LEGAL

Data Processing Agreement (DPA)

Part of the Terms, version 2.12 · Effective November 13, 2026

This is a translation for information only. The binding text is the German Auftragsverarbeitungsvertrag (AVV). It is part of the Korpus Terms of Service and applies automatically as soon as you store other people's personal data for a company or another organisation in a team on a paid plan; no signature is needed. It does not apply to purely private use. PDF of this version · PDF of the binding German text

§ 1 Parties, subject matter, term

(1) This agreement applies between the provider of Korpus (processor, Annex 1) and the user of Korpus who processes personal data in bundles of a team on a paid plan (Pro or Business) for purposes that are not purely personal or household (Art. 2(2)(c) GDPR), as controller (the "customer"). Whoever uses Korpus for a company or another organisation concludes this agreement for it and warrants being authorised to do so; it is then the customer. This agreement does not apply to teams on the free plan; there, the customer stores no personal data of other people for such purposes (§ 6 of the Terms).

(2) The agreement is concluded in electronic form when the Terms are accepted (Art. 28(9) GDPR). It applies to the service the provider runs at `korpus.cloud`. Korpus in a dedicated instance or in the customer's own AWS account (Business) is governed by a separate contract.

(3) Its subject matter is providing Korpus under the Terms. In doing so, the provider processes the content the customer stores in the bundles of these teams on the customer's behalf.

(4) The agreement applies while a team of the customer is on a paid plan, and after that to the data stored until then, until the customer has deleted it; it ends with the Terms at the latest. § 4(1) (confidentiality) and § 10 (deletion) continue to apply.

§ 2 Nature and purpose, data, data subjects

(1) **Nature of the processing:** storing, organising, showing, searching, linking, copying, exporting and deleting content, and making it available to the people, teams, agents and connected apps the customer gives access.

(2) **Purpose:** providing Korpus and support at the customer's request. What the provider opens bundles and checks content automatically for as a controller of its own is set out in § 3(4) and (6).

(3) **Types of data:** all personal data that the customer, or members, agents and apps on its behalf, store in bundles: texts, files and their metadata, such as relations, tags and mentions, plus the bundles' change log (who changed what and when). Special categories under Art. 9 GDPR must not be stored (§ 8 of the Terms).

(4) **Data subjects:** people whose data the customer stores, typically the customer's employees, customers, prospects, suppliers and business partners and their contact persons, and members of its teams and people it shares bundles with.

(5) Not covered are the account, billing, audit and security data the provider processes as a controller of its own; the Privacy Policy covers those.

§ 3 Instructions

(1) The provider processes the data only on the customer's documented instructions, including for transfers to third countries (Art. 28(3)(a) GDPR). The instructions are this agreement and the use of Korpus by the customer and those it authorises. If the law requires the provider to process otherwise, it tells the customer beforehand, unless the law forbids it.

(2) The customer gives further instructions in text form to me@till-it-works.de. Anything beyond Korpus's features the parties agree separately.

(3) If the provider considers that an instruction infringes data protection law, it tells the customer without delay. It may suspend carrying it out until the customer confirms or changes it.

(4) The provider opens bundles read only, and only in the cases of § 6 of the Terms. At the customer's request (support), it acts on the customer's instruction. For the security of the service, against abuse or unlawful content, to meet a legal duty and to review a submitted publication, it opens bundles as a controller of its own, as far as needed for that purpose (Privacy Policy B.7). Content reaches no AI app and no AI model in doing so, except in the review of a version the customer submitted for publication in the catalog. Every opening is recorded in the audit trail; on request, the provider tells the customer the openings of its bundles.

(5) What the customer or its agent writes in a support ticket or a message to the provider, it passes to the provider as a controller of its own (Privacy Policy B.9). The customer includes only what is needed to handle it.

(6) For the operation, security and quality of the service, for example to detect abuse, security risks and unlawful or harmful content, to check versions submitted for publication beforehand and to sort support tickets, the provider may check content automatically as a controller of its own, also with AI models, as far as needed for that purpose (Privacy Policy B.7). It uses AI models for this only at the sub-processors named in Annex 3, and only so that the data is not used to train AI models. The result of a check is a hint: a person decides on every measure that affects the customer, such as a rejection, a block or a deletion. An automated check is not an opening under (4); if the provider then looks at a bundle, (4) applies.

§ 4 Duties of the provider

(1) The provider gives access to the data only to people who are bound to confidentiality or under a statutory duty of secrecy (Art. 28(3)(b) GDPR); only such people are given a role with access to content.

(2) The provider does not use the data for purposes of its own, except in the cases of § 3(4) and (6). It does not sell it and does not use it to train AI models.

(3) The provider keeps a record of processing activities under Art. 30(2) GDPR and cooperates with the supervisory authority on request.

(4) The provider is not required to designate a data protection officer (§ 38(1) BDSG). The contact for data protection is the owner (Annex 1).

§ 5 Technical and organisational measures

(1) The provider takes the measures under Art. 32 GDPR described in Annex 2.

(2) The measures follow technical progress. The provider may replace them with equivalent or better ones; the level of protection of Annex 2 must not fall. It documents material changes in Annex 2. It reviews the measures regularly and on every material change to the service.

§ 6 Sub-processors

(1) The customer gives general authorisation to engage sub-processors (Art. 28(2) GDPR). Those named in Annex 3 are authorised.

(2) The provider tells the customer at least 14 days before it adds or replaces a sub-processor, by email to the address of its account and in Annex 3. If it must replace a sub-processor at short notice, for security or because the sub-processor stops its service, it tells the customer without delay afterwards. Within 14 days of being told, the customer may object to the change in text form for an important data protection reason. If the provider keeps the change, either party may terminate the Terms without notice; fees paid in advance for the time after are refunded pro rata. Otherwise the change applies once the period has passed.

(3) The provider engages sub-processors only if they are bound by contract to data protection duties that meet Art. 28(4) GDPR (Annex 3). It is liable for them as for its own acts, within § 12.

(4) Services the customer connects or uses itself are not sub-processing, in particular AI apps it connects to its bundles, nor are services of controllers of their own that get no content (Annex 3).

§ 7 Data subjects' rights

(1) Korpus lets the customer fulfil access, rectification, erasure and portability itself: content can be read, changed, exported and deleted at any time.

(2) If a data subject contacts the provider, it refers them to the customer, where it can tell who that is, and forwards the request to the customer without delay. Without an instruction, it does not answer itself.

(3) The provider gives further assistance (Art. 28(3)(e) GDPR) on request; the customer pays for the effort as agreed beforehand, unless the request results from a breach by the provider.

§ 8 Assistance and personal data breaches

(1) The provider assists the customer with the duties under Art. 32 to 36 GDPR, taking into account the nature of the processing and the information available to it, first through this agreement and its annexes. Further assistance, for example with a data protection impact assessment, is given on request; the customer pays for the effort as agreed beforehand, unless it is needed because of a breach by the provider.

(2) The provider reports a personal data breach affecting the customer's data without undue delay after becoming aware of it, by email to the owner of the team the bundle concerned is in. The report contains, as far as known, the information under Art. 33(3) GDPR; what is not yet known follows later. The provider takes reasonable measures to contain the breach. Where the breach results from a breach of duty by the provider, it assists the customer with its notifications under Art. 33 and 34 GDPR free of charge. A report is not an admission of fault.

§ 9 Place of processing

(1) The data is stored and processed in the EU, at the locations named in Annex 3. Where Annex 3 names a location outside the European Economic Area, paragraph 2 applies.

(2) Where a sub-processor processes data in a third country, or a third country can access it, for example because the sub-processor belongs to a company in the USA, the transfer rests on the safeguards under Art. 44 et seq. GDPR named in Annex 3, such as an adequacy decision or standard contractual clauses. The data is also encrypted in transit and at rest (Annex 2).

(3) Transfers the customer causes itself, for example to connected AI apps, to people it shares with, or by an export, are its own responsibility.

§ 10 Deletion and return

(1) The customer can export its content at any time, files included, as one archive, and delete it. The export is the return under Art. 28(3)(g) GDPR.

(2) When the customer deletes content, a bundle or its account, the provider removes the database records at once; copies in backups and deleted or replaced files lapse within the periods of the Privacy Policy (B.12), at the latest after 35 days.

(3) If the Terms end without the customer having deleted its account, the provider deletes the customer's content within 30 days of the end; until then the customer can export it. Paragraph 2 then applies to files and backups.

(4) The provider keeps the audit trail (account IDs and events, no content) and support tickets as the Privacy Policy sets out (B.8, B.9, B.12). Statutory retention duties are not affected.

(5) Copies made by other users with the customer's access, and the customer's contributions to other users' bundles, belong to those bundles and are handled under those users' agreements.

(6) On request, the provider confirms the deletion in text form.

§ 11 Evidence and audits

(1) The provider demonstrates compliance through this agreement and its annexes, through information in text form and, for the infrastructure, through the publicly available certifications and audit reports of its sub-processors (for AWS, for example ISO/IEC 27001 and BSI C5).

(2) If that is not enough in a particular case, the customer may carry out an inspection itself or through an auditor bound to confidentiality who is not a competitor of the provider. It takes place remotely first, by providing documents and in a video call, and on site only if that is not enough. It is announced at least 30 days ahead in text form, takes place during business hours without disrupting operations, and at most once per calendar year; the notice period and frequency do not apply where a breach affecting the customer's data or an order of the supervisory authority gives cause. Other customers' data and the provider's trade secrets are excluded. Sub-processors' data centres are not visited; paragraph 1 applies to them.

(3) Each party bears its own costs.

(4) The provider allows audits by the competent supervisory authority.

§ 12 Liability

(1) Liability towards data subjects follows Art. 82(1) to (4) GDPR and is not affected by this agreement.

(2) Between the customer and the provider, § 10 of the Terms and the following paragraphs apply to all claims under or in connection with this agreement, including recourse under Art. 82(5) GDPR.

(3) The provider is liable without limitation for intent and gross negligence, including that of its legal representatives and vicarious agents, for injury to life, body or health, for fraudulently concealed defects (§ 444 BGB), under a guarantee and under the Product Liability Act.

(4) For slight negligence, the provider is liable only for breach of a material contractual obligation, meaning an obligation that makes proper performance of the agreement possible in the first place and on whose fulfilment the customer may regularly rely, and only for the damage typical and foreseeable for this kind of contract.

(5) If the customer is a business (§ 14 BGB), a legal entity under public law or a special fund under public law, liability under paragraph 4 is limited per damaging event to the higher of: the fees paid for Korpus to the provider or to the seller of Pro (§ 4 of the Terms) in the 12 months before the event, or EUR 25,000. Several breaches with the same cause count as one damaging event.

(6) For all damaging events in a contract year together, liability under paragraph 5 is limited to the higher of: the fees under paragraph 5, or EUR 50,000. A contract year is twelve months; the first starts when the customer first accepts the Terms.

(7) For loss of data, the provider is liable under paragraphs 4 to 6 only for the effort that restoring it would have taken had the customer exported its content at reasonable intervals.

(8) Paragraphs 4 to 7 also apply to liability for sub-processors (§ 6(3)) and to the personal liability of the provider's vicarious agents. Each paragraph of this section stands on its own; if one is invalid, the others remain.

(9) Statements in this agreement and its annexes describe services and measures; they are a guarantee only where expressly called one.

§ 13 Final provisions

(1) Where this agreement conflicts with the Terms, it prevails on data protection. Liability is governed solely by § 10 of the Terms and § 12 of this agreement. The customer's own templates or terms for data processing apply only if the provider accepts them in text form.

(2) Changes to this agreement follow § 13 of the Terms: what affects the customer's rights or obligations takes effect only once it accepts it in the app. Changes to Annex 3 follow § 6(2); changes to Annex 2 under § 5(2) take effect without acceptance.

(3) German law applies. The place of jurisdiction follows § 14 of the Terms.

(4) The German version is binding, even though the Terms are otherwise in English (§ 14 of the Terms). This English translation is for information only.

(5) If a provision is invalid, the rest of the agreement remains valid; the statutory rule takes its place.

(6) The customer can save this version as a PDF at any time. On request, the provider confirms in text form when the customer's account accepted it, and sends it unchanged and signed by the provider.

Annex 1: Parties and contacts

Processor:

Tilman Krauß
Till IT works
Bismarckstraße 17a
42799 Leichlingen
Germany

Data protection: me@till-it-works.de. No data protection officer designated (§ 38(1) BDSG). Competent supervisory authority: Landesbeauftragte für Datenschutz und Informationsfreiheit Nordrhein-Westfalen (LDI NRW).

Controller: the customer, as given in its account; the contact is that account's email address.

Annex 2: Technical and organisational measures (Art. 32 GDPR)

1. Confidentiality

- **Physical access:** The provider runs no servers of its own. Its sub-processors' data centres are physically secured as their certifications attest (for AWS, for example ISO/IEC 27001, BSI C5).
- **System access:** sign-in through a managed sign-in service (Amazon Cognito) with a passkey, a one-time code sent to the email address or, where offered, a sign-in provider the person chooses. Access tokens are valid for at most 1 hour, refresh tokens for at most 30 days. Keys for programs expire after at most 1 year, lapse when left unused, and can be revoked at any time. Only a hash of tokens and keys is stored. Details: Privacy Policy B.4 and B.12.
- **Data access:** rights per bundle (read, write, or single paths), checked on every request in the application and again in the database (row level security). Agents never get more rights than the person they act for. Each service signs in to the database as a user of its own with a short-lived IAM token, without a stored password; users' requests run under a role that cannot bypass row level security. The provider's inspection only under § 3(4), read only and logged; automated checks only under § 3(6). The pipeline that rolls out new versions cannot sign in to the database (an explicit deny in its roles); schema changes run in a separate function.
- **Operations:** the provider's administrative access only with multi-factor authentication or a passkey. Its work devices are encrypted, with a screen lock and current security updates.
- **Separation:** bundles are kept apart in the database by row level security. Production and development run in separate AWS accounts; development uses no production data.
- **Encryption:** transport with TLS 1.2 or higher, also to the database, with the certificate checked. The database (Amazon Aurora) and files (Amazon S3) are stored encrypted (AES-256, with keys managed by AWS). Files are reachable only through individually signed links that expire after at most 15 minutes; public access to the storage is blocked.
- **Lean logs:** the audit trail holds account IDs, not email addresses; a bundle's change log holds account ID and username. Error logs are designed to hold no content and are deleted after at most 30 days (Privacy Policy B.11, B.12).

2. Integrity

- **Transfer:** encrypted only. Exports wait behind a signed link, are deleted after one day and then lapse like deleted files (§ 10(2)).
- **Input:** every bundle keeps a change log (who, when, which path, which change). Security-relevant events are kept in the audit trail (§ 10(4)).

3. Availability and resilience

- The database storage is replicated across several availability zones. The database is backed up continuously, can be restored to an earlier point in time (backups at most 35 days) and is protected against deletion.
- Deleted or replaced files can be recovered for a limited time (§ 10(2)).
- The application runs serverless across several availability zones. A web application firewall in front of the web app and throttling on every interface limit overload.

4. Regular review

- The infrastructure is described as code. Every change is reviewed, tested automatically, including the access rules, and rolled out by a pipeline.
- The measures are reviewed regularly and on every material change to the service (§ 5(2)).
- Personal data breaches are reported under § 8(2); their cause is fixed and documented.
- Sub-processors are engaged only under a contract per Art. 28 GDPR (Annex 3).

Annex 3: Sub-processors

Company	Service	Location	Safeguards
Amazon Web Services EMEA SARL, 38 Avenue John F. Kennedy, L-1855 Luxembourg	Cloud infrastructure: computing, database, file storage, sign-in, email delivery, delivery of the web app; AI models on Amazon Bedrock (also Anthropic's) for automated checks (AVV § 3(6))	EU (Frankfurt); Amazon Bedrock only in AWS regions within the EU; the web app's code, no content, also through edge locations worldwide	AWS Data Processing Addendum; EU-US Data Privacy Framework and standard contractual clauses (2021/914)
Anthropic Ireland, Limited, 6th Floor, South Bank House, Barrow Street, Dublin 4, D04 TR29, Ireland	AI models through the Anthropic API for automated checks (AVV § 3(6)); the data is not used for training	USA (Anthropic, PBC and its sub-processors)	Anthropic Data Processing Addendum; standard contractual clauses (2021/914)

Not sub-processors, because they get no customer content or are controllers of their own:

- The seller of Pro (§ 4 of the Terms) and its payment service, as controllers of their own (Privacy Policy B.5).
- Sign-in providers a person chooses, for example Google or Microsoft, as controllers of their own; they get no content.
- The provider's email service for email to it, under its own responsibility (Privacy Policy B.14); no content of bundles or support tickets reaches it.
- AI apps and programs the customer connects itself: recipients under its responsibility (§ 6(4)).