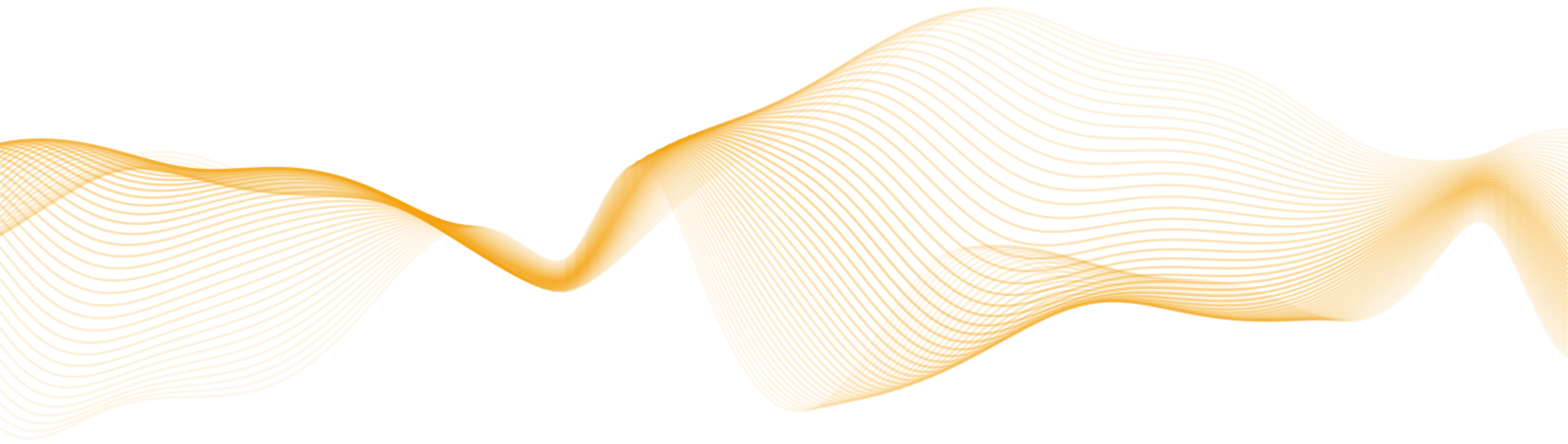
techtropy

Privacy notice



Operator

techtropy GmbH
Am Anger 1
87672 Roßhaupten
Germany
Amtsgericht Kempten (Allgäu)
HRB 19212

Version of

November 21, 2026

This English version is a translation. Where it differs, the German version (https://techtropy.com/de/datenschutzerklaerung) prevails.

This privacy notice explains how techtropy GmbH (“we”) processes personal data when you visit our website or use the service.

1 Controller

1.1 The controller for processing personal data in connection with the service is techtropy GmbH, Am Anger 1, 87672 Roßhaupten, Germany. Contact details are listed in the legal notice (https://techtropy.com/legal-notice).

1.2 For privacy questions, reach us at: privacy@techtropy.com.

2 Our role

For your account, the website and its statistics, our emails and logs, email enquiries, the strategy fox on the home page, support requests, vulnerability reports and the market research in Intelligence we are the controller. For your membership, your roles, the content you submit to an organization and the records of a simulation the controller is our customer for which the organization is kept in the service, for example your university or your employer. We process that data on its behalf under the data processing agreement (https://techtropy.com/data-processing-agreement). Questions about it go to that customer.

3 Data we process

3.1 You give us your name and email address when you create an account or submit content. Both are required for an account. We process them to perform the contract for your account (Article 6 (1) (b) GDPR) and keep them until you delete your account. A customer may also give us your name and email address itself, to invite you, for example to a seminar. The customer is then the controller for your membership, and we process it on its behalf.

3.2 If you write to us by email, we process your name, your email address and your message to answer it (Article 6 (1) (f) GDPR, or (b) where it concerns a contract). We delete the message within a year after the matter is settled, unless commercial or tax law requires us to keep it, as a business letter for six years or as an accounting record for eight (Section 257 HGB, Section 147 AO, Article 6 (1) (c) GDPR). For a report of a security vulnerability the period stated for it below applies.

3.3 When a support request is sent from your organization, or you reply to one, we process your name, your email address and the text of the request in order to answer it (Article 6 (1) (b) and (f) GDPR). Your organization's administrators and our team see the request. It is deleted with the organization, or earlier on request.

3.4 If you report a security vulnerability to us, we process your name, your email address and the content of your report in order to handle it (Article 6 (1) (f) GDPR). We delete them 3 years after the report is closed, except a name you asked us to publish and the message in which you asked for it, which we keep as long as your name is published. If you ask to be named, we publish your name on the page of our vulnerability disclosure policy (https://techtropy.com/vulnerability-disclosure) until you withdraw your consent (Article 6 (1) (a) GDPR).

3.5 Documents and strategies that an organization's teams submit to Strategy we process on the customer's behalf. When a person calls an AI feature, the text concerned goes to a model, as described under data transfer and in the AI transparency notice (https://techtropy.com/ai-transparency-notice).

3.6 Our servers write technical data to log files. That is your IP address, browser type, the pages requested, and the date and time. We use this data only to run the service reliably, to secure it and to detect abuse (Article 6 (1) (f) GDPR). The log files have a fixed size, and the oldest entries are overwritten continuously. Warnings and errors of the service are also kept for 30 days, with the identifier of the account concerned.

3.7 For each day you are signed in, we store that your account was active that day, nothing more. We use it to count how many people use the service and whether they return (Article 6 (1) (f) GDPR). The record is deleted with your account.

3.8 With each sign-in we store your IP address and your browser's identification, such as its name, version and operating system, so that we can investigate misuse of your account (Article 6 (1) (f) GDPR). We delete both when you sign out or delete your account. Otherwise a sign-in expires at the latest 30 days after you last used it, and we delete both within a day after that.

3.9 We count page views without cookies and without storing anything on your device. For each view we store the kind of page, the referring website, a campaign or document code carried by the link, your country, the type of device, browser and operating system, and whether you were signed in (Article 6 (1) (f) GDPR). The records are deleted after 25 months.

3.10 To recognize several page views on the same day, we form a pseudonym from your IP address, your browser identifier and a random value that is new each day and deleted the next. After that the pseudonym cannot be traced back to you. We never store the address or the identifier, and we never link page views to your account.

3.11 For every email we send, we store the recipient address, the subject, the kind of email and the delivery status our email delivery provider reports. This lets us show that an email was delivered and fix problems (Article 6 (1) (f) GDPR). We delete the content as soon as the email is sent. The record is deleted after 90 days, or earlier with your account.

3.12 If you ask the strategy fox on our home page a question, we store the question, the answer, the sources named, the language, the time and your rating, to check and improve the answers (Article 6 (1) (f) GDPR). We store nothing that identifies you, neither an account nor your IP address nor a browser identifier, so we cannot relate a stored question to you or delete it for you specifically (Article 11 GDPR). Do not write personal data into a question. We hold your IP address briefly in memory only, to limit how many questions arrive at once. The records are deleted after 90 days.

3.13 To limit questions per visitor and day, we also count each question to the strategy fox without its content, with the time, the outcome and the tokens used, under the daily pseudonym described above (Article 6 (1) (f) GDPR). The count is deleted after 25 months.

3.14 The cookie notice (https://techtropy.com/cookie-notice) explains which cookies we set and why.

4 Simulations of business customers

4.1 Inside a simulation we record which pages and sections you open, when you arrived and how long you stayed, and your moves, such as a changed decision field. The other people in the simulation see which page you are on right now and whether you have gone idle. We process this on behalf of the customer your organization belongs to. That customer is the controller for it and informs you about the legal basis. The customer decides whether a facilitator sees the time per page for each person or only the total per company. Only the simulation is recorded, nothing you do elsewhere in the service.

4.2 A simulation evaluates no person, and the customer may not use the service to recruit, select, assess or monitor employees or job candidates, or to decide on their employment, tasks, promotion or dismissal.

4.3 We delete the page visits recorded in a simulation after 365 days, or earlier with your account. Your moves stay with the company in the simulation. If you delete your account, we remove your name from them.

5 Simulations in education

5.1 Inside a simulation we record which pages and sections you open, when you arrived and how long you stayed, and your moves, such as a changed decision field or a committed period. The other people in the room and the instructor see which page you are on right now and whether you have gone idle. We process this on behalf of the customer that runs the simulation, which is the controller for it and informs you about the legal basis. It decides whether the instructor sees the time per page for each person or only the total per company. Only the simulation is recorded, nothing you do elsewhere in the service.

5.2 We delete the page visits recorded in a simulation after 365 days, or earlier with your account. Your moves stay with the company in the simulation. If you delete your account, we remove your name from them.

6 Agent credentials and connected apps

6.1 If you create an agent credential or connect an app such as an AI assistant, an agent can act as you in one of your organizations. For each credential we store its name, the organization, the access it grants, its creation, last use and expiry, and the first characters and a hash of the credential, never the whole credential. We store a connected app's name, the address it returns you to and your consent, and its tokens only as hashes. The legal basis is performance of the contract for your account (Article 6 (1) (b) GDPR).

6.2 Our log files record which agent credential a request came through but never contain the credential itself or the data sent with it. This serves to secure the service and detect abuse (Article 6 (1) (f) GDPR).

6.3 A change an agent makes in an organization names the agent credential it came through, which is why a revoked credential is kept. A connected app's tokens are deleted when they expire or the credential is revoked. Deleting your account or the organization deletes the credential itself.

6.4 The organization's administrators see each agent credential's name, owner, access, creation, last use and expiry, never the credential itself, and can revoke one or not allow credentials at all.

6.5 What an agent reads goes to the app it runs in, which you chose. The app's provider is not our processor, and what happens to the data there is outside this notice.

7 Data not obtained from you

7.1 We read public sources for the market research in Intelligence, namely news articles, company websites, job postings, public registers and companies' mandatory filings. In doing so we process the name of an article's author and the name, professional position and employer of people named in the text, together with the context in which they were published. The legal basis is our legitimate interest in verifiable market research (Article 6 (1) (f) GDPR). Recipients are our customers with access to Intelligence and the service providers named under sharing of data.

7.2 We keep an entry as long as market research needs it, and source text only as long as an entry cites it. If you object, we keep your name alone, so that it is not recorded again, for as long as your objection stands.

7.3 You have the rights set out below. Because informing every person individually would involve disproportionate effort, we inform you here (Article 14 (5) (b) GDPR).

8 Purposes and legal bases

We use your data to provide the service and your account (Article 6 (1) (b) GDPR) and to communicate with you, improve the service and detect abuse and technical problems (Article 6 (1) (f) GDPR). We make no decision based solely on automated processing that produces legal effects concerning you or similarly significantly affects you (Article 22 GDPR), and we do not rate individual people.

9 Data retention

The periods are stated above with each kind of data. Backups of the service are kept for 7 days and serve only to restore it. When you delete your account, we delete the data belonging to it unless a statutory retention duty prevents this. Content you submitted to an organization stays with it.

10 Data transfer

10.1 The data of the service is held on servers in Germany, and our providers for hosting and sending email are based in the European Union.

10.2 Messages you send to our email addresses are held by our mailbox provider, which is based in Switzerland and stores them on its own servers in Switzerland, Germany or Norway. For Switzerland the European Commission has found an adequate level of protection (Decision 2000/518/EC, Article 45 GDPR).

10.3 For features that use an AI model we engage a provider in the USA, which receives the text processed in each case and passes it to the provider of the model in use, which may be located in the USA or another third country. We allow only model providers that do not retain the text after processing, except where required by law or to prevent misuse, and do not use it for training. The transfer is based on the European Commission's standard contractual clauses (Article 46 (2) (c) GDPR), a copy of which we provide on request.

11 Sharing of data

11.1 We share data with service providers that process it on our behalf under Article 28 GDPR, namely (a) dataforest GmbH, Kriftel, Germany, for hosting our servers, (b) AhaSend B.V., Amsterdam, Netherlands, for sending emails, (c) OpenRouter Inc., New York, USA, which routes requests from AI features to the providers of the models in use, and (d) Proton AG, Plan-les-Ouates, Switzerland, for the mailboxes of our email addresses, which hold the messages you send us.

11.2 Where you work in an organization, its members see your name and the content you submit there.

11.3 Beyond the recipients named in this notice, we share data only where the law requires it or to enforce our rights.

12 Access by our team

Named members of our team can open an organization to support it, to keep it secure and to set up what was ordered. We log every such access for 365 days, and the organization's administrators can read the log.

13 Transactional emails

13.1 Transactional emails, such as sign-in codes and invitations, are sent for us by an email delivery provider in the European Union, which processes your email address on our behalf under Article 28 GDPR and only to deliver them. A sign-in code email, and the email that tells you your recovery phrase was used, also state the IP address and the time, so that you can recognize a sign-in or request that was not yours (Article 6 (1) (f) GDPR). We delete the content of these emails as soon as they are sent.

13.2 The emails that state an IP address also name the country it belongs to, looked up in a database on our own server. The database is IP to Country Lite by DB-IP, Creative Commons Attribution 4.0: IP Geolocation by DB-IP (https://db-ip.com/).

14 Your rights

14.1 You have the right to access your data (Article 15 GDPR), to rectification (Article 16), to erasure (Article 17), to restriction of processing (Article 18) and to data portability (Article 20).

14.2 You can complain to a data protection supervisory authority (Article 77 GDPR), for example the one competent for us, the Bavarian State Office for Data Protection Supervision (Bayerisches Landesamt für Datenschutzaufsicht, BayLDA), Promenade 18, 91522 Ansbach, Germany.

14.3 Where processing rests on your consent, you can withdraw it at any time with effect for the future (Article 7 (3) GDPR).

15 Right to object

You can object at any time where we process data on the basis of our legitimate interest (Article 21 (1) GDPR), which is stated above with each kind of data. After your objection we no longer process your data, unless we demonstrate compelling legitimate grounds that override your interests or the data serves to assert or defend against legal claims. An email is enough: privacy@techtropy.com.

16 Security

We protect your data with technical and organizational measures under Article 32 GDPR, which the data processing agreement (https://techtropy.com/data-processing-agreement) describes.

17 Changes to this privacy notice

This version was published on the date stated above. Before a material change applies, we inform everyone with an account by email and in the service when they next use it.