Data processing agreement (DPA)

As of 6 November 2026 · Version 2026-11-06 · Test mode

The contracting party and invoice issuer is the operator ([to follow]); Wichtli is one of its brands.

Version 2026-11-06. Between the customer (controller) and [to follow] (processor, «we»). The DPA is annex 1 of the terms and is accepted in checkout; we store version and time with the order. Translation for convenience; the German version prevails.

1. Subject and duration

We process personal data on behalf of the customer to run a Wichtli round. The DPA applies for the duration of the round and until the data is deleted under section 11.

2. Nature and purpose

Invitation, voluntary sign-up, draw, anonymous chat, Advent calendar, reveal, report and ordered extras (incl. delivery). No use for advertising or own purposes; statistics only in aggregate.

3. Types of data

- name, work email, optionally team, location, manager email;
- acceptance, draw, questionnaire, wishlist, hints, office days, desk, fun facts;
- content and metadata of messages in the anonymous chat;
- postcards: the recipient's first and last name and office address, the scene with their first name, the card text;
- home address (only for an ordered delivery, encrypted);
- sensitive data: health (food intolerances), voluntary, only with explicit consent.

4. Data subjects

Employees and other people invited by the customer, and its admins.

5. Instructions

We process the data only on the customer's documented instructions; the round's settings count as instructions. We inform the customer if, in our view, an instruction breaches data protection law.

Standing instruction: «Review of reported messages only; disclosure of the sender's identity only on written request of the HR contact named in the Runde after a report; logged.» We disclose data to authorities only on a valid legal order.

6. Confidentiality

Everyone at our side with access to the data is bound to confidentiality.

7. Technical and organisational measures (annex 2, TOMs)

- Data minimisation: only the fields needed; private by default.
- Transport encryption (TLS) for all connections; HSTS.
- Storage in Cloudflare D1 with EU jurisdiction.

- Home addresses and food intolerances: AES-256-GCM encryption per record with a key derived per company; keys only as Worker secrets, never in code. Food intolerances never appear in emails, exports or reports.
- No endpoint reads addresses; decryption happens only in the fulfilment export, and every decryption is logged (who, when, no address).
- HR and admins never see who drew whom, wishlists or messages.
- Role-based access; two-factor authentication for operator access; sign-in by one-time link.
- Logs without content and without addresses; kept 30 days.
- Emails never contain pairs, the name of the Wichtelkind or Wichtel, and by default no message text. Sender domain with SPF, DKIM and DMARC.
- Automatic deletion under section 11; backups expire after 30 days at most.
- Incident process: contain, assess, log; breach log kept 2 years.

8. Sub-processors (annex 3)

The customer approves the following sub-processors. We announce new or changed sub-processors by email 30 days ahead; the customer may object for a valid data protection reason and, if we find no solution, terminate the contract for future services. We bind sub-processors by contract to equivalent duties.

Sub-processors

Provider · Purpose · Country of seat · Storage / processing location · Transfer mechanism · Status

Cloudflare Inc. (Workers, D1, R2, CDN) · hosting, DB · US (parent) · EU storage (D1 EU jurisdiction); global edge · DPF (EU-US, Swiss-US) + SCCs in the Cloudflare DPA · active

Cloudflare Email Service · transactional mail, chat relay · US (parent) · global edge, transit only · DPF + SCCs (Cloudflare DPA) · not yet active

Stripe Payments Europe Ltd. / Stripe Inc. · payment (business contact + card data; Stripe is independent controller for payment compliance) · IE / US · EU/US · Stripe certified to EU-US DPF incl. Swiss-US DPF; Data Transfers Addendum as fall-back · not yet active

Gelato (print, gift, home delivery) · process recipient name and address · NO (EEA) · CH/EU/EEA, only once confirmed in writing (DPA or API setting) before activation; Gelato's own sub-processors listed or linked here before activation · EEA, adequate; signed DPA before activation · not yet active

Prodigi Group Ltd (print, backup) · process recipient name and address · UK · UK, EU; CH/EU/EEA/UK only once confirmed in writing before activation · UK adequacy (CH and EU) · not yet active

Swiss Post (when live) · printing and posting postcards: the recipient's name and office address, first name on the front, card text · CH · CH, only once confirmed in writing before activation · none needed (domestic) · not yet active

AI/GIF generation provider (if used) · personalised GIFs · not yet chosen · not yet chosen · only with DPA; no real photos of persons uploaded at launch, text-based personalisation only · not yet active

9. Assistance

We assist the customer with data subject requests (access, rectification, erasure, portability, objection): requests sent to us are forwarded within 3 business days, and we carry out instructions within 5 business days. Participants can export and delete their data in the app themselves. We also assist with data protection impact assessments and notifications to authorities.

10. Breach notification

We notify the customer by email of every personal data breach within 24 hours of becoming aware of it, without a prior risk test. The notice contains, as far as known: the nature of the breach, the data and people concerned, likely consequences, and measures taken or proposed (template following the FDPIC guide). Notifying the FDPIC (Art. 24 revDSG) or the supervisory authority within 72 hours (Art. 33 GDPR) is the customer's duty.

11. Retention and deletion

On 31 January after the season we delete the round's data automatically; 14 days before, the customer gets a reminder with an export option (participant list, no wishlists). At the customer's choice we return the data at the end of the contract (export) or delete it; statutory retention duties remain reserved. The following table applies:

Retention and deletion

Data · Where · Keep · Delete

Invite records unconfirmed (invited, neither joined nor declined) · D1 · until J + 1 day · J + 1 day, automatic job purge-unjoined; non-joiners then only as a count

Declined invite («Nein, danke») · D1 · name and data: none; salted email hash for this Runde only · data at once; hash 31.1.

Allergy field (encrypted, consent) · D1 · until withdrawal or season end · on withdrawal, else 31.1.

Participant profile (name, work email, wishlist, hint text) · D1 · until season end · 31.1. automatic job; plus self-service delete anytime

Draw/pairing · D1 · until season end · 31.1.

Messages and hints (anonymous relay) content · D1 · until season end; reported messages and hints, including the sender's identity, kept as evidence up to 90 days after the report · 31.1. (flagged: +90 days)

Delivery address (encrypted) · D1 · from entry until delivery confirmed · 14 days after delivered (no delivery report: 30 days after shipping), 14 days after a failed or credited order, by 31.1. at the latest; decrypt only for the fulfilment export

Personalised GIF/card assets · D1 (file: R2 EU once enabled) · until season end; earlier if sender or recipient leaves · 31.1.

Year-two pair memory (keyed HMAC, per-company secret; only if the company chooses it) · D1 · until the next Runde, max. 13 months · at 13 months, on cancellation of the Abo/renewal, or on the participant's own deletion request

Company account (admin name, email) · D1 · while customer relationship runs · on request; inactive 24 months: deleted

«Für 2027 vormerken» (double opt-in email + timestamp) · D1 · until 31.10.2027 · 31.10.2027 or on unsubscribe

Invoices, Stripe payment records, order records · Stripe + D1 · 10 years statutory (Art. 958f OR) · after 10 years

Security/access logs (no content) · Workers logs · 30 days · rolling

Address-decrypt audit log (who/when, no address) · D1 · 12 months · rolling

Breach log · internal · 2 years from report · then delete

Backups/Time Travel · D1 · up to 30 days · rolls off

J = the join deadline of the Runde. Season end is 31 January. Aggregated, non-personal statistics (e.g.

participants per Runde) may be kept.

12. Audit

The customer may verify compliance with this DPA once a year based on documents, at its own cost. We provide the information needed. If the documents are not sufficient or a supervisory authority requires it, audits including inspections by the customer or an auditor it mandates who is bound to confidentiality are possible, with 30 days' notice, during business hours and at the customer's cost.

13. Cross-border transfers

The data is stored in the EU. Transfers to the US go only to sub-processors certified under the Data Privacy Framework (EU-US and Swiss-US), additionally safeguarded by standard contractual clauses. Contact: privacy@wichtli.ch.