Vertrag über die Auftragsverarbeitung (AVV)

Muster · Fassung AVV-2026-09-14 · Stand: 14. September 2026

- **Muster – nicht angenommen**

VERTRAGSSCHLUSS

Fassung	AVV-2026-09-14
Prüfwert Vertragstext (SHA-256)	5aab8224cde4e1a0e4d808a53d24d47f43be227a5fc3dc8694f1504d260ceaf4
Auftragsverarbeiter	iqmeta GmbH, Am Sonnenhang 24, 71111 Waldenbuch
Signaturzertifikat (SHA-256)	d57271d68791b3e4847417de6a233b4ae8fbd02ab5bd0bceecfa30968459902b

Muster – nicht angenommen. Der Vertrag wird elektronisch im Kundenkonto geschlossen; danach erhalten Sie dort ein PDF mit Ihren Angaben. Auch dieses Muster ist digital signiert.

VERTRAGSPARTEIEN

zwischen dem Kunden (Inhaber des Kundenkontos bei zplCloud.com bzw. die Firma, der das Konto zugeordnet ist, mit den im Kundenkonto oder in einer Bestätigung nach § 12 Abs. 1 angegebenen Daten) – nachfolgend „Verantwortlicher“ –

und iqmeta GmbH, Am Sonnenhang 24, 71111 Waldenbuch, Deutschland, vertreten durch den Geschäftsführer Otto Neff, Amtsgericht Stuttgart, HRB 748338 – nachfolgend „Auftragsverarbeiter“ –

§ 1 GEGENSTAND, DAUER UND VERHÄLTNIS ZUM HAUPTVERTRAG

1. Der Auftragsverarbeiter erbringt für den Verantwortlichen Leistungen über die Plattform zplCloud.com (Label-Designer, Rendering, REST-API, Weblink-Dienst, Remote-Drucker, Datenquellen, Stream-Konnektoren, Print Views, Integrationen) auf Grundlage der Allgemeinen Geschäftsbedingungen und des gebuchten Plans (zusammen „Hauptvertrag“). Dabei verarbeitet er personenbezogene Daten, für die der Verantwortliche verantwortlich ist.

2. Gegenstand, Art und Zweck der Verarbeitung, die Arten personenbezogener Daten und die Kategorien betroffener Personen ergeben sich aus Anlage 1.

3. Dieser Vertrag gilt für die Laufzeit des Hauptvertrags. Er endet nicht, solange der Auftragsverarbeiter noch personenbezogene Daten des Verantwortlichen verarbeitet (§ 10).

4. Dieser Vertrag gilt nicht für Verarbeitungen, bei denen der Auftragsverarbeiter selbst Verantwortlicher ist, insbesondere die Verwaltung des Kundenkontos, die Abrechnung, Vertragsnachweise, Sicherheitsprotokolle, die Support-Kommunikation mit dem Kunden und die Website. Für diese gilt die Datenschutzerklärung.

5. Bei Widersprüchen geht dieser Vertrag in Fragen des Datenschutzes dem Hauptvertrag vor.

§ 2 WEISUNGEN

1. Der Auftragsverarbeiter verarbeitet die Daten nur auf dokumentierte Weisung des Verantwortlichen, auch in Bezug auf Übermittlungen in Drittländer, es sei denn, er ist durch das Recht der Union oder eines Mitgliedstaats dazu verpflichtet. In diesem Fall teilt er dem Verantwortlichen diese Anforderungen vor der Verarbeitung mit, sofern das Recht dies nicht wegen eines wichtigen öffentlichen Interesses verbietet (Art. 28 Abs. 3 lit. a DSGVO).

2. Die Weisungen ergeben sich aus diesem Vertrag, dem Hauptvertrag und den Einstellungen, die der Verantwortliche oder seine berechtigten Nutzer in der Plattform vornehmen – zum Beispiel, welche Datenquelle abgefragt, an welchen Drucker gedruckt oder an welches Webhook-Ziel oder welchen Messaging-Dienst gesendet wird. Weitere Weisungen erteilt der Verantwortliche in Textform an support@zplcloud.com.

3. Weisungsberechtigt sind die Nutzer mit der Firmenrolle „Admin“ im Kundenkonto sowie die Person, die diesen Vertrag angenommen hat. Weisungsempfänger beim Auftragsverarbeiter ist dessen Geschäftsführung.

4. Ist der Auftragsverarbeiter der Ansicht, dass eine Weisung gegen Datenschutzvorschriften verstößt, informiert er den Verantwortlichen unverzüglich. Er darf die Ausführung der Weisung aussetzen, bis der Verantwortliche sie bestätigt oder ändert.

§ 3 VERTRAULICHKEIT

Der Auftragsverarbeiter setzt nur Personen ein, die auf Vertraulichkeit verpflichtet sind oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen und die mit den maßgeblichen Datenschutzbestimmungen vertraut gemacht wurden (Art.

28 Abs. 3 lit. b, Art. 29, Art. 32 Abs. 4 DSGVO). Die Verpflichtung gilt über das Ende der Tätigkeit hinaus fort.

§ 4 TECHNISCHE UND ORGANISATORISCHE MAßNAHMEN

1. Der Auftragsverarbeiter trifft die in Anlage 2 beschriebenen Maßnahmen nach Art. 32 DSGVO.

2. Die Maßnahmen unterliegen dem technischen Fortschritt. Der Auftragsverarbeiter darf sie durch gleichwertige oder bessere Maßnahmen ersetzen; das Schutzniveau darf nicht unterschritten werden. Solche Anpassungen sind keine Änderung dieses Vertrags; die jeweils aktuelle Fassung von Anlage 2 wird auf dieser Seite bereitgestellt. Änderungen, die darüber hinausgehen, sind Änderungen dieses Vertrags nach § 12 Abs. 2 und erhalten eine neue Fassung mit neuem Prüfwert.

3. Die Plattform ist nicht für besondere Kategorien personenbezogener Daten (Art. 9 DSGVO) und Daten über strafrechtliche Verurteilungen und Straftaten (Art. 10 DSGVO) ausgelegt, etwa Gesundheitsdaten auf Patienten- oder Apothekenetiketten. Will der Verantwortliche solche Daten verarbeiten, prüft er vorher, ob die Maßnahmen nach Anlage 2 ausreichen; eine solche Verarbeitung bedarf einer gesonderten Vereinbarung in Textform. Die beabsichtigte Verarbeitung teilt er dem Auftragsverarbeiter vorher mit; bis zum Abschluss der gesonderten Vereinbarung darf der Auftragsverarbeiter die Verarbeitung solcher Daten aussetzen. Stellt eine Partei nachträglich fest, dass solche Daten verarbeitet werden, informiert sie die andere unverzüglich.

§ 5 UNTERSTÜTZUNGSPFLICHTEN

1. Betroffenenrechte: Der Auftragsverarbeiter unterstützt den Verantwortlichen mit geeigneten Maßnahmen bei der Beantwortung von Anträgen nach Kapitel III DSGVO (Art. 28 Abs. 3 DSGVO). Er stellt dafür Funktionen zum Einsehen, Ändern und Löschen der Inhalte in der Plattform bereit und auf Anforderung einen Export der Daten. Wendet sich eine betroffene Person direkt an ihn, leitet er die Anfrage unverzüglich an den Verantwortlichen weiter und beantwortet sie nicht selbst, soweit keine Weisung vorliegt.

2. Pflichten nach Art. 32 bis 36 DSGVO: Der Auftragsverarbeiter unterstützt den Verantwortlichen unter Berücksichtigung der ihm vorliegenden Informationen bei der Sicherheit der Verarbeitung, bei Meldungen und Benachrichtigungen im Fall von Datenschutzverletzungen, bei einer Datenschutz-Folgenabschätzung und bei einer vorherigen Konsultation der Aufsichtsbehörde (Art. 28 Abs. 3 lit. e DSGVO).

3. Datenschutzverletzungen und Verdachtsfälle: Der Auftragsverarbeiter meldet dem Verantwortlichen eine Verletzung des Schutzes personenbezogener Daten unverzüglich, spätestens innerhalb von 48 Stunden, nachdem sie ihm bekannt geworden ist; einen begründeten Verdacht meldet er unverzüglich, auch wenn er noch nicht bestätigt ist (Art. 33 Abs. 2 DSGVO). Die Meldung geht an die im Kundenkonto hinterlegte E-Mail-Adresse des Kontoinhabers und an alle Nutzer mit der Firmenrolle „Admin“. Sie enthält, soweit bekannt, die Angaben nach Art. 33 Abs. 3 DSGVO: Art der Verletzung, betroffene Kategorien und ungefähre Zahl der Personen und Datensätze, Ansprechpartner, wahrscheinliche Folgen sowie ergriffene oder vorgeschlagene Maßnahmen. Informationen, die noch nicht vorliegen, reicht er ohne unangemessene weitere Verzögerung nach.

4. Der Auftragsverarbeiter informiert den Verantwortlichen unverzüglich über Kontrollhandlungen und Maßnahmen einer Aufsichtsbehörde, soweit sie diesen Vertrag betreffen.

5. Unterstützungsleistungen, die über die Funktionen der Plattform und die gesetzlichen Pflichten hinausgehen und nicht durch einen Verstoß des Auftragsverarbeiters veranlasst sind, kann der Auftragsverarbeiter nach vorheriger Ankündigung nach Aufwand berechnen.

§ 6 PFLICHTEN DES VERANTWORTLICHEN

1. Der Verantwortliche ist für die Rechtmäßigkeit der Verarbeitung verantwortlich, insbesondere für die Rechtsgrundlage, die Information der betroffenen Personen (Art. 13, 14 DSGVO) und die Auswahl der Daten, die er in die Plattform einbringt oder über Datenquellen, Streams und Integrationen abrufen lässt.

2. Er informiert den Auftragsverarbeiter unverzüglich, wenn er Fehler oder Unregelmäßigkeiten bei der Verarbeitung feststellt.

3. Er ist für die von ihm selbst betriebenen Komponenten verantwortlich, insbesondere Weblink-Container, Agent und CLI, eigene Datenbanken, Message-Broker, Objektspeicher, Drucker und Netzwerke.

4. Er hält die Zugangsdaten seiner Nutzer, API-Keys und Drucker-Zertifikate vertraulich, beschränkt den Zugang zum Kundenkonto auf berechtigte Personen und entfernt ausgeschiedene Nutzer sowie nicht mehr benötigte API-Keys unverzüglich.

§ 7 UNTERAUFTRAGSVERARBEITER

1. Der Verantwortliche erteilt die allgemeine Genehmigung, weitere Auftragsverarbeiter („Unterauftragsverarbeiter“) einzusetzen (Art. 28 Abs. 2 Satz 1 DSGVO). Die bei Vertragsschluss eingesetzten Unterauftragsverarbeiter sind in Anlage 3 aufgeführt und gelten als genehmigt. Die aktuelle Liste ist unter zplcloud.com/de/subprocessors abrufbar.

2. Der Auftragsverarbeiter gibt den Einsatz eines neuen oder den Austausch eines bestehenden Unterauftragsverarbeiters mindestens 30 Tage vor dem Wirksamwerden in der Liste unter zplcloud.com/de/subprocessors bekannt (Art. 28 Abs. 2 Satz 2

DSGVO). Der Verantwortliche behält diese Liste im Blick und kann sich angekündigte Änderungen zusätzlich per E-Mail an die im Kundenkonto hinterlegte Adresse mitteilen lassen.

3. Der Verantwortliche kann der Änderung innerhalb von 14 Tagen nach der Bekanntgabe nach Abs. 2 aus datenschutzrechtlich berechtigten Gründen in Textform widersprechen. Die Parteien suchen dann eine einvernehmliche Lösung. Gelingt dies nicht, kann der Verantwortliche den Hauptvertrag zum Wirksamwerden der Änderung außerordentlich kündigen; bereits bezahlte Entgelte für die Zeit danach werden anteilig erstattet. Weitere Ansprüche wegen der Änderung bestehen nicht.

4. Der Auftragsverarbeiter erlegt jedem Unterauftragsverarbeiter vertraglich dieselben Datenschutzpflichten auf, die in diesem Vertrag festgelegt sind, insbesondere hinreichende Garantien für geeignete technische und organisatorische Maßnahmen (Art. 28 Abs. 4 DSGVO). Kommt ein Unterauftragsverarbeiter seinen Pflichten nicht nach, haftet der Auftragsverarbeiter gegenüber dem Verantwortlichen für dessen Pflichterfüllung.

5. Keine Unterauftragsverarbeiter im Sinne dieses Paragrafen sind: a) Dienste und Empfänger, die der Verantwortliche selbst in der Plattform auswählt und konfiguriert, etwa eigene Webhook-Ziele, Messaging-Dienste (Telegram, Signal, WhatsApp, ntfy, Gotify), Message-Broker und Cloud-Dienste (Kafka, Azure Service Bus, MQTT, AMQP, RabbitMQ, Amazon SQS, Google Pub/Sub, Amazon S3, Azure Blob Storage), Marktplatz- und Versanddienste (Shopify, ShipStation, Veeqo, Amazon) und die Deutsche Post (INTERNETMARKE); die Übermittlung an diese Empfänger erfolgt auf Weisung des Verantwortlichen, das Vertragsverhältnis mit dem Empfänger liegt beim Verantwortlichen; b) Nebenleistungen, die der Auftragsverarbeiter bei Dritten in Anspruch nimmt und die keinen Zugriff auf Daten des Verantwortlichen umfassen, etwa reine Telekommunikations- und Transportleistungen. Die Pflicht zu angemessenen Sicherheitsvorkehrungen bleibt unberührt.

§ 8 ORT DER VERARBEITUNG UND DRITTLANDÜBERMITTLUNG

1. Die Verarbeitung einschließlich der Datensicherungen findet – unbeschadet der Übermittlungen, die der Verantwortliche selbst veranlasst (insbesondere nach § 7 Abs. 5) – ausschließlich in Rechenzentren der Hetzner Online GmbH in Deutschland statt, derzeit im Rechenzentrumspark Falkenstein (Vogtland, Sachsen). Die Rechenzentren sind nach ISO/IEC 27001 zertifiziert. Für den Notfall (Ausfall des Produktionsservers) und für Wiederherstellungstests kann die Verarbeitung vorübergehend in einem Rechenzentrum der netcup GmbH in Deutschland erfolgen (Anlage 3). Ein Wechsel des Standorts innerhalb Deutschlands ist keine Änderung im Sinne von § 7 Abs. 2.

2. Eine Übermittlung in ein Land außerhalb des Europäischen Wirtschaftsraums oder an eine internationale Organisation – auch durch Unterauftragsverarbeiter und auch durch Fernzugriff – erfolgt nur, wenn die Voraussetzungen der Art. 44 ff. DSGVO erfüllt sind, insbesondere auf Grundlage eines Angemessenheitsbeschlusses oder der Standardvertragsklauseln nach Durchführungsbeschluss (EU) 2021/914, jeweils mit einer dokumentierten Bewertung des Übermittlungsrisikos. Anlage 3 nennt für jeden Unterauftragsverarbeiter den Verarbeitungsort und die Garantie.

§ 9 NACHWEISE UND KONTROLLEN

1. Der Auftragsverarbeiter stellt dem Verantwortlichen die erforderlichen Informationen zum Nachweis der Einhaltung der Pflichten aus Art. 28 DSGVO zur Verfügung (Art. 28 Abs. 3 lit. g). Der Nachweis wird vorrangig durch Unterlagen erbracht, insbesondere die aktuelle Fassung von Anlage 2, die Zertifikate der eingesetzten Rechenzentren (ISO/IEC 27001), Selbstauskünfte und Auszüge aus dem Änderungsprotokoll über Zugriffe des Supports auf die Daten des Verantwortlichen.

2. Reichen diese Nachweise im Einzelfall nachweislich nicht aus, kann der Verantwortliche eine Kontrolle selbst oder durch einen zur Verschwiegenheit verpflichteten Prüfer durchführen, der nicht im Wettbewerb mit dem Auftragsverarbeiter steht. Die Kontrolle ist mindestens 30 Tage vorher in Textform anzukündigen, findet während der üblichen Geschäftszeiten statt und wird vorrangig als Dokumenten- oder Fernprüfung durchgeführt. Sie darf den Betrieb sowie die Sicherheit und Vertraulichkeit der Daten anderer Kunden nicht gefährden und ist höchstens einmal im Kalenderjahr zulässig, es sei denn, es liegt ein konkreter Anlass vor, etwa eine Datenschutzverletzung, oder eine Aufsichtsbehörde verlangt sie.

3. Die Rechenzentren werden von Unterauftragsverarbeitern betrieben; ein Zutritt für den Verantwortlichen oder seine Prüfer ist dort nicht möglich. Insoweit wird der Nachweis durch die Zertifizierungen und Prüfberichte der Unterauftragsverarbeiter erbracht.

4. Die Kosten einer Kontrolle nach Abs. 2 einschließlich des Aufwands des Auftragsverarbeiters trägt der Verantwortliche, es sei denn, die Kontrolle ergibt einen wesentlichen Verstoß des Auftragsverarbeiters gegen diesen Vertrag. Den voraussichtlichen Aufwand teilt der Auftragsverarbeiter vorher mit.

5. Die Befugnisse der Aufsichtsbehörden bleiben unberührt.

§ 10 LÖSCHUNG UND RÜCKGABE NACH VERTRAGSENDE

1. Nach Ende des Hauptvertrags stellt der Auftragsverarbeiter dem Verantwortlichen auf Anforderung innerhalb von 30 Tagen einen Export seiner Daten in einem maschinenlesbaren Format (JSON) bereit (Abschnitt 5.5 der AGB).

2. Der Verantwortliche wählt zwischen der Rückgabe und der Löschung der Daten (Art. 28 Abs. 3 lit. f DSGVO); die Rückgabe erfolgt durch den Export nach Abs. 1. Wählt er die Rückgabe, löscht der Auftragsverarbeiter alle personenbezogenen Daten

des Verantwortlichen, sobald der Export bereitgestellt ist; wählt er die Löschung, löscht er sie innerhalb von 30 Tagen nach Ende des Hauptvertrags oder unverzüglich nach einem späteren Verlangen des Verantwortlichen, soweit nicht nach Unionsrecht oder dem Recht eines Mitgliedstaats eine Pflicht zur Speicherung besteht. Daten in Datensicherungen werden im Rahmen der regulären Rotation spätestens nach 30 Tagen überschrieben; bis dahin werden sie nicht mehr aktiv verarbeitet und nur für eine Wiederherstellung des Gesamtsystems verwendet.

3. Unterlagen, die dem Nachweis der ordnungsgemäßen Verarbeitung dienen, insbesondere das Änderungsprotokoll, darf der Auftragsverarbeiter entsprechend den gesetzlichen Aufbewahrungs- und Verjährungsfristen über das Vertragsende hinaus aufbewahren.

4. Auf Verlangen bestätigt der Auftragsverarbeiter die Löschung in Textform.

§ 11 HAFTUNG

1. Gegenüber betroffenen Personen haften die Parteien nach Art. 82 DSGVO; sind an derselben Verarbeitung mehrere Verantwortliche oder Auftragsverarbeiter beteiligt, so ist jede Partei für den gesamten Schaden verantwortlich (Art. 82 Abs. 4 DSGVO).

2. Im Verhältnis der Parteien zueinander trägt jede Partei den Schaden, der auf ihren Verantwortungsbereich zurückgeht; hat eine Partei nach Art. 82 Abs. 4 DSGVO den gesamten Schaden ersetzt, kann sie von der anderen Partei den Anteil zurückverlangen, der deren Verantwortung entspricht (Art. 82 Abs. 5 DSGVO). Wird der Auftragsverarbeiter von einer betroffenen Person, einem Dritten oder einer Aufsichtsbehörde wegen einer Verarbeitung in Anspruch genommen, die auf einer Weisung des Verantwortlichen, auf von ihm eingebrachten oder ausgewählten Daten oder auf einer Verletzung seiner Pflichten aus § 6 beruht, stellt der Verantwortliche den Auftragsverarbeiter von diesen Ansprüchen einschließlich der angemessenen Kosten der Rechtsverteidigung frei.

3. Im Übrigen gelten für die Haftung der Parteien untereinander die Regelungen des Hauptvertrags (Abschnitt 13 der AGB) einschließlich ihrer Haftungsbeschränkungen, soweit gesetzlich zulässig. Unberührt bleibt die Haftung für Vorsatz und grobe Fahrlässigkeit, für Schäden aus der Verletzung des Lebens, des Körpers oder der Gesundheit sowie nach zwingenden gesetzlichen Vorschriften.

4. Geldbußen, die gegen eine Partei wegen einer Pflichtverletzung der anderen Partei verhängt werden, sowie die erforderlichen Kosten der Rechtsverteidigung trägt die andere Partei. Die Haftungsbeschränkungen nach Abs. 3 gelten entsprechend.

§ 12 SCHLUSSBESTIMMUNGEN

1. Dieser Vertrag ist Bestandteil der Allgemeinen Geschäftsbedingungen (Abschnitt 11.2) und kommt mit deren Annahme bei der Registrierung oder bei der Buchung eines Plans elektronisch zustande (Art. 28 Abs. 3 DSGVO). Die Anlagen 1 bis 3 sind Bestandteil dieses Vertrags. Der Auftragsverarbeiter speichert die Zustimmung mit Zeitpunkt, Nutzerkonto sowie AGB- und Vertragsfassung. Zusätzlich kann der Verantwortliche den Vertrag im Kundenkonto unter Angabe der Firma, der Anschrift und der handelnden Person bestätigen; der Auftragsverarbeiter speichert diese Bestätigung mit Fassung, Zeitpunkt, Nutzerkonto und einem Prüfwert des Vertragstextes und stellt den Vertrag als digital signiertes PDF bereit.

2. Der Auftragsverarbeiter kann diesen Vertrag mit Wirkung für die Zukunft ändern, soweit dies wegen geänderter Rechtslage, Rechtsprechung oder Anforderungen der Aufsichtsbehörden, neuer Funktionen der Plattform oder geänderter Unterauftragsverarbeiter erforderlich, für den Verantwortlichen zumutbar ist und das Schutzniveau für die Daten des Verantwortlichen nicht sinkt. Die geänderte Fassung teilt er mindestens sechs Wochen vor ihrem Wirksamwerden per E-Mail an die im Kundenkonto hinterlegte Adresse des Kontoinhabers und an alle Nutzer mit der Firmenrolle „Admin“ mit; die Mitteilung gilt mit der Absendung an diese Adresse als zugegangen. Widerspricht der Verantwortliche nicht bis zum Wirksamwerden, gilt die geänderte Fassung als angenommen; auf diese Folge, das Widerspruchsrecht und die Frist weist der Auftragsverarbeiter in der Mitteilung besonders hin. Widerspricht der Verantwortliche, gilt die Änderung ihm gegenüber nicht; die bisherige Fassung gilt fort. Jede Partei kann den Hauptvertrag zum Wirksamwerden der Änderung kündigen. Der Auftragsverarbeiter dokumentiert die Mitteilung und den Zeitpunkt des Wirksamwerdens der geänderten Fassung. Anpassungen der Maßnahmen nach Anlage 2 richten sich nach § 4 Abs. 2, Änderungen der Unterauftragsverarbeiter nach § 7.

3. Es gilt das Recht der Bundesrepublik Deutschland. Der Gerichtsstand richtet sich nach dem Hauptvertrag.

4. Sollte eine Bestimmung unwirksam sein, bleibt der Vertrag im Übrigen wirksam. Die unwirksame Bestimmung wird durch eine Regelung ersetzt, die den Anforderungen des Art. 28 DSGVO entspricht und dem wirtschaftlichen Zweck der unwirksamen Bestimmung am nächsten kommt.

5. Maßgeblich ist die deutsche Fassung. Die englische Fassung dient der Information.

ANLAGE 1: GEGENSTAND, ART UND ZWECK DER VERARBEITUNG, DATENARTEN, BETROFFENE

Der Verantwortliche bestimmt durch seine Nutzung, welche der aufgeführten Daten tatsächlich anfallen.

1. Gegenstand und Zweck

Bereitstellung der SaaS-Plattform zplCloud.com zur Gestaltung, Erzeugung, Umwandlung, Speicherung und Ausgabe von Etiketten (insbesondere ZPL), einschließlich:

Leistung	Verarbeitung personenbezogener Daten
Label-Designer, Vorlagen, Versionierung, Freigabe	Speichern von Designs mit Testdaten und Feldinhalten; Protokoll von Ersteller, Prüfer und Kommentar
Rendering und Konvertierung (Web, REST-API, Batch)	Erzeugen von ZPL, PDF und PNG aus Daten des Verantwortlichen; Batch-Ergebnisse bis zu einer Stunde im Arbeitsspeicher
Druck über Weblink, Remote-Drucker (Agent) und virtuelle Drucker	Übermitteln und Protokollieren von Druckaufträgen einschließlich Etiketteninhalt und Druckerantwort
Datenquellen und Stream-Konnektoren	Abrufen von Datensätzen aus Datenbanken und Message-Brokern des Verantwortlichen, Umwandeln in Etiketten, Speichern fehlgeschlagener Nachrichten zur Fehlerbehebung, Ausgabe an Objektspeicher, Broker oder Webhooks des Verantwortlichen
Integrationen (Deutsche Post INTERNETMARKE, Shopify, ShipStation, Veeqo, Amazon)	Abrufen von Bestellungen, Übermitteln von Adressdaten für Versandmarken, Transaktionsprotokoll mit Marke (PDF/ZPL)
Print Views	Bereitstellen von Druckformularen für vom Verantwortlichen freigegebene Personen
Benachrichtigungen, Webhooks, Etiketten per E-Mail	Versand vom Verantwortlichen festgelegter Inhalte an von ihm bestimmte Empfänger
Team, Kunden-Arbeitsbereiche, Änderungsprotokoll mit elektronischer Unterschrift	Verwaltung der Nutzer des Verantwortlichen, Nachvollziehbarkeit von Änderungen
Support im Einzelfall	Einsicht in Daten des Verantwortlichen nur, soweit zur Fehlerbehebung erforderlich; jeder Zugriff wird im Änderungsprotokoll des Verantwortlichen festgehalten (Anlage 2 Nr. 3)

2. Art der Verarbeitung

Erheben, Erfassen, Speichern, Anpassen, Auslesen, Abfragen, Verwenden, Übermitteln an vom Verantwortlichen bestimmte Empfänger, Abgleichen, Einschränken und Löschen (Art. 4 Nr. 2 DSGVO).

3. Arten personenbezogener Daten

Kategorie	Beispiele
Kontakt- und Adressdaten	Name, Firma, Anschrift, Telefon und E-Mail von Empfängern und Absendern
Sendungs- und Bestelldaten	Bestellnummer, Positionen, Sendungsnummer, Gewicht, Produkt, Portobetrag
Kennzeichnungsdaten	Barcode- und RFID-Inhalte (z. B. SSCC, SGTIN/EPC, GS1-Datenbezeichner), sofern mit Personen verknüpfbar
Datensätze aus Systemen des Verantwortlichen	beliebige Spalten aus Datenbanken und Nachrichten, z. B. Mitarbeiter-, Kunden- oder Artikeldaten
Nutzer- und Protokolldaten der Nutzer des Verantwortlichen	E-Mail-Adresse, Name, Rolle, Zeitpunkte, IP-Adresse, Browserkennung, Aktionen, Gründe elektronischer Unterschriften
Kommunikationsinhalte	Texte von Benachrichtigungen, Webhook-Inhalte, Print-View-Formulare
Geräte- und Netzwerkdaten	IP-Adresse, Hostname, MAC-Adresse und Seriennummer von Druckern; Hostname und lokale IP-Adressen der Agent-Rechner
Freie Inhalte	Grafiken, Logos, Schriften und Freitexte in Etiketten

Keine besonderen Kategorien personenbezogener Daten (Art. 9 DSGVO) und keine Daten über strafrechtliche Verurteilungen und Straftaten (Art. 10 DSGVO), sofern nicht gesondert vereinbart (§ 4 Abs. 3).

4. Kategorien betroffener Personen

• Beschäftigte und sonstige Nutzer des Verantwortlichen (Team-Mitglieder, API-Nutzer, Print-View-Nutzer)

• Kunden, Empfänger und Absender von Sendungen des Verantwortlichen

• Kunden des Verantwortlichen in Kunden-Arbeitsbereichen (etwa bei Agenturen und Dienstleistern)

• Personen, deren Daten in angebundenen Datenquellen und Nachrichtenströmen des Verantwortlichen enthalten sind

• Empfänger von Benachrichtigungen und Etiketten-E-Mails

5. Dauer

Laufzeit des Hauptvertrags; Speicherfristen nach Anlage 2 Nr. 8; Löschung nach § 10.

ANLAGE 2: TECHNISCHE UND ORGANISATORISCHE MAßNAHMEN (ART. 32 DSGVO)

Die Maßnahmen gelten für die Plattform zplCloud.com einschließlich des Weblink-Dienstes. Für Komponenten, die der Verantwortliche selbst betreibt (§ 6 Abs. 3), ist er selbst verantwortlich.

1. Zutrittskontrolle

• Server und Datensicherungen stehen im Rechenzentrumspark Falkenstein der Hetzner Online GmbH in Deutschland, zertifiziert nach ISO/IEC 27001, mit Zutrittskontrolle, Videoüberwachung und Sicherheitspersonal des Rechenzentrumsbetreibers.

• Der Auftragsverarbeiter hat keinen physischen Zugang zu den Servern, nur einen administrativen Fernzugang.

2. Zugangskontrolle

• Anmeldung nur mit bestätigter E-Mail-Adresse (Double-Opt-in); Passwörter mit mindestens 12 Zeichen, gespeichert ausschließlich als kryptografischer Hash.

• Sperrung des Kontos nach wiederholten Fehlversuchen.

• Zwei-Faktor-Authentifizierung (Authenticator-App, E-Mail-Code, Wiederherstellungscodes) für alle Nutzer verfügbar.

• Anzeige und Beendigung aktiver Sitzungen, serverseitige Prüfung jeder Sitzung.

• Anmelde-Cookie nicht per Skript lesbar (HttpOnly) und mit SameSite-Schutz.

• Begrenzung der Anfragen je Konto bzw. IP-Adresse für API und Online-Werkzeuge (Rate-Limiting).

• Zugangsdaten der Systeme liegen außerhalb des Quellcodes in zugriffsgeschützten Dateien auf den Servern.

• Administrativer Zugang zu den Servern ausschließlich durch die Geschäftsführung.

3. Zugriffskontrolle

• Jeder Datensatz ist einem Konto bzw. einer Firma zugeordnet; Abfragen filtern auf den eigenen Mandanten.

• Firmenrollen „Admin“ und „Mitglied“: Teamverwaltung, Freigabe von Designs, Einsicht in IP-Adressen des Änderungsprotokolls und Löschen fremder API-Keys sind Admins vorbehalten.

• API-Keys je Nutzer bzw. Firma, gespeichert nur als SHA-256-Hash und nur beim Anlegen einmal angezeigt; getrennte Sandbox-Keys ohne Zugriff auf reale Drucker.

• Beim Löschen eines API-Keys werden verbundene Agenten sofort getrennt und die daran gebundenen Drucker-Zertifikate widerrufen.

• Administrativer Zugriff des Auftragsverarbeiters auf Kundendaten über genau ein Supervisor-Konto; jede Identitätsübernahme und jeder Supervisor-Zugriff wird im Änderungsprotokoll der betroffenen Firma festgehalten und ist für deren Admins sichtbar.

4. Trennungskontrolle

• Logische Trennung der Mandanten in einer gemeinsamen Datenbank (siehe Nr. 3).

• Getrennte Datenbanken, Container und Datenverzeichnisse für Produktion und Test.

5. Verschlüsselung und Pseudonymisierung

• TLS 1.2 oder 1.3 für alle öffentlichen Verbindungen, Zertifikate über ACME, HTTP Strict Transport Security.

• Drucker verbinden sich per gegenseitiger TLS-Authentifizierung (mTLS) mit einer eigenen Zertifizierungsstelle; widerrufene oder gelöschte Zertifikate werden beim Verbindungsaufbau abgewiesen, bestehende Verbindungen innerhalb von 30 Sekunden getrennt.

• Der private Schlüssel der Zertifizierungsstelle liegt nur im Datenverzeichnis des Servers und in den verschlüsselten Sicherungen, nicht im Quellcode.

• Zugangsdaten zu Datenquellen, Streams, Objektspeichern und Push-Kanälen werden mit AES-256-GCM verschlüsselt gespeichert; der Schlüssel liegt außerhalb des Quellcodes.

• Datensicherungen werden verschlüsselt gespeichert.

6. Integrität, Weitergabe- und Eingabekontrolle

• Webhooks werden mit HMAC signiert; eine Zustellung an private Netzadressen ist ausgeschlossen.

• Änderungsprotokoll mit SHA-256-Hash-Kette; die Tabelle ist nur um Einträge ergänzbar, jede nachträgliche Änderung ist prüfbar; elektronische Unterschrift mit erneuter Passworteingabe und Grund.

• Versionierung von Designs mit Prüfer und Freigabe.

• Schutz von Formularen vor Cross-Site-Request-Forgery; Sicherheits-Header (X-Content-Type-Options, Referrer-Policy, Permissions-Policy).

7. Verfügbarkeit und Belastbarkeit

• Deployment ohne Unterbrechung (Blue-Green) mit Gesundheitsprüfung und automatischem Rückfall auf die vorherige Version.

• Überwachung mit Metriken und Traces; Rotation der Protokolldateien.

• Datensicherung aller Server als verschlüsseltes Image alle sechs Stunden auf einen getrennten Speicher in Deutschland; Aufbewahrung höchstens 30 Tage.

• Wiederherstellung wird monatlich getestet und protokolliert.

• Notfallbetrieb: Wiederherstellung der Images bei einem zweiten Anbieter (netcup GmbH, Deutschland).

• Redundante Strom-, Klima- und Netzversorgung durch das zertifizierte Rechenzentrum.

• Verfügbarkeitsziel 99 % im Monatsmittel (Abschnitt 9.1 der AGB).

8. Speicherbegrenzung und Löschung

• Automatische Löschung von Druckaufträgen, Sandbox-Drucken, fehlgeschlagenen Stream-Nachrichten, Webhook-Zustellungen, Nutzungsstatistiken und Integrations-Transaktionen nach 7, 30 oder 90 Tagen je nach Plan.

• Löschung des Kontos durch den Nutzer selbst.

• Export auf Anforderung und Löschung aller Daten des Verantwortlichen nach Vertragsende mit Löschprotokoll (§ 10); Daten in Sicherungen werden nach spätestens 30 Tagen überschrieben.

9. Organisation und Überprüfung

• Zugriff auf Daten des Verantwortlichen ausschließlich durch die Geschäftsführung des Auftragsverarbeiters.

• Ansprechpartner für den Datenschutz ist die Geschäftsführung; ein Datenschutzbeauftragter ist nicht zu benennen (§ 38 BDSG).

• Verzeichnis von Verarbeitungstätigkeiten als Verantwortlicher und als Auftragsverarbeiter (Art. 30 DSGVO).

• Dokumentierter Prozess für Datenschutzverletzungen mit Meldung an den Verantwortlichen spätestens binnen 48 Stunden (§ 5 Abs. 3).

• Sorgfältige Auswahl der Unterauftragsverarbeiter und Abschluss von Verträgen nach Art. 28 DSGVO (Anlage 3).

• Überprüfung und Aktualisierung dieser Maßnahmen mindestens einmal jährlich.

ANLAGE 3: UNTERAUFTRAGSVERARBEITER

Aufgeführt sind die Dienstleister, die Daten des Verantwortlichen im Auftrag des Auftragsverarbeiters verarbeiten. Die jeweils aktuelle Liste und angekündigte Änderungen stehen unter zplcloud.com/de/subprocessors.

Hetzner Online GmbH

Unterauftragsverarbeiter	Hetzner Online GmbH, Industriestr. 25, 91710 Gunzenhausen
Leistung	Rechenzentrum, dedizierter Server und getrennter Speicher für die Datensicherungen
Daten	alle Daten der Plattform einschließlich der Datensicherungen
Standort	Deutschland, Rechenzentrumspark Falkenstein (Vogtland, Sachsen)
Garantie	EU; Vertrag nach Art. 28 DSGVO; ISO/IEC 27001

netcup GmbH

Unterauftragsverarbeiter	netcup GmbH, Daimlerstraße 25, 76185 Karlsruhe
Leistung	Ausweich-Rechenzentrum: Wiederherstellung der Datensicherungen bei Ausfall des Produktionsservers und für Wiederherstellungstests
Daten	im Notfall und bei Wiederherstellungstests alle Daten der Plattform

Standort	Deutschland, Rechenzentrum Nürnberg
Garantie	EU; Vertrag nach Art. 28 DSGVO; ISO/IEC 27001 und ISO/IEC 27701