OCTO and the GDPR

Version 1.4.5 · Updated 6 October 2026 · English

Current review — supplier, tracking and retention checks remain open.

This version describes the website and the selected limited security/delivery approach. Service availability does not establish that the remaining provider, email-tracking or deletion requirements have been verified. This notice does not certify that an exemption applies.

This overview summarises the Privacy Policy; it is not a certification of compliance. The GDPR protects personal data and provides individual rights, not only for EU citizens.

Who is responsible?

Axel Van Mechelen and Robbe Heynderickx operate OCTO personally as joint controllers. Axel coordinates privacy requests; Robbe coordinates suppliers, deletion and backup expiry. You can exercise your rights against either founder at admin@octo-tool.com or Isabellakaai 60, 9000 Ghent, Belgium.

What data and choices are involved?

The website processes necessary request/security data and your cookie choice. GA4 loads only after statistics consent. When registration is available, the free waitlist uses email, language, participation status and times, age/guardian declarations and versioned consent/Terms evidence. Education and referral answers are optional; we do not ask for a name or date of birth. Newsletter consent and confirmation are separate.

The 16+ rule and guardian permission for ages 16–17 are OCTO's participation requirements, not the general GDPR consent age. Product accounts, uploads, AI and payments need separate information before introduction.

Which cookies and storage?

CookieConsent remembers your choice for one calendar month. Cookiebot's separate published End User Data retention is 12 months. With statistics consent, _ga and _ga_CCXN1DEMRF have lifetimes up to 180 days; activity can renew the session cookie. GA4 user/event data have a separate two-month retention setting, without renewal on activity. Aggregated reports are outside that setting.

octo-language local storage remembers your explicitly chosen language until cleared. Use Cookie settings to remove it or change analytics choices. Rejecting analytics does not restrict website access. Withdrawal stops new measurement and removes the GA cookies we control; it does not automatically erase historical measurements. Security storage in the signup flow still needs a complete inventory.

Who supplies the service?

Cloudflare provides hosting/security and encrypted R2 backup storage; Supabase provides the database/server functions; Brevo handles requested emails and optional newsletters; Neo hosts contact mailboxes; Cookiebot/Usercentrics manages consent; Google supplies optional analytics. The Privacy Policy describes known locations and links to provider terms. EU hosting alone does not establish that every operation stays in the EEA.

Account-specific processing agreements, locations, subprocessors and international-transfer safeguards still need complete verification. Joining the waitlist does not make OCTO your processor or require you to enter a data processing agreement with OCTO.

What remains under review?

Service availability does not establish completion of the checks below. OCTO retains Brevo and intends to use email technical records only for necessary delivery and security, not engagement analytics or marketing profiles. Both anonymous-tracking settings and the per-contact refusal setting are used, but Brevo still inserts pixels/rewritten links and controlled checks found individual open/click details. These controls are therefore not a promise of tracking-free delivery.

To rely on an exemption, we must substantiate any strictly necessary exemption for the actual processing, including minimum data, purpose, retention and provider responsibilities. A general security explanation, legitimate interests, Terms acceptance, newsletter permission or website-analytics consent does not automatically authorise every email-tracking operation. Processing outside a valid exemption needs an effective consent route or must be disabled. Privacy Policy section 4.2 explains objections, old messages and the limits of preference controls.

The documented retention limits require manual work: automatic permanent cleanup is not enabled, and full provider, mailbox and backup expiry still requires verification. Supabase's account documents confirm that its DPA is incorporated into its Terms; this does not complete the checks for every supplier, processing location or international transfer.

Preference changes are saved in OCTO first; updates to Brevo are queued and may take time. A message already accepted by the email provider for delivery may still arrive. We check current permission before further sending and investigate failed synchronization; a delay does not restore consent.

Privacy Policy sections 5 and 6 set out the supplier-location/transfer checks and the data-category schedule covering database, Brevo, mailbox, exports, logs and backups, with the applicable periods and Axel/Robbe responsibilities. They also require a complete test-registration deletion check, separate original-date backup-expiry verification, reapplication of newer deletions before a restore is used, and retention of only justified minimum evidence. These are requirements with explicitly recorded remaining verification, not a declaration that supplier erasure or a tracking exemption has been proved.

Our sending configuration uses Brevo automations triggered by adding a contact to a dedicated list for confirmation, newsletter welcome or preference recovery. The subscriber workers do not send these messages directly through an SMTP/email-send API. They set the available contact pixel-tracking preference to No before enrolment. The two account-wide anonymous-tracking settings are enabled; these are separate controls. OCTO does not import open/click callbacks for engagement analysis. Checking that configuration does not prove what Brevo retains internally.

Robbe must obtain a service-specific explanation from Brevo of exactly what remains recorded when tracking is refused: which identifiers, message/contact links, open/click counts or times, network/device information and target-link data are processed; the purpose and necessity of each operation; the applicable role and legal basis; the retention and deletion trigger for each category; and what happens after withdrawal or when an old message is opened. The explanation must cover our actual list-triggered automations and both tracking settings, not only a different direct-send product. Until that evidence is verified, no definite provider-internal retention period or successful tracking refusal is claimed.

How do I exercise my rights?

Cookie withdrawal, newsletter unsubscribe, leaving the waitlist and removing optional answers are separate choices. Email preferences does not itself erase every provider, mailbox or backup record. Contact us for full erasure, access, correction, restriction, portability or an objection, subject to GDPR conditions.

We respond without undue delay and within one month; a permitted extension of up to two further months must be explained within the first month. Consent withdrawal does not make earlier lawful processing unlawful. You may complain directly to the Belgian Data Protection Authority or another competent authority, or seek a judicial remedy. This legal release is available in English and Dutch.