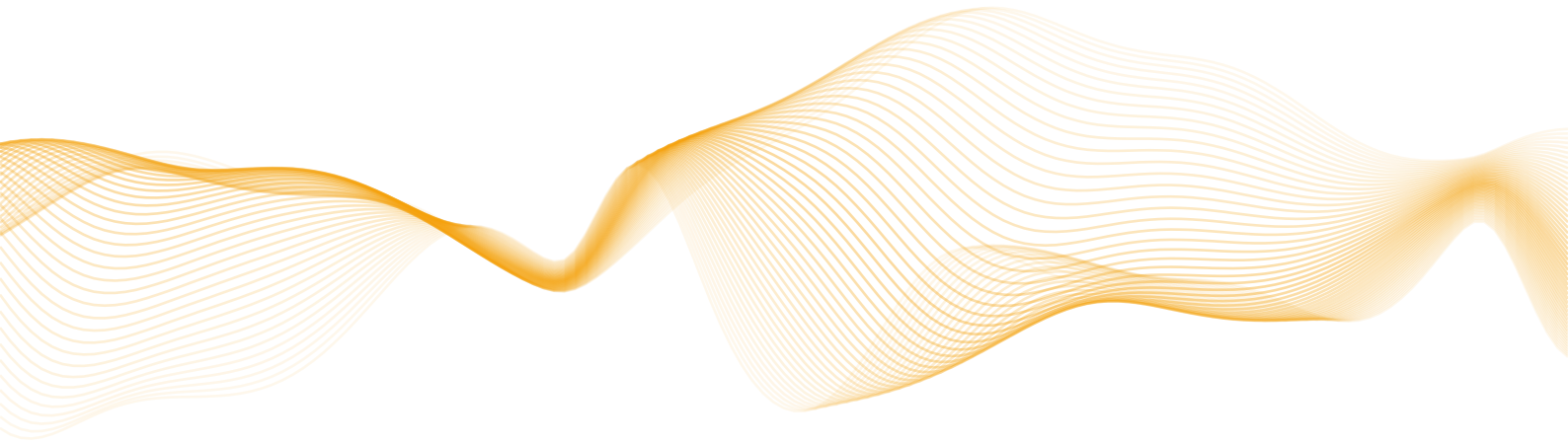
techtropy

Data processing agreement



Customer (controller)

Organization

Address

Processor

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/auftragsverarbeitungsvertrag) prevails.

This is the data processing agreement under Article 28 GDPR (“Agreement”) between the Customer as defined in the terms of service (“Terms”), as controller (“Customer”), and techtropy GmbH, Am Anger 1, 87672 Roßhaupten, Germany, as processor (“we”). “Service” and “organization” have the meaning the Terms give them. “Users” within the meaning of this Agreement are the members of the Customer's organization and the people it invites. Where an agent acts with a User's agent credential, that counts as the User acting (3.6). The Customer is the controller of the personal data its Users submit to the Service and that arises about them there, except where we are the controller under 2.1.

1 How it applies

1.1 This Agreement forms part of the Terms (https://techtropy.com/terms-of-service). It applies to every Customer on whose behalf we process personal data.

1.2 This Agreement is concluded in an electronic format (Article 28 (9) GDPR) when a person authorized to represent the Customer accepts the Terms for it.

1.3 Where this Agreement and the Terms disagree on data protection, this Agreement applies. Otherwise the Terms apply, including for governing law, place of jurisdiction and changes to this Agreement.

1.4 Annexes 1 to 6 form part of this Agreement.

2 Roles

2.1 For the Users' accounts, server logs, page statistics, the email log and support requests we are the controller ourselves, as the privacy notice (https://techtropy.com/privacy-notice) describes. We process a User's membership in the Customer's organization and that User's roles and content on the Customer's behalf.

2.2 There is no joint controllership under Article 26 GDPR.

3 Instructions

3.1 We process the data the Customer is responsible for only to run the Service and only on the Customer's documented instructions.

3.2 The Customer gives instructions (a) through the settings of the Service, (b) by using the features of the Service, and (c) in text form through its administrators to the address stated in section 14.

3.3 Processing that is necessary to set up the ordered products, support the Customer's Users and keep the Service secure also counts as instructed.

3.4 The Customer pays us reasonable remuneration for extra effort that is caused by instructions, audits or support and goes beyond running the Service, unless we are responsible for that effort.

3.5 When one of the Customer's Users calls an AI feature, the Customer thereby instructs us to transmit the text to the sub-processor that Annex 3 names for AI features, which is located in a third country.

3.6 What one of the Customer's Users reads or changes through an agent credential or a connected app is processing on the Customer's instruction, like the User's own use of the Service. The app is not our sub-processor.

3.7 The Customer is responsible for the lawfulness of the processing and for safeguarding the data subjects' rights, and informs them under Articles 13 and 14 GDPR.

3.8 Annexes 4 and 5 add instructions for each kind of Customer.

3.9 If Union or Member State law to which we are subject requires us to process the data otherwise, we inform the Customer of that legal requirement before processing, unless that law prohibits such information on important grounds of public interest.

3.10 If we consider that an instruction infringes the GDPR or other Union or Member State data protection provisions, we inform the Customer immediately. We may suspend carrying out the instruction until the Customer confirms or changes it.

4 Anonymous statistics

The Customer instructs us to form anonymized, aggregated analyses from the simulation's data that identify neither a person nor the Customer.

5 Confidentiality and access

5.1 Everyone we authorize to process data is bound to confidentiality.

5.2 Only named members of our team can open an organization. We record each such access with the person, the time and what was done, keep the record for 365 days and show it to the organization's administrators.

6 Sub-processors

6.1 The Customer gives us general authorization to engage the sub-processors named in Annex 3. Each of them is bound by contract to data protection obligations that match in substance those we have under this Agreement (Article 28 (4) GDPR). We remain liable to the Customer for their performance.

6.2 Except in the cases in Annex 3, we process the data only in the European Union or the European Economic Area. The Customer allows a further transfer to a third country through the procedure for new sub-processors, and it takes place only under Chapter V GDPR.

6.3 Ancillary services without a specific link to the Service, such as telecommunications, postal and transport services or maintenance, are not sub-processing. We keep confidentiality there too.

6.4 If we want to add or replace a sub-processor, we tell the Customer's administrators at least 30 days in advance by email.

6.5 The Customer may object on reasonable data protection grounds until the change takes effect and must state those grounds. If we then find no reasonable solution, either side may terminate the affected products as of the date the change takes effect. In that case we refund prepaid fees pro rata.

7 Security

7.1 We take the technical and organizational measures under Article 32 GDPR described in Annex 2.

7.2 We may change the measures as long as their level of protection is not lowered. On request we explain them to the Customer in more detail, in confidence.

7.3 Backups are stated in Annex 6.

8 Security incidents

8.1 If we learn of a personal data breach affecting data the Customer is responsible for, we inform its administrators by email without undue delay, and at the latest within 48 hours. The notice contains what Article 33 (3) GDPR requires, as far as known, and we add to it as soon as we know more.

8.2 We inform authorities and data subjects only on the Customer's instruction.

8.3 We support the Customer in its duties under Articles 32 to 36 GDPR, as far as we have the information.

9 Rights of data subjects

9.1 We support the Customer with appropriate measures in answering data subjects' requests under Articles 15 to 22 GDPR.

9.2 A request that reaches us directly we forward to the Customer without undue delay and do not answer ourselves. The same applies to requests from authorities and third parties about the data for which the Customer is responsible, as far as the law allows.

10 Audit and evidence

10.1 We give the Customer the information it needs to demonstrate compliance with the obligations under Article 28 GDPR and this Agreement.

10.2 We allow audits by the Customer or by an auditor it appoints who is bound to confidentiality, and we contribute to them.

10.3 An audit is announced at least 14 days in advance and takes place during our business hours and, without a specific reason, a maximum of once a year. It may not disturb the Service or reach other Customers' data.

10.4 Where a current audit report or certification, including our hosting provider's, answers the question, that evidence suffices.

11 Liability

11.1 As between the parties, we are not liable for damage that results from our following an instruction of the Customer, provided we met our duty to inform under 3.10. Our unlimited liability under the Terms, in particular for intent, gross negligence and injury to life, body or health, remains unaffected. Otherwise the limitation of liability in the Terms applies.

11.2 Liability toward data subjects under Article 82 GDPR is unaffected.

12 Return and deletion

12.1 When an organization is deleted or the processing ends, the Customer may request the return of its data in a common machine-readable format for 30 days thereafter. After that we delete the data with all copies, unless the law requires us to keep it. Backup copies follow within 7 days.

12.2 We confirm the deletion on request.

12.3 When a User deletes their own account, their contributions stay with the Customer.

13 Language

This Agreement is available in German and English. In the event of a discrepancy or doubt as to interpretation, the German version alone prevails.

14 Contact

Address for this Agreement and for questions about this page: dpa@techtropy.com.

A1 Annex 1 on the processing

A1.1 The subject matter is running the Service for the Customer in the products it has ordered.

A1.2 We store the data, compute with it, display it and transmit it to the people the Customer authorizes.

A1.3 The purpose is the collaboration of the Customer's Users, the running of its seminars and simulations, and the support of the Customer by our team.

A1.4 Processing lasts until the data is returned or deleted under this Agreement.

A1.5 The data subjects are the Customer's Users and the people who appear in the Customer's content.

A1.6 The data comprises name, email address, the permissions per product, the teams and the content created, including uploaded documents. In the simulation, the moves, each person's current page and the time per page are added.

A1.7 Special categories of personal data under Article 9 GDPR are not the subject of the Service, and the Customer does not bring them in.

A2 Annex 2 on technical and organizational measures

A2.1 Connections to the Service over public networks are encrypted with TLS 1.3, for older clients with TLS 1.2 and forward secrecy, and use a hybrid post-quantum key exchange where the client supports it. The Service reaches its database over TLS 1.3 as well, and servers and databases are not reachable from the internet directly.

A2.2 The volumes that hold the database, the file storage and the containers are encrypted with LUKS2 and AES-256 in XTS mode, and the keys that unlock them are kept apart from these volumes. This protects the data when a volume or a copy of it leaves the server, but not against the hosting provider or access to the running server.

A2.3 Support requests are additionally encrypted in the application with AES-256-GCM under a key of the organization's own, so that a copy of the database alone does not reveal them.

A2.4 Sign-in uses one-time codes by email, with limits on how often they are sent and checked, and roles and permissions decide what a person sees and may change.

A2.5 Members of our team also sign in with a second factor, and their access rights are separated by task.

A2.6 We record every access by our team to an organization under 5.2.

A2.7 The Service accesses the database with a role that may read and write data but not change the database's structure.

A2.8 The applications run in hardened containers without administrator rights and with a read-only file system.

A2.9 We store agent credentials, OAuth tokens and invitation tokens only as hashes.

A2.10 Data is kept separate per organization, and every query is limited to the organizations of the requesting person.

A2.11 The server checks input against defined schemas before it processes it.

A2.12 We rehearse every change to the database structure on a copy of the database before it is deployed, and we additionally back up the database before such a deployment.

A2.13 dataforest keeps the daily backups under Annex 6 in Frankfurt.

A2.14 How we restore the database and file storage is set down in writing.

A2.15 We check every minute that the Service is reachable and are notified by email when it is down.

A2.16 The Service deletes simulation visits and access records automatically after the periods in the privacy notice.

A2.17 We remove secrets, tokens and cookies from logs, and email addresses appear only masked. Warnings and errors of the Service, which we keep for 30 days, contain no IP addresses.

A2.18 Our hosting provider dataforest GmbH operates an information security management system certified to ISO/IEC 27001 (TÜV Saarland) and data centers in Frankfurt am Main.

A2.19 On every change we check the dependencies, and on every deployment the container images, automatically for known vulnerabilities. Before a release that touches sign-in or access rights, we review the changes for security separately.

A3 Annex 3 on sub-processors

A3.1 dataforest GmbH, Kriftel, Germany. Hosting of our servers in data centers in Frankfurt, Germany.

A3.2 AhaSend B.V., Amsterdam, Netherlands. Sending of emails, processed in the European Union.

A3.3 OpenRouter Inc., New York, USA. Passes text to the provider of the AI model in use when a User calls an AI feature. The model providers are further sub-processors of OpenRouter. OpenRouter selects and replaces them and binds them by contract to data protection obligations equivalent to its own (Article 28 (4) GDPR). The model providers may be located in the USA or another third country. We have every call routed only to 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. OpenRouter shows which providers these currently are at Provider Logging (https://openrouter.ai/docs/guides/privacy/provider-logging). The Customer agrees that a change among these model providers is communicated through the list published there. The Customer may object to a model provider at any time on reasonable data protection grounds. The second and third sentences of 6.5 then apply correspondingly, and the termination takes effect when it is received. For OpenRouter itself 6.4 and 6.5 apply. The transfer is based on the European Commission's standard contractual clauses (Article 46 (2) (c) GDPR).

A3.4 Proton AG, Plan-les-Ouates, Switzerland. Mailboxes of our email addresses, such as the address in section 14. Proton processes data for which the Customer is the controller only where a message to or from one of these addresses contains such data, for example an instruction from an administrator or a data subject's request that we forward to the Customer. This concerns the names and email addresses of the people writing and named, and the content of the message. Proton stores the messages on its own servers in Switzerland, Germany or Norway. For Switzerland the transfer is based

on Commission Decision 2000/518/EC of 26 July 2000, which finds an adequate level of protection there and remains in force under Article 45 (9) GDPR.

A4 Annex 4 for business customers

A4.1 This Annex applies to Customers that use the Service as business customers, as recorded for their organization.

A4.2 The people in the same simulation see which page the others are on and whether they have gone idle, and the simulation records page visits and moves per person.

A4.3 Only a facilitator the Customer appoints sees the time per page, per person or only per company, as the Customer decides in the settings of its organization.

A4.4 Where a works council exists, the Customer obtains its consent before it evaluates the time per page per person (Section 87 (1) no. 6 BetrVG).

A4.5 The Customer does not use the Service (a) to recruit, select, assess or monitor employees or job candidates, or (b) to decide on their employment, tasks, promotion or dismissal.

A5 Annex 5 for educational institutions

A5.1 This Annex applies to universities, business schools and other Customers that use the Service in teaching, as recorded for their organization.

A5.2 In a simulation, the Customer decides in the settings of its organization whether the instructor sees the time per page for each person or only the total per company.

A5.3 Where required, the Customer obtains the consent of its works council or staff council before it evaluates the time per page per person (Section 87 (1) no. 6 BetrVG or the corresponding provision of staff-representation law).

A6 Annex 6 on instances

A6.1 An organization's data is held on the shared instance of the Service or, where agreed, on a dedicated instance with its own database and file storage. Only backups hold copies of it.

A6.2 dataforest backs up each instance daily and keeps the last 7 backups.

A6.3 A backup serves only to restore the instance.

A6.4 An instance reports to us only operating totals that name no person and contain no content of an organization.

Only the prevailing German version is signed: https://techtropy.com/de/auftragsverarbeitungsvertrag.pdf