des Auftraggebers aus dieser Vereinbarung gegenüber dem Subunternehmer auszuüben.

(8) Der Auftragnehmer hat die Einhaltung der Pflichten des Subunternehmers angemessen zu überprüfen. Die Prüfung und ihr Ergebnis sind so aussagekräftig zu dokumentieren, dass sie für einen fachkundigen Dritten nachvollziehbar sind. Der Auftragnehmer bewahrt die Dokumentation über durchgeführte Prüfungen mindestens bis zum Ablauf des dritten Kalenderjahres nach Beendigung der Auftragsverarbeitung auf und legt diese dem Auftraggeber auf Verlangen jederzeit vor.

(9) Kommt der Subunternehmer seinen Datenschutzpflichten nicht nach, so haftet hierfür der Auftragnehmer gegenüber dem Auftraggeber.

(10) Zurzeit sind die in **Anhang 4** mit Namen, Anschrift und Auftragsinhalt bezeichneten Subunternehmer mit der Verarbeitung von personenbezogenen Daten in dem dort genannten Umfang beschäftigt und durch den Auftraggeber genehmigt. Die hier niedergelegten sonstigen Pflichten des Auftragnehmers gegenüber Subunternehmern bleiben unberührt.

(11) Unterauftragsverhältnisse im Sinne dieses Vertrags sind nur solche Leistungen, die einen direkten Zusammenhang mit der Erbringung der Hauptleistung aufweisen. Nebenleistungen, wie beispielsweise Transport, Wartung und Reinigung sowie die Inanspruchnahme von Telekommunikationsdienstleistungen (E-Mail, Telefonie), Rechenzentren (reine Colocation) oder Benutzerservice sind nicht erfasst. Die Pflicht des Auftragnehmers, auch in diesen Fällen die Beachtung von Datenschutz und Datensicherheit sicherzustellen, bleibt unberührt.

8 Rechte und Pflichten des Auftraggebers

(1) Für die Beurteilung der Zulässigkeit der beauftragten Verarbeitung sowie für die Wahrung der Rechte von Betroffenen ist allein der Auftraggeber verantwortlich.
(2) Der Auftraggeber erteilt alle Aufträge, Teilaufträge oder Weisungen dokumentiert. In Eilfällen können Weisungen mündlich erteilt werden. Solche Weisungen wird der Auftraggeber unverzüglich dokumentiert bestätigen.
(3) Der Auftraggeber informiert den Auftragnehmer unverzüglich, wenn er Fehler oder Unregelmäßigkeiten bei der Prüfung der Auftragsergebnisse feststellt.
(4) Der Auftraggeber ist berechtigt, die Einhaltung der Vorschriften über den Datenschutz und der vertraglichen Vereinbarungen beim Auftragnehmer in angemessenem Umfang selbst oder durch Dritte, insbesondere durch die Einholung von Auskünften und die Einsichtnahme in die gespeicherten Daten und die Datenverarbeitungsprogramme sowie sonstige Kontrollen vor Ort zu kontrollieren. Den mit der Kontrolle betrauten Personen ist vom Auftragnehmer soweit erforderlich Zutritt und Einblick zu ermöglichen. Der Auftragnehmer ist verpflichtet, erforderliche Auskünfte zu erteilen, Abläufe zu demonstrieren und Nachweise zu führen, die zur Durchführung einer Kontrolle erforderlich sind. Der Auftragnehmer ist berechtigt, Kontrollen durch Dritte zu verweigern, soweit diese mit ihm in einem Wettbewerbsverhältnis stehen oder ähnlich gewichtige Gründe vorliegen.
(5) Kontrollen beim Auftragnehmer haben ohne vermeidbare Störungen seines Geschäftsbetriebs zu erfolgen. Soweit nicht aus vom Auftraggeber zu dokumentierenden, dringlichen Gründen anders angezeigt, finden Kontrollen nach angemessener Vorankündigung und zu Geschäftszeiten des Auftragnehmers, sowie nicht häufiger als alle 12 Monate statt. Soweit der Auftragnehmer den Nachweis der korrekten Umsetzung der vereinbarten Datenschutzpflichten wie unter Kapitel 5 (8) dieses Vertrages vorgesehen erbringt, soll sich eine Kontrolle auf Stichproben beschränken.

9 Mitteilungspflichten

(1) Der Auftragnehmer teilt dem Auftraggeber Verletzungen des Schutzes im Auftrag verarbeiteter personenbezogener Daten unverzüglich mit. Auch begründete Verdachtsfälle hierauf sind mitzuteilen. Die Mitteilung hat spätestens innerhalb von 24 Stunden ab Kenntnis des Auftragnehmers vom relevanten Ereignis an eine vom Auftraggeber benannte Adresse zu erfolgen. Sie muss mindestens folgende Angaben enthalten:
    a. eine Beschreibung der Art der Verletzung des Schutzes personenbezogener Daten, soweit möglich mit Angabe der Kategorien und der ungefähren Zahl der betroffenen Personen, der betroffenen Kategorien und der ungefähren Zahl der betroffenen personenbezogenen Datensätze;
    b. den Namen und die Kontaktdaten des Datenschutzbeauftragten oder einer sonstigen Anlaufstelle für weitere Informationen;
    c. eine Beschreibung der wahrscheinlichen Folgen der Verletzung des Schutzes personenbezogener Daten;
    d. eine Beschreibung der vom Auftragnehmer ergriffenen oder vorgeschlagenen Maßnahmen zur Behebung der Verletzung des Schutzes personenbezogener Daten und gegebenenfalls Maßnahmen zur Abmilderung ihrer möglichen nachteiligen Auswirkungen

(2) Ebenfalls unverzüglich mitzuteilen sind erhebliche Störungen bei der Auftragserledigung sowie Verstöße des Auftragnehmers oder der bei ihm beschäftigten Personen gegen datenschutzrechtliche Bestimmungen oder die in diesem Vertrag getroffenen Festlegungen.
(3) Der Auftragnehmer informiert den Auftraggeber unverzüglich von Kontrollen oder Maßnahmen von Aufsichtsbehörden oder anderen Dritten, soweit diese Bezüge zur Auftragsverarbeitung aufweisen.
(4) Der Auftragnehmer sichert zu, den Auftraggeber bei dessen Pflichten nach Art. 33 und 34 Datenschutz-Grundverordnung im erforderlichen Umfang zu unterstützen.

10 Weisungen

(1) Der Auftraggeber behält sich hinsichtlich der Verarbeitung im Auftrag ein umfassendes Weisungsrecht vor.

(2) Auftraggeber und Auftragnehmer benennen die zur Erteilung und Annahme von Weisungen ausschließlich befugten Personen in **Anhang 2**.
(3) Bei einem Wechsel oder einer längerfristigen Verhinderung der benannten Personen sind der anderen Partei Nachfolger bzw. Vertreter unverzüglich mitzuteilen.
(4) Der Auftragnehmer wird den Auftraggeber unverzüglich darauf aufmerksam machen, wenn eine vom Auftraggeber erteilte Weisung seiner Meinung nach gegen gesetzliche Vorschriften verstößt. Der Auftragnehmer ist berechtigt, die Durchführung der entsprechenden Weisung solange auszusetzen, bis sie durch den Verantwortlichen beim Auftraggeber bestätigt oder geändert wird.
(5) Der Auftragnehmer hat ihm erteilte Weisungen und deren Umsetzung zu dokumentieren.

11 Beendigung des Auftrags

(1) Befinden sich bei Beendigung des Auftragsverhältnisses im Auftrag verarbeitete Daten oder Kopien derselben noch in der Verfügungsgewalt des Auftragnehmers, hat dieser des nach Wahl des Auftraggebers die Daten entweder zu vernichten oder an den Auftraggeber zu übergeben. Die Wahl hat der Auftraggeber innerhalb von 2 Wochen nach entsprechender Aufforderung durch den Auftragnehmer zu treffen. Die Vernichtung hat so zu erfolgen, dass eine Wiederherstellung auch von Restinformationen mit vertretbarem Aufwand nicht mehr möglich ist.
(2) Der Auftragnehmer ist verpflichtet, die unverzügliche Vernichtung bzw. Rückgabe auch bei Subunternehmern herbeizuführen.
(3) Der Auftragnehmer hat den Nachweis der ordnungsgemäßen Vernichtung zu führen und dem Auftraggeber unverzüglich vorzulegen.
(4) Dokumentationen, die dem Nachweis der ordnungsgemäßen Datenverarbeitung dienen, sind durch den Auftragnehmer mindestens bis zum Ablauf des dritten Kalenderjahres nach Vertragsende hinaus aufzubewahren. Er kann sie zu seiner Entlastung dem Auftraggeber übergeben.

12 Vergütung

Die Vergütung des Auftragnehmers ist abschließend durch die digitale Beauftragung eines **pCDS**-Paketes geregelt. Eine gesonderte Vergütung oder Kostenerstattung im Rahmen dieses Vertrages erfolgt nicht.

13 Haftung

(1) Für den Ersatz von Schäden, die eine Person wegen einer unzulässigen oder unrichtigen Datenverarbeitung im Rahmen des Auftragsverhältnisses erleidet, haften Auftraggeber und Auftragnehmer als Gesamtschuldner.
(2) Der Auftragnehmer trägt die Beweislast dafür, dass ein Schaden nicht Folge eines von ihm zu vertretenden Umstandes ist, soweit die relevanten Daten von ihm unter dieser Vereinbarung verarbeitet wurden. Solange dieser Beweis nicht erbracht wurde, stellt der Auftragnehmer den Auftraggeber auf erste Anforderung von allen Ansprüchen frei, die im Zusammenhang mit der Auftragsverarbeitung gegen den Auftraggeber erhoben werden. Unter diesen Voraussetzungen ersetzt der Auftragnehmer dem Auftraggeber ebenfalls sämtliche entstandenen Kosten der Rechtsverteidigung.
(3) Der Auftragnehmer haftet dem Auftraggeber für Schäden, die der Auftragnehmer, seine Mitarbeiter bzw. die von ihm mit der Vertragsdurchführung Beauftragten oder die von ihm eingesetzten Subdienstleister im Zusammenhang mit der Erbringung der beauftragten vertraglichen Leistung schuldhaft verursachen.
(4) Nummern (2) und (3) gelten nicht, soweit der Schaden durch die korrekte Umsetzung der beauftragten Dienstleistung oder einer vom Auftraggeber erteilten Weisung entstanden ist.

14 Sonderkündigungsrecht

(1) Der Auftraggeber kann die bestehende Beauftragung und diese Vereinbarung jederzeit ohne Einhaltung einer Frist kündigen („außerordentliche Kündigung“), wenn nachweisbar ein schwerwiegender Verstoß des Auftragnehmers gegen Datenschutzvorschriften oder die Bestimmungen dieser Vereinbarung vorliegt, der Auftragnehmer eine rechtmäßige Weisung des Auftraggebers nicht ausführen kann oder will oder der Auftragnehmer Kontrollrechte des Auftraggebers vertragswidrig verweigert.
(2) Ein schwerwiegender Verstoß liegt insbesondere vor, wenn der Auftragnehmer die in dieser Vereinbarung bestimmten Pflichten, insbesondere die vereinbarten technischen und organisatorischen Maßnahmen in erheblichem Maße nicht erfüllt oder nach einmaliger schriftlicher Abmahnung und Aufforderung zur Behebung der Mängel absehbar nicht erfüllen kann.

(3) Bei Verstößen setzt der Auftraggeber dem Auftragnehmer eine angemessene Frist zur Abhilfe. Erfolgt die Abhilfe nicht rechtzeitig, so ist der Auftraggeber zur außerordentlichen Kündigung wie in diesem Abschnitt beschrieben berechtigt.
(4) Der Auftragnehmer hat dem Auftraggeber Kosten zu erstatten, die diesem unmittelbar durch die verfrühte Beendigung der bestehenden Beauftragung oder dieses Vertrages in Folge einer außerordentlichen Kündigung durch den Aufraggeber entstehen.

15 Sonstiges

(1) Beide Parteien sind verpflichtet, alle im Rahmen des Vertragsverhältnisses erlangten Kenntnisse von Geschäftsgeheimnissen und Datensicherheitsmaßnahmen der jeweils anderen Partei auch über die Beendigung des Vertrages vertraulich zu behandeln. Bestehen Zweifel, ob eine Information der Geheimhaltungspflicht unterliegt, ist sie bis zur schriftlichen Freigabe durch die andere Partei als vertraulich zu behandeln.
(2) Sollte Eigentum des Auftraggebers beim Auftragnehmer durch Maßnahmen Dritter (etwa durch Pfändung oder Beschlagnahme), durch ein Insolvenz- oder Vergleichsverfahren oder durch sonstige Ereignisse gefährdet werden, so hat der Auftragnehmer den Auftraggeber unverzüglich zu verständigen.
(3) Für Nebenabreden sind die Schriftform und die ausdrückliche Bezugnahme auf diese Vereinbarung erforderlich.
(4) Die Einrede des Zurückbehaltungsrechts i. S. v. § 273 BGB wird hinsichtlich der im Auftrag verarbeiteten Daten und der zugehörigen Datenträger ausgeschlossen.
(5) Sollten einzelne Teile dieser Vereinbarung unwirksam sein, so berührt dies die Wirksamkeit der Vereinbarung im Übrigen nicht.

Anhang 1 – Technische und organisatorische Maßnahmen

Die nachstehend dargestellten TOM gelten für die Verarbeitungen von personenbezogenen Daten, welche in den Räumlichkeiten der propdation Systems GmbH sowie des Colocation Anbieters GHOSTnet GmbH / firstcolo GmbH automatisiert (mit Unterstützung von IT-Systemen) und auch nicht-automatisiert durchgeführt werden.

Mittels einer Richtlinie, welche an Mitarbeiter im Rahmen ihrer Einstellung ausgeben wird, wird die „Informationssicherheit am Arbeitsplatz“ geregelt (einschließlich mobiler Arbeiten).

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

- Zutrittskontrolle:
  Kein unbefugter Zutritt zu Datenverarbeitungsanlagen durch:
  - Die Server der propdation Systems GmbH und zur Unterstellung bereitgestellte Kunden-Server sind im Rechenzentrum der firstcolo GmbH in einem eigenen separaten Rack mit Stahlkäfig und separatem Schlüssel untergebracht, Standort: Kruppstr. 105, 60388 Frankfurt am Main.
  - Für den Fall, dass betriebsfremde Personen Zutritt zu Gebäudebereichen des Rechenzentrums benötigen, bestehen ausdrückliche Regelungen oder festgelegte Prozesse (etwa für den Zutritt für Wartungsarbeiten durch externes Personal).
  - Die genutzten Colocation Räume (https://firstcolo.net/colocation/) unterstehen der Zutrittskontrolle. Das Rechenzentrum kontrolliert den Zutritt und gewährt nur dem von propdation Systems benannten Personenkreis mit einstündiger Voranmeldung Zutritt zu den angemieteten Flächen (Identifikation z.B. durch Personalausweis).
  - Nur nach klaren Kriterien als befugt eingestufte Mitarbeiter haben Zutritt zu Gebäudebereichen des Rechenzentrums sowie Unternehmensservern in Racks.
  - Es existiert zusätzlich ein IT-gestütztes Zutrittskontrollsystem zur Überwachung des Betretens der Gebäudebereiche des Rechenzentrums.
  - Es besteht eine Kennzeichnungspflicht für betriebsfremde Personen durch sichtbar zu tragende Besucherausweise.
  - Das Rechenzentrum der firstcolo GmbH ist TÜV-zertifiziert (DIN EN 50600 und ISO/IEC 27001).

- Zugangskontrolle:
  Keine unbefugte Systembenutzung durch:
  - Der Zugang zu Arbeitsplätzen (PC’s, Laptops etc.) ist mit User-Kennungen und sicheren Passwörtern gesichert.
  - Die Arbeitsplätze (PC’s, Laptops etc.) werden bei Verlassen des Arbeitsplatzes gesperrt.
  - Datenablagen auf Arbeitsplätzen (PCs, Laptops etc.) unterliegen der personenspezifischen Verschlüsselung.
  - Die produktive serverseitige Gesamtsystemumgebung ist durch eine Firewall mit dedizierter Protokoll-/Portfreischaltung geschützt.
  - Virenscanner sind aktiviert und erkennen Unregelmäßigkeit auf den IT-Systemen.
  - Die Einsteuerung von Aufträgen und Abholung von Ergebnissen der Dienstleistungen geschieht ausschließlich unter Verwendung von (System-) Benutzerkonten mit Passwort-Schutz.
  - Bestimmte IT-Anwendungen sind zusätzlich mit einer 2-Faktor-Authentifizierung gesichert.
  - Der Systemzugriff, sei es durch Anwendungen, Systeme oder Personal des Kunden/Lieferanten, wird ausschließlich über Zugangssoftware ermöglicht, basiert auf den gängigen (auf Wunsch verschlüsselten) Protokollen (SFTP, FTPS, HTTPS, SSH/Socket), ist jeweils auf die für den Kunden/Lieferanten-Prozess relevanten Ablagestrukturen eingeschränkt und wird über die systemimmanenten Anwendungs- und System-Log-Dateien mitgeschrieben (z.B. Firewall (IDS)-, Web Server Logs, SFTP-Logs etc.).
  - Vertrauliche physikalische Dokumente (z.B. Dokumente zu Mitarbeitern) werden in Schränken verschlossen aufbewahrt.

- Zugriffskontrolle:
  Kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen innerhalb des Systems durch:
  - Ein Berechtigungskonzept regelt den Zugriff auf die Ressourcen der IT-Systeme, entweder mittels Rollen und Rechten oder durch Anweisung der Geschäftsführung.
  - Der Zugriff für pCDS/Portal-Kunden wird durch einen geregelten digitalen Freigabeprozesses erteilt.
  - Zugriff auf die produktiven Server haben ausschließlich der System-Administrator und dediziertes Support-Personal über entsprechende Benutzerschnittstellen, Werkzeuge und benutzerspezifischen Zugangskonten.
  - Der Zugriff auf Datenbanken ist durch zusätzliche Benutzerkonten mit unterschiedlichen Schreib/Lese-Rechten und teilweise verschlüsselter Ablage gesichert.
  - Der allgemeine Systemzugriff, sei es durch Anwendungen oder Personal, wird über die systemimmanenten Anwendungs- und System-Log-Dateien mitgeschrieben (z.B. Datenbank-Logs, Applikationslogs, Firewall-Logs mit Endpoint-IDS) und regelmäßig kontrolliert.
  - Vereinzelte serverseitige manuelle Eingriffe zur Systempflege und Betrieb wie z.B. Sicherungskopien oder Software-/Systemupgrades geschehen ausschließlich durch dediziertes Personal mit VPN-Zugang und personalisierten Administratoren-Konten und werden anhand organisatorischer Maßnahmen überwacht.
  - Es existieren Anweisungen zum Umgang mit nicht mehr benötigten Datenträgern. Dies schließt den Umgang mit beschriebenem oder bedrucktem Papier ein.
  - Es existiert eine Anweisung zur Entsorgung oder Weiterverwendung von Geräten, die mit Speichermedien ausgerüstet sind.
  - Dokumente und Datenträger, deren gesetzliche, vertragliche oder satzungsmäßige Aufbewahrungsdauer abgelaufen ist, werden vernichtet.

- Trennungskontrolle:
  Getrennte Verarbeitung von Daten, die zu unterschiedlichen Zwecken erhoben wurden, durch:
  - Basis der Software-Architektur, Schnittstellen und Infrastruktur ist zweckgebundene Konfigurierbarkeit der Dateiablagen, Datenbanktabellen und Verarbeitungslogikbausteine über adäquate Konfigurationsparameter der technischen Prozesskomponenten.
  - Auf Wunsch kann für jeden Kunden ein eigenes Datenbankschema und damit eine entsprechend separierte Datenablage sowie ein separater Kundenprozess mit eigener Prozess-Konfiguration realisiert werden.
  - Im Übrigen folgt die Verarbeitung der Anforderungen einer logischen Trennung der verarbeiteten Daten. Dies betrifft sowohl personenbezogene als auch nicht-personenbezogene Daten.
  - Entwicklungs- und Produktivsysteme werden in voneinander getrennten Servern betrieben.
  - Zu Test- und Entwicklungszwecken kommen ausschließlich Testdaten zum Einsatz.

- Pseudonymisierung (Art. 32 Abs. 1 lit. a DS-GVO; Art. 25 Abs. 1 DS-GVO):
  Im Falle, dass der Personenbezug für eine Verarbeitung nicht benötigt wird, kann eine Pseudonymisierung der zur Personen-Identifikation relevanten Daten umgesetzt werden durch:
  - Pseudonymisierung, in der Form, dass die Daten, welche verarbeitet werden ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden können.
  - Gesonderte Aufbewahrung dieser zusätzlichen Informationen mit entsprechenden technischen und organisatorischen Maßnahmen zur Gewährleistung der Vertraulichkeit.

- Verschlüsselung (Art. 32 Abs. 1 lit. a DS-GVO):
  - E-Mails: TLS, zusätzlich wird bei vertraulichen Dokumenten die ZIP Verschlüsselung genutzt.
  - Anlagen in E-Mails: Verschlüsselung mit ZIP.
  - Webseiten: HTTPS
  - Server: FTPS
  - Firmennetzwerk/WLAN: Verschlüsselter Datentransfer.
  - Externer Zugriff auf Unternehmensnetzwerk: VPN.
  - Dedizierte Datenspeicher, insb. mobile Speichermedien: Verschlüsselung der Festplatten.

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

- Weitergabekontrolle:
  Kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen bei elektronischer Übertragung oder Transport durch:
  - Die elektronische Datenübermittlung erfolgt verschlüsselt (s. zuvor) und wird i.d.R. durch die jeweiligen IT-Anwendungen protokolliert.
  - Bei der Übergabe mobiler Speichermedien erfolgt ebenfalls in verschlüsselter Form (s. zuvor).
  - Die Übergabe von physikalischen Dokumenten erfolgt (i.d.R. persönlich durch die Unternehmensleitung) in verschlossenen Umschlägen.
  - Der externe Zugriff auf das Unternehmensnetzwerk erfolgt nur mittels VPN (s. zuvor).
  - Im Rahmen der Dienstleistungen findet auf dem Produktions- und Prelive-System grundsätzlich keine manuelle Weitergabe von Daten an Dritte statt. Ausgenommen hiervon sind lediglich Informationen im Zusammenhang mit dem Support von Einzelfallanfragen.
  - Die Aufbereitung, Weitergabe und Entgegennahme der Ergebnisse aus den Regelprozessen der Dienstleistungen geschieht vollautomatisch. Hierbei werden alle relevanten Informationen (Zeitpunkt, externe Quelle, eindeutige IDs, Steuerkennzeichen, Auftragsdaten, Ergebnisdaten) mitgeschrieben und zu Support-Zwecken vorgehalten. Dies betrifft personenbezogene als auch nicht-personenbezogene Daten.
  - Alle Mitarbeiter, die personenbezogene Daten verarbeiten, sind auf das Datengeheimnis verpflichtet.
  - Neue Mitarbeiter erhalten Informationen zum Datenschutz bei dem Umgang mit personenbezogenen Daten.
  - Die Vernichtung von physikalischen Dokumenten und Datenträgern wird fachgerecht durchgeführt.

- Eingabekontrolle:
  Feststellung, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind, durch:
  - Eingabedaten aus den Kundenaufträgen werden auf der Plattform grundsätzlich nicht manuell verändert, sondern im Original abgelegt, ggf. automatisch kopiert, zur Weiterverarbeitung vereinheitlicht (z.B. Formatanpassungen, Werte-Normierung) und während der Verarbeitung angereichert.
  - Alle Zwischenergebnisse der Verarbeitung werden nachvollziehbar gespeichert und dienen ausschließlich Supportzwecken im Einzelfall.
  - Im Zusammenhang mit eventuellen kundenspezifischen Konfigurationsänderungen nach Aufnahme des Produktivbetriebs können alle Anpassungen mit Zeitstempel und Kennzeichnung des Sachbearbeiters dokumentiert werden. Dies betrifft sowohl personenbezogene als auch nicht-personenbezogene Daten.
  - Die Eingabekontrolle auf einem Mobilen Endgerät (Laptop) geschieht durch organisatorischen Handlungsanweisungen und Kennzeichnung der Änderungen durch den jeweiligen Autor, entweder manuell oder über automatisierte Einträge der genutzten Werkzeuge.

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

- Verfügbarkeitskontrolle und rasche Wiederherstellbarkeit (Art. 32 Abs. 1 lit. c DS-GVO):
  Schutz gegen zufällige oder mutwillige Zerstörung bzw. Verlust durch:
  - Alle von Kunden und Lieferanten eingesteuerten und jeweils zurückgelieferten Daten werden in einem internen –von außen nicht zugänglichen- Datei-Archiv abgelegt.
  - Daten aus der Verarbeitung auf der propdation-Plattform werden in regelmäßigen Zeitabständen (wöchentlich) gesichert und dienen ausschließlich der raschen Wiederherstellung nach gegebenem Ausfall im Backup/Recovery-Szenario.
  - Die Wiederherstellung der Back-Up-Daten wird regelmäßig getestet.
  - Alle protokollierten Daten verbleiben zu jeder Zeit auf der verarbeitenden Plattform, eine Auslagerung auf externe Medien ist derzeit nicht erforderlich. Dies betrifft sowohl personenbezogene als auch nicht-personenbezogene Daten.

4. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung (Art. 32 Abs. 1 lit. d DS-GVO; Art. 25 Abs. 1 DS-GVO)

- Das Datenschutz-Management mit zugeordneter Aufbau- und Ablauforganisation wird durch einen externen Datenschutzbeauftragen betreut. Dieser ist schriftlich bestellt und besitzt die notwendige Fachkunde. Es erfolgen u.a.:
  - Verpflichtung der Mitarbeiter auf das Datengeheimnis
  - Regelmäßige Schulung und Sensibilisierung der Mitarbeiter.
  - Aufbau und regelmäßige Aktualisierung der Datenschutz-Dokumentation.
  - Regelmäßige Durchführung von Datenschutz-Audits.
  - Aktive Einbeziehung des externen Datenschutzbeauftragten hinsichtlich der Gestaltung von Verarbeitungen von personenbezogenen Daten.

- Die Geschäftsführung der propdation unterstützt den Datenschutzbeauftragten und binden ihn frühzeitig in Prozesse zur Verarbeitung von personenbezogenen Daten ein.

- Bei der Konfiguration und Einstellung von IT-Systemen werden die Grundsätze für die Verarbeitung personenbezogener Daten berücksichtigt:
  - Rechtmäßigkeit
  - Transparenz
  - Zweckbindung
  - Datenminimierung
  - Richtigkeit
  - Speicherbegrenzung
  - Integrität
  - Vertraulichkeit

- Das Incident-Response-Management mit zugeordneter Aufbau- und Ablauforganisation wird direkt durch die propdation Geschäftsführung gesteuert.

- Auftragskontrolle:
  Keine Auftragsverarbeitung im Sinne von Art. 28 DS-GVO ohne entsprechende Weisung des Auftraggebers, durch:
  - Alle Auftragnehmer sind vertraglich durch den Auftraggeber gebunden. Der schriftliche Auftrag erfüllt den Regelungskatalog von Artikel 28 Abs. 3 DS-GVO.
  - propdation überzeugt sich vor Beginn der Verarbeitung von der Einhaltung des Datenschutzes bei Auftragnehmern in den Bereichen, die nicht durch Zertifikate nachgewiesen werden und kontrolliert Auftragnehmer sodann regelmäßig.
    Der Auftraggeber benennt gegenüber dem Auftragnehmer die weisungsberechtigten Personen. Der Auftragnehmer stellt dem Auftraggeber eine Liste der befugten Weisungsempfänger zur Verfügung. Weisungen erfolgen schriftlich. Der Auftragnehmer prüft die Identität des Weisungsgebers.
  - Aufträge, Zwischenergebnisse und ausgelieferte Endergebnisse der automatisierten Verarbeitung werden in dienstleistungs- oder kundenspezifischen Datenbanktabellen und Datei-Ablagen ausschließlich zu Revisions- und zu Support-Zwecken gespeichert und mit Zugriffs- und Zugangsschutz zugänglich gemacht.
  - Im Falle verschiedener Auftragsarten für eine spezielle Dienstleistung, wird diese in Form einer Produkt-ID bei allen Ergebnissen und Zwischenergebnissen abgelegt.
  - Jeder Einzelauftrag ist im System durch eine eindeutige interne Auftrags-ID für eine spezielle Dienstleistung und einen speziellen Kunden gekennzeichnet. Dies betrifft personenbezogene sowie nicht-personenbezogene Daten, die im Kundenauftrag anhand der vorgegebenen Dienstleistungen verarbeitet werden.
  - Des Weiteren betrifft dies ebenso die Verarbeitung von Aufträgen an und Ergebnisse von Datendienstleistern:
    Daten zur Verarbeitung auf den Plattformen weiterer Datendienstleister werden ausschließlich in Form der gesendeten Aufträge und zurückgelieferten Ergebnisse gespeichert. Dies schließt sowohl personenbezogene als auch nicht-personenbezogene Daten ein.

Anhang 2 – Weisungsberechtige Personen, Adresse zur Meldung von Datenschutzverletzungen

Folgende Personen sind zur Erteilung und Entgegennahme von Weisungen befugt:

- Auftragnehmer: Dr. Raffaele Mattiello, Geschäftsführer, Egerländer Str. 1, 35510 Butzbach
- Auftraggeber: Hauptansprechpartner gemäß digitaler Beauftragung und Hinterlegung im persönlichen Profil des Hauptnutzers

Kontakt zur Meldung über die Verletzung personenbezogener Daten:

- Auftragnehmer: Dr. Raffaele Mattiello, Geschäftsführer, Egerländer Str. 1, 35510 Butzbach
- Auftraggeber: Hauptansprechpartner gemäß digitaler Beauftragung und Hinterlegung im persönlichen Profil des Hauptnutzers

Anhang 3 – Datenschutzbeauftragter des Auftragnehmers

Derzeit ist als externer Datenschutzbeauftragter beim Auftragnehmer bestellt:
Dr. Marc Leutsch
GDD EU zertifizierter Datenschutzbeauftragter
dpo@propdation.com
Egerländer Str. 1
35510 Butzbach

Anhang 4 – Subunternehmer

Subauftragnehmer	Leistung	