

Privacy policy

1. At a glance

The following information gives a simple overview of what happens to your personal data when you visit this website. Personal data is any data that can be used to identify you personally.

2. Controller

The controller responsible for data processing on this website pursuant to Art. 4 (7) GDPR is:

traqx GmbH

Represented by the managing directors: Alexander Schrot and Daniel Herrmann

Enzweilerweg 3a · 66709 Weiskirchen · Germany

Phone: +49 171 3697577

Email: info@traqx.io

A data protection officer has not been appointed; the controller is your point of contact for all data protection matters.

3. Server logs (technically required)

When you visit this website, the hosting provider automatically collects technical information in server log files: IP address (anonymised after 7 days), date and time of access, page accessed, referrer, user agent. Legal basis: Art. 6 (1) (f) GDPR — legitimate interest in technically reliable operation. Retention: 7 days, then automatic deletion. No merger with other data sources takes place.

4. Contact

If you contact us via form, email or phone — including product demo, use-case check, callback or product enquiries — we store the information you provide to process the enquiry and for follow-up questions. Depending on the form this may include first and last name, company, email address, phone number where provided, message or context text, selected use cases or process scope, source/page URL, language and timestamps. The request is stored as an internal lead/request record in WordPress and mirrored into our self-hosted CRM/list management inside WordPress (FluentCRM) for 1:1 follow-up. A request does not create a newsletter subscription. Legal basis: Art. 6 (1) (b) GDPR (pre-contractual measures) and Art. 6 (1) (f) GDPR (legitimate interest in answering and managing B2B enquiries). Retention: deletion as soon as the enquiry has been finally processed, at the latest after 12 months, unless statutory retention obligations apply.

4a. Direct appointment booking via Brevo Meetings

Buttons for direct appointment booking open a Brevo Meetings booking form embedded in the trax website. The external form is loaded only after you activate the booking function; a directly shared booking link loads it when the booking page is opened. Provider: Sendinblue, SAS (Brevo), 9–17 rue Salneuve, 75017 Paris, France. When the form is loaded, Brevo processes technical connection data such as IP address, browser/device information, request time and referrer URL. If you book an appointment, we process your first and last name, email address, phone number, company, answer regarding the GxP work case and appointment details. Brevo adds these data to our contact database and records the meeting booking; the contact is not automatically added to a marketing list and the booking does not create a newsletter subscription. Brevo sends the booking confirmation and the configured email reminders. Our connected Outlook calendar is used by Brevo to compare availability, prevent double bookings and create or update the appointment in Microsoft 365/Exchange. We use these data to schedule and conduct the requested meeting. Legal basis for our processing: Art. 6 (1) (b) GDPR (pre-contractual appointment) and Art. 6 (1) (f) GDPR (efficient B2B scheduling). We review the appointment and contact data stored in Brevo and the connected calendar for continued necessity no later than after 12 months and delete them unless statutory retention obligations or an ongoing business context require further storage. Details are available in the [Brevo Privacy Policy](#). You can alternatively contact us by email without using the booking form.

5. Lead magnets (PDF downloads)

To request our practical guides (e.g. our “10 GxP-AI Prompt Patterns”) we ask for your name, business email address, company and role; if you also request a callback, we may additionally ask for a phone number. We also store the requested material, source/page URL, language, newsletter opt-in status and callback request status. The data is used to provide the requested material, document the request and handle any requested follow-up. Legal basis: Art. 6 (1) (b) GDPR (requested material / pre-contractual request), Art. 6 (1) (f) GDPR (legitimate interest in B2B lead management) and, where you separately opt in to the newsletter, Art. 6 (1) (a) GDPR. Retention: until withdrawal, at most 24 months. The newsletter subscription is offered as a separate opt-in checkbox on the lead-magnet form (no coupling — you can request the material without subscribing). No marketing emails are sent without separate consent.

5a. Newsletter (double opt-in)

Procedure: If you sign up for our newsletter, we use the double-opt-in procedure: after entering your email address and name you receive a confirmation email with a verification link. Only after you click that link do we activate the subscription and document your consent.

Data: email address, name where provided, language/source, subscription status, request timestamp, confirmation timestamp and a single-use confirmation token or confirmation log.

Purpose: sending the monthly traqx newsletter with practice insights, plus documentation of the consent process pursuant to Art. 7 (1) GDPR.

Legal basis: Art. 6 (1) (a) GDPR (consent), § 7 (2) No. 3 UWG.

Retention: for as long as your subscription is active; consent logs are additionally retained for 3 years after the end of the subscription as evidence in the event of complaints.

Withdrawal: every newsletter contains an unsubscribe option in the footer. Alternatively a short email to info@traqx.io is sufficient.

Processor: transactional emails and the newsletter are sent via the Google Workspace SMTP relay (Google Ireland Limited, Gordon House, Barrow Street, Dublin 4, Ireland); the Google Workspace data-processing agreement applies. Recipient, list and sequence management for the newsletter is self-hosted in WordPress / FluentCRM. The separate processing for webinar registrations is described in section 5b.

5b. Webinar registration, email communication and Microsoft Teams

Procedure and purpose: If you register for a specific traqx webinar, we use the data you enter to verify your email address by double opt-in, create your personal access to that Microsoft Teams webinar, send the confirmation, event reminders and event-related follow-up, and document the registration. No newsletter subscription is created. Microsoft Teams attendee emails are disabled; the event-specific communication is sent by traqx through Brevo.

Data: first name, last name, business email address, company, selected event, language/source, request and confirmation timestamps, privacy and process version, pseudonymised security metadata, Microsoft Teams registration ID and personal join link, delivery/status data and, where available after the event, attendance status. The personal join link must not be forwarded because it is assigned to the registration.

Legal basis: Art. 6 (1) (b) GDPR for the requested registration and delivery of the webinar, including the operational emails needed for it; Art. 6 (1) (f) GDPR for abuse prevention, technical evidence and reliable event operation. General newsletters or unrelated marketing require a separate legal basis and are not activated by the webinar registration.

Processors: event-specific email delivery, contact-list separation and automation are provided by Sendinblue GmbH (Brevo), Köpenicker Straße 126, 10179 Berlin, Germany, under a data-processing agreement. The live session and personal event registration are provided through Microsoft Teams by Microsoft Ireland Operations Limited, One Microsoft Place, South County Business Park, Leopardstown, Dublin 18, Ireland, under the Microsoft Products and Services Data Protection Addendum. Both provider groups may involve processing outside the EEA under their applicable transfer safeguards, including EU Standard Contractual Clauses and, where applicable, the EU-US Data Privacy Framework. Further information: [Brevo privacy policy](#) and [Microsoft privacy statement](#).

Retention and cancellation: the active event record, event-specific Brevo list membership and operational delivery data are deleted or anonymised no later than 90 days after the event, unless a complaint, security incident or statutory obligation requires longer retention. A minimal registration and verification record may be retained for up to 3 years to evidence the requested communication. You can stop further webinar emails at any time using the event-specific unsubscribe link in every message or by emailing info@traqx.io. This does not create an unsubscribe from other communications you may have requested separately.

5c. Retention overview & justifications

A consolidated view of all retention periods with the rationale behind each one — the principle: minimal storage, clear purpose, documented basis.

DATA CATEGORY	RETENTION	JUSTIFICATION
Server logs	7 days	Sufficient for technical fault analysis & security forensics — Art. 6 (1) (f) GDPR. IP anonymisation kicks in immediately on log close.
Contact enquiries	12 months	B2B sales cycles in pharma typically run 6–9 months. 12 months covers follow-ups without unnecessary stockpiling. Statutory retention (e.g. § 257 HGB) only applies once a contract is concluded.
Appointment bookings	12-month review period	Needed to arrange, conduct and follow up on the requested B2B meeting. At the end of the review period, deletion takes place unless the record is still required or statutory retention obligations apply.
Lead magnets	up to 24 months	Until withdrawal; the 24-month cap covers documentation of the request, any consent and a typical re-engagement cycle. Withdrawal at any time, deletion within 7 days of request.
Newsletter subscription	active subscription + 3 yrs consent log	Email + name only as long as the subscription is active. The consent log (request and confirmation timestamps, source/status and confirmation record) is retained for 3 years to cover the statutory limitation period (§ 195 BGB) for complaints under § 7 UWG.
Webinar registration	event + 90 days; minimal record up to 3 yrs	Operational data and event-specific list membership are needed only for delivery and short event-related follow-up. A reduced request/verification record may be retained to evidence the requested communication.
Cookies (incl. analytics)	30 min – 14 months	Per tool, detailed in 6.9. GA4 capped at 14 months (the GA4 minimum; shorter is only possible via property reset); all other tools are below or at industry standard.

DATA CATEGORY	RETENTION	JUSTIFICATION
Cookiebot consent	12 months	Maximum window the EDPB considers reasonable for repeat consent requests. After 12 months a fresh banner appears.

6. Cookies, analytics & tracking

This website uses analytics and tracking tools that go beyond pure reach measurement and create usage profiles. Personal data may be processed (in particular IP address, device and browser information, behaviour data) and transferred to third countries (including the USA). Legal basis is your consent pursuant to § 25 (1) TDDDG and Art. 6 (1) (a) GDPR. Consent is granted on your first visit via our cookie banner and can be withdrawn at any time with effect for the future — see section 6.10 below. Withdrawal is as simple as granting consent (Art. 7 (3) GDPR); the lawfulness of processing carried out on the basis of consent prior to withdrawal remains unaffected.

6.0 Consent management (Cookiebot)

PROVIDER	Cybot A/S, Havnegade 39, 1058 Copenhagen, Denmark (a Usercentrics company) — EU-based provider.
PURPOSE	Cookiebot is the consent management platform (CMP) we use to document your consent in line with § 25 TDDDG and Art. 7 GDPR and to block analytics and tracking tools until you opt in.
DATA	Cookiebot stores a "CookieConsent" cookie containing your consent state (categories, timestamp, anonymous identifier) and a server-side consent log.
RETENTION	up to 12 months from the moment consent is given; renewed on the next visit after expiry.
LEGAL BASIS	the processing of the consent data itself rests on Art. 6 (1) (c) GDPR (legal obligation to document consent).
THIRD-COUNTRY TRANSFER	primary processing in the EU; sub-processors may include service providers outside the EEA under EU Standard Contractual Clauses.
DATA PROCESSING AGREEMENT	concluded with Cybot A/S.

6.1 Google Analytics 4

PROVIDER	Google Ireland Limited, Gordon House, Barrow Street, Dublin 4, Ireland (parent company: Google LLC, USA).
----------	---

PURPOSE Tracking tool that goes beyond pure reach measurement. Google uses the collected data for the operation of GA4 and partly for its own purposes (to that extent no commissioned processing in the narrow sense).

DATA pseudonymous identifiers (client ID), IP address (shortened on an EU server, see below), page views, dwell time, scroll depth, click events, device and browser information, approximate location (country / region from IP).

RETENTION up to 14 months for event-level data, then automatic deletion.

IP SHORTENING The IP address is shortened on an EU server before being forwarded to the USA (the "_anonymizelp" equivalent in GA4 is active by default).

THIRD-COUNTRY TRANSFER processing on servers in the USA. Safeguards: EU Standard Contractual Clauses and the EU-US Data Privacy Framework (adequacy decision of 10 July 2023). Note: the supervisory authorities point out that the legal certainty gained may only be temporary; the predecessor regimes (Safe Harbor, Privacy Shield) were invalidated by the CJEU.

DATA PROCESSING AGREEMENT concluded with Google Ireland Ltd.

6.2 Microsoft Clarity

PROVIDER Microsoft Ireland Operations Ltd., One Microsoft Place, South County Business Park, Leopardstown, Dublin 18, Ireland (parent: Microsoft Corporation, USA).

PURPOSE Session recordings and heatmaps to improve usability. Note: session recordings are a particularly intensive form of processing — they can capture sensitive content even though input fields are masked by default. We have configured the strictest masking level ("Strict") for all form fields.

DATA mouse movements, clicks, scroll behaviour, page views, device and browser information, shortened IP address, country.

RETENTION up to 12 months from the last recorded session.

THIRD-COUNTRY TRANSFER Microsoft is a US group; data may be processed on servers in the USA. Safeguards: EU Standard Contractual Clauses and the EU-US Data Privacy Framework. The reservations noted above for GA4 apply analogously.

DATA PROCESSING AGREEMENT Microsoft Online Services DPA concluded.

6.3 Leadfeeder (Dealfront)

PROVIDER Dealfront Germany GmbH (Leadfeeder), Markgrafenstraße 36, 10117 Berlin, Germany — EU-based provider.

PURPOSE	B2B identification of visiting companies based on commercially licensed IP-address databases (e.g. RIPE, ARIN, public corporate IP ranges) to inform our sales outreach. The aim is identification of the company, not of an individual user. Important note from a data protection perspective: IP addresses can constitute personal data, particularly when combined with other data. We therefore treat Leadfeeder processing as relevant under the GDPR.
DATA	IP address, page views, timestamp, dwell time, referrer.
DATA SOURCES	Dealfront enriches IP data with publicly available company information and licensed B2B databases.
RETENTION	up to 12 months on visit level; aggregated reports may be retained longer.
THIRD-COUNTRY TRANSFER	Dealfront operates primarily on EU infrastructure; sub-processors may include US service providers under EU Standard Contractual Clauses.
DATA PROCESSING AGREEMENT	concluded with Dealfront Germany GmbH.

6.4 Google Ads (conversion tracking & remarketing)

PROVIDER	Google Ireland Limited, Gordon House, Barrow Street, Dublin 4, Ireland (parent: Google LLC, USA).
PURPOSE	We use Google Ads conversion tracking and (where activated) remarketing to measure the success of advertising campaigns and to address visitors with relevant ads.
DATA	pseudonymous click ID (gclid), conversion event, conversion timestamp, device and browser information. Cookies used include "_gcl_au" (conversion linker) and "test_cookie" (technical test cookie from doubleclick.net).
RETENTION	"_gcl_au" up to 90 days; conversion logs in the Google Ads account according to Google's retention settings.
THIRD-COUNTRY TRANSFER	processing on Google servers, including in the USA. Safeguards: EU Standard Contractual Clauses and the EU-US Data Privacy Framework.
DATA PROCESSING AGREEMENT	concluded with Google Ireland Ltd.

6.5 LinkedIn Insight Tag

PROVIDER	LinkedIn Ireland Unlimited Company, Wilton Plaza, Wilton Place, Dublin 2, Ireland (parent: LinkedIn Corporation, USA).
PURPOSE	The LinkedIn Insight Tag enables campaign measurement, audience analytics and (where activated) retargeting for LinkedIn ad campaigns.
DATA	IP address (truncated), timestamp, page URL, device characteristics, LinkedIn member ID where the visitor has been logged in to LinkedIn. Cookies used include "bcookie", "lidc", "bscookie".

RETENTION up to 6 months for directly identifying data; aggregated campaign reports may be retained longer.

THIRD-COUNTRY TRANSFER processing on LinkedIn servers, including in the USA. Safeguards: EU Standard Contractual Clauses and the EU-US Data Privacy Framework.

DATA PROCESSING AGREEMENT concluded with LinkedIn Ireland Unlimited Company.

6.6 Google Tag Manager

PROVIDER Google Ireland Limited (see 6.1).

PURPOSE Google Tag Manager (GTM) is a tag-management system that loads other tracking tags on this website (e.g. Google Analytics, Google Ads, LinkedIn Insight Tag). GTM itself does not set any cookies and does not collect personal data per se; it only orchestrates the tags loaded after consent.

DATA technical request data (IP address, timestamp, user agent) is briefly processed by Google's GTM loader server. GTM itself sets no persistent identifier.

THIRD-COUNTRY TRANSFER the GTM loader is hosted on Google infrastructure, including in the USA. Safeguards as in 6.1.

NOTE we have configured GTM so that no measurement tag fires before you have given consent via our Cookiebot banner.

6.7 Cloudflare (CDN & bot management)

PROVIDER Cloudflare, Inc., 101 Townsend Street, San Francisco, CA 94107, USA, with EU representative Cloudflare Germany GmbH, Rosental 7, c/o Mindspace, 80331 Munich.

PURPOSE Cloudflare is used by our hosting provider as a content delivery network (CDN) and security layer. The "__cf_bm" cookie is set by Cloudflare's bot management to distinguish humans from automated traffic in real time and to mitigate DDoS attacks and content scraping.

NECESSITY Without bot mitigation our website would be vulnerable to credential stuffing, scraping and DDoS attacks that would compromise availability, integrity and the security of the personal data we process (e.g. lead-magnet form submissions, newsletter sign-ups). Bot mitigation is therefore a technical security measure within the meaning of Art. 32 GDPR (security of processing). Cloudflare itself classifies "__cf_bm" as "strictly necessary" ([Cloudflare cookie documentation](#)). Forgoing Cloudflare bot management would weaken the security of personal-data processing on this site.

DATA IP address, request headers, technical fingerprint of the request. No persistent, cross-site identifier.

RETENTION the "__cf_bm" cookie expires after at most 30 minutes of inactivity. Aggregated security logs at Cloudflare are retained briefly under Cloudflare's standard retention.

LEGAL BASIS § 25 (2) No. 2 TDDDG (technically required for the service requested by the user) and Art. 6 (1) (f) GDPR (overriding legitimate interest in a secure, available website).

THIRD-COUNTRY TRANSFER Cloudflare is a US group; data may be processed on servers in the USA. Safeguards: EU Standard Contractual Clauses and the EU-US Data Privacy Framework (adequacy decision of 10 July 2023). Note: the legal certainty of the framework may be limited; annulment proceedings are pending before the General Court of the EU (case T-553/23).

DATA PROCESSING AGREEMENT concluded as part of the hosting contract.

6.8 Google Search Console

PROVIDER Google Ireland Limited (see 6.1).

PURPOSE Google Search Console (GSC) lets us monitor how this website performs in Google's search results — indexing status, search queries that lead to the site, click-through rates and technical crawl errors.

COOKIES / TRACKING GSC itself sets no cookies on visitors of this website and loads no client-side script. Ownership of the domain is verified via a static HTML meta tag and / or a DNS TXT record.

DATA aggregated search analytics from Google (search queries, impressions, clicks) — not directly linked to individual visitors. The data is made available to us in aggregated form only.

LEGAL BASIS Art. 6 (1) (f) GDPR — legitimate interest in monitoring the site's search visibility.

THIRD-COUNTRY TRANSFER the aggregated reports are generated on Google infrastructure (including the USA). Safeguards as in 6.1.

6.9 Cookie storage durations

Session cookies are deleted when the browser is closed. Persistent cookies have the following maximum lifetimes: Google Analytics 4 — up to 14 months (data retention shortened to 14 months in the GA4 settings); Microsoft Clarity — up to 12 months; Google Ads ("_gcl_au") — up to 90 days; LinkedIn ("bcookie") — up to 6 months; Cloudflare ("__cf_bm") — at most 30 minutes of inactivity; Leadfeeder — typically session-based, no client-side storage; CookieConsent (Cookiebot) — up to 12 months from the moment consent is given.

6.9a Cookie declaration

6.10 Withdrawal of consent

As easy as granting it — you can withdraw your consent at any time with effect for the future:

1. **Open the cookie settings:** click the "Cookie settings" link in the footer to re-open the banner and adjust your choice (this controls GA4, Clarity, Google Ads, LinkedIn and Leadfeeder alike).

2. **By email:** send a short message to info@traqx.io — we will block the relevant tools for you.
3. **Per tool:** for Google Analytics the official browser opt-out is available; for Google Ads via the ad personalisation settings; for LinkedIn via the LinkedIn opt-out. Microsoft Clarity and Leadfeeder are controlled exclusively via our cookie banner.

The lawfulness of processing carried out on the basis of consent prior to withdrawal remains unaffected (Art. 7 (3) GDPR).

7. Web fonts

This website uses self-hosted web fonts delivered from our own website assets. During normal page views no separate request to Google Fonts is made for font delivery. Legal basis for local font delivery is Art. 6 (1) (f) GDPR — legitimate interest in a consistent, performant and privacy-friendly typographic presentation.

8. Technical and organisational measures (TOM)

To protect your data we implement appropriate technical and organisational measures pursuant to Art. 32 GDPR — among them: TLS encryption (HTTPS) for the entire site, encrypted database connections, server hosting in the EU (Kinsta / GCP Frankfurt), restricted admin access via individual accounts with strong passwords and 2FA, regular automatic backups, role-based access control, a documented record of processing activities pursuant to Art. 30 GDPR, and data minimisation at the application level. We review and update these measures continuously.

9. Your rights as a data subject

Under the GDPR you have the following rights:

- **Right of access** (Art. 15 GDPR) — information about which of your personal data we process.
- **Right to rectification** (Art. 16 GDPR) — correction of inaccurate data.
- **Right to erasure** (Art. 17 GDPR) — deletion of your data where the legal conditions are met.
- **Right to restriction of processing** (Art. 18 GDPR).
- **Right to data portability** (Art. 20 GDPR) — receipt of your data in a structured, commonly used, machine-readable format.

- **Right to object** (Art. 21 GDPR) — to processing based on legitimate interest, including direct marketing. See the highlighted notice below.
- **Right to withdraw consent** (Art. 7 (3) GDPR) — at any time with effect for the future, see section 6.10.
- **Right to lodge a complaint** (Art. 77 GDPR) — with a supervisory authority, in particular in the EU member state of your residence, your workplace or the place of the alleged infringement. Competent supervisory authority for our registered office: Unabhängiges Datenschutzzentrum Saarland (Independent Data Protection Centre Saarland), Fritz-Dobisch-Straße 12, 66111 Saarbrücken.

Special notice · Art. 21 GDPR

Right to object pursuant to Art. 21 GDPR. You have the right, on grounds relating to your particular situation, at any time to object to processing of personal data concerning you which is based on Art. 6 (1) (f) GDPR (legitimate interests), including profiling based on those provisions. If you object, we will no longer process the personal data unless we can demonstrate compelling legitimate grounds that override your interests, rights and freedoms, or unless the processing serves the establishment, exercise or defence of legal claims. Where personal data is processed for direct marketing purposes, you have the right to object at any time; following an objection, the personal data will no longer be processed for such purposes.

How to exercise the right: a short email to info@traqx.io is sufficient. We confirm receipt and act within the statutory time limits.

Requests regarding these rights are to be directed to: info@traqx.io. We respond within the statutory period (usually one month).

10. Currency of this privacy policy

Last updated: 25 July 2026. We reserve the right to adapt this policy so that it always meets current legal requirements. The current version can always be retrieved from this website.