Vereinbarung zur Auftragsverarbeitung gem. Art. 28 DSGVO

Diese Anlage konkretisiert die Verpflichtungen der Vertragsparteien zum Datenschutz. Sie findet Anwendung auf alle Tätigkeiten, die Leistungserbringung in Zusammenhang stehen und bei denen der Auftragnehmer (**Paperless-Solutions GmbH**) personenbezogene Daten (Daten) des Kunden (Auftraggeber) verarbeitet.

§ 1 Gegenstand, Dauer und Spezifizierung der Auftragsverarbeitung
Diese Vereinbarung zum Datenschutz findet Anwendung als Ergänzung zum bestehenden Vertragsverhältnis über den Einsatz einer Anwendung / App des Auftragnehmers durch den Kunden über den d.velop store.

Auftragsgegenstand / Zweck der Verarbeitung:
Der Gegenstand des Auftrags und der Zweck der Verarbeitung ergibt sich aus dem bestehenden Vertragsverhältnis und der Produktbeschreibung über die Nutzung der Anwendung „docusign Schnittstelle".

Auftragsdauer:
Die Auftragsdauer ergibt sich aus dem bestehenden Vertragsverhältnis.

Kategorien der personenbezogenen Daten:
Die von der Verarbeitung betroffenen Kategorien personenbezogener Daten hängt von der Nutzung der Anwendung durch den Kunden ab. Gegenstand der Verarbeitung personenbezogener Daten können insbesondere folgende Datenarten / -kategorien sein:

- Stamm- und Nutzerdaten
- Kontaktdaten (Name, E-Mail, ggf. Telefon)
- Nutzungsdaten
- Inhaltsdaten

Kategorien betroffener Personen:
Die von der Verarbeitung betroffenen Kategorien betroffener Personen hängt von der Nutzung der Anwendung durch den Kunden ab. Die Kategorien der durch die Verarbeitung betroffenen Personen können insbesondere umfassen:

- Anwender

§ 2 Anwendungsbereich und Verantwortlichkeit

(1) Der Auftragnehmer verarbeitet personenbezogene Daten im Auftrag des Kunden. Dies umfasst Tätigkeiten, die im Vertrag und/oder in der Leistungsbeschreibung konkretisiert sind. Der Kunde ist im Rahmen dieses Vertrages für die Einhaltung der gesetzlichen Bestimmungen der Datenschutzgesetze, insbesondere für die Rechtmäßigkeit der Datenweitergabe an den Auftragnehmer sowie für die Rechtmäßigkeit der Datenverarbeitung allein verantwortlich (»Verantwortlicher« im Sinne des Art. 4 Nr. 7 DSGVO).

(2) Die Weisungen werden anfänglich durch den Vertrag festgelegt und können vom Kunden danach in schriftlicher Form oder in einem elektronischen Format (Textform) an die vom Auftragnehmer bezeichnete Stelle durch einzelne Weisungen geändert, ergänzt oder ersetzt werden (Einzelweisung). Weisungen, die im Vertrag nicht vorgesehen sind, werden als Antrag auf Leistungsänderung behandelt. Mündliche Weisungen sind unverzüglich schriftlich oder in Textform zu bestätigen.

§ 3 Pflichten des Auftragnehmers

(1) Der Auftragnehmer darf Daten von betroffenen Personen nur im Rahmen des Auftrages und der Weisungen des Kunden verarbeiten außer es liegt ein Ausnahmefall im Sinne des Artikel 28 Abs. 3 a) DSGVO vor. Der Auftragnehmer informiert den Kunden unverzüglich, wenn er der Auffassung ist, dass eine Weisung gegen anwendbare Gesetze verstößt. Der Auftragnehmer darf die Umsetzung der Weisung solange aussetzen, bis sie vom Kunden bestätigt oder abgeändert wurde.

(2) Der Auftragnehmer wird in seinem Verantwortungsbereich die innerbetriebliche Organisation so gestalten, dass sie den besonderen Anforderungen des Datenschutzes gerecht wird. Er wird technische und organisatorische Maßnahmen zum angemessenen Schutz der Daten des Kunden treffen, die den Anforderungen der Datenschutz-Grundverordnung (Art. 32 DSGVO) genügen. Der Auftragnehmer hat technische und organisatorische Maßnahmen zu treffen, die die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung auf Dauer sicherstellen. Dem Kunden sind diese technischen und organisatorischen Maßnahmen bekannt und er trägt die Verantwortung dafür, dass diese für die Risiken der zu verarbeitenden Daten ein angemessenes Schutzniveau bieten. Die vom Auftragnehmer etablierten Maßnahmen sind als Anlage zu dieser Vereinbarung beigefügt. Eine Änderung der getroffenen Sicherheitsmaßnahmen bleibt dem Auftragnehmer vorbehalten, wobei jedoch sichergestellt sein muss, dass jegliche Sicherheitsmaßnahmen dem Stand der Technik entsprechen sowie das vertraglich vereinbarte Schutzniveau nicht unterschritten wird.

(3) Der Auftragnehmer unterstützt soweit vereinbart den Kunden im Rahmen seiner Möglichkeiten bei der Erfüllung der Anfragen und Ansprüche betroffener Personen gem. Kapitel III der DSGVO sowie bei der Einhaltung der in Artt. 33 bis 36 DSGVO genannten Pflichten.
(4) Der Auftragnehmer gewährleistet, dass er den mit der Verarbeitung der Daten des Kunden befassten Mitarbeitern und andere für den Auftragnehmer tätigen Personen untersagt ist, die Daten außerhalb der Weisung zu verarbeiten. Ferner gewährleistet der Auftragnehmer, dass sich die zur Verarbeitung der personenbezogenen Daten befugten Personen zur Vertraulichkeit verpflichtet haben.
(5) Der Auftragnehmer unterrichtet den Kunden unverzüglich, wenn ihm Verletzungen des Schutzes personenbezogener Daten des Kunden bekannt werden, die das konkrete Auftragsverhältnis betreffen. Der Auftragnehmer trifft die erforderlichen Maßnahmen zur Sicherung der Daten und zur Minderung möglicher nachteiliger Folgen der betroffenen Personen und spricht sich hierzu mit dem Kunden ab.
(6) Der Auftragnehmer hat einen Datenschutzbeauftragten benannt. Dieser kann vom Kunden über folgende Kontaktdaten erreicht werden:
    - Markus Olbring, externer Datenschutzbeauftragter
    - comdatis it-consulting GmbH & Co.KG, Deventer Weg 8, 48683 Ahaus
    - E-Mail: datenschutz@ppls.de
    - Telefon: 02567-8290000
(7) Der Auftragnehmer gewährleistet, seinen Pflichten nach Art. 32 Abs. 1 lit. d) DSGVO nachzukommen, ein Verfahren zur regelmäßigen Überprüfung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung einzusetzen.
(8) Der Auftragnehmer berichtigt oder löscht die vertragsgegenständlichen Daten, wenn der Kunde dies anweist und dies vom Weisungsrahmen umfasst ist.
(9) Der Auftragnehmer löscht Daten 30 Tage nach Ende des Vertragsverhältnisses.
(10) Im Falle einer Inanspruchnahme des Kunden durch eine betroffene Person hinsichtlich etwaiger Ansprüche nach Art. 82 DSGVO, verpflichtet sich der Auftragnehmer den Kunden bei der Bearbeitung im Rahmen seiner Möglichkeiten zu unterstützen.
(11) 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. Eine Verarbeitung in einem Drittland ist nur zulässig, wenn ein angemessenes Datenschutzniveau i.S.d. Art. 44 DSGVO gegeben ist.

§ 4 Pflichten des Kunden

(1) Der Kunde hat den Auftragnehmer unverzüglich und vollständig zu informieren, wenn er in den Auftragsergebnissen Fehler oder Unregelmäßigkeiten bzgl. datenschutzrechtlicher Bestimmungen feststellt.
(2) Im Falle einer Inanspruchnahme des Kunden durch eine betroffene Person hinsichtlich etwaiger Ansprüche nach Art. 82 DSGVO, gilt §3 Abs. 10 entsprechend.
(3) Der Kunde nennt dem Auftragnehmer auf Anfrage den Ansprechpartner für im Rahmen des Vertrages anfallende Datenschutzfragen.

§ 5 Anfragen betroffener Personen

(1) Wendet sich eine betroffene Person mit Forderungen zur Berichtigung Löschung oder Auskunft an den Auftragnehmer, wird der Auftragnehmer die betroffene Person an den Kunden verweisen, sofern eine Zuordnung an den Kunden nach Angaben der betroffenen Person möglich ist. Der Auftragnehmer leitet den Antrag der betroffenen Person unverzüglich an den Kunden weiter. Der Auftragnehmer unterstützt den Kunden im Rahmen seiner Möglichkeiten auf Weisung soweit vereinbart. Der Auftragnehmer haftet nicht, wenn das Ersuchen der betroffenen Person vom Kunden nicht, nicht richtig oder nicht fristgerecht beantwortet wird.

§ 6 Nachweismöglichkeiten und Kontrollrechte

(1) Der Auftragnehmer weist dem Kunden die Einhaltung der in diesem Vertrag niedergelegten Pflichten mit geeigneten Mitteln auf Anfrage nach.
(2) Der Kunde hat das Recht, im Benehmen mit dem Auftragnehmer Überprüfungen durchzuführen oder durch im Einzelfall zu benennende Prüfer durchführen zu lassen. Diese werden zu den üblichen Geschäftszeiten ohne Störung des Betriebsablaufs nach Anmeldung unter Berücksichtigung einer Terminvereinbarung durchgeführt. Der Auftragnehmer darf diese von der vorherigen Anmeldung mit angemessener Vorlaufzeit und von der Unterzeichnung einer Verschwiegenheitserklärung hinsichtlich der Daten anderer Kunden und der eingerichteten technischen und organisatorischen Maßnahmen abhängig machen. Sollte der durch den Kunden beauftragte Prüfer in einem Wettbewerbsverhältnis zu dem Auftragnehmer stehen, hat der Auftragnehmer gegen diesen ein Einspruchsrecht. Für die Unterstützung bei der Durchführung einer Inspektion erhält der Auftragnehmer eine Aufwandsentschädigung.
(3) Sollte eine Datenschutzaufsichtsbehörde oder eine sonstige hoheitliche Aufsichtsbehörde des Kunden eine Inspektion vornehmen, gilt grundsätzlich Absatz 2 entsprechend. Eine Unterzeichnung einer Verschwiegenheitsverpflichtung ist nicht erforderlich, wenn diese Aufsichtsbehörde einer berufsrechtlichen oder gesetzlichen Verschwiegenheit unterliegt, bei der ein Verstoß nach dem Strafgesetzbuch strafbewehrt ist.

§ 7 Subunternehmer (weitere Auftragsverarbeiter)

(1) Der Kunde stimmt zu, dass der Auftragnehmer Subunternehmer hinzuzieht. Vor Hinzuziehung oder Ersetzung der Subunternehmer informiert der Auftragnehmer den Kunden rechtzeitig. Der Kunde kann der Änderung innerhalb von 4 Wochen nach Kenntnisnahme und nur aus wichtigem Grund gegenüber dem Auftragnehmer widersprechen. Erfolgt kein Widerspruch innerhalb der Frist gilt die Zustimmung als gegeben. Liegt ein wichtiger datenschutzrechtlicher Grund vor, und sofern eine einvernehmliche Lösungsfindung zwischen den Parteien nicht möglich ist, wird dem Kunden und dem Auftragnehmer ein Sonderkündigungsrecht eingeräumt. Je nach konkretem Auftragsverhältnis können Subunternehmer für den Auftragnehmer tätig werden, zum Zeitpunkt des Abschlusses dieser Vereinbarung können folgende Subunternehmer, in Abhängigkeit von der konkreten Beauftragung, tätig sein:

Unternehmen	Auftragsgegenstand
ambiFOX GmbH, Ahaus	Hosting der für die Schnittstelle relevanten Datenverarbeitung in einem gem. ISO/IEC 27001 zertifizierten Rechenzentrum der DATAHAUS GmbH (Ahaus).

(2) Ein zustimmungspflichtiges Subunternehmerverhältnis liegt vor, wenn der Auftragnehmer weitere Auftragnehmer mit der ganzen oder einer Teilleistung der vereinbarten Leistung beauftragt. Der Auftragnehmer wird mit diesen Dritten im erforderlichen Umfang Vereinbarungen treffen, um angemessene Datenschutz- und Informationssicherheitsmaßnahmen zu gewährleisten.

(3) Erteilt Auftragnehmer Aufträge an Subunternehmer, so obliegt es dem Auftragnehmer, seine datenschutzrechtlichen Pflichten aus diesem Vertrag dem Subunternehmer zu übertragen.

§ 8 Informationspflichten, Schriftformklausel, Rechtswahl

(1) Sollten die Daten des Kunden 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 Kunden unverzüglich darüber zu informieren. Der Auftragnehmer wird alle in diesem Zusammenhang Verantwortlichen unverzüglich darüber informieren, dass die Hoheit und das Eigentum an den Daten ausschließlich beim Kunden als »Verantwortlicher « im Sinne der Datenschutz-Grundverordnung liegen.

(2) Änderungen und Ergänzungen dieser Anlage und aller ihrer Bestandteile – einschließlich etwaiger Zusicherungen des Auftragnehmers – bedürfen einer schriftlichen Vereinbarung, die auch in einem elektronischen Format (Textform) erfolgen kann, und des ausdrücklichen Hinweises darauf, dass es sich um eine Änderung bzw. Ergänzung dieser Bedingungen handelt. Dies gilt auch für den Verzicht auf dieses Formerfordernis.

(3) Bei etwaigen Widersprüchen gehen Regelungen dieser Anlage zum Datenschutz den Regelungen des Vertrages vor. Sollten einzelne Teile dieser Anlage unwirksam sein, so berührt dies die Wirksamkeit der Anlage im Übrigen nicht.

(4) Es gilt deutsches Recht.

§ 9 Haftung und Schadensersatz

Kunde und Auftragnehmer haften gegenüber betroffener Personen entsprechend der in Art. 82 DS-GVO getroffenen Regelung.

Anlage: Sicherheit der Verarbeitung / Technische und org. Maßnahmen gem. Art. 32 DS-GVO

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

trifft der Auftragsverarbeiter geeignete technische und organisatorische Maßnahmen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten.

Bei der Beurteilung des angemessenen Schutzniveaus sind insbesondere die Risiken zu berücksichtigen, die mit der Verarbeitung verbunden sind, insbesondere durch - ob unbeabsichtigt oder unrechtmäßig - Vernichtung, Verlust, Veränderung oder unbefugte Offenlegung von beziehungsweise unbefugten Zugang zu personenbezogenen Daten, die übermittelt, gespeichert oder auf andere Weise verarbeitet wurden.

Der Auftragsverarbeiter ergreift folgende Maßnahmen:

1. Maßnahmen zur Verschlüsselung

☒ Verschlüsselung von Email mittels TLS
☒ Gesicherte Datenweitergabe (z.B. SSL, FTPS, TLS)
☒ Gesichertes WLAN

2. Maßnahmen zur Sicherstellung von Vertraulichkeit

a. Zutrittskontrolle *(Maßnahmen durch die Unbefugten der Zutritt verwehrt wird)*

☒ Besetzter Empfang während der Geschäftszeiten
☒ Zutrittskontrollsystem, Ausweisleser
☒ Türsicherungen
☒ Schlüsselverwaltung/Dokumentation der Schlüsselvergabe
☒ Spezielle Schutzvorkehrungen des Serverraums
☒ Es existiert ein Zutrittsberechtigungskonzept für die Sicherheitszonen
☒ Besucherregelung (Bspw. Abholung am Empfang, Begleitung zum Besprechungsraum)

b. Zugangskontrolle *(Maßnahmen die verhindern, dass Unbefugte die Verarbeitungssysteme nutzen können)*
☒ Persönlicher und individueller User-Log-In bei Anmeldung am System bzw. Unternehmensnetzwerk
☒ Zugang wird nach mehreren Fehlanmeldungen automatisch gesperrt
☒ Begrenzung der befugten Benutzer
☒ Definierte Kennwortverfahren
☒ Protokollierung des Zugangs
☒ Zusätzlicher System-Log-In für bestimmte Anwendungen
☒ Automatische Sperrung der Clients nach gewissem Zeitablauf ohne Useraktivität

c. Zugriffskontrolle *(Maßnahmen die gewährleisten, dass nur berechtigte Personen auf die Verarbeitungssysteme zugreifen und personenbezogene Daten nicht unbefugt lesen, kopieren, verändern oder entfernen können)*

☒ Verwaltung und Dokumentation von differenzierten Berechtigungen
☒ Auswertungen/Protokollierungen von Datenverarbeitungen
☒ Genehmigungsroutinen
☒ Profile/Rollen

d. Trennungskontrolle *(Maßnahmen die gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können)*

☒ Getrennte Systeme und Datenbanken
☒ Zugriffsberechtigungen nach funktioneller Zuständigkeit
☒ Getrennte Datenverarbeitung durch differenzierende Zugriffsregelungen
☒ Mandantenfähigkeit von IT-Systemen
☒ Verwendung von Testdaten
☒ Trennung von Entwicklungs- und Produktionsumgebung

3. Maßnahmen zur Sicherstellung von Integrität

☒ Zugriffsrechte
☒ Systemseitige Protokollierungen
☒ Dokumenten Management System (DMS) mit Änderungshistorie
☒ Sicherheits-/Protokollierungssoftware
☒ Funktionelle Verantwortlichkeiten, organisatorisch festgelegte Zuständigkeiten
☒ Getunnelte Datenfernverbindungen (VPN = Virtuelles Privates Netzwerk)

☒ Protokollierung von Datenübertragung oder Datentransport
☒ Protokollierung von lesenden Zugriffen
☒ Protokollierung des Kopierens, Veränderns oder Entfernens von Daten

4. Maßnahmen zur Sicherstellung und Wiederherstellung von Verfügbarkeit

☒ Back-Up Verfahren
☒ Aufbewahrungsprozess für Back-Ups (brandgeschützter Safe, getrennter Brandabschnitt, etc.)
☒ Spiegeln von Festplatten
☒ Einrichtung einer unterbrechungsfreien Stromversorgung (USV)
☒ Geeignete Archivierungsräumlichkeiten für Papierdokumente
☒ Klimatisierter Serverraum
☒ Virenschutz für lokale Rechner/Server (Softwareschutz)und Hardwareschutz
☒ Der Viren- und Malwareschutz ist insgesamt mehrstufig ausgelegt.
☒ Firewall
☒ Auslagerung von Datensicherungen

5. Maßnahmen zur Sicherstellung der Belastbarkeit

☒ Ausreichende Kapazität von IT-Systemen und Anlagen

6. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen

☒ Verfahren für regelmäßige Kontrollen/Audits
☒ Jährliche Qualitätssicherung der Unterlagen zum Datenschutz
☒ Ernennung eines Datenschutzbeauftragten

7. „Weisungskontrolle/Auftragskontrolle"

☒ Vertrag zur Auftragsdatenverarbeitung gem.
Art. 28 Abs. 3 DS-GVO mit Regelungen zu den Rechten und Pflichten des Auftragsverarbeiters und Verantwortlichen
☒ Bestimmung von Ansprechpartnern und/oder verantwortlichen Mitarbeitern
☒ Schulungen/Einweisung aller zugriffsberechtigten Mitarbeiter beim Auftragsverarbeiter
☒ Aktuelle Nachweise über durchgeführte Mitarbeiterschulungen / Sensibilisierungsmaßnahmen zum Datenschutz / Informationssicherheit liegen vor.
☒ Verpflichtung der Mitarbeiter zur Vertraulichkeit
☒ Benennung eines Datenschutzbeauftragten gemäß Art. 37 ff. DS-GVO
☒ Der Datenschutzbeauftragte ist der Geschäftsleitung direkt unterstellt.
☒ Ein aktueller Fachkundenachweis für den Datenschutzbeauftragten kann nachgewiesen werden
☒ Führen eines Verzeichnisses von Verarbeitungstätigkeiten gemäß
Art. 30 Abs. 2 DS-GVO
☒ Dokumentations- und Eskalationsprozess für Verletzungen des Schutzes personenbezogener Daten
☒ Richtlinien/Vorgaben zur Gewährleistung von technisch-organisatorischer Maßnahmen zur Sicherheit der Verarbeitung

8. Datenschutz durch Technikgestaltung und datenschutzfreundliche Voreinstellungen (Art. 25 DSGVO)

☒ Konzeptionelle Definition und Dokumentation der Anforderungen zum Datenschutz durch Technikgestaltung einschließlich Abstimmung mit dem Kunden

☒ Konzeptionelle Definition und Dokumentation der Anforderungen zur datenschutzfreundlichen Voreinstellungen einschließlich Abstimmung mit dem Kunden