Website & free waitlist

OCTO Privacy Policy

Version 1.4.6 · Updated 7 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.

1 Who we are and what this policy covers

Axel Van Mechelen and Robbe Heynderickx operate OCTO in their own names and are joint data controllers. OCTO is currently a project, with no registered business or VAT number. Contact either founder through admin@octo-tool.com, +32 472 97 43 23, or Isabellakaai 60, 9000 Ghent, Belgium.

Axel coordinates privacy information and requests. Robbe coordinates suppliers, security, deletion and backup expiry. Both remain responsible for the joint processing; you may exercise your rights against either founder. This is the essence of our allocation of responsibilities; ask us for further information about the arrangement.

This policy covers our public website, contact with us, and the free waitlist and optional newsletter when available. The form indicates whether registration is available. We will provide separate privacy information before offering product accounts, uploads, AI chats or payments.

2 Website, cookies and browser storage

We receive information from your browser, your messages and submissions, and service providers' security and email-delivery records. Website requests can include your IP address, browser and device details, requested pages and error records. We use necessary technical data to deliver and protect the website, on the basis of legitimate interests in operating a secure service (Article 6(1)(f) GDPR). Our retention rule for OCTO-controlled routine technical and delivery logs is up to 30 days; section 6 explains the outstanding verification of provider logs.

Cookiebot by Usercentrics remembers your cookie choice. Managing and recording consent supports our consent obligations (Article 6(1)(c)). The language preference provides the setting you request (Article 6(1)(f)). Optional Google Analytics 4 (GA4) requires separate consent (Article 6(1)(a)). Merely browsing, joining the waitlist or accepting the Terms does not grant analytics consent.

Current browser storage, checked on 6 October 2026

Name and provider	Purpose and scope	Lifetime and choice
CookieConsent — Cookiebot / Usercentrics	Consent identifier, time and category choices. First-party cookie on the visited OCTO hostname, path /.	One calendar month after your choice. Necessary to remember and apply that choice; a new choice may reset its expiry.
_ga — Google	Pseudonymous browser identifier. Cookie on octo-tool.com (including subdomains), path /.	Up to 180 days from setting. Its expiry did not renew in our revisit check. Statistics consent required.
_ga_CCXN1DEMRF — Google	Analytics session information. Cookie on octo-tool.com (including subdomains), path /.	Up to 180 days; activity can renew this session cookie's expiry. Statistics consent required.
octo-language — OCTO	Local storage on each website origin, containing the language you explicitly select (English or Dutch). It is not an analytics cookie.	No automatic expiry. Remove it through Cookie settings or your browser's site-data controls.

Cookiebot also holds consent records separately from the browser cookie. Its published policy states a 12-month retention period for End User Data. This is distinct from OCTO's one-month browser-choice setting; the account-specific record and deletion arrangements remain under review.

Cloudflare Turnstile is configured to check new waitlist and newsletter signups for automated abuse using browser, device and network signals. Pre-clearance is disabled; it is not required to unsubscribe. The full security-storage inventory for the signup flow still needs verification. We do not represent this table as a verified inventory of every provider-internal security record. See Cloudflare's Turnstile notice.

3 Optional analytics

GA4 is available on the public website but loads only after you allow statistics cookies. Rejecting them leaves the website available. Our controls block Google Analytics requests, including cookieless signals, before consent and after rejection or withdrawal. Analytics does not load on confirmation, newsletter or email-preferences pages.

With consent, we measure visits and sessions, page views, 90% scrolling, waitlist-button clicks, form starts, accepted signup requests and language changes. An accepted request is not proof of verified email ownership or a newsletter subscription. Data include pseudonymous browser/session identifiers, timestamps, fixed page names, referring-site origins, approved campaign labels, browser/device details, language and approximate location. We do not send email addresses, optional answers, signed links or other form content to GA4, or link analytics to waitlist records. Advertising features, Google signals and user-provided data collection are disabled.

Google describes IP addresses as used to derive location without storing them in GA4. Analytics data are pseudonymous, not anonymous. User and event retention is configured to two months without resetting on new activity, subject to Google's deletion cycle. This setting does not govern browser-cookie expiry or aggregated standard reports. We review the need for those reports annually and delete the property when the website-improvement purpose ends.

Use Cookie settings at any time to change or withdraw your choice. Withdrawal stops further measurement, removes the GA cookies we control and reloads a page that loaded Analytics; this can reset an unfinished form. It does not automatically erase past measurements. You may request deletion and, where needed, supply a browser identifier so we can locate the relevant data. Your choice is browser-specific; changing device, clearing storage or expiry may require a new choice.

4 Waitlist, newsletter and contact data

4.1 Free waitlist and optional answers

When registration is available, we use your email address, selected language, signup time and participation status to add you to the waitlist immediately and send a registration notification and the availability notification you request, with your consent (Article 6(1)(a)). You do not need to click an email link to join. Signup alone does not verify ownership of the email address. The email address and required declarations are necessary to apply; providing them is voluntary. We do not ask for your name or date of birth.

We record your age-group declaration (16–17 or 18+), parental/guardian-permission declaration where required, Terms acceptance, and consent choices with their timestamps, versions, displayed wording and relevant document reference/hash. The 16+ eligibility rule and permission requirement for 16–17-year-olds are OCTO participation rules, not a statement of the general GDPR consent age. We do not require an identity document as part of ordinary registration.

Education level and how you found us are optional, with separate purpose-specific choices. We use education to plan introductory groups and referral answers to improve communication. You may skip either question or withdraw permission for an answer separately. These purposes rely on consent (Article 6(1)(a)).

A successful website submission adds a new registration directly to the waitlist. The email only notifies you that you have been added; email delivery or a click is not required for participation. Existing withdrawals and delivery suppressions are respected and cannot be undone through an anonymous duplicate submission; contact us if you previously left. We keep the active profile until withdrawal, launch/closure of the waitlist or the end of 31 January 2027 in Brussels, whichever comes first, followed by deletion or irreversible anonymisation within 30 days. Continuing afterwards requires a new choice. Legacy unconfirmed requests, if any, retain their original 48-hour verification-link and subsequent 30-day deletion limits. Separate valid newsletter consent is handled independently. Verification of these operating limits remains outstanding, as explained in section 6.

4.2 Optional newsletter and email delivery

Newsletter marketing needs separate consent and separate confirmation (Article 6(1)(a)); joining the waitlist does not subscribe you. We process your email, language, newsletter status, preferences and consent evidence. Unconfirmed newsletter links expire after 14 days; the deletion rule is within 30 days afterwards. Confirmed marketing ends on withdrawal, the end of the activity or 24 months after the last explicit confirmation, whichever is earlier. Sending must stop when permission ends; the active marketing profile must be removed within 30 days, subject to the separate evidence and suppression rules below.

Security and delivery are our only intended uses of email technical records. Brevo processes recipient addresses, message content, delivery status, bounces, complaints and related technical records. OCTO uses the records needed to deliver requested messages, protect verification and recovery, investigate misuse and honour opt-outs. Our waitlist system does not import open/click events for engagement analytics. We do not use email-open or click histories for marketing profiles, personalised promotions, scoring or behaviour-triggered marketing.

Ordinary delivery and security processing relies on our legitimate interests in providing and protecting requested communications (Article 6(1)(f) GDPR), subject to necessity, proportionality and your rights. This basis does not itself permit access to information on your device. Any use of an email tracker without consent must separately satisfy the applicable strictly necessary transmission or requested-service exemption. We do not treat a provider's general reference to security, anti-abuse or deliverability as proof that every pixel, redirect or event history qualifies. Optional engagement measurement would require a separate lawful arrangement and, where required, prior valid consent before it starts.

What Brevo currently does. Brevo can insert an invisible image and rewrite links through its servers. Opening a message or following a rewritten link may create event times and counts linked to the message or recipient. Both account-wide anonymous-tracking settings are enabled and OCTO sets the available per-contact tracking preference to No. Those settings do not remove the pixel or link rewriting. Our latest controlled checks found anonymised main logs but open/click counts and times still visible within the recipient's message details. We therefore do not promise tracking-free messages or complete unlinking from individuals.

Verification remains outstanding. We must establish which residual operations are necessary for the stated security or delivery purpose, the minimum data and retention required, provider responsibilities and the applicable legal conditions. Operations outside a substantiated exemption must be disabled or handled through effective consent controls. Merely joining the waitlist, requesting a newsletter, accepting the Terms or allowing website analytics does not grant permission for unrelated email tracking. A revised notice does not retrospectively authorise earlier processing.

You can object to processing based on legitimate interests or make a privacy request at admin@octo-tool.com. We assess such requests under the applicable GDPR rules, including the unconditional right to object to direct marketing. Newsletter unsubscribe and leaving the waitlist stop the corresponding sending permission; they do not remove pixels from messages already received. Requests concerning those messages and Brevo's existing records require provider handling. We cannot promise that changing a preference deletes every provider log or backup; section 6 distinguishes our retention rules from provider periods.

Our sending configuration uses Brevo automations triggered by adding a contact to a dedicated list for registration notification, 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.

The current registration-notification template also contains an optional newsletter invitation and promotional project text. Its registration purpose, automation channel or transactional label does not by itself make all content or tracking strictly necessary. That mixed content must be included in the purpose and necessity assessment before relying on an exemption.

4.3 Enquiries and essential notices

We use your contact details and message to answer enquiries on the basis of legitimate interests (Article 6(1)(f)), or Article 6(1)(b) for pre-contract steps you request. Our rule is to retain correspondence for up to 12 months after resolution, apart from a specific legal obligation or dispute. Neo supplies our mailboxes.

The same enquiry rules cover investor and pitch-deck requests, mentoring, student collaboration, technical introductions, press and ocean-initiative enquiries. Relevant correspondence may include your name, organisation, contact details, interests and attachments that you choose to send. These pages open your own email application; submitting an enquiry does not subscribe you to marketing or create an investment, employment or collaboration agreement. Please do not send unnecessary sensitive information or third-party personal data without an appropriate reason.

Our social-media and research links take you to external services when you choose to follow them. Those services apply their own privacy information. We do not load social-media tracking embeds simply because you view an OCTO page. Data in correspondence are handled through our mailboxes, separately from waitlist and analytics records.

Necessary participation, closure or material-Terms notices serve administration of the waitlist agreement (Article 6(1)(b)); security and misuse notices serve legitimate interests (Article 6(1)(f)), or a legal obligation where applicable (Article 6(1)(c)). They must contain no promotional material and do not require newsletter consent. We keep only the contact and delivery evidence needed for the relevant purpose and period. We must answer privacy requests and provide legally required notices regardless of signup availability.

5 Providers, sharing and international transfers

We do not sell personal data. The following providers support the service. Public provider terms explain possible processing arrangements; they are not proof that every account-specific contract, location or safeguard has been checked.

- **Cloudflare:** Pages hosting and network security process website requests; Turnstile checks signup abuse. R2 holds encrypted OCTO backups in an EU-jurisdiction bucket. That bucket restriction does not establish that all Cloudflare support, network or security processing stays in the EEA. Cloudflare data processing terms.
- **Supabase:** forms, database and server functions handle submitted data, participation, consent/Terms evidence and delivery jobs. The current project region is eu-west-1 (Ireland). This does not restrict every support or subprocessor operation to Ireland. Supabase data processing terms. Its account documents confirm that the data processing addendum is incorporated into the Terms for all organisations.
- **Brevo:** requested emails and optional newsletter delivery use addresses, preferences, content, delivery records and the tracking operations described in section 4.2. Its public hosting information identifies France and Germany; other processing, support and subprocessors require separate checks. Brevo hosting information.
- **Neo:** hosts our contact mailboxes and handles correspondents' addresses, messages, attachments and mailbox records. Our account's processing locations, retention and transfer arrangements are still being verified. Neo privacy information.
- **Cookiebot / Usercentrics A/S, Denmark:** supplies the consent interface, technical delivery and consent records. Its one-month browser choice and published 12-month End User Data period are distinct. Account-specific locations, subprocessors and contractual coverage remain to be checked. Cookiebot privacy information.
- **Google Ireland Limited, with Google LLC and authorised subprocessors:** supplies optional GA4 and receives the analytics data in section 3. Processing may occur in the United States and other countries. Google processing terms and transfer arrangements.

Providers may process data outside the European Economic Area. Such transfers require an applicable adequacy decision or appropriate safeguards, such as Standard Contractual Clauses with the necessary assessment and supplementary measures. The EU–US Data Privacy Framework can apply only to an eligible transfer to an actively certified recipient. Cookie consent does not substitute for transfer safeguards.

Verification outstanding: we have not completed the provider-by-provider record of contracting entities, accepted processing agreements, all locations/subprocessors, applicable transfer mechanisms and

deletion terms. The public links above do not resolve that gap. Contact us for the information currently available or a copy of applicable safeguards. We will update this notice as the verification is completed.

We may disclose necessary information to professional advisers or competent authorities where required for a legal obligation or justified claim. Access must be limited to the task, with confidentiality and processing terms where required.

For each supplier, Robbe maintains a restricted record of the service and data categories, contracting entity and applicable agreement, primary hosting and any support/subprocessor processing countries, and the actual transfer arrangement for processing outside the EEA. It must identify the relevant adequacy decision or other safeguard, such as the applicable Standard Contractual Clauses with the necessary transfer assessment and supplementary measures. A country of incorporation, an EU database region or a generic DPA link alone does not establish this. We must be able to explain the verified arrangement and how you can obtain a copy of the relevant safeguards. These checks also apply now to suppliers used by the already-public website.

The locations described above are the facts currently established, not a completed country-by-country inventory. Unconfirmed locations or transfer arrangements stay recorded as open issues; we do not replace missing supplier evidence with a promise of Europe-only processing. Cookiebot's public DPA describes permitted third-country transfers and a processor-backup deletion exception of up to six months after termination; its applicability to our account still needs checking. That exception is separate from its published 12-month End User Data period and our own backup rule. See Cookiebot's processing agreement.

6 Retention, deletion and security

Axel handles privacy requests; Robbe owns the manual deletion and backup-expiry process. Automated permanent cleanup is not enabled. The periods above and below are our documented operating rules, not evidence that every historical record or provider copy has already been deleted. Provider log lifetimes, mailbox cleanup and backup expiry have not yet been fully verified. Those checks remain outstanding; operational availability is not evidence of their completion.

Limited consent and privacy-request evidence supports legal obligations (Article 6(1)(c)); necessary Terms, eligibility and claim evidence supports legitimate interests in administering and defending the arrangement (Article 6(1)(f)). Keep only necessary evidence, normally for up to three years after participation/consent ends or a request is resolved. A longer period requires a specific legal requirement or claim, with a recorded review date.

Minimal suppression records prevent unwanted re-import or sending while that risk exists and are reviewed annually. They do not permit continued marketing. The rule for OCTO-controlled backup copies is a maximum of 90 days from their original creation, with deletion requests reapplied before any restored data are used. Copying a backup must not restart its lifetime. Provider-internal copies have separate contractual limits that still need confirmation; we cannot describe them as covered by OCTO's backup rule.

We use encrypted connections and restricted access; no security measure guarantees absolute protection. We do not make solely automated decisions with legal or similarly significant effects or create behavioural advertising profiles. When consent ends, identifiable data must be erased without undue delay unless another valid basis permits limited retention. Truly anonymous statistics may be kept longer.

Google's processing terms describe up to 180 days for certain service-supported deletion instructions or end-of-term deletion, subject to their conditions. This is not a general OCTO retention period and does not extend the GDPR deadline for responding to your request.

Data locations, retention rules and responsible operators

Data category	Where copies may be held	Deadline, owner and limits
Waitlist profile and optional answers	Supabase database; Brevo contact, trigger lists and message-link attributes where needed for sending. Optional education/referral answers remain in Supabase.	Direct signup: withdrawal, launch/closure or end of 31 January 2027, then removal within 30 days. Legacy pending requests: original 48-hour link plus at most 30 days. Robbe executes; Axel checks the request and any independent purpose.
Newsletter profile and preferences	Supabase purpose/evidence records; Brevo contact, lists and opt-out state.	Pending: 14-day link plus at most 30 days. Confirmed: stop at withdrawal, activity closure or 24 months from explicit confirmation; remove active profile within 30 days. Robbe; preserve only a separate valid purpose.
Delivery, recovery, security and operational records	Supabase jobs, recovery sessions and events; Brevo messages/events; Cloudflare and other supplier logs; operational-alert mailbox copies.	Routine OCTO-controlled technical/delivery records: up to 30 days. Expired links and sessions cannot authorize use. Supplier-internal copies have separate unverified periods; a mailbox copy of a routine alert does not get an automatic 12-month extension. Robbe; Axel reviews specific incident/claim exceptions.
Enquiries, privacy correspondence and attachments	Neo inbox, sent items and Trash; necessary forwarded or downloaded copies.	Ordinary enquiries: up to 12 months after resolution, subject to a specific obligation or claim. A message in Trash is not proof of full erasure. Axel handles the case; Robbe verifies mailbox/copy removal. Minimal privacy-case evidence follows the evidence row below.
Exports and working copies	Necessary CSV/access exports, downloaded attachments and temporary local or hosted working copies.	Record purpose, original creation and an exact expiry. Remove when the purpose ends or the source-data deadline arrives, whichever is earlier. Campaign exports expire within one day; keep other copies only for the documented short operational need. Copying never restarts expiry. Robbe; Axel approves request-related scope.
Consent, Terms, eligibility and request evidence	Restricted Supabase evidence/case records and the minimum independent erasure/preference ledger needed for recovery.	Only necessary fields: purpose/status, dates, applicable wording/version and proportionate verification/decision evidence. Normally up to three years after the purpose ends or case closes; earlier if unnecessary. Axel determines necessity and review date; Robbe restricts and erases copies.
Suppression against unwanted re-import or sending	Minimal restricted identifiers and purpose/status in Supabase and applicable Brevo suppression state.	Only while the risk remains; review at least annually. Not a full profile, message archive or renewed marketing permission. Robbe operates the control; Axel reviews necessity.

Data category	Where copies may be held	Deadline, owner and limits
OCTO-controlled backups and restore copies	Encrypted R2 backups, encrypted local downloads and isolated restore-test copies.	Maximum 90 days from original creation, with earlier removal of temporary restore copies when no longer needed. Original dates follow every copy. Robbe verifies expiry and post-restore removal; Axel checks any justified exception. Provider-internal backups are separate and not represented as covered by this limit.
Website consent and optional analytics	Visitor browser; Cookiebot consent records; Google Analytics, separately from waitlist records.	Browser and GA periods are in sections 2–3: one calendar month, up to 180 days, and two-month GA user/event retention. Cookiebot states 12 months for End User Data. Robbe checks settings and supplier execution; Axel handles rights requests. Provider deletion cycles and aggregated-report review remain separate.

The table is our operating schedule, not proof that every supplier copy has expired. Robbe records actual systems, original dates, due dates, outcomes and exceptions in a restricted register; Axel reviews the necessity of any retained evidence. Automated permanent cleanup remains disabled. Deletion failures are escalated and do not silently extend the limit.

The required complete deletion check must follow a single clearly marked test registration through its entire lifecycle: inventory database records, Brevo contact/list/attributes and events, received/sent mail and attachments, exports/working copies, logs and backups; stop the relevant purposes and queued sends; perform authorized scoped deletion; then independently recheck each store for absence or a specifically justified retained minimum. The record must state what was checked, by whom and when, the result and any remaining supplier deadline. Separate tests on disposable database, Brevo, R2 and local-copy fixtures have passed, but they are not proof of one complete registration's erasure across every system. Mailbox, provider-internal and actual aged-backup expiry evidence remains incomplete.

Backup expiry is checked separately against each original capture date and all known copies; no current young backup is treated as proof of the 90-day expiry. Before any restore becomes operational, intake and sending stay disabled. Robbe must obtain the latest independent erasure, withdrawal and suppression records, reapply every newer deletion and preference change, invalidate obsolete links and jobs, and verify both the restored database and provider state. Axel reviews the retained minimum and outstanding exceptions. If the latest register is missing or reconciliation fails, service sending must not resume. Delete temporary restore copies when the check ends and retain only the necessary restricted result, not another full test profile or message archive.

7 Your rights and separate choices

Subject to GDPR conditions, you can request access, correction, erasure, restriction and portability; object to legitimate-interest processing for reasons relating to your situation; and object to direct marketing at any time. You may withdraw consent without affecting earlier lawful processing.

Cookie settings controls analytics. Newsletter unsubscribe controls marketing. Email preferences separates waitlist participation, newsletter permission and optional answers. Leaving one purpose does not automatically end another valid purpose. Stopping emails or removing an optional answer is not the same as erasing all records across the database, mailboxes, providers and backups.

For full erasure or another privacy request, contact admin@octo-tool.com or either founder at our postal address. We will explain any data that must be retained and the reason. We respond without undue delay

and within one month. A permitted extension of up to two further months requires an explanation within the first month. Requests are normally free; if we reasonably doubt identity, we ask only for what is necessary to verify it.

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.

8 Complaints and changes

You may complain directly to the Belgian Data Protection Authority or another competent EEA supervisory authority and seek a judicial remedy. You do not have to contact us first.

We date revisions, preserve previous versions and notify affected people of material changes where required. A new purpose requires fresh consent where applicable. This release is available in English and Dutch.