VEREINBARUNG ÜBER EINE AUFTRAGSVERARBEITUNG nach Art 28 DSGVO
abgeschlossen zwischen

Scanpoint GmbH
FN 287641 b, HG Wien
Rochusplatz 1
1030 Wien
(im folgenden „Auftragsverarbeiter“)

und

<Firma>
FN <FN Nummer>, <zuständiges Gericht>
<Geschäftsanschrift>
<PLZ, Ort>
(im folgenden „Verantwortlicher“)

1. **Gegenstand der Vereinbarung**

[detaillierte Beschreibung der Aufgaben/Tätigkeiten des Auftragsverarbeiters oder Name und Datum des Hauptleistungs-/Rahmenvertrages, zu dem die gegenständliche Vereinbarung zum Datenumgang abgeschlossen wird]

Im Rahmen dieses Vertrages sind unter „personenbezogenen Daten“, solche personenbezogenen Daten zu verstehen, die der Verantwortliche dem Auftragsverarbeiter im Rahmen des oben näher beschriebenen Vertrages überlässt bzw. deren Verarbeitung dem Auftragsverarbeiter im jenem Vertrag aufgetragen wird.

Verarbeitet werden Kategorien personenbezogener Daten und Kategorien betroffener Personen gemäß Anlage 1.

2. Pflichten des Auftragsverarbeiters

a) Der Auftragsverarbeiter verpflichtet sich, personenbezogene Daten und Verarbeitungsergebnisse ausschließlich im Rahmen der schriftlichen (E-Mail ausreichend) Aufträge des Verantwortlichen zu verarbeiten.

b) Der Auftragsverarbeiter ist nicht befugt, personenbezogene Daten des Verantwortlichen ohne dessen schriftliche Einwilligung Dritten offenzulegen.

c) Soweit der Auftragsverarbeiter dazu aufgrund gesetzlicher Bestimmungen verpflichtet ist, hat er den Verantwortlichen unverzüglich im Vorhinein zu informieren.

d) Die Übermittlung von personenbezogenen Daten an Dritte, zu der keine gesetzliche Verpflichtung des Auftragsverarbeiters besteht, setzt einen schriftlichen (E-Mail ausreichend) Auftrag des Verantwortlichen voraus.

e) Eine Verarbeitung der personenbezogenen Daten für eigene Zwecke des Auftragsverarbeiters darf nur nach vorherigem schriftlichem (E-Mail ausreichend) Einverständnis des Verantwortlichen erfolgen.

f) Der Auftragsverarbeiter verpflichtet sich zur Wahrung des Datengeheimnisses und erklärt rechtsverbindlich, dass er alle mit der Datenverarbeitung beauftragten Personen vor Aufnahme der Tätigkeit zur Vertraulichkeit verpflichtet hat oder diese einer angemessenen gesetzlichen Verschwiegenheitsverpflichtung unterliegen.
Er hat alle mit der Datenverarbeitung betrauten Personen verpflichtet, personenbezogene Daten, die diesen ausschließlich auf Grund ihrer berufsmäßigen Beschäftigung anvertraut oder zugänglich werden, unbeschadet sonstiger gesetzlicher Verschwiegenheitsverpflichtungen, geheim zu halten, soweit kein rechtlich zulässiger Grund für eine Übermittlung/Bekanntgabe der Daten besteht.
Insbesondere bleibt die Verschwiegenheitsverpflichtung der mit der Datenverarbeitung beauftragten Personen auch nach Beendigung ihrer Tätigkeit und Ausscheiden beim Auftragsverarbeiter aufrecht.

g) Der Auftragsverarbeiter erklärt rechtsverbindlich, dass er alle erforderlichen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung nach Art 32 DSGVO ergriffen hat.
Der Auftragsverarbeiter sichert zu, die in Anlage 2 beschriebenen und ausgewählten, dem Risiko angemessenen, technischen und organisatorischen Maßnahmen ergriffen zu haben und auch in Zukunft zu ergreifen, um die personenbezogenen Daten vor zufälliger oder unrechtmäßiger Zerstörung und vor Verlust zu schützen, um ihre ordnungsgemäße Verarbeitung und die Nichtzugänglichkeit für unbefugte Dritte sicherzustellen. Der Auftragsverarbeiter verpflichtet sich dazu, die technischen und organisatorischen Maßnahmen in obigem Sinne auf dem Stand der Technik zu halten und nach technischem Fortschritt bzw. geänderter Bedrohungslage zu aktualisieren bzw. anzupassen.

h) Der Auftragsverarbeiter stellt sicher, dass der Verantwortliche die Rechte der betroffenen Person nach Kapitel III der DSGVO (Information, Auskunft, Berichtigung und Löschung, Datenübertragbarkeit, Widerspruch sowie automatisierte Entscheidungsfindung im Einzelfall) und unter Berücksichtigung des österreichischen Bundesgesetzes zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten (DSG idgF) innerhalb der gesetzlichen Fristen jederzeit erfüllen kann, überlässt dem Verantwortlichen alle dafür notwendigen Informationen und unterstützt diesen bei der Erfüllung diesbezüglicher Pflichten nach besten Kräften. Wird ein entsprechender Antrag, mit dem Betroffenenrechte geltend gemacht werden, an den Auftragsverarbeiter gerichtet und ist aus dem Inhalt des Antrages ersichtlich, dass der Antragsteller den Auftragsverarbeiter irrtümlich für den Verantwortlichen der von ihm für den Verantwortlichen durchgeführten Verarbeitungstätigkeit hält, hat der Auftragsverarbeiter den Antrag unverzüglich an den Verantwortlichen weiterzuleiten und dies dem Antragsteller unter Bekanntgabe des Datums des Einlangens des Antrages mitzuteilen.

i) Der Auftragsverarbeiter unterstützt den Verantwortlichen bei der Einhaltung der in den Art 32 bis 36 DSGVO genannten Pflichten (Datensicherheitsmaßnahmen, Meldungen von Verletzungen des Schutzes personenbezogener Daten an die Aufsichtsbehörde, Benachrichtigung der von einer Verletzung des Schutzes personenbezogener Daten betroffenen Person, Datenschutz-Folgeabschätzung, vorherige Konsultation) nach besten Kräften.

j) Der Auftragsverarbeiter verpflichtet sich, dem Verantwortlichen jene Informationen zur Verfügung zu stellen, die zur Kontrolle der Einhaltung der in dieser Vereinbarung genannten Verpflichtungen notwendig sind.
Über Ersuchen des Verantwortlichen wird diesem im Einzelfall auch die Erklärung über die Wahrung des Datengeheimnisses hinsichtlich jener Personen vorgelegt, die mit der Durchführung des Auftrags betraut sind.

k) Dem Verantwortlichen wird hinsichtlich der Verarbeitung der von ihm überlassenen personenbezogenen Daten das Recht eingeräumt, selbst durch qualifizierte und zur Geheimhaltung verpflichtete Mitarbeiter oder durch eine zur Berufsverschwiegenheit verpflichtete Person (gerichtlich zertifizierter Sachverständiger etc.) beim Auftragsverarbeiter die Ordnungsgemäßheit der Datenverarbeitung nach vorheriger Ankündigung von mindestens 30 Werktagen (ausgenommen Samstag) auf eigene Kosten zu überprüfen. Dies während der büroüblichen Zeiten und in Abstimmung mit dem Datenschutzbeauftragten des Auftragsverarbeiters oder einer sonst für den Datenschutz verantwortlichen Person.

l) Der Auftragsverarbeiter ist nach Beendigung des Auftrags verpflichtet, dem Verantwortlichen alle Verarbeitungsergebnisse und Unterlagen, die vertragsgegenständliche personenbezogene Daten enthalten, zu übergeben; davon unberührt bleibt die Speicherung der dem Auftragsverarbeiter überlassenen personenbezogenen Daten und Verarbeitungsergebnisse soweit und solange dieser für seine Leistungen Gewähr zu leisten hat.
Nach Ablauf der Gewährleistungsfrist hat der Auftragsverarbeiter sämtliche vertragsgegenständliche personenbezogene Daten zu löschen oder diese nach Aufforderung des Verantwortlichen vor Durchführung der Löschung sicher zu verwahren. Dies gilt insbesondere, soweit der Auftragsverarbeiter zu einer weiteren Aufbewahrung von personenbezogenen Daten nicht aufgrund zwingender gesetzlicher Bestimmungen verpflichtet ist.
Über Ersuchen des Verantwortlichen bestätigt der Auftragsverarbeiter die Datenlöschung schriftlich.
Wenn der Auftragsverarbeiter die personenbezogenen Daten in einem speziellen technischen Format verarbeitet, ist er verpflichtet, die personenbezogenen Daten nach Beendigung des Auftrags entweder in diesem Format oder nach Wunsch des Auftragsverarbeiters in dem Format, in dem er die personenbezogenen Daten vom Verantwortlichen erhalten hat oder in einem anderen gängigen Format herauszugeben.

m) Die Haftung richtet sich nach gesetzlichen Vorschriften und allfälligen datenschutzrechtlichen Haftungsbestimmungen der Hauptleistungsvereinbarung.
Sie ist mit der Höhe eines einjährigen Auftragsvolumens der Hauptleistungsvereinbarung gemäß Punkt 1a) begrenzt, sofern darin oder gesetzlich keine für den Auftragsverarbeiter günstigere Regelung besteht.

3. Sub-Auftragsverarbeiter

a) Der Auftragsverarbeiter kann Sub-Auftragsverarbeiter heranziehen. Er hat den Verantwortlichen von der beabsichtigten Heranziehung so rechtzeitig zu verständigen, dass er dies allenfalls untersagen kann.
Nicht hierzu gehören Nebendienstleistungen, die der Auftragsverarbeiter z.B. als Post-/Transport-/Telekommunikationsdienstleistungen oder zur Wartung/ Servicierung von Datenträgern und Datenverarbeitungsanlagen in Anspruch nimmt.

b) Der Auftragsverarbeiter schließt die erforderlichen Vereinbarungen im Sinne des Art 28 Abs 4 DSGVO mit dem Sub-Auftragsverarbeiter ab. Dabei ist sicherzustellen, dass der Sub-Auftragsverarbeiter dieselben Verpflichtungen eingeht, die dem Auftragsverarbeiter auf Grund dieser Vereinbarung obliegen. Die Überbindung der Verpflichtungen ist dem Verantwortlichen über Aufforderung nachzuweisen.

c) Kommt der Sub-Auftragsverarbeiter seinen Datenschutzpflichten nicht nach, so haftet der Auftragsverarbeiter gegenüber dem Verantwortlichen für die Einhaltung der Pflichten des Sub-Auftragsverarbeiters.

d) Der Verantwortliche erteilt seine Zustimmung zur Heranziehung der in Anlage 3 genannten Sub- Auftragsverarbeiter.

4. Dauer der Vereinbarung

(Zutreffendes ankreuzen)

☒ Die Laufzeit der Vereinbarung richtet sich nach der Verarbeitungstätigkeitsdauer der in Punkt 1a) genannten Beschreibung der Aufgaben/Tätigkeiten des Auftragsverarbeiters für den Verantwortlichen oder bezieht sich auf unter Punkt 1a) angegebenen Vertrag.

☐ Die Vereinbarung ist auf unbestimmte Zeit geschlossen und kann von beiden Parteien mit einer Frist von drei Monaten zum Monatslende schriftlich gekündigt werden. Die Möglichkeit zur fristlosen Kündigung aus wichtigem Grund bleibt unberührt.

Insofern eine datenschutzrechtliche Dienstleistervereinbarung zwischen den Vertragspartnern zur bezugnehmenden Hauptleistung schon besteht, wird sie durch die gegenständliche Vereinbarung über eine Auftragsdatenverarbeitung ersetzt.

a) Sonstige Bestimmungen

a) Sämtliche Streitigkeiten aus und im Zusammenhang mit diesem Vertrag unterliegen österreichischem Recht, unter Ausschluss des UN-Kaufrechts und kollisionsrechtlicher Bestimmungen. Für sämtliche Streitigkeiten wird das für 1030 Wien sachlich und örtlich zuständige Gericht vereinbart.

b) Verbindlich ist nur, was schriftlich vereinbart ist; es bestehen keine mündlichen Nebenabreden. Änderungen und Ergänzungen der Vereinbarung bedürfen zu ihrer Gültigkeit der Schriftform; dies gilt auch für ein Abgehen vom Formerfordernis der Schriftlichkeit.

c) Sämtliche Rechte und Pflichten aus dieser Vereinbarung gehen auf allfällige Rechtsnachfolger beider Vertragsparteien über.

d) Die Parteien vereinbaren, den Abschluss dieser Vereinbarung und deren Inhalt vertraulich zu behandeln. Dies gilt, insoweit die gegenständliche Vereinbarung

keine entgegenstehenden Bestimmungen enthält und keine gesetzlichen Auskunftspflichten bestehen.

e) Der Verantwortliche verpflichtet sich, (i) dass sich seine gesetzlichen Vertreter, Mitarbeiter und eingesetzte und/oder beauftragte Subunternehmer an sämtliche geltenden gesetzlichen Bestimmungen im Zusammenhang mit Anti-Korruptionsvorschriften halten sowie (ii) geeignete Maßnahmen zu setzen, um die Einhaltung der Anti-Korruptionsvorschriften sicherzustellen. Ein Verstoß gegen Anti-Korruptionsvorschriften berechtigt den Auftragsverarbeiter – unbeschadet sonstiger Rücktritts- und Kündigungsrechte – zur fristlosen außerordentlichen Kündigung der Vereinbarung sowie zur Geltendmachung allfälliger Schadenersatzansprüche.

f) Sollten einzelne Bestimmungen der Vereinbarung ungültig oder unwirksam sein oder werden, so werden die Vertragsparteien einvernehmlich eine gültige bzw. wirksame Bestimmung festlegen, die den ungültigen bzw. unwirksamen Bestimmungen wirtschaftlich am nächsten kommt.
Die Ungültigkeit oder Unwirksamkeit einzelner Bestimmungen hat keine Auswirkung auf die Gültigkeit bzw. Wirksamkeit des gesamten Vertrages.

g) Dieser Vertrag wird in zwei Originalen errichtet, von denen jeder Vertragspartner eines erhält.

h) Die Anlagen 1, 2 und 3 gelten als integrierte Bestandteile des Vertrages.

Für den „Verantwortlichen“	Für den „Auftragsverarbeiter“
_____	_____
Name, Unterschrift, Stempel	Name, Unterschrift
	Wien,
_____	_____
Ort, Datum	Ort, Datum

Anlage 1- Kategorien personenbezogener Daten und betroffener Personen

a) Folgende Kategorien personenbezogener Daten werden verarbeitet (Zutreffendes wurde vom Verantwortlichen angekreuzt)

☐ Personenstammdaten (Vor- und Nachname, akademische Titel, Geburtsdatum, Familienstand, Geschlecht, Staatsangehörigkeit etc.)

☐ Kontaktdaten (Telefonnummer, E-Mail-Adresse, Fax)

☐ Adressdaten (postalische Anschrift)

☐ Identifikationsdaten (Personalausweis-/Reisepass-/Führerscheinnummer etc.)

☐ Vertragsdaten (Daten betreffend das Vertragsverhältnis)

☐ Bonitätsdaten (Daten betreffend die Bonität einer Person)

☐ Bestelldaten (Daten betreffend den Inhalt einer Bestellung z.B. im Onlineshop)

☐ Zahlungsdaten (Kontoverbindung, Kreditkartennummer etc.)

☐ Marketingdaten (Zustimmung zur Marketingverwendung, Merkmale wie Einkommen, Kaufverhalten, Interessen, etc.)

☐ Dokumenten- Inhaltsdaten (Daten betreffend Dokumenteninhalte)

☐ Sonstige:_____

_____

_____

b) Zu folgenden Kategorien betroffener Personen werden personenbezogene Daten verarbeitet (Zutreffendes wurde vom Verantwortlichen angekreuzt)

☐ Mitarbeiter

☐ Kunden

☐ Lieferanten

☐ Geschäftspartner

☐ Kinder bis 14 Jahre

☐ Sonstige:_____

Anlage 2 - Technisch - organisatorische Maßnahmen

(Alle zu treffenden Maßnahmen sind konkret zu bestimmen, daher wurde Zutreffendes vom Auftragsverarbeiter angekreuzt)

1) VERTRAULICHKEIT

Zutrittskontrolle - Schutz vor unbefugtem Zutritt zu Datenverarbeitungsanlagen

☒ Alarmanlage	☒ Sicherheitspersonal
☒ Schlüsselregelung	☒ Videoüberwachung der Zugänge
☒ Sicherheitsschlösser	☒ Personenkontrolle beim Empfang
☒ Berechtigungsausweise	☒ Protokollierung Besucher

Zugangskontrolle - Schutz vor unbefugter Systembenutzung

☒ Rollenbasierte Zuordnung von Benutzerrechten	☒ Security Incident Management
☒ sichere Kennwörter/Passwortrichtlinie	☒ automatische Sperrmechanismen/Bildschirmsperre

Zugriffskontrolle - Schutz vor unbefugtem Lesen, Kopieren, Verändern od. Entfernen innerhalb des Systems

☒ Berechtigungskonzept „need to know-Basis“	☒ sichere Aufbewahrung von Datenträgern
☒ Protokollierung von Zugriffen	☒ Firewall
☒ Verschlüsselung von Datenträgern	☒ datenschutzkonforme Entsorgung der Datenträger und Protokollierung
☒ Verwaltung der Rechte durch Systemadministratoren	☒ Standardprozesse bei Wechsel/Ausscheiden von Mitarbeitern
☒ Klassifikationsschema für Daten	
☒ VPN-Technologie	

2) INTEGRITÄT

Weitergabekontrolle - Schutz vor unbefugtem Lesen, Kopieren, Verändern oder Entfernen bei Übermittlung

☒ verschlüsselte Datenübertragung	☒ Dokumentation der Datenempfänger
☒ sichere Transportbehältnisse	☒ Anti-Viren-Software
☒ Datenträgerverschlüsselung	☒ Übersicht über regelmäßige Abruf - und Übermittlungsvorgänge
☒ Intrusion-Detection-System	

Eingabekontrolle - Feststellung, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind

☒ Dokumentenmanagement	

3) VERFÜGBARKEIT UND BELASTBARKEIT

Verfügbarkeitskontrolle - Schutz vor Zerstörung und Verlust von Daten

☒ Backup & Restore-Tests	☒ Feuer- und Rauchmeldeanlagen
☒ unterbrechungsfreie Stromversorgung	☒ Recovery-Konzept/Wiederaufbauplan
☒ Redundanzkonzepte/Notversorgungsplan	☒ Klimaanlage
☒ Löschungsfristen	☒ Meldewege und Notfallpläne

4) VERFAHREN ZUR ÜBERPRÜFUNG, BEWERTUNG UND EVALUIERUNG

☒ Datenschutz-Management	☒ regelmäßige Mitarbeiterschulungen
☒ Sicherheitsmanagement	☒ Security Checks auf Infrastruktur- und Applikationsebene

5) SONSTIGE

☒ datenschutzfreundliche Voreinstellungen/ Techniken	☒ formalisiertes Auftragsmanagement
☒ eindeutige Vertragsgestaltung	☒ Kontroll-/Auditrecht
☒ sorgfältige Auswahl von Dienstleistern	☒ physische/logische Trennung von Daten
☒ Prüfung und Dokumentation von Sicherheitsmaßnahmen	☒ Trennung von Produktiv- und Testsystem
☒ Verpflichtung auf Datengeheimnis (z. B.Mitarbeiter)	