Data Processing Agreement (DPA)

Sample · Version AVV-2026-09-14 · Last updated: 14 September 2026

- **Sample – not accepted**

CONCLUSION OF THE AGREEMENT

Version	AVV-2026-09-14
Agreement text checksum (SHA-256)	f0f60e6017ef7125594c6c2a66fc1a811710c03bc8ef8700073de4adbaaf7ae1
Processor	iqmeta GmbH, Am Sonnenhang 24, 71111 Waldenbuch
Signing certificate (SHA-256)	d57271d68791b3e4847417de6a233b4ae8fbd02ab5bd0bceecfa30968459902b

Sample – not accepted. The agreement is concluded electronically in the customer account; you then receive a PDF with your details there. This sample is digitally signed as well.

PARTIES

between the customer (the holder of the customer account at zplCloud.com or the company to which the account is assigned, with the details stated in the customer account or in a confirmation under Section 12 (1)) – hereinafter the “controller” –

and iqmeta GmbH, Am Sonnenhang 24, 71111 Waldenbuch, Germany, represented by Managing Director Otto Neff, Local Court (Amtsgericht) Stuttgart, HRB 748338 – hereinafter the “processor” –

SECTION 1 SUBJECT MATTER, DURATION AND RELATIONSHIP TO THE MAIN AGREEMENT

1. The processor provides services to the controller via the zplCloud.com platform (label designer, rendering, REST API, Weblink service, remote printers, data sources, stream connectors, Print Views, integrations) on the basis of the Terms of Service and the booked plan (together the “Main Agreement”). In doing so, it processes personal data for which the controller is responsible.

2. The subject matter, nature and purpose of the processing, the types of personal data and the categories of data subjects are set out in Annex 1.

3. This Agreement applies for the term of the Main Agreement. It does not end as long as the processor still processes personal data of the controller (Section 10).

4. This Agreement does not apply to processing for which the processor is itself the controller, in particular the administration of the customer account, billing, contract records, security logs, support communication with the customer and the website. Such processing is governed by the Privacy Policy.

5. In the event of conflicts, this Agreement takes precedence over the Main Agreement in matters of data protection.

SECTION 2 INSTRUCTIONS

1. The processor processes the data only on documented instructions from the controller, including with regard to transfers to third countries, unless it is required to do so by Union or Member State law. In that case, it informs the controller of these requirements before processing, unless that law prohibits such information on important grounds of public interest (Art. 28 (3) (a) GDPR).

2. The instructions result from this Agreement, the Main Agreement and the settings that the controller or its authorised users make in the platform – for example, which data source is queried, which printer is printed to, or which webhook target or messaging service data is sent to. The controller issues further instructions in text form (e.g. email) to support@zplcloud.com.

3. Persons authorised to issue instructions are the users with the company role “Admin” in the customer account and the person who accepted this Agreement. The recipient of instructions at the processor is its management.

4. If the processor is of the opinion that an instruction infringes data protection provisions, it informs the controller without undue delay. It may suspend the execution of the instruction until the controller confirms or amends it.

SECTION 3 CONFIDENTIALITY

The processor only engages persons who are bound to confidentiality or are under an appropriate statutory obligation of confidentiality and who have been made familiar with the relevant data protection provisions (Art. 28 (3) (b), Art. 29, Art. 32 (4) GDPR). This obligation continues to apply after the end of their activity.

SECTION 4 TECHNICAL AND ORGANISATIONAL MEASURES

1. The processor implements the measures described in Annex 2 in accordance with Art. 32 GDPR.

2. The measures are subject to technical progress. The processor may replace them with equivalent or better measures; the level of protection must not fall below the level provided. Such adjustments are not a change to this Agreement; the current version of Annex 2 is made available on this page. Changes going beyond this are changes to this Agreement under Section 12 (2) and receive a new version with a new checksum.

3. The platform is not designed for special categories of personal data (Art. 9 GDPR) or personal data relating to criminal convictions and offences (Art. 10 GDPR), such as health data on patient or pharmacy labels. If the controller wishes to process such data, it checks in advance whether the measures under Annex 2 are sufficient; such processing requires a separate agreement in text form (e.g. email). The controller informs the processor of the intended processing in advance; until the separate agreement is concluded, the processor may suspend the processing of such data. If either party subsequently establishes that such data is being processed, it informs the other party without undue delay.

SECTION 5 OBLIGATIONS TO ASSIST

1. Data subject rights: The processor assists the controller by appropriate measures in responding to requests under Chapter III GDPR (Art. 28 (3) GDPR). For this purpose, it provides functions for viewing, changing and deleting the content in the platform and, on request, an export of the data. If a data subject contacts the processor directly, the processor forwards the request to the controller without undue delay and does not respond to it itself in the absence of an instruction.

2. Obligations under Art. 32 to 36 GDPR: Taking into account the information available to it, the processor assists the controller with the security of processing, with notifications and communications in the event of personal data breaches, with a data protection impact assessment and with a prior consultation of the supervisory authority (Art. 28 (3) (e) GDPR).

3. Personal data breaches and suspected cases: The processor notifies the controller of a personal data breach without undue delay and at the latest within 48 hours after becoming aware of it, and notifies a reasonable suspicion without undue delay, even if it has not yet been confirmed (Art. 33 (2) GDPR). The notification is sent to the email address of the account holder stored in the customer account and to all users with the company role “Admin”. To the extent known, it contains the information required under Art. 33 (3) GDPR: the nature of the breach, the categories concerned and the approximate number of persons and records, a contact point, the likely consequences and the measures taken or proposed. The processor provides information that is not yet available subsequently, without undue further delay.

4. The processor informs the controller without undue delay of inspections and measures by a supervisory authority insofar as they relate to this Agreement.

5. Assistance services that go beyond the functions of the platform and the statutory obligations and are not caused by a breach on the part of the processor may be charged by the processor on a time and expense basis after prior notice.

SECTION 6 OBLIGATIONS OF THE CONTROLLER

1. The controller is responsible for the lawfulness of the processing, in particular for the legal basis, for informing the data subjects (Art. 13, 14 GDPR) and for the selection of the data that it brings into the platform or has retrieved via data sources, streams and integrations.

2. It informs the processor without undue delay if it detects errors or irregularities in the processing.

3. It is responsible for the components it operates itself, in particular Weblink containers, the agent and the CLI, its own databases, message brokers, object storage, printers and networks.

4. It keeps its users' credentials, API keys and printer certificates confidential, restricts access to the customer account to authorised persons and removes users who have left as well as API keys that are no longer required without undue delay.

SECTION 7 SUB-PROCESSORS

1. The controller grants general authorisation to engage other processors (“sub-processors”) (Art. 28 (2) sentence 1 GDPR). The sub-processors engaged at the time this Agreement is concluded are listed in Annex 3 and are deemed authorised. The current list is available at zplcloud.com/en/subprocessors.

2. The processor announces the engagement of a new sub-processor or the replacement of an existing one at least 30 days before it takes effect in the list at zplcloud.com/en/subprocessors (Art. 28 (2) sentence 2 GDPR). The controller keeps that list under review and may additionally have announced changes notified to it by email to the address stored in the customer account.

3. The controller may object to the change in text form (e.g. email) within 14 days of the announcement under paragraph 2 on justified grounds under data protection law. The parties then seek an amicable solution. If this is not achieved, the controller may terminate the Main Agreement extraordinarily with effect from the date on which the change takes effect; fees already paid for the period thereafter are refunded pro rata. No further claims exist on account of the change.

4. The processor contractually imposes on each sub-processor the same data protection obligations as are set out in this Agreement, in particular sufficient guarantees for appropriate technical and organisational measures (Art. 28 (4) GDPR). Where a sub-processor fails to fulfil its obligations, the processor is liable to the controller for the performance of that sub-processor's obligations.

5. The following are not sub-processors within the meaning of this Section: a) services and recipients that the controller itself selects and configures in the platform, such as its own webhook targets, messaging services (Telegram, Signal, WhatsApp, ntfy, Gotify), message brokers and cloud services (Kafka, Azure Service Bus, MQTT, AMQP, RabbitMQ, Amazon SQS, Google Pub/Sub, Amazon S3, Azure Blob Storage), marketplace and shipping services (Shopify, ShipStation, Veeqo, Amazon) and Deutsche Post (INTERNETMARKE); the transmission to these recipients takes place on the instructions of the controller, and the contractual relationship with the recipient lies with the controller; b) ancillary services that the processor obtains from third parties and that do not involve access to the controller's data, such as pure telecommunications and transport services. The obligation to take appropriate security precautions remains unaffected.

SECTION 8 PLACE OF PROCESSING AND TRANSFERS TO THIRD COUNTRIES

1. Processing, including backups, takes place – without prejudice to transfers initiated by the controller itself (in particular under Section 7 (5)) – exclusively in data centres of Hetzner Online GmbH in Germany, currently in the Falkenstein data centre park (Vogtland, Saxony). The data centres are certified to ISO/IEC 27001. In an emergency (failure of the production server) and for recovery tests, processing may take place temporarily in a data centre of netcup GmbH in Germany (Annex 3). A change of location within Germany does not constitute a change within the meaning of Section 7 (2).

2. A transfer to a country outside the European Economic Area or to an international organisation – including by sub-processors and including by remote access – takes place only if the conditions of Art. 44 et seq. GDPR are met, in particular on the basis of an adequacy decision or of the standard contractual clauses pursuant to Implementing Decision (EU) 2021/914, in each case with a documented assessment of the transfer risk. Annex 3 states the place of processing and the safeguard for each sub-processor.

SECTION 9 EVIDENCE AND AUDITS

1. The processor makes available to the controller the information necessary to demonstrate compliance with the obligations under Art. 28 GDPR (Art. 28 (3) (g)). Evidence is provided primarily by means of documents, in particular the current version of Annex 2, the certificates of the data centres used (ISO/IEC 27001), self-declarations and extracts from the audit trail on access by support to the controller's data.

2. If, in an individual case, this evidence is demonstrably insufficient, the controller may carry out an audit itself or have it carried out by an auditor who is bound to confidentiality and is not a competitor of the processor. The audit must be announced in text form (e.g. email) at least 30 days in advance, takes place during normal business hours and is carried out primarily as a document review or remote audit. It must not endanger operations or the security and confidentiality of other customers' data and is permitted no more than once per calendar year, unless there is a specific cause, such as a personal data breach, or a supervisory authority requires it.

3. The data centres are operated by sub-processors; physical access for the controller or its auditors is not possible there. In this respect, evidence is provided by the certifications and audit reports of the sub-processors.

4. The costs of an audit under paragraph 2, including the processor's own time and expense, are borne by the controller, unless the audit reveals a material breach of this Agreement by the processor. The processor informs the controller of the expected time and expense in advance.

5. The powers of the supervisory authorities remain unaffected.

SECTION 10 DELETION AND RETURN AFTER THE END OF THE CONTRACT

1. After the end of the Main Agreement, the processor provides the controller, on request, within 30 days with an export of its data in a machine-readable format (JSON) (Section 5.5 of the Terms).

2. The controller chooses between the return and the deletion of the data (Art. 28 (3) (f) GDPR); the return is made by the export under paragraph 1. If it chooses the return, the processor deletes all personal data of the controller once the export has been made available; if it chooses deletion, it deletes the data within 30 days after the end of the Main Agreement or without undue delay after a later request by the controller, unless Union or Member State law requires storage. Data in backups is overwritten as part of the regular rotation after 30 days at the latest; until then, it is no longer actively processed and is used only to restore the system as a whole.

3. The processor may retain documents that serve as evidence of proper processing, in particular the audit trail, beyond the end of the contract in accordance with the statutory retention and limitation periods.

4. On request, the processor confirms the deletion in text form (e.g. email).

SECTION 11 LIABILITY

1. Towards data subjects, the parties are liable in accordance with Art. 82 GDPR; where several controllers or processors are involved in the same processing, each party is liable for the entire damage (Art. 82 (4) GDPR).

2. As between the parties, each party bears the damage attributable to its sphere of responsibility; where a party has compensated the entire damage under Art. 82 (4) GDPR, it may claim from the other party the share corresponding to that party's responsibility (Art. 82 (5) GDPR). If a data subject, a third party or a supervisory authority asserts claims against the processor on account of processing that is based on an instruction of the controller, on data brought in or selected by the controller, or on a breach of the controller's obligations under Section 6, the controller indemnifies the processor against these claims, including the reasonable costs of legal defence.

3. In all other respects, the liability of the parties towards each other is governed by the provisions of the Main Agreement (Section 13 of the Terms), including its limitations of liability, to the extent permitted by law. Liability for intent and gross negligence, for damage resulting from injury to life, body or health, and under mandatory statutory provisions remains unaffected.

4. Fines imposed on one party as a result of a breach of duty by the other party, together with the necessary costs of legal defence, are borne by that other party. The limitations of liability under paragraph 3 apply accordingly.

SECTION 12 FINAL PROVISIONS

1. This Agreement forms part of the Terms of Service (section 11.2) and is concluded electronically when they are accepted on registration or when a plan is booked (Art. 28 (3) GDPR). Annexes 1 to 3 form part of this Agreement. The processor stores the consent together with the time, the user account and the versions of the Terms of Service and of this Agreement. In addition, the controller may confirm the Agreement in the customer account, stating the company name, the address and the person acting; the processor stores this confirmation together with the version, the time, the user account and a checksum of the agreement text, and provides the Agreement as a digitally signed PDF.

2. The processor may amend this Agreement with effect for the future where this is necessary due to changes in the legal situation, case law or requirements of the supervisory authorities, new functions of the platform or changes in sub-processors, is reasonable for the controller and the level of protection for the controller's data does not decrease. The processor communicates the amended version by email to the email address of the account holder stored in the customer account and to all users with the company role “Admin” at least six weeks before it takes effect; the notice is deemed received when it is sent to that address. If the controller does not object by the time it takes effect, the amended version is deemed accepted; the processor specifically draws attention in the notice to this consequence, the right to object and the deadline. If the controller objects, the amendment does not apply to it and the previous version continues to apply. Either party may terminate the Main Agreement with effect from the date on which the amendment takes effect. The processor documents the notice and the date on which the amended version takes effect. Adjustments of the measures under Annex 2 are governed by Section 4 (2), changes in sub-processors by Section 7.

3. The law of the Federal Republic of Germany applies. The place of jurisdiction is determined by the Main Agreement.

4. Should any provision be invalid, the remainder of this Agreement remains valid. The invalid provision is replaced by a provision that meets the requirements of Art. 28 GDPR and comes closest to the economic purpose of the invalid provision.

5. The German version is authoritative. The English version is provided for information.

ANNEX 1: SUBJECT MATTER, NATURE AND PURPOSE OF THE PROCESSING, TYPES OF DATA, DATA SUBJECTS

Through its use, the controller determines which of the data listed actually arise.

1. Subject matter and purpose

Provision of the SaaS platform zplCloud.com for designing, generating, converting, storing and outputting labels (in particular ZPL), including:

Service	Processing of personal data
Label designer, templates, versioning, approval	Storage of designs with test data and field contents; log of creator, reviewer and comment
Rendering and conversion (web, REST API, batch)	Generation of ZPL, PDF and PNG from the controller's data; batch results held in memory for up to one hour
Printing via Weblink, remote printers (agent) and virtual printers	Transmission and logging of print jobs including label content and printer response
Data sources and stream connectors	Retrieval of records from the controller's databases and message brokers, conversion into labels, storage of failed messages for troubleshooting, output to the controller's object storage, brokers or webhooks

Service	Processing of personal data
Integrations (Deutsche Post INTERNETMARKE, Shopify, ShipStation, Veeqo, Amazon)	Retrieval of orders, transmission of address data for postage stamps, transaction log with stamp (PDF/ZPL)
Print Views	Provision of print forms for persons authorised by the controller
Notifications, webhooks, labels by email	Sending of content defined by the controller to recipients designated by the controller
Team, customer workspaces, audit trail with electronic signature	Management of the controller's users, traceability of changes
Support in individual cases	Access to the controller's data only to the extent necessary for troubleshooting; every access is recorded in the controller's audit trail (Annex 2 no. 3)

2. Nature of the processing

Collection, recording, storage, adaptation, retrieval, consultation, use, transmission to recipients designated by the controller, alignment, restriction and erasure (Art. 4 (2) GDPR).

3. Types of personal data

Category	Examples
Contact and address data	Name, company, address, telephone and email of recipients and senders
Shipment and order data	Order number, line items, tracking number, weight, product, postage amount
Marking data	Barcode and RFID contents (e.g. SSCC, SGTIN/EPC, GS1 Application Identifiers), where they can be linked to persons
Records from the controller's systems	any columns from databases and messages, e.g. employee, customer or item data
User and log data of the controller's users	Email address, name, role, timestamps, IP address, browser identifier, actions, reasons for electronic signatures
Communication content	Texts of notifications, webhook contents, Print View forms
Device and network data	IP address, hostname, MAC address and serial number of printers; hostname and local IP addresses of agent computers
Free content	Graphics, logos, fonts and free text in labels

No special categories of personal data (Art. 9 GDPR) and no personal data relating to criminal convictions and offences (Art. 10 GDPR), unless separately agreed (Section 4 (3)).

4. Categories of data subjects

• Employees and other users of the controller (team members, API users, Print View users)

• Customers, recipients and senders of shipments of the controller

• Customers of the controller in customer workspaces (e.g. in the case of agencies and service providers)

• Persons whose data is contained in the controller's connected data sources and message streams

• Recipients of notifications and label emails

5. Duration

Term of the Main Agreement; retention periods according to Annex 2 no. 8; deletion in accordance with Section 10.

ANNEX 2: TECHNICAL AND ORGANISATIONAL MEASURES (ART. 32 GDPR)

The measures apply to the zplCloud.com platform including the Weblink service. The controller is itself responsible for components that it operates itself (Section 6 (3)).

1. Physical access control

• Servers and backups are located in the Falkenstein data centre park of Hetzner Online GmbH in Germany, certified to ISO/IEC 27001, with access control, video surveillance and security staff of the data centre operator.

• The processor has no physical access to the servers, only administrative remote access.

2. System access control

• Sign-in only with a confirmed email address (double opt-in); passwords with at least 12 characters, stored exclusively as a cryptographic hash.

• Account lockout after repeated failed attempts.

• Two-factor authentication (authenticator app, email code, recovery codes) available to all users.

• Display and termination of active sessions, server-side validation of every session.

• Sign-in cookie not readable by scripts (HttpOnly) and with SameSite protection.

• Limiting of requests per account or IP address for the API and online tools (rate limiting).

• System credentials are kept outside the source code in access-protected files on the servers.

• Administrative access to the servers exclusively by the management.

3. Data access control

• Every record is assigned to an account or a company; queries are filtered to the respective tenant.

• Company roles “Admin” and “Member”: team management, approval of designs, viewing IP addresses in the audit trail and deleting other users' API keys are reserved for Admins.

• API keys per user or company, stored only as a SHA-256 hash and displayed only once when created; separate sandbox keys without access to real printers.

• When an API key is deleted, connected agents are disconnected immediately and the printer certificates bound to it are revoked.

• Administrative access by the processor to customer data via exactly one supervisor account; every impersonation and every supervisor access is recorded in the audit trail of the company concerned and is visible to its Admins.

4. Separation control

• Logical separation of tenants in a shared database (see no. 3).

• Separate databases, containers and data directories for production and test.

5. Encryption and pseudonymisation

• TLS 1.2 or 1.3 for all public connections, certificates via ACME, HTTP Strict Transport Security.

• Printers connect via mutual TLS authentication (mTLS) with an in-house certificate authority; revoked or deleted certificates are rejected when a connection is established, and existing connections are terminated within 30 seconds.

• The private key of the certificate authority is stored only in the server's data directory and in the encrypted backups, not in the source code.

• Credentials for data sources, streams, object storage and push channels are stored encrypted with AES-256-GCM; the key is kept outside the source code.

• Backups are stored in encrypted form.

6. Integrity, transfer control and input control

• Webhooks are signed with HMAC; delivery to private network addresses is blocked.

• Audit trail with SHA-256 hash chain; entries can only be appended to the table, and any subsequent change is verifiable; electronic signature with password re-entry and reason.

• Versioning of designs with reviewer and approval.

• Protection of forms against cross-site request forgery; security headers (X-Content-Type-Options, Referrer-Policy, Permissions-Policy).

7. Availability and resilience

• Deployment without interruption (blue-green) with health checks and automatic rollback to the previous version.

• Monitoring with metrics and traces; rotation of log files.

• Backup of all servers as an encrypted image every six hours to separate storage in Germany; retention for a maximum of 30 days.

• Recovery is tested and logged monthly.

• Emergency operation: restoration of the images at a second provider (netcup GmbH, Germany).

• Redundant power, air-conditioning and network supply provided by the certified data centre.

• Availability target of 99% on a monthly average (Section 9.1 of the Terms).

8. Storage limitation and deletion

• Automatic deletion of print jobs, sandbox prints, failed stream messages, webhook deliveries, usage statistics and integration transactions after 7, 30 or 90 days depending on the plan.

• Deletion of the account by the user themselves.

• Export on request and deletion of all data of the controller after the end of the contract, with a deletion log (Section 10); data in backups is overwritten after 30 days at the latest.

9. Organisation and review

• Access to the controller's data exclusively by the processor's management.

• The contact for data protection is the management; no data protection officer is required to be designated (Section 38 of the German Federal Data Protection Act, BDSG).

• Records of processing activities as controller and as processor (Art. 30 GDPR).

• Documented process for personal data breaches with notification to the controller within 48 hours at the latest (Section 5 (3)).

• Careful selection of sub-processors and conclusion of agreements pursuant to Art. 28 GDPR (Annex 3).

• Review and update of these measures at least once a year.

ANNEX 3: SUB-PROCESSORS

Listed below are the service providers that process the controller's data on behalf of the processor. The current list and announced changes are available at zplcloud.com/en/subprocessors.

Hetzner Online GmbH

Sub-processor	Hetzner Online GmbH, Industriestr. 25, 91710 Gunzenhausen
Service	Data centre, dedicated server and separate storage for backups
Data	all platform data including backups
Location	Germany, Falkenstein data centre park (Vogtland, Saxony)
Safeguard	EU; agreement under Art. 28 GDPR; ISO/IEC 27001

netcup GmbH

Sub-processor	netcup GmbH, Daimlerstraße 25, 76185 Karlsruhe
Service	Backup data centre: restoring backups if the production server fails and for recovery tests
Data	all platform data in an emergency and during recovery tests
Location	Germany, Nuremberg data centre
Safeguard	EU; agreement under Art. 28 GDPR; ISO/IEC 27001 and ISO/IEC 27701