Vertrag zur Auftragsverarbeitung gemäß Art. 28 DSGVO mit Geltung ab dem 25.05.2018

Vereinbarung

zwischen

_____
_____
_____
_____
(im Folgenden „Verantwortlicher“ genannt)

und

GunzX GmbH, (Dr. Headshot)
Fenzlgasse 1/14
A-1150 Wien
Österreich
(im Folgenden „Auftragsverarbeiter“ genannt)

(im Folgenden gemeinsam als „Parteien“ bezeichnet)

Präambel

Der Auftragsverarbeiter hat sich verpflichtet, die in § 3 beschriebenen Datenverarbeitungen gegenüber dem Verantwortlichen zu erbringen. Dieser Vertrag regelt die datenschutzrechtlichen Rechte und Pflichten der Parteien im Zusammenhang mit dieser Verarbeitung.

§ 1 Begriffsbestimmungen

Für die Zwecke dieses Vertrages gelten die Begriffsdefinitionen der Datenschutzgrundverordnung („DSGVO“).

§ 2 Ansprechpartner für Datenschutz

Da der Auftragsverarbeiter gesetzlich nicht zur Bestellung eines Datenschutzbeauftragten verpflichtet ist, wird folgender Ansprechpartner für datenschutzrechtliche Angelegenheiten benannt:
Jürgen Gunz, E-Mail: support@drheadshot.com

§ 3 Gegenstand, Umfang und Zweck der Datenverarbeitung

(1) Gegenstand, Umfang und Zweck der Datenverarbeitung durch den Auftragsverarbeiter ergeben sich primär aus dem zwischen den Parteien geschlossenen Hauptvertrag über die Nutzung der Dienste von Dr. Headshot.

(2) Zweck und Gegenstand der Datenverarbeitungen sind:
* Die Erstellung und Bearbeitung von KI-generierten Porträtbildern auf Basis von durch den Verantwortlichen bzw. dessen Mitarbeitenden hochgeladenen Fotos.

(3) Kategorien der betroffenen Personen:
* Mitarbeitende des Verantwortlichen.

(4) Kategorien der personenbezogenen Daten:
* Name, E-Mail-Adresse, Geschlecht, hochgeladene Fotos, generierte Porträtbilder, IP-Adresse, Nutzungsdaten.

§ 4 Dauer des Auftrags

Die Laufzeit dieses Vertrages richtet sich nach der Laufzeit des Hauptvertrages.

§ 5 Ort der Datenverarbeitung

(1) Der Auftragsverarbeiter verarbeitet personenbezogene Daten grundsätzlich auf Servern innerhalb der Europäischen Union (EU) bzw. des Europäischen Wirtschaftsraums (EWR). Die primäre Speicherung der Daten erfolgt in einem Rechenzentrum der Contabo GmbH in Deutschland.

(2) Eine Übermittlung von Daten in ein Drittland (außerhalb der EU/des EWR) durch den Auftragsverarbeiter oder dessen Sub-Auftragsverarbeiter ist nur zulässig, sofern die besonderen Voraussetzungen der Art. 44 ff. DSGVO erfüllt sind (z.B. durch einen Angemessenheitsbeschluss der Kommission, Standardvertragsklauseln oder andere geeignete Garantien).

§ 6 Weisungsrecht des Verantwortlichen

(1) Der Auftragsverarbeiter verarbeitet die personenbezogenen Daten ausschließlich entsprechend den Vereinbarungen des Hauptvertrages und gemäß dokumentierter Weisungen des Verantwortlichen, sofern er nicht durch das Recht der Union oder der Mitgliedstaaten, dem er unterliegt, zu einer anderen Verarbeitung verpflichtet ist.

(2) Der Auftragsverarbeiter informiert den Verantwortlichen unverzüglich, falls er der Ansicht ist, dass eine Weisung gegen die DSGVO oder andere anwendbare Datenschutzbestimmungen verstößt. Der Auftragsverarbeiter ist berechtigt, die Durchführung einer solchen Weisung auszusetzen, bis sie vom Verantwortlichen bestätigt oder geändert wird.

§ 7 Vertraulichkeit

Der Auftragsverarbeiter gewährleistet, dass sich alle zur Verarbeitung der personenbezogenen Daten befugten Personen zur Vertraulichkeit verpflichtet haben oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen.

§ 8 Technische und organisatorische Maßnahmen (TOMs)

(1) Der Auftragsverarbeiter ergreift alle gemäß Artikel 32 DSGVO erforderlichen technischen und organisatorischen Maßnahmen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten.

(2) Die konkret implementierten Sicherheitsmaßnahmen sind in Anlage 1 dieses Vertrages detailliert beschrieben.

(3) Der Auftragsverarbeiter ist berechtigt, die Sicherheitsmaßnahmen an den technischen Fortschritt anzupassen, solange das vertraglich vereinbarte Schutzniveau nicht unterschritten wird. Wesentliche Änderungen sind zu dokumentieren.

§ 9 Einsatz von Sub-Auftragsverarbeitern

(1) Der Verantwortliche erteilt hiermit die allgemeine Genehmigung, dass der Auftragsverarbeiter weitere Auftragsverarbeiter (im Folgenden „Sub-Auftragsverarbeiter“) heranziehen darf.

(2) Der Verantwortliche genehmigt explizit den Einsatz der in Anlage 2 namentlich genannten Sub-Auftragsverarbeiter.

(3) Beabsichtigt der Auftragsverarbeiter, einen neuen Sub-Auftragsverarbeiter hinzuzuziehen oder einen bestehenden zu ersetzen, so informiert er den Verantwortlichen hierüber vorab in Textform. Der Verantwortliche kann gegen die beabsichtigte Änderung binnen einer Frist von 4 Wochen nach Zugang der Information Einspruch erheben. Erfolgt kein Einspruch innerhalb der Frist, gilt die Zustimmung als erteilt.

(4) Bei Beauftragung eines Sub-Auftragsverarbeiters stellt der Auftragsverarbeiter vertraglich sicher, dass diesem dieselben Datenschutzpflichten auferlegt werden, die auch für den Auftragsverarbeiter gemäß diesem Vertrag gelten.

§ 10 Unterstützung des Verantwortlichen und Rechte der Betroffenen

(1) Soweit möglich, unterstützt der Auftragsverarbeiter den Verantwortlichen mit geeigneten technischen und organisatorischen Maßnahmen bei der Erfüllung seiner Pflichten, insbesondere bei der Beantwortung von Anträgen auf Wahrnehmung der Betroffenenrechte (z.B. Auskunft, Berichtigung, Löschung). Wendet sich eine betroffene Person direkt an den Auftragsverarbeiter, wird er dieses Ersuchen unverzüglich an den Verantwortlichen weiterleiten.

(2) Der Auftragsverarbeiter unterstützt den Verantwortlichen bei der Einhaltung seiner Pflichten gemäß Art. 32 bis 36 DSGVO (Sicherheit der Verarbeitung, Meldung von Datenschutzverletzungen, Datenschutz-Folgenabschätzung).

§ 11 Meldung von Datenschutzverletzungen

Der Auftragsverarbeiter meldet Verletzungen des Schutzes personenbezogener Daten unverzüglich nach Bekanntwerden an den Verantwortlichen.

§ 12 Kontrollrechte des Verantwortlichen

(1) Der Auftragsverarbeiter stellt dem Verantwortlichen alle erforderlichen Informationen zum Nachweis der Einhaltung der in diesem Vertrag und in Art. 28 DSGVO niedergelegten Pflichten zur Verfügung.

(2) Der Nachweis der Einhaltung der technischen und organisatorischen Maßnahmen kann insbesondere durch die Vorlage von aktuellen Testaten, Berichten unabhängiger Instanzen (z.B. Wirtschaftsprüfer, Datenschutzauditoren) oder einer geeigneten Zertifizierung nach einem genehmigten Zertifizierungsverfahren (gemäß Art. 42 DSGVO) erbracht werden. Eine Vor-Ort-Inspektion ist nur bei Vorliegen eines besonderen, zu begründenden Anlasses und nach angemessener Vorankündigung während der üblichen Geschäftszeiten durchzuführen.

§ 13 Löschung und Rückgabe von Daten

Nach Abschluss der Erbringung der Verarbeitungsleistungen löscht der Auftragsverarbeiter nach Wahl des Verantwortlichen alle personenbezogenen Daten oder gibt diese zurück, sofern keine gesetzliche Speicherpflicht entgegensteht. Für den mit der Rückgabe der Daten verbundenen Aufwand kann der Auftragsverarbeiter ein angemessenes Entgelt verlangen.

§ 14 Haftung

(1) Die Haftung beider Parteien ist auf grobes Verschulden und Vorsatz beschränkt. Eine Haftung für bloße Vermögensschäden ist ausgeschlossen.

(2) Der Verantwortliche hält den Auftragsverarbeiter für sämtliche Ansprüche, Bußgelder oder Sanktionen, die auf einem Verstoß des Verantwortlichen gegen geltende Datenschutzgesetze beruhen, vollständig schad- und klaglos.

§ 15 Schlussbestimmungen

(1) Änderungen und Ergänzungen dieses Vertrages bedürfen der Schriftform. Dies gilt auch für die Aufhebung dieses Schriftformerfordernisses.

(2) Es gilt österreichisches Recht unter Ausschluss der Verweisungsnormen. Gerichtsstand für sämtliche Streitigkeiten aus oder im Zusammenhang mit diesem Vertrag ist das sachlich zuständige Gericht am Sitz des Auftragsverarbeiters.

(3) Sollte eine Bestimmung dieses Vertrages unwirksam sein oder werden, so wird die Wirksamkeit der übrigen Bestimmungen davon nicht berührt.

Ort, Datum: Unterschrift, Auftragsverarbeiter	Ort, Datum: Unterschrift, Verantwortlicher

Anlage 1: Technische und organisatorische Maßnahmen (TOMs)
Anlage 2: Genehmigte Sub-Auftragsverarbeiter

Anlage 1: Technische und organisatorische Maßnahmen (TOMs)

Gemäß Art. 32 DSGVO zum Schutz der personenbezogenen Daten beim Auftragsverarbeiter.

Die Datenspeicherung und -verarbeitung erfolgt in einem professionellen Rechenzentrum der Contabo GmbH in Deutschland. Die folgenden Maßnahmen beschreiben die Sicherung der Daten sowohl auf Infrastruktur- als auch auf Anwendungsebene.

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

- Physische Zugangskontrolle: Unbefugten wird der Zutritt zu Datenverarbeitungsanlagen verwehrt. Dies wird durch mehrstufige Sicherheitszonen, Zutrittskontrollsysteme, Videoüberwachung und Sicherheitspersonal am Rechenzentrumsstandort unseres Hosting-Providers (Contabo GmbH) gewährleistet. Der Zugang zu unseren Büroräumlichkeiten in Wien ist ebenfalls gesichert.
- Logische Zugriffskontrolle: Der Zugriff auf IT-Systeme erfolgt ausschließlich nach erfolgreicher Authentifizierung (z.B. durch Benutzername und Passwort). Es gilt das „Need-to-know“-Prinzip, d.h. Mitarbeiter erhalten nur die Berechtigungen, die sie zur Erfüllung ihrer Aufgaben benötigen. Administrative Zugänge werden nur für dedizierte Aufgaben verwendet.
- Datenzugriffskontrolle: Es wird sichergestellt, dass zur Verarbeitung befugte Personen ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können. Zugriffe auf Anwendungen, insbesondere die Eingabe, Änderung und Löschung von Daten, werden protokolliert.
- Trennungskontrolle: Daten, die für unterschiedliche Zwecke erhoben wurden, werden getrennt verarbeitet. Die mandantenfähige Architektur der Anwendung stellt sicher, dass die Daten des Verantwortlichen logisch von den Daten anderer Kunden getrennt sind.

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

- Weitergabekontrolle: Personenbezogene Daten werden bei der elektronischen Übertragung mittels starker Verschlüsselungsprotokolle (z.B. TLS 1.2 oder höher) geschützt, um eine unbefugte Kenntnisnahme oder Veränderung zu verhindern.
- Eingabekontrolle: Es wird protokolliert, ob und von wem personenbezogene Daten in die Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind.

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

- Verfügbarkeitskontrolle: Die Daten werden durch den Einsatz von Firewalls, Virenschutz und redundanten Systemen bei unserem Hosting-Provider vor zufälliger Zerstörung oder Verlust geschützt.
- Rasche Wiederherstellbarkeit: Es werden regelmäßig Backups der Daten erstellt und sicher aufbewahrt. Es existiert ein Konzept zur raschen Wiederherstellung der Datenverfügbarkeit nach einem physischen oder technischen Zwischenfall.
- Belastbarkeit: Die Systeminfrastruktur ist so ausgelegt, dass sie auch bei hoher Auslastung funktionsfähig bleibt.

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

- Datenschutz-Management: Die internen Prozesse werden regelmäßig auf ihre Konformität mit den gesetzlichen Datenschutzanforderungen und diesem Vertrag überprüft.
- Auftragskontrolle: Die Verarbeitung personenbezogener Daten erfolgt ausschließlich im Einklang mit den Weisungen des Verantwortlichen.
- Management von Sicherheitsvorfällen: Es ist ein Prozess etabliert, der sicherstellt, dass Sicherheitsverletzungen frühzeitig erkannt und unverzüglich an den Verantwortlichen gemeldet werden können, um gesetzliche Meldefristen einzuhalten.
- Sicherheits-Updates: Sicherheitsrelevante Patches und Updates für die eingesetzte Software werden zeitnah installiert, um bekannte Sicherheitslücken zu schließen.

Anlage 2: Genehmigte Sub-Auftragsverarbeiter

Der Verantwortliche genehmigt zum Zeitpunkt des Vertragsschlusses den Einsatz der folgenden Sub-Auftragsverarbeiter:

Firma	Leistung	Land
RunPod Inc	GPU Cloud	EU/USA
Contabo GmbH	Server Hosting	EU
Google Cloud	Cloud Service Provider	EU
Google Firebase	User Authentication	USA
PostHog	Analytics	EU/USA
Brevo	E-Mail Provider	EU