Vereinbarung zur Auftragsverarbeitung gemäß Art. 28 DSGVO

zwischen

Anett Rothhardt
Pruppacher Weg 25a
91126 Rednitzhembach

-nachfolgend: Verantwortlicher (Du/Dich)

und

PicDrop GmbH
Am Treptower Park 28-30
12435 Berlin

-nachfolgend: Auftragsverarbeiter (wir/uns)

Präambel

Wir werden von Dir mit der Erfüllung eines Auftrages im Rahmen einer Datenverarbeitung beauftragt. Wir kommen hierbei in Berührung mit personenbezogenen Daten.

In dieser Vereinbarung werden Regelungen festgelegt, die gewährleisten, dass wir sorgsam mit den Daten umgehen und dass ein hoher Datenschutzstandard bei uns eingehalten wird.

1. Gegenstand, Dauer und Geltungsbereich

Zwischen Dir und uns besteht ein Auftragsverhältnis. Die vorliegende Vereinbarung konkretisiert die datenschutzrechtlichen Verpflichtungen aus dem zugrundeliegenden Nutzungsvertrag (der Nutzung der PicDrop-Plattform und -Funktionen). Die Dauer dieser Vereinbarung entspricht der Laufzeit des Nutzungsvertrages.

Gegenstand des Auftrags ist die Nutzung der PicDrop-Plattform und -Funktionen (u. a. die Bereitstellung einer Bildübertragungsplattform für professionelle Fotografen, dabei z. B. die Bereitstellung einer Galerie für den Upload und Download von Bildern des Verantwortlichen und seiner Kunden) gemäß dem zugrundliegenden Nutzungsvertrag.

Diese Vereinbarung gilt für sämtliche Beauftragungen bei denen Du uns zur Durchführung des jeweiligen Auftrages erforderliche Kunden- und sonstige Personendaten (z. B. Personenfotografien) für die Dauer der Auftragsabwicklung überlässt oder bei denen es zu einer Verarbeitung oder Wahrnehmung von personenbezogenen Daten durch uns kommen kann.

2. Art und Zweck der Datenverarbeitung

Art und Zweck der Verarbeitung der personenbezogenen Daten durch uns ergeben sich aus dem Nutzungsvertrag. Wir verarbeiten personenbezogene Daten von Deinen Mitarbeitern und Kunden. Bei den Daten handelt es sich insbesondere um Personenstammdaten (Vor- und Nachname), Kontaktdaten (E-Mail-Adresse) sowie Fotografien.

3. Deine Rechte und Pflichten als Verantwortlicher

Für die Beurteilung der Zulässigkeit der Datenverarbeitung sowie zur Wahrung der Rechte der Betroffenen bist allein Du zuständig und somit für die Verarbeitung Verantwortlicher im Sinne des Art. 4 Nr.7 DSGVO.

Du bist berechtigt, Weisungen über Art, Umfang und Verfahren der Datenverarbeitung zu erteilen. Weisungen sind auf Dein Verlangen von uns schriftlich oder in Textform (z. B. per E-Mail) zu bestätigen.

Du informierst uns unverzüglich, wenn Fehler oder Unregelmäßigkeiten im Zusammenhang mit der Verarbeitung personenbezogener Daten durch uns festgestellt werden.

4. Unsere Pflichten als Auftragsverarbeiter, technische und organisatorische Maßnahmen

Wir werden personenbezogene Daten ausschließlich nach Maßgabe dieser Vereinbarung und/oder des zugrundeliegenden Nutzungsvertrages sowie nach Deinen Weisungen verarbeiten.

Wir werden Dir bei der Erfüllung der Rechte der Betroffenen, insbesondere im Hinblick auf Berichtigung, Einschränkung der Verarbeitung und Löschung, Benachrichtigung und Auskunftserteilung, im Rahmen unserer Möglichkeiten unterstützen.

Die Verarbeitung und Nutzung der Daten findet grundsätzlich im Gebiet der Bundesrepublik Deutschland, in einem Mitgliedsstaat der Europäischen Union oder in einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum statt. Jede Verlagerung in ein Drittland bedarf Deiner vorherigen schriftlichen Zustimmung, die Du nicht ohne berechtigten Grund verweigern kannst, und darf nur erfolgen, wenn die besonderen Voraussetzungen der Art. 44 ff. DSGVO erfüllt sind.

Wir verpflichten uns, insbesondere unter Beachtung der Grundsätze ordnungsgemäßer Datenverarbeitung gem. Art 32 i. V. m. Art. 5 Abs. 1 DSGVO, durch geeignete Kontrollen sicherzustellen, dass die verarbeiteten oder überlassenen personenbezogenen Daten ausschließlich nach Maßgabe dieser Vereinbarung, des zugrundeliegenden Nutzungsvertrages und Deinen entsprechenden Weisungen verarbeitet werden.

Wir sichern einen datenschutzkonformen und sicheren Umgang mit den personenbezogenen Daten zu und gewährleisten insbesondere folgende Sicherungsmaßnahmen:

- Unbefugte Personen haben keinen Zugriff auf die personenbezogenen Daten;
- Computersysteme sind durch Passwörter gesichert und technisch auf dem aktuellen Stand;
- Personenbezogenen Daten werden nur von den Personen eingesehen und bearbeitet, die mit der konkreten Auftragsabwicklung betraut und zum vertraulichen Umgang mit personenbezogenen Daten verpflichtet sind;
- Die uns übertragene Bereitstellung von Uploads und Downloads erfolgt aufgabenbezogen getrennt von anderen Beauftragungen und sonstigen Datenbeständen;
- Soweit möglich, erfolgt die Dienstleistung am Bildschirm ohne Speicherung. Sofern wir Daten im Wege der Beauftragung durch Dich erhalten, verpflichten wir uns, die Daten auf geeignete Weise zu kennzeichnen. Sofern die Daten für verschiedene Zwecke verarbeitet werden, werden wir die Daten mit dem jeweiligen Zweck kennzeichnen;
- Wir unterstützen Dich bei der Erfüllung der Rechte der betroffenen Personen, insbesondere im Hinblick auf Berichtigung, Einschränkung der Verarbeitung und Löschung, Benachrichtigung und Auskunftserteilung, auf erstes

Anfordern im Rahmen unserer Möglichkeiten. Sollte eine datenschutzrechtliche Anfrage eines Betroffenen bei uns eingehen, werden wir diese Anfrage unverzüglich an Dich weiterleiten und Dir die Beantwortung der Anfrage überlassen.

- Sollten wir personenbezogene Daten in Deinem Auftrag erheben und sind diese Daten Gegenstand eines Verlangens auf Datenportabilität gem. Art. 20 DSGVO, werden wir Dir den betreffenden Datensatz unverzüglich auf Anforderung innerhalb der gesetzten Frist, im Übrigen innerhalb von 10 Werktagen, in einem strukturierten, gängigen und maschinenlesbaren Format zur Verfügung stellen.
- Details zu den technischen und organisatorischen Maßnahmen finden sich in Anlage 1

5. Berichtigung, Löschung und Sperrung von Daten, Löschung bei Vertragsbeendigung

Nach Beendigung des Nutzungsvertrages und auf Deine Weisung sind wir verpflichtet, sämtliche in unserem Besitz gelangten personenbezogenen Daten, Unterlagen und Ausdrucke, die im Zusammenhang mit dem Auftragsverhältnis stehen, gegebenenfalls an Dich auszuhändigen und datenschutz- und datensicherheitskonform zu löschen bzw. zu vernichten. Aufzeichnungen, die wir aus gesetzlichen Gründen (z. B. zur Buchführung) aufbewahren müssen, sind für die Dauer der gesetzlichen Fristen von der sofortigen Löschpflicht ausgenommen.

6. Unsere Informationspflichten

Wir werden Dich unverzüglich darauf aufmerksam machen, wenn eine von Dir erteilte Weisung unserer Meinung nach gegen gesetzliche Vorschriften verstößt. Wir sind berechtigt, die Durchführung der entsprechenden Weisung solange auszusetzen, bis sie durch Dich bestätigt oder geändert wird.

Wir werden Dich bei der Einhaltung der in den Artikeln 32 bis 36 DSGVO genannten Pflichten unter Berücksichtigung der Art der Verarbeitung und der uns zur Verfügung stehenden Informationen unterstützen.

Bei eventuellen Kontrollmaßnahmen einer Datenschutzaufsichtsbehörde sowie bei anderweitigen Anfragen, Ermittlungen oder Erkundigungen der Datenschutzaufsichtsbehörde, werden wir Dich nach Kenntniserlangung über die Durchführung der Kontrollmaßnahme unverzüglich informieren, soweit personenbezogenen Daten von Dir hiervon betroffen sind.

7. Datenschutzkontrolle

Wir erklären uns nach rechtzeitiger vorheriger Anmeldung zu den üblichen Geschäftszeiten ohne Störung unseres Geschäftsbetriebes oder Gefährdung der Sicherheitsmaßnahmen für andere Kunden oder Verantwortliche und auf Deine eigenen Kosten damit einverstanden, die Einhaltung der Vorschriften über den Datenschutz und der vertraglichen Vereinbarungen im erforderlichen Umfang durch Dich oder durch Dritte kontrollieren zu lassen.

8. Unterauftragsverhältnisse

Du ermächtigst uns, weitere Auftragsverarbeiter gemäß den nachfolgenden Absätzen in dieser Vereinbarung in Anspruch zu nehmen. Diese Ermächtigung stellt eine allgemeine schriftliche Genehmigung i. S. d. Art. 28 Abs. 2 DSGVO dar.

Wir sind berechtigt, weitere Auftragsverarbeiter zu beauftragen oder bereits beauftragte zu ersetzen. Wir werden Dich vorab über jede beabsichtigte Änderung in Bezug auf die Hinzuziehung oder die Ersetzung eines weiteren Auftragsverarbeiters informieren. Du kannst gegen eine beabsichtigte Änderung Einspruch erheben.

Der Einspruch gegen die beabsichtigte Änderung ist innerhalb von 2 Wochen nach Zugang der Information über die Änderung gegenüber uns zu erheben. Im Fall des Einspruchs können wir nach eigener Wahl die Leistung ohne die beabsichtigte Änderung erbringen oder einen alternativen weiteren Auftragsverarbeiter vorschlagen und mit Dir abstimmen. Sofern uns die Erbringung der Leistung ohne die beabsichtigte Änderung nicht zumutbar ist – etwa aufgrund von damit verbundenen unverhältnismäßigen Aufwendungen für uns – oder die Abstimmung eines weiteren Auftragsverarbeiters fehlschlägt, können Du und wir diese Vereinbarung sowie den Nutzungsvertrag mit einer Frist von einem Monat zum Monatsende kündigen.

Bei Einschaltung eines weiteren Auftragsverarbeiters muss stets ein Schutzniveau, welches mit demjenigen dieser Vereinbarung vergleichbar ist, gewährleistet werden. Wir sind gegenüber Dir als Verantwortlichen für sämtliche Handlungen und Unterlassungen der von uns eingesetzten weiteren Auftragsverarbeiter verantwortlich.

Sofern wir derzeit bei der Erfüllung des Auftrags mit Subunternehmern zusammenarbeiten, teilen wir Dir diese nachfolgend mit. Mit diesen Unterauftragsverhältnissen erklärt sich der Auftraggeber einverstanden.

Hosting Plattform & Dateien

- Boreus GmbH, Deutschland, boreus.de als betreuende Instanz für Amazon Web Services EMEA SARL, Luxemburg (Server-Standort: Europa, Europäischer Wirtschaftsraum), aws.amazon.com

E-Mail-Versand

- The Rocket Science Group LLC d/b/a MailChimp, USA, mailchimp.com

9. Folgen eines Verstoßes gegen Datenschutzbestimmungen

Wir haften Dir gegenüber gemäß den gesetzlichen Regelungen für sämtliche Schäden durch schuldhafte Verstöße gegen diese Vereinbarung oder die gesetzlichen Datenschutzbestimmungen, die wir, unsere Mitarbeiter bzw. die eingesetzten Subunternehmer bei der Auftragserfüllung verursachen. Eine Ersatzpflicht von uns besteht nicht, sofern wir nachweisen, dass wir die uns überlassenen Daten von Dir ausschließlich nach Deinen Weisungen verarbeitet und seinen speziell den uns auferlegten Pflichten aus der DSGVO nachgekommen ist.

Du stellst uns von allen Ansprüchen Dritter frei, die aufgrund einer schuldhaften Verletzung der Verpflichtungen aus dieser Vereinbarung oder geltenden datenschutzrechtlichen Vorschriften durch Dich gegen uns geltend gemacht werden.

10. Sonstiges

Im Falle von Widersprüchen zwischen den Bestimmungen in dieser Vereinbarung und den Regelungen des Nutzungsvertrages gehen die Bestimmungen dieser Vereinbarung vor.

Änderungen und Ergänzungen dieser Vereinbarung müssen schriftlich oder in Textform erfolgen und bedürfen der ausdrücklichen Angabe, dass damit die vorliegenden Bestimmungen geändert und/oder ergänzt werden. Dies gilt auch für den Verzicht auf dieses Formerfordernis.

Sollte eine Bestimmung dieser Vereinbarung unwirksam oder nicht durchsetzbar sein oder werden, so bleiben die übrigen Bestimmungen dieser Vereinbarung hiervon unberührt. Die unwirksame oder nicht durchsetzbare Bestimmung ist durch eine wirksame und durchsetzbare Bestimmung zu ersetzen, welche dem Zweck der ersetzenden Bestimmung am nächsten kommt.

Berlin, 12.1.2023

Dieser Vertrag wurde elektronisch abgeschlossen und ist daher auch ohne Unterschrift gültig.

Anlage 1: Technische und organisatorische Maßnahmen

Pseudonymisierung und Verschlüsselung

- Verwendung von Pseudonymen wie IDs oder Keys soweit möglich
- Zugriff auf bzw. Kommunikation zwischen Systemen nur über verschlüsselte Verbindungen (SSL, SSH, etc.)
- Speicherung von Daten auf verschlüsselten Datenträgern
- alle Arbeitsgeräte (Notebooks, Telefone) arbeiten mit Vollverschlüsselung

Zutrittskontrolle

- Büroräume:
  - verschlossene Eingangstür zum Büro, kein Zutritt ohne Schlüssel
  - dokumentierte Schlüsselvergabe an Mitarbeiter und Beauftragte
  - Zutritt von Gästen nur in Begleitung eines Mitarbeiters
- Anlagen von Auftragsverarbeitern:
  - Zutritt gemäß AVV-Vereinbarung entsprechend der Anforderungen an DSGVO

Zugangskontrolle

- Zugang zu verarbeitenden Systemen nur individuell nach Bedarf
  - erteilte Zugänge sind dokumentiert
  - Erteilung erfolgt nur durch Geschäftsführung
  - regelmäßige Überprüfung der vergebenen Zugänge
- Passwörter werden für jeden Zugang individuell erstellt und in einem Passwort-Manager gespeichert
- nach Möglichkeit werden Zugänge über Zwei-Faktor-Authentisierung (2FA) zusätzlich gesichert
- Betrieb der Server mit Firewalls

Zugriffskontrolle

- Zugangsvergabe nach Berechtigungskonzept
  - nur minimal notwendige Zugriffsrechte

    - Vergabe nach Aufgabenfeldern
    - regelmäßige Überprüfung
- Datenträger werden sicher gelöscht oder physisch vernichtet
- Dokumente werden mittels Aktenvernichter vernichtet

Trennungskontrolle

- logische Trennung von Daten verschiedener Kunden
- Zweckbindung von Datennutzung
- verschiedene Betriebs-Umgebungen
    - Produktions- und Test-Systeme sind voneinander getrennt
    - Zugriff auf Produktionsumgebung auf minimale Anzahl an Personen begrenzt

Weitergabekontrolle

- Weitergabe von Daten nur nach gesetzlichen Vorgaben oder betrieblicher Erfordernis
- Auftragsverarbeiter werden auf Anforderungen nach DSGVO geprüft und AVV abgeschlossen
- elektronische Übertragung von Daten nur über verschlüsselte Verbindungen
- Weitergabe von Daten wird im Verfahrensverzeichnis dokumentiert

Eingabekontrolle

- Eingabe, Änderung und Löschung von Daten im Regelfall nur durch Kunden selbst
- Eingabe von Zahlungsinformationen ausschließlich durch Kunden, kein Zugriff durch Mitarbeiter möglich
- keine Änderung von Daten durch Mitarbeiter ohne vorherige Anfrage über Kundensupport (Protokollierung über die Support-Anfrage)

Gewährleistung der Verfügbarkeit und Belastbarkeit

- Betrieb ausschließlich bei spezialisierten Dienstleistern
    - stellen Verfügbarkeit auf Infrastruktur-Ebene (Strom, Netzwerk-Uplink) sicher
    - ermöglicht schnellen Bereitstellung von Hardwareersatz
- regelmäßige Updates
- regelmäßige Backups (mindestens täglich); getrennte Speicherung
- Wiederherstellung wird regelmäßig geprobt

Verfahren regelmäßiger Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen

- Mitarbeiter sind vertraglich auf Vertraulichkeit und Einhaltung der Datenschutzgesetze verpflichtet
- regelmäßige Sensibilisierung bzw. Schulung der Mitarbeiter
- regelmäßige Überprüfung der Schutzmaßnahmen, Verfahren und Dokumentation
- Datenschutz-Folgeabschätzung bei Produktentwicklung