Auftragsverarbeitungsvereinbarung

Zwischen

der Photostore24.online GmbH, vertreten durch Geschäftsführer Markus Reichl, Erkrather Straße 401, 40231 Düsseldorf**,** Deutschland

– im Folgenden: „Anbieter/Auftragnehmer“ –

und

dem registrierten Nutzer der Plattform Scrappbook (https://www.scrappbook.de),

– im Folgenden: „Kunde/Auftraggeber“ –

- gemeinsam im Folgenden: die Parteien -

wird folgender Vertrag zur Auftragsdatenverarbeitung gemäß Art. 28 DSGVO geschlossen:

§ 1 Gegenstand des Vertrages

(1) Gegenstand dieses Auftragsverarbeitungsvertrages ist die Verarbeitung personenbezogener Daten durch den Anbieter im Rahmen des Angebots der Onlineplattform Scrappbook (https://www.scrappbook.de) zur Bereitstellung von Fotogalerien, Rechnungserstellung und Druckaufträgen durch den Kunden.

(2) Die Verarbeitung erfolgt im Rahmen des zwischen den Parteien bestehenden Nutzungsverhältnisses über die Plattform Scrappbook (https://www.scrappbook.de), welches durch die Registrierung und Akzeptanz der Allgemeinen Geschäftsbedingungen (AGB) des Anbieters zustande kommt.

(3) Der Anbieter stellt die Plattform und zugehörige Dienste zur Verfügung und verarbeitet personenbezogene Daten ausschließlich im Auftrag des Kunden.

§ 2 Umfang, Art und Zweck sowie Kreis der Betroffenen

(1) Die Art der Verarbeitung umfasst insbesondere:

- Speicherung und Hosting von Bilddaten,
- Datenbankverarbeitung von Kunden- und Bestelldaten,
- Verarbeitung von Zahlungsinformationen,
- Einsatz von Gesichtserkennung zur internen Filterung von Fotos (biometrische Daten), sofern aktiviert,
- technische Analyse und Fehlerbehebung im Rahmen des Supports.

(2) Zweck der Verarbeitung ist die Bereitstellung, Verwaltung und Nutzung von Online-Fotogalerien und zugehöriger Dienste durch den Auftraggeber gegenüber dessen Endkunden.

(3) Es können insbesondere folgende Arten personenbezogener Daten verarbeitet werden:

- Fotos mit erkennbaren Personen (ggf. mit biometrischen Merkmalen),
- Name, E-Mail-Adresse, Lieferadresse, Zahlungsinformationen der Endkunden,
- Nutzerkennungen und IP-Adressen,
- Rechnungsinformationen,
- Informationen aus Logdaten und Nutzerinteraktionen.

(4) Es können insbesondere folgende Kategorien betroffener Personen betroffen sein:

- Kundinnen und Kunden des Auftraggebers (Fotokäufer, Besucher der Galerie),
- ggf. Mitarbeitende des Auftraggebers (bei Nutzung interner Funktionen,

§ 3 Technische und organisatorische Maßnahmen

(1) Die zum Zeitpunkt des Vertragsschlusses geltenden technischen und organisatorischen Maßnahmen gemäß Art. 32 DSGVO sind in der **Anlage** zu dieser Vereinbarung dargestellt. Der Auftragnehmer wird diese Maßnahmen regelmäßig überprüfen, bei Bedarf anpassen und dem Auftraggeber auf Anforderung zur Verfügung stellen.

(2) Der Auftraggeber kann Änderungen an den technischen und organisatorischen Maßnahmen verlangen, sofern sich wegen der Art, dem Umfang, dem Zweck sowie dem Kreis der Betroffenen zusätzliche oder geänderte Anforderungen an die Auftragsverarbeitung ergeben.

(3) Der Auftragnehmer kann jederzeit wegen erkannter Lücken und neuen bzw. bislang unbekannten Sicherungsmaßnahmen und -erfordernissen die Anlage anpassen, sofern das vereinbarte Sicherungsniveau nicht unterschritten wird. Der Auftragnehmer informiert den Auftraggeber über Änderungen unter Vorlage der angepassten Anlage.

§ 4 Berichtigung, Sperrung und Löschung von Daten

Der Auftraggeber allein ist berechtigt, die Berichtigung, Sperrung und Löschung von im Auftrag beim Auftragnehmer verarbeiteten Daten zu veranlassen. Der Auftragnehmer hat diesbezügliche Aufforderungen von Betroffenen entgegenzunehmen und diese unverzüglich an den Auftraggeber zur Entscheidung und anschließenden Umsetzung weiterzuleiten.

§ 5 Datenschutzkontrolle und -pflichten des Auftragnehmers

Im Rahmen der Datenschutzkontrolle hat der Auftragnehmer ergänzend zu den hier vereinbarten Pflichten und Maßnahmen folgende Pflichten:

(1) Der Auftragnehmer verarbeitet personenbezogene Daten ausschließlich in Systemen, die für den Betrieb der Plattform Scrappbook erforderlich sind. Er hat keine Einsichtnahme in die Inhalte der Fotoalben oder personenbezogenen Daten, es sei denn, dies ist zur technischen Fehlerbehebung erforderlich.

(2) Im Falle der Aktivierung der Gesichtserkennungsfunktion verpflichtet sich der Auftragnehmer, deren technische Verarbeitung nur bei aktiver Freigabe durch den Auftraggeber durchzuführen. Die Aktivierung setzt eine dokumentierte Bestätigung des Auftraggebers voraus, dass eine Einwilligung der betroffenen Personen nach Art. 9 Abs. 2 lit. a DSGVO eingeholt wurde.

(3) Der Auftragnehmer verpflichtet alle im Rahmen dieses Auftrags eingesetzten Mitarbeitenden auf Vertraulichkeit und dokumentiert dies. Eine Übersicht über die Kategorien der eingesetzten Personen kann auf Anfrage zur Verfügung gestellt werden.

(4) Formale Bestellung eines betrieblichen Datenschutzbeauftragten gemäß § 38 BDSG i.V.m. Art. 37 DSGVO:

Name:
Dr. Hauke Hansen
FPS Rechtsanwaltsgesellschaft mbH & Co. KG
Eschersheimer Landstraße 25-27
60322 Frankfurt am Main

E-Mail: hansen@fps-law.de

Über Änderungen bei der Bestellung des Datenschutzbeauftragten wird der Auftraggeber informiert.

§ 6 Unterauftragnehmer

(1) Die Einschaltung von Unterauftragnehmern ist nur mit vorheriger gesonderter oder allgemeiner schriftlicher Genehmigung des Auftraggebers zulässig.

(2) Zum Zeitpunkt des Vertragsschlusses bestehen folgende Unterauftragsverhältnisse, die hiermit gemäß Art. 28 Abs. 2 DSGVO als durch den Auftraggeber genehmigt gelten. Diese Dienstleister verarbeiten personenbezogene Daten ausschließlich im Auftrag des Auftragnehmers:

- Heroku (Salesforce.com, Hosting der Anwendung),

- Wasabi (Cloud-Speicher für Bilder),
- Intercolo (Cloud-Speicher für Bilder),
- MongoDB (Datenbankbetrieb, Verwaltung von Benutzerkonten, Fotos etc.),
- Amazon Web Services (Server-Infrastruktur),
- Cloudflare (Content Delivery Network),
- JetAdmin (Admin-Interface, Zugriff auf Nutzerdaten),
- Pathway (Stripe-Integration, ggf. Datev-Export).,
- FinAPI (API für Kontobewegungen, sofern genutzt)
- AnyAPI (Prüfung von USt-IDs, sofern im Einsatz).

(3) Andere eingesetzte Dienste, insbesondere Zahlungsdienstleister (z. B. Stripe, PayPal), Druckdienstleister (z. B. nPhoto, PixelfotoExpress, Picanova) sowie Tracking- und Analyse-Tools (z. B. Google Analytics, Meta Pixel), gelten nicht als Unterauftragsverarbeiter, da sie Daten entweder als eigenständige Verantwortliche verarbeiten oder eine eigene Rechtsgrundlage zur Datenverarbeitung haben. Ihre Einbindung wird in der Datenschutzerklärung erläutert.

Eine aktuelle Liste ist in der Datenschutzerklärung veröffentlicht und wird auf Wunsch zur Verfügung gestellt.

§ 7 Kontrollrechte des Auftraggebers

(1) Der Auftraggeber ist berechtigt, die erforderliche Auftragskontrolle in Abstimmung mit dem Auftragnehmer unter Berücksichtigung dessen betrieblicher Belange einschließlich der Maßnahmen zur Einhaltung der Anforderungen an die Auftragsverarbeitung anderer Auftraggeber durchzuführen oder durchführen zu lassen.

(2) Der Auftragnehmer verpflichtet sich, dem Auftraggeber auf Anforderung die zur Erfüllung der Pflichten zur Auftragskontrolle erforderlichen Auskünfte zu geben und die entsprechenden Nachweise und Dokumentationen zur Verfügung zu stellen.

(3) Vor-Ort-Kontrollen bedürfen grundsätzlich einer Ankündigung mit angemessener Frist. Eine verkürzte Ankündigungsfrist kann nur erfolgen, wenn konkrete Hinweise auf eine datenschutzrechtliche Pflichtverletzung vorliegen. Vor-Ort-Kontrollen erfolgen maximal einmal jährlich, sofern kein konkreter Anlass besteht.

§ 8 Mitteilung bei Verstößen des Auftragnehmers

(1) Nach Art. 33 DSGVO bestehen für Vorfälle der unrechtmäßigen Übermittlung oder Kenntniserlangung und drohender schwerwiegender Beeinträchtigung der Betroffenen Melde- und Informationspflichten des Verantwortlichen (Auftraggeber). Der Auftragnehmer meldet dem Auftraggeber alle bestätigten Verstöße durch ihn oder die bei ihm beschäftigten Personen gegen Vorschriften und Vorkehrungen zum Schutz personenbezogener Daten oder gegen die im Auftragsverhältnis vereinbarten Maßnahmen sowie konkrete Anhaltspunkte, die auf einen datenschutzrelevanten Vorfall hindeuten.

(2) Gegenstand des Auftragsverhältnisses sind unter anderem besondere personenbezogene Daten im Sinne der Art. 9 DSGVO (biometrische Daten). Der Auftragnehmer wird daher in derartigen Fällen den Auftraggeber unverzüglich informieren und ihm alle Informationen zur Verfügung stellen bzw. nach Abwägung gemäß § 29 BDSG auf Anforderung des Auftraggebers bei der Information an die Aufsichtsbehörde und die Betroffenen mitwirken.

(3) Der Auftragnehmer ergreift unverzüglich angemessene Maßnahmen, um die Störung und den Zugriff auf die Daten der Betroffenen zu unterbinden. Zugleich dokumentiert der Auftragnehmer die Anhaltspunkte für die Sicherheitslücke, die getroffenen Sofortmaßnahmen und schlägt dem Auftraggeber eine geeignete Anpassung der technischen und organisatorischen Maßnahmen zur Vermeidung von Wiederholungsfällen vor.

§ 9 Weisungsbefugnis des Auftraggebers

(1) Der Auftragnehmer verarbeitet und nutzt die Daten ausschließlich für die Zwecke der vertragsgegenständlichen Auftragsverarbeitung auf generelle oder Weisung im Einzelfall des Auftraggebers. Der Auftragnehmer befolgt Weisungen des Auftraggebers, soweit sie im Rahmen des vereinbarten Leistungsumfangs sowie der datenschutzrechtlichen Vorschriften zulässig und nicht offensichtlich rechtswidrig sind.

(2) Der Auftraggeber benennt die weisungsberechtigten Personen gegenüber dem Auftragnehmer in Textform. Änderungen teilt er unverzüglich mit.

(3) Auskünfte an Dritte oder die Betroffenen darf der Auftragnehmer nur nach vorheriger schriftlicher Zustimmung durch den Auftraggeber erteilen, sofern nicht eine gesetzliche Verpflichtung zur Auskunft besteht. In einem solchen Fall informiert der Auftragnehmer den Auftraggeber unverzüglich über die Auskunftsanfrage und die beabsichtigte Offenlegung, sofern ihm dies nicht gesetzlich untersagt ist.

(4) Der Auftragnehmer fertigt auf Weisung des Auftraggebers Kopien, Duplikate und Zusammenstellungen und übermittelt diese ebenso nur auf Weisung des Auftraggebers an Dritte. Sicherungskopien fertigt der Auftragnehmer entsprechend den in der **Anlage** genannten Standards und den Anforderungen der DSGVO an.

(5) Soweit der Auftragnehmer Kopien zur Einhaltung eigener gesetzlicher Aufbewahrungspflichten fertigt, hat er den Auftraggeber über Art, Umfang und Dauer der Verwahrung der Kopie zu informieren. Kopien oder Screenshots von im Rahmen von Serviceeinsätzen eingesehenen Endkundendaten sind grundsätzlich untersagt, es sei denn, dies ist zur Dokumentation eines schwerwiegenden technischen Vorfalls erforderlich oder erfolgt auf ausdrückliche Weisung.

§ 10 Löschung von Daten und Rückgabe von Datenträgern

(1) Nach Beendigung des Auftragsverhältnisses und auf entsprechende Weisung des Auftraggebers wird der Auftragnehmer alle im Rahmen der Auftragsverarbeitung verarbeiteten personenbezogenen Daten sowie Verarbeitungs- und Nutzungsergebnisse datenschutzgerecht löschen oder – sofern vereinbart – an den Auftraggeber zurückgeben. Die Rückgabe oder Löschung erfolgt im Rahmen des technisch und wirtschaftlich zumutbaren Aufwands. Die Datenrückgabe erfolgt über ein geeignetes, sicheres Übertragungsverfahren; die Zugangsdaten werden gesondert übermittelt. Die datenschutzgerechte Löschung wird dokumentiert und dem Auftraggeber auf Anforderung nachgewiesen. Eine Löschung erfolgt nicht, soweit eine gesetzliche Verpflichtung zur Aufbewahrung oder ein berechtigtes Interesse an einer eingeschränkten Nachhaltung besteht (z. B. zur Abwehr von Haftungsansprüchen oder zur Nachweisführung).

(2) Dokumentationen, die dem Nachweis der auftrags- und ordnungsgemäßen Datenverarbeitung dienen, bewahrt der Auftragnehmer entsprechend der jeweiligen Aufbewahrungsfristen über das Vertragsende hinaus auf. Der Auftraggeber kann auf Anforderung Einsicht in diese Dokumentationen erhalten, sofern und soweit ein berechtigtes Interesse besteht.

§ 11 Vertragslaufzeit

(1) Diese Vereinbarung wird wirksam, sobald der Auftraggeber im Rahmen der Registrierung auf der Plattform Scrappbook (https://www.scrappbook.de) die Auftragsverarbeitungsvereinbarung durch aktives Setzen einer Checkbox akzeptiert.

(2) Die Vereinbarung gilt für die Dauer des bestehenden Nutzungsverhältnisses zwischen dem Auftraggeber und dem Auftragnehmer über die Plattform Scrappbook.

(3) Mit Beendigung des Nutzungsverhältnisses endet auch diese Vereinbarung, sofern nicht gesetzliche Aufbewahrungsfristen oder andere datenschutzrechtliche Gründe eine fortbestehende Datenverarbeitung durch den Auftragnehmer erfordern. In diesem Fall gelten die Regelungen zur Löschung bzw. Rückgabe personenbezogener Daten gemäß § 10.

§ 12 Sonderkündigungsrecht

(1) Der Auftraggeber ist berechtigt, diese Vereinbarung aus wichtigem Grund ohne Einhaltung einer Frist außerordentlich zu kündigen. Ein wichtiger Grund liegt insbesondere vor, wenn der Auftragnehmer trotz vorheriger schriftlicher Abmahnung einen schwerwiegenden Verstoß gegen die

Bestimmungen dieser Vereinbarung oder gegen geltende Datenschutzvorschriften begeht, der geeignet ist, die Interessen des Auftraggebers erheblich zu beeinträchtigen.

Ein wichtiger Grund kann insbesondere vorliegen, wenn

- der Auftragnehmer wiederholt rechtmäßige Weisungen des Auftraggebers nicht umsetzt,
- Kontrollrechte des Auftraggebers in erheblicher Weise verweigert werden oder
- die vereinbarten technischen und organisatorischen Maßnahmen nachhaltig und in erheblichem Umfang nicht eingehalten werden.

(2) Vor Ausspruch einer außerordentlichen Kündigung ist dem Auftragnehmer eine angemessene Frist zur Abhilfe einzuräumen, es sei denn, eine solche Fristsetzung ist dem Auftraggeber unter Abwägung beiderseitiger Interessen nicht zumutbar.

(3) Im Fall einer berechtigten außerordentlichen Kündigung, die auf ein vorsätzliches oder grob fahrlässiges Verhalten des Auftragnehmers zurückzuführen ist, kann der Auftraggeber Ersatz der ihm nachweislich entstandenen unmittelbaren Mehrkosten verlangen, die ihm durch die vorzeitige Vertragsbeendigung entstehen. Eine weitergehende Haftung bleibt den gesetzlichen Bestimmungen vorbehalten.

(4) Nach Beendigung der Vereinbarung gibt der Auftragnehmer alle personenbezogenen Daten, relevanten Dokumentationen sowie Zugangsdaten auf Anforderung des Auftraggebers heraus. Auf Wunsch des Auftraggebers löscht der Auftragnehmer die verbleibenden Daten datenschutzkonform und weist dies nach, soweit dem keine gesetzlichen Aufbewahrungspflichten entgegenstehen.

§ 13 Haftung/Versicherung

(1) Der Auftragnehmer haftet gegenüber dem Auftraggeber für Schäden, die durch eine schuldhafte Verletzung seiner Pflichten aus dieser Vereinbarung oder den einschlägigen Datenschutzvorschriften entstehen. Bei vorsätzlicher oder grob fahrlässiger Pflichtverletzung haftet der Auftragnehmer unbeschränkt. Bei einfach fahrlässiger Verletzung wesentlicher Vertragspflichten (Kardinalpflichten) ist die Haftung auf den vertragstypischen, vorhersehbaren Schaden begrenzt. Die Haftung für sonstige Fälle einfacher Fahrlässigkeit ist ausgeschlossen.

(2) Im Verhältnis der Parteien untereinander trägt jede Partei die Verantwortung für etwaige von ihr verschuldete Datenschutzverstöße gegenüber betroffenen Personen gemäß Art. 82 DSGVO. Wird eine Partei aufgrund eines solchen Verstoßes von Dritten in Anspruch genommen, stellt sie die andere Partei nur insoweit von der Inanspruchnahme frei, als sie den Verstoß nachweislich zu vertreten hat. Die Parteien arbeiten zur Klärung der Verantwortlichkeit vertrauensvoll zusammen.

§ 14 Schlussbestimmungen

(1) Sollten einzelne Bestimmungen dieses Vertrags unwirksam sein oder werden oder eine Lücke enthalten, so bleiben die übrigen Bestimmungen hiervon unberührt. Die Parteien verpflichten sich, anstelle der unwirksamen Regelung eine solche gesetzlich zulässige Regelung zu treffen, die dem Zweck der unwirksamen Regelung am nächsten kommt und den Anforderungen des Art. 28 DSGVO am besten gerecht wird.

(2) Im Fall von Widersprüchen zwischen diesem Vertrag und sonstigen Vereinbarungen zwischen den Parteien, insbesondere dem Hauptvertrag, gehen die Regelungen dieses Vertrags vor.

Anlage: Technische und organisatorische Maßnahmen

Anlage

Technische und organisatorische Maßnahmen

Teil I: Datenschutzrechtliche Grundsätze (Art. 5 DSGVO)

1. Transparenz

Transparenz im Sinne von Art. 5 Abs. 1 lit. a) der DSGVO ist gewährleistet, wenn die Daten in einer für die betroffene Person verständlichen Weise verarbeitet werden. Zu diesem Zweck muss der für die Verarbeitung Verantwortliche gemäß Art. 12 Abs. 1 der DSGVO geeignete Maßnahmen ergreifen, um den Informations- und Meldepflichten gemäß Art. 13 und 14 der DSGVO nachzukommen und die entsprechenden Informationen in präziser, transparenter, verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache bereitstellen zu können. Transparenz wird erreicht durch:

- Bereitstellung klarer und verständlicher Datenschutzinformationen (z. B. auf der Website),
- Nachvollziehbarkeit von Datenflüssen und Datenempfängern,
- Unterstützung bei der Erfüllung von Informationspflichten gegenüber Betroffenen.

2. Zweckbindung

Zweckbindung im Sinne von Art. 5 Abs. 1 lit. b) der DS-GVO ist gewährleistet, wenn die Daten für festgelegte, eindeutige und rechtmäßige Zwecke erhoben und nicht in einer mit diesen Zwecken nicht zu vereinbarenden Weise weiterverarbeitet werden. Dies wird sichergestellt durch:

- Zweckbindung auch bei der Auswahl und Nutzung von IT-Systemen und Tools,
- Trennung von Daten mit unterschiedlichen Verarbeitungszwecken (siehe Trennungsgebot in den TOM).

3. Datenminimierung

Datenminimierung im Sinne von Art. 5 Abs. 1 lit. c) der DS-GVO ist gewährleistet, wenn der Umfang der Datenerhebung angemessen und für den oder die Zweck/e relevant ist und auf das für die Zwecke der Verarbeitung notwendige Maß beschränkt wird. Maßnahmen zur Datensparsamkeit und -minimierung sind:

- Prinzip der Datenminimierung bei Systemeinführungen („Privacy by Design“),
- regelmäßige Datenlöschungen gemäß interner Löschkonzepte,
- Einschränkung von Zugriffsrechten nach dem Prinzip der Erforderlichkeit („Need to know“),
- keine Speicherung über den erforderlichen Zeitraum hinaus.

4. Richtigkeit

Richtigkeit i.S.d. Art. 5 Abs. 1 lit. d) DS-GVO ist gewährleistet, wenn die verarbeiteten Daten sachlich richtig und, soweit erforderlich, auf dem neuesten Stand sind und Daten, die im Hinblick auf die Zwecke ihrer Verarbeitung unrichtig sind, unverzüglich gelöscht oder berichtigt werden. Die Richtigkeit wird gewährleistet durch:

- Dokumentation und Nachweisbarkeit der Herkunft der Daten
- Unverzügliche Berichtigung unzutreffender Daten nach Kenntniserlangung

5. Vertraulichkeit

Vertraulichkeit im Sinne von Art. 32 Abs. 1 lit. b) in Verbindung mit Erwägungsgrund 39 und 83 der DS-GVO ist hinreichend gewährleistet, wenn Unbefugte keinen Zugang zu den Daten haben und die Daten oder die Geräte, mit denen sie verarbeitet werden, nicht nutzen können und die Daten auch

gegen unbefugte oder unrechtmäßige Verarbeitung und gegen zufälligen Verlust gemäß Art. 5 Abs. 1 lit. f) DS-GVO geschützt sind. Dies ist durch umfassende technische und organisatorische Maßnahmen sichergestellt (vgl. Zugriffskontrolle, Zugangskontrolle etc.in den TOM). Zusätzlich gilt:

- Vertraulichkeitsverpflichtung von Beschäftigten, wo nötig,
- systematische Verwaltung und Dokumentation von Benutzerrechten,
- Sicherheitsvorkehrungen gegen unbefugten Zugriff auf physischer und digitaler Ebene.

6. Integrität

Integrität im Sinne von Art. 32 Abs. 1 lit. b) in Verbindung mit Art. 5 Abs. 1 lit. f) DS-GVO ist gewährleistet, wenn Daten gegen zufälligen Verlust, zufällige Zerstörung oder zufällige Beschädigung geschützt sind, dh die Daten vollständig, unverändert und unversehrt sind. Die Integrität personenbezogener Daten wird durch folgende ergänzende Maßnahmen geschützt:

- Nutzung sicherer Protokolle (z. B. TLS, VPN) für Übertragungen,
- kontrollierte Software-Updates,
- Vermeidung unautorisierter oder unbeabsichtigter Datenänderungen durch rollenbasiertes Berechtigungsmanagement.

7. Verfügbarkeit und Ausfallsicherheit

Integrität im Sinne von Art. 32 Abs. 1 lit. b) in Verbindung mit Art. 5 Abs. 1 lit. f) DS-GVO ist gewährleistet, wenn Daten gegen zufälligen Verlust, zufällige Zerstörung oder zufällige Beschädigung geschützt sind, dh die Daten vollständig, unverändert und unversehrt sind. Gemäß Art. 32 Abs. 1 lit. b) DS-GVO muss die Ausfallsicherheit dauerhaft gewährleistet sein und bezieht sich auf Systeme und Dienste im Zusammenhang mit der Verarbeitung von personenbezogenen Daten. Die Systeme und Daten sind dauerhaft verfügbar und ausfallsicher:

- regelmäßige, getestete Backups (On- und Offsite),
- dokumentierte Notfallpläne und Wiederanlaufstrategien,
- redundante Infrastruktur bei kritischen Diensten,
- Monitoring- und Frühwarnsysteme.

8. Rechenschaftspflicht

Die Rechenschaftspflicht nach Art. 5 Abs. 2 DS-GVO ist erfüllt, wenn der Auftraggeber als Verantwortlicher die Einhaltung der Grundsätze für die Verarbeitung personenbezogener Daten nachweisen kann.

- Dokumentation der technischen und organisatorischen Maßnahmen (TOM),
- regelmäßige Überprüfung und Aktualisierung der Schutzmaßnahmen,
- AV-Verträge und Dienstleister-Dokumentation,
- Benennung eines Datenschutzbeauftragten und jährliche Schulungen der Mitarbeitenden.

Teil II: Technische und organisatorische Maßnahmen (Art. 32 DSGVO)

1. Zutrittskontrolle

Ziel: Verhinderung unbefugten physischen Zugriffs auf Datenverarbeitungsanlagen

Maßnahmen:

- Alle produktiven Systeme werden ausschließlich in professionellen Rechenzentren betrieben.
- Zutrittsregelungen der Rechenzentrumsbetreiber (z. B. AWS, Wasabi) stellen sicher, dass ausschließlich autorisiertes Personal Zugang hat.
- Besucherzugänge bei Scrappbook-internen Büros erfolgen nur in Begleitung autorisierter Mitarbeiter.
- Büroarbeitsplätze sind durch Bildschirmsperre und persönliche Zugangsdaten gesichert.
- Mobile Geräte (z. B. Laptops) sind verschlüsselt und passwortgeschützt.

2. Zugangskontrolle

Ziel: Verhinderung unbefugten Zugriffs auf IT-Systeme
Maßnahmen:

- Zugriff auf Systeme erfolgt über persönliche Benutzerkonten mit sicheren Passwortrichtlinien.
- Zwei-Faktor-Authentifizierung (2FA) ist für alle administrativen Zugänge obligatorisch.
- Rollenbasierte Berechtigungskonzepte sind umgesetzt.
- VPN-Zugänge sind technisch beschränkt und werden nur im Ausnahmefall aktiviert.
- Gastnetzwerke (z. B. Büro-WLAN) sind logisch vom Unternehmensnetz getrennt.

3. Zugriffskontrolle

Ziel: Sicherstellung, dass nur berechtigte Personen Daten verarbeiten können
Maßnahmen:

- Rechtevergabe erfolgt nach dem Prinzip der minimalen Berechtigung („Need to know“) und wird regelmäßig überprüft.
- Zugriffe auf sensible Daten (z. B. Fotodatenbanken, Rechnungsinformationen) werden protokolliert.
- Es erfolgt keine Verarbeitung auf On-Premise-Servern – alle Datenverarbeitung erfolgt in verschlüsselten Cloud-Systemen.
- Zugänge zu sensiblen Funktionen (z. B. Bildfilter, Gesichtserkennung) sind technisch gesichert.

4. Weitergabekontrolle

Ziel: Verhinderung unbefugter Datenweitergabe
Maßnahmen:

- Exporte personenbezogener Daten sind rollenbasiert limitiert und erfordern berechtigten Zugriff.
- Zugriffe durch Auftragsverarbeiter sind vertraglich geregelt und werden regelmäßig überprüft.

5. Auftragskontrolle

Ziel: Sicherstellung der datenschutzkonformen Verarbeitung durch Dienstleister
Maßnahmen:

- Abschluss und Dokumentation von Auftragsverarbeitungsverträgen (AVV) mit allen relevanten Dienstleistern.
- Technische Einbindung nur nach vorheriger Prüfung der Datenschutz- und Sicherheitsstandards.
- Unterauftragnehmerlisten werden intern gepflegt und regelmäßig aktualisiert.

6. Verfügbarkeitskontrolle

Ziel: Schutz personenbezogener Daten vor Verlust oder Zerstörung
Maßnahmen:

- Automatische, verschlüsselte Backups werden täglich erstellt.
- Backup-Wiederherstellung wird regelmäßig getestet.
- Server sind mit unterbrechungsfreier Stromversorgung (USV) abgesichert.
- Rechenzentren verfügen über Notstromversorgung, Klimatisierung und Brandschutzmaßnahmen.
- Monitoring-Systeme zur Früherkennung von Ausfällen (z. B. Uptime-Monitoring) sind im Einsatz.

7. Trennungsgebot

Ziel: Trennung von Daten mit unterschiedlichen Verarbeitungszwecken
Maßnahmen:

- Unterschiedliche Datenarten (z. B. Endkundendaten, Mitarbeiterdaten) sind technisch logisch getrennt.
- Zugriffsrechte sind nach Datenkategorien getrennt zugewiesen.

- Daten werden nur zweckgebunden verarbeitet.

8. Organisatorische Maßnahmen und Datenschutzmanagement
Ziel: Sicherstellung eines umfassenden Datenschutzes auf organisatorischer Ebene
Maßnahmen:

- Mitarbeitende werden zu Datenschutzthemen angemessen geschult (z. B. bei Eintritt oder bei Änderungen).
- Ein externer Datenschutzbeauftragter ist bestellt.
- Verarbeitungsverzeichnisse werden geführt und regelmäßig aktualisiert.
- Datenschutz-Folgenabschätzungen (DSFA) erfolgen bei Funktionen mit hohem Risiko, z. B. Gesichtserkennung.
- Regelmäßige Überprüfung und Aktualisierung der TOMs im Rahmen des internen Kontrollsystems.