

ProxyHub - Privacy Notice

Version: 16 September 2026

Non-binding English translation. The legally binding version of this document is the German original. In the event of any discrepancy, the German version prevails.

We process personal data in connection with the provision of the "ProxyHub" service. ProxyHub enables the receipt, capture, storage, digital provision, forwarding, return and destruction of letters and parcels as well as the creation of shipping labels for self-shipping.

1. Controller

The controller is: Hodlmayr GmbH, Höhenstr. 10, 70736 Fellbach, Germany, Managing Director: Ronny Mütschele, e-mail: support@proxyhub.space. A telephone hotline is not offered.

2. Data processed

Depending on use, we process in particular the following data:

- Master data: name, company, contact person, customer number, e-mail address;
- Address data: billing address, delivery address, receiving address;
- Access data: login data, technical identifiers, security information;
- Contract data: tariff, booked services, term, included services, additional services;
- Payment data: payment method, payment status, credit balance, invoice data;
- Mail data: sender, recipient, date of receipt, type of item, dimensions, weight, status, storage duration;
- Shipping label data: recipient data provided by the customer (name, address, where applicable telephone number and e-mail address of the recipient), shipment details (dimensions, weight, description of contents, value of goods, customs data), shipment number, shipment history, per-shipment confirmations by the customer;
- User data: in tariffs with user management, name, e-mail address and roles of the users created by the customer;
- Image data: envelope images, parcel photos;
- Content data: scan files and OCR texts, insofar as the customer orders the opening and scanning of letters;
- Communication data: e-mails, notifications, support requests;
- Usage data: portal accesses, orders, instructions, log data.

3. Purposes of processing

We process data for the registration and administration of the customer account, for the provision and activation of receiving addresses, for the assignment and management of incoming mail, for notification of mail receipts, for carrying out orders to open, scan, forward, archive, destroy or return, for creating shipping labels and engaging shipping service providers including the handling of additional charges, returns and damage claims, for billing chargeable services including storage and archive fees, for managing credit balances and payment status, for fulfilling legal obligations, for the prevention of misuse, for security and verifiability, for processing customer inquiries, and for the technical provision and improvement of the portal.

4. Legal bases

Processing takes place insofar as it is necessary for the provision of the service, for the performance of the contract or for carrying out pre-contractual measures.

Insofar as we are subject to statutory retention or verification obligations, processing takes place to fulfil legal obligations.

Insofar as we process data for the prevention of misuse, system security, securing of evidence or enforcement of rights, this takes place on the basis of legitimate interests.

The storage of status, order and notification logs takes place in particular to document the orders placed by the customer, for the traceability of mail processes, for handling inquiries, and for the assertion, exercise or defence of legal claims.

Insofar as consent is required or the customer places a separate order, in particular for the opening and scanning of letters, processing takes place on the basis of this consent or express instruction.

5. Opening and scanning of letters

Letters are only opened and scanned if the customer expressly orders this. Content may be processed that contains personal or particularly sensitive information. We have no influence over the content of incoming mail. The customer should therefore only order opening and scanning if they are authorized to take note of and digitize the content.

The scan files and OCR data are provided in the portal and deleted in accordance with the storage and deletion periods. The order to open and scan is documented on a per-item basis; in particular, user, item ID, time and selected action are logged.

6. Parcels

Parcels are not opened. We capture in particular externally recognizable information, dimensions, weight, photos and status data. After expiry of the free period, parcels are stored further against a storage fee; for this purpose we process storage duration and charges and send reminders. At the latest 180 days after expiry of the free period, parcels may be returned to the sender after prior notice.

6a. Shipping labels and transfer to shipping service providers

If the customer creates a shipping label or orders a forwarding, we transmit the data required for carriage (sender and recipient details, dimensions, weight, shipment number, for cross-border shipments description of contents, value of goods and customs data, and, where provided by the customer, telephone number or e-mail address of the recipient for delivery notifications) to the shipping service provider used for the shipment (parcel and express service providers established in the European Union; the respective shipping service provider is displayed to the customer before the shipping label is created or the order is placed). The shipping service providers process this data under their own responsibility in accordance with their privacy notices; in the case of internationally operating shipping service providers and cross-border shipments, processing may take place outside the European Economic Area (see Section 8).

The recipient data originates from the customer. The customer is responsible for having collected this data lawfully and for being permitted to pass it on to us and the shipping service provider. We process recipient data exclusively for carrying out the respective shipment, for handling additional charges, returns and damage claims, and for evidence purposes.

The confirmation given by the customer before creating a label (no excluded goods, accuracy of the information) is logged with user, time and shipment data.

7. Recipients of the data and service providers

To provide the service, we use service providers. These may include in particular hosting providers, e-mail service providers, document management and OCR systems, payment service providers, invoicing and accounting systems, shipping and fulfilment systems, shipping service providers, as well as analytics and marketing services.

As things currently stand, the following are used in particular: Strato for hosting and e-mail, Paperless NGX for document capture and OCR, Shopify / Shopify Payments for order and payment processing, PayPal and further payment providers, Coinsnap for Bitcoin payments, JTL-Wawi / FFN Connect or comparable shipping and fulfilment systems, easybill and DATEV interfaces, parcel and

express service providers for forwardings, returns and shipping labels, Google Ads and Google Analytics.

The above list reflects the current state of deployment at the launch of the service and will be adapted if the service providers used change.

8. Transfers to third countries

Insofar as service providers process data outside the European Union or the European Economic Area, this takes place only on the basis of appropriate safeguards or an adequacy decision. This may be relevant in particular for individual payment, analytics or marketing services as well as for shipping service providers: internationally operating shipping service providers also transfer shipment data within their group to countries outside the EEA; for shipments to third countries, recipient and customs data are necessarily transmitted to bodies in the destination country. The legal basis in this respect is the necessity for the performance of the shipment ordered by the customer (Art. 49(1)(b), (c) GDPR) or the safeguards used by the shipping service provider.

9. Storage period

We store personal data only for as long as this is necessary for the respective purposes or statutory retention obligations exist.

For mail and content data, the following storage logic applies in particular:

- **Letter mail, scan files and OCR data:** Letter mail is destroyed after expiry of the contractual storage period and after prior notification of the customer. If a letter is opened and scanned, the scan file and OCR data remain available in the portal until completion of the respective process. Once the item has reached a final state, in particular destruction, forwarding or return, a technical transitional period of currently 30 days begins. After expiry of this period, scan files and OCR data are deleted, insofar as no statutory retention obligations or legitimate evidence purposes conflict with this.
- **Parcel photos and other mail files:** Parcel photos and other item-related files are retained for a technical transitional period of currently 30 days after the item reaches its final state and are subsequently deleted, insofar as no statutory retention obligations or legitimate evidence purposes conflict with this.
- **Shipping label data:** The label file itself is available for retrieval in the portal for three days after creation (for forwardings, three days after dispatch) and is then deleted. Recipient data and shipment details from shipping labels and forwardings are deleted or anonymized 30 days after the shipment reaches its final state (delivery or return). If the customer has reported a loss or damage within this period, the data of the affected shipment remains stored until the damage claim has been settled. Non-personal shipment data (shipment number, destination country, price) is retained permanently for billing and evidence purposes. The confirmation logged before label creation is treated like order logs.
- **Mail data:** Mail data is deleted or anonymized after the respective item reaches its final state, insofar as it is not required for billing, verification, prevention of misuse or enforcement of rights. Insofar as necessary for traceability, non-personal database entries about actions carried out may remain.
- **Shipping and forwarding addresses:** Shipping and forwarding addresses deleted by the customer are retained for a technical transitional period of 30 days and subsequently anonymized. After anonymization, in particular city and country as well as non-personal information for the traceability of shipping processes may remain.
- **Technical access logs including IP address:** Technical access logs including IP address are generally deleted or anonymized after 90 days. Longer storage takes place only insofar as this is necessary due to a security incident, suspicion of misuse, a specific dispute or the enforcement of rights.

- **Status, order and notification logs:** Logs of status changes, orders, data changes and customer notifications, insofar as they do not contain an IP address, may be stored for evidence purposes for up to three years after the end of the calendar year in which the respective process was completed. Longer storage takes place only insofar as statutory obligations, a specific dispute or legitimate interests in the enforcement of rights require this.
- **Communication data:** Communication data and support requests are deleted as soon as they are no longer required for handling the respective matter, insofar as no statutory retention obligations or legitimate evidence purposes conflict with this.
- **Invoicing and accounting data:** Invoicing and tax-relevant data is stored in accordance with the statutory retention obligations.
- **Anonymized data:** Anonymized data in which there is no longer any personal reference may be stored without time limit for statistical, technical or economic purposes.

10. Rights of data subjects

Data subjects have, in accordance with the statutory provisions, rights to information, rectification, erasure, restriction of processing, data portability and objection.

Insofar as processing is based on consent, the consent may be withdrawn with effect for the future.

Data subjects also have the right to lodge a complaint with a data protection supervisory authority.

11. Obligation to provide data

Certain data is necessary for the use of the service. Without this data, individual functions cannot be provided. This concerns in particular name, e-mail address, customer address, billing data and mail data.

12. Automated decision-making

Automated decision-making within the meaning of data protection law does not take place, unless expressly stated otherwise.

13. Note on website analytics and advertising

Insofar as Google Analytics, Google Ads or comparable services are used, this takes place only in accordance with the applicable legal requirements. In particular, the necessary cookie or consent mechanisms, provider information, storage periods, third-country references and withdrawal options are set out in the general website privacy policy or in the consent banner.