Technical and organisational measures (annex 2, TOMs)

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.

- 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.