LEGAL

Data Processing Agreement

Annex 1 to the General Terms and Conditions

Version 2.1 · valid from 18 November 2026

Structify Solutions UG (haftungsbeschränkt) · Gartenstraße 8 · 92348 Berg · Germany · Amtsgericht Nürnberg HRB 46012
The version published at structify.solutions/rechtliches is authoritative. In the event of discrepancies between the German and the English version, the German version prevails.

Data Processing Agreement

Annex 1 to the General Terms and Conditions of Structify Solutions UG (haftungsbeschränkt)
Version 2.1 · valid from 18 November 2026

The German version prevails.

Preamble – Parties and Conclusion

(1) This Data Processing Agreement (DPA) applies between the Customer as controller within the meaning of Article 4(7) GDPR (the "Controller") and Structify Solutions UG (haftungsbeschränkt), Gartenstraße 8, 92348 Berg, Germany, Local Court (Amtsgericht) of Nuremberg HRB 46012, as processor within the meaning of Article 4(8) GDPR ("Structify").

(2) The Controller is an entrepreneur (Unternehmer) within the meaning of Section 14 of the German Civil Code (BGB) or a legal entity under public law.

(3) This DPA is an annex to and forms part of Structify's General Terms and Conditions (the "Terms"). It is concluded in Text Form upon their acceptance by a person authorised to represent the Controller; this electronic format satisfies Article 28(9) GDPR. A separate signature is not required. Structify logs the time and the version of the acceptance. The DPA can be accessed and saved at any time at structify.solutions/rechtliches/avv.

(4) If the parties have concluded an individual data processing agreement, that agreement takes precedence (§ 11).

§ 1 Subject Matter and Duration

(1) The subject matter is the processing of personal data on behalf of the Controller in the provision of the products Structify (in the browser, for macOS and Windows and for iOS and Android) and Structify Operate and of the underlying platform (together the "Platform") under the contract that the parties have concluded on the basis of the Terms (the "Main Agreement").

(2) The DPA begins with the Main Agreement and ends with it, without the need for termination. Obligations relating to erasure, return and confidentiality continue to apply after the end of the contract.

§ 2 Nature, Purpose and Place of Processing

(1) The nature and purpose of the processing, the types of data and the categories of data subjects are described for each product in Schedule 1 to this DPA.

(2) Hosting and storage of the Platform data take place in Germany (EU), in data centres of Hetzner Online GmbH in Nuremberg and Falkenstein. For AI analyses (voice, text, images), Structify uses US providers (OpenAI, Anthropic); further service providers with a third-country connection are listed in Schedule 3. Transfers to third countries take place only in accordance with § 8.

§ 3 Obligations of Structify (Article 28(3) GDPR)

Structify
a) processes personal data only on documented instructions from the Controller, including with regard to transfers to third countries, unless Structify is required to process them by Union or Member State law; in such a case, Structify informs the Controller of that legal requirement beforehand, unless that law prohibits it. If Structify considers an instruction to be unlawful, Structify informs the Controller without undue delay and may suspend its execution until it is confirmed or amended;

b) ensures that all persons authorised to process the data have committed themselves to confidentiality or are under a statutory obligation of confidentiality, including after the end of their activity;
c) takes all technical and organisational measures required under Article 32 GDPR in accordance with Schedule 2 and develops them further in line with the state of the art, without falling below the agreed level of protection;
d) complies with the conditions for sub-processors under § 5;
e) assists the Controller by appropriate measures in responding to requests from data subjects (Articles 12 to 23 GDPR), in particular through access, rectification, erasure and export functions, and forwards requests received by Structify to the Controller without undue delay;
f) assists the Controller with the obligations under Articles 32 to 36 GDPR, in particular with notifications of personal data breaches, communication to data subjects, data protection impact assessments and prior consultations;
g) after the end of the provision of services, deletes all personal data or makes them available for export, unless there is an obligation to store them (§ 10);
h) makes available all information necessary to demonstrate compliance with the obligations under Article 28 GDPR and allows for audits in accordance with § 7.

§ 4 Instructions

(1) This DPA and the Main Agreement constitute the documented instructions. The use of the Platform features in accordance with the contract by the Controller, its users and the external parties it has invited is deemed an instruction for the corresponding processing. This also covers transfers that the Controller initiates itself, for example to calendar or storage services in its own accounts, to project participants or by email. This also applies to the map display of the location where photos were taken: the map section from the OpenStreetMap Foundation is only loaded when a user expressly requests it („Karte laden“ ("Load map")); the user's browser then retrieves the map directly from the OpenStreetMap Foundation, which acts as an independent controller in doing so and is not a sub-processor.

(2) The Controller is responsible for the lawfulness of the processing and for the rights of the data subjects. This includes informing data subjects, for example where employees or third parties are captured in photos or voice recordings or where location data relating to recordings are stored.

(3) The Controller issues individual instructions in Text Form, for example by email to support@structify.solutions; it confirms oral instructions in Text Form without undue delay. The persons authorised to issue instructions are the Controller's legal representatives, the persons designated by them in Text Form and the users with the Management role.

(4) If an individual instruction requires services beyond the contractual scope, Structify may demand reasonable remuneration for the additional effort, provided that Structify points this out in advance.

(5) **Two-factor authentication.** Structify provides two-factor authentication for all user accounts and expressly recommends that it be set up (Schedule 2 No. 1). Whether the Controller's users set up a second factor is the responsibility of the Controller and its users; the Controller takes this into account in its own assessment of the appropriateness of the security measures (Article 32 GDPR) and, by means of appropriate instructions to its users, works towards their setting it up. Where damage results from a second factor offered not having been set up, it is attributable to the Controller as between the parties, unless an infringement of the GDPR or of this DPA by Structify, for example a security vulnerability of the Platform, contributed to causing the damage; in that case, the damage is apportioned in proportion to the respective contribution to causation (§ 11(1), Article 82(4) and (5) GDPR, Section 254 BGB). Liability towards data subjects under Article 82 GDPR remains unaffected.

§ 5 Sub-processors

(1) The Controller grants Structify general authorisation to engage other processors (sub-processors) (Article 28(2) GDPR). The sub-processors engaged are listed in Schedule 3; the current list is available at structify.solutions/rechtliches.

(2) **Prior information.** Structify informs the Controller in Text Form **at least 30 days in advance** of any intended addition or replacement of a sub-processor. The information states the name, registered office, service, data location and the basis of any third-country transfer.

(3) **Objection.** The Controller may object to the change in Text Form **within 14 days of receipt** of the information for an important reason relating to data protection. If the Controller does not object in due time, the change is deemed approved; Structify points out the deadline and this consequence in the information.

(4) If the Controller objects with justification, the parties seek an amicable solution, for example that the new sub-processor is not used for this Controller. If this is not successful, the Controller may terminate the Main Agreement with effect from the date of the change; Structify refunds, on a pro rata basis, fees already paid for the period thereafter.

(5) **Urgent cases.** If Structify has to replace a sub-processor at short notice because the sub-processor discontinues its service or there is a significant security risk, the period under paragraph 2 may be shorter. Structify then informs the Controller without undue delay; the right of objection and termination under paragraphs 3 and 4 remains in place.

(6) Structify imposes on each sub-processor by contract the same data protection obligations as set out in this DPA (Article 28(4) GDPR) and is liable to the Controller for their compliance.

§ 6 Notification of Personal Data Breaches

(1) Structify notifies the Controller of any breach of the security of the data processed on its behalf without undue delay after becoming aware of it. The notification contains, where available, the information under Article 33(3) GDPR; Structify provides any missing information in phases without undue further delay.

(2) Structify assists the Controller with the obligations under Articles 33 and 34 GDPR and documents every breach. The assessment of the notification obligation, the notification to the supervisory authority and the communication to data subjects are the responsibility of the Controller.

§ 7 Audits

(1) The Controller may satisfy itself of compliance with this DPA before the start of and during the processing. Structify provides evidence primarily by means of current self-assessments, reports from independent bodies, where available, and evidence from the sub-processors.

(2) Where necessary, Structify allows on-site inspections by the Controller or by an auditor bound to confidentiality who is not a competitor of Structify, after reasonable notice in Text Form, during normal business hours, without disproportionate disruption and while safeguarding trade secrets and the data of other customers.

(3) Each party bears its own costs. For audits without specific cause that take place more than once per calendar year, Structify may demand reasonable remuneration; audits for a specific cause remain unaffected.

§ 8 Transfers to Third Countries

(1) Hosting and storage of the Platform data take place in Germany (EU), in data centres of Hetzner Online GmbH: the database in the data centre in Nuremberg, and the file storage and the encrypted backup copies

in the data centre in Falkenstein.

(2) A transfer to a country outside the EU and the European Economic Area (third country) takes place only if the conditions of Articles 44 et seq. GDPR are met. The basis for all sub-processors with a third-country connection is the **standard contractual clauses adopted by the European Commission** under Article 46(2)(c) GDPR (Commission Implementing Decision (EU) 2021/914), **Module Three** (transfer from processor to processor). Structify is the data exporter, and the respective sub-processor is the data importer. Structify passes on the Controller's instructions to the sub-processor.

(3) If a sub-processor is certified under the EU-U.S. Data Privacy Framework (adequacy decision (EU) 2023/1795), Schedule 3 states this in addition. The certification does not replace the standard contractual clauses; if it ceases to apply, the standard contractual clauses remain authoritative. Structify checks the information in the official register at least once a year.

(4) For each sub-processor with a third-country connection, Structify has assessed the consequences of the transfer (Clause 14 of the standard contractual clauses) and has laid down supplementary measures, in particular transport encryption, the contractual exclusion of training AI models with content, the limitation of the storage period at the sub-processor, the selection of a processing region in the EU where available, and data minimisation. The assessment is reviewed at least once a year and in the event of material changes.

(5) On request, the Controller receives a copy of the standard contractual clauses and a summary of the assessment; trade secrets and security details may be redacted.

§ 9 No AI Training, Anonymised Statistics

(1) Structify has contractually agreed with all AI providers that they will not use the Controller's content for training AI models.

(2) Structify itself does not use the Controller's content for training AI models unless the Controller has given its express consent in accordance with § 14(2) of the Terms. Such consent is an instruction within the meaning of § 4; it may be withdrawn at any time.

(3) **Anonymised usage statistics.** The Controller instructs Structify to aggregate usage events (which feature was used and when, timestamps and technical metrics), without content, into anonymous, consolidated statistics. Structify may use these anonymous statistics for its own purposes, namely to improve the products, to safeguard operations, to plan capacity and to substantiate its own performance claims. Anonymisation is carried out in such a way that a link to a person and a link to the individual Controller can no longer be established; raw data containing personal data are deleted after aggregation, at the latest after 90 days. Once anonymised, the statistics are no longer subject to this DPA.

§ 10 Term, End of the Contract and Erasure

(1) After the end of the Main Agreement, the Controller's previous users have **read-only access for 30 days** in order to view and export data (§ 25 of the Terms). Export in common, machine-readable formats constitutes the return of the data within the meaning of Article 28(3)(g) GDPR. The Controller may request a different form of return against reimbursement of the effort involved.

(2) After the 30 days have expired, Structify erases all personal data processed on behalf of the Controller. Structify erases them earlier on instruction. On request, Structify confirms the erasure in Text Form.

(3) Data are not removed individually from backup copies. They expire with the respective backup state, in the database after six months at the latest and in the file storage after 90 days (Schedule 2 No. 3), and are protected against any further processing until then. The confirmation of erasure points this out.

(4) Structify restricts the processing of data that it is required to retain under Union or Member State law and erases them once the retention period has expired.

(5) The confidentiality obligations continue to apply after the end of the contract.

§ 11 Liability and Order of Precedence

(1) Article 82 GDPR applies to liability towards data subjects. As between the parties, each party is liable for the part of the damage that is attributable to its breach of the GDPR or of this DPA. Otherwise, the liability provisions of the Terms apply, unless mandatory law provides otherwise.

(2) In matters of data protection, this DPA takes precedence over the Terms, the Terms of Use and any other agreements. An individual data processing agreement between the parties takes precedence over this DPA. Mandatory law, in particular the GDPR, takes precedence over all contractual provisions.

§ 12 Controllers in Switzerland

If the Controller is established in Switzerland or the processing is subject to the Swiss Federal Act on Data Protection (FADP), the following applies in addition:
a) References to the GDPR include the corresponding provisions of the FADP.
b) The competent supervisory authority for processing under the FADP is the Federal Data Protection and Information Commissioner (FDPIC).
c) Under Swiss law, Germany and the EU are deemed to be states with an adequate level of data protection. For transfers to third countries, the standard contractual clauses under § 8 apply with the adaptations for Switzerland recognised by the FDPIC.
d) The term "Member State" in the standard contractual clauses includes Switzerland, so that data subjects habitually resident in Switzerland can enforce their rights there.

For Controllers in Liechtenstein, the GDPR applies directly; the competent authority is the Data Protection Authority of Liechtenstein (Datenschutzstelle Liechtenstein).

§ 13 Final Provisions

(1) The law of the Federal Republic of Germany applies, excluding the United Nations Convention on Contracts for the International Sale of Goods, including for Controllers established in Austria, Switzerland or Liechtenstein; mandatory data protection law at the Controller's place of establishment remains unaffected.

(2) Amendments to this DPA are made in accordance with the procedure for amendments to the Terms (§ 26 of the Terms). In addition, § 5 applies to new or replaced sub-processors.

(3) This DPA is available in German and English; in the event of any discrepancy, the German version prevails.

(4) If any provision is invalid, the remaining provisions remain valid; the invalid provision is replaced by the statutory provisions, in particular the GDPR.

Schedule 1 – Description of the Processing by Product

A. Common to all products

Nature of the processing: collection, recording, organisation, storage, adaptation, retrieval, consultation, use, disclosure by transmission to recipients designated by the Controller, alignment, restriction, erasure.

Categories of data subjects:

- employees and other users of the Controller;
- external parties invited by the Controller (for example contractors, subcontractors, clients (building owners), bidders, specialist planners, viewers);

- contact persons of clients, public authorities, suppliers and service providers;
- persons captured in photos, videos or voice recordings or named in documents.

General types of data: master data of users (name, email address, role, function), contact details of participants, communication and minutes content, usage and log data (login times, IP addresses in the case of security events, technical logs).

B. Structify in the browser and for macOS and Windows

Purpose: project management and project documentation for planning and construction, in particular project and task organisation, contact and customer management (CRM), tickets, defects and acceptance inspections, drawing and document management, construction diary and site documentation with photo, video and audio recordings and their transcription, tendering and contract award including a bidder portal, appointments and calendars, time recording, fee calculation, invoicing and dunning, sending of emails and notifications, electronic signature, interfaces (API, MCP, CLI, webhooks, calendar feeds) and AI-supported features (assistant "KAI", analyses, suggestions).

Additional types of data: project, construction and defect data; photo, video and audio material and transcripts; location information for photos, where available; drawing and document content; bid and tender data of bidders; billing and fee data relating to individuals; signature data of the signatories.

The app for macOS and Windows accesses the same data as Structify in the browser; locally, the desktop app stores only session data (the login encrypted in the operating system's keychain), settings and, temporarily, incomplete entries such as drafts and technical information on uploads not yet completed.

C. Structify for iOS and Android

Purpose: data capture on the construction site and at installations (site inspections, voice notes, dictations, photos, tickets, defects, acceptance inspections, site measurements), synchronisation with the Platform, analysis by AI features, login by device pairing.

Additional types of data: photos including metadata (time of capture, device model, location, where enabled); voice recordings and transcripts; location at the time of a recording (only where enabled, not in the background); device identifier as a hash value, platform designation and times of pairing.

Particularity: Data captured without a network connection are held locally on the device by the app until they are transferred and are deleted after successful transfer. After the end of the Main Contract or of a test and demo account, entries that have not yet been transferred remain on the device for up to 30 days (§ 25(6) of the Terms). Local data are subject to the protection of the device; Structify does not back them up.

D. Structify Operate

Purpose: digital operations log for operators of technical installations, for example heating plants, heating networks, biomass and utility plants: operating and log entries, maintenance and deadlines, faults and tickets, input materials, deliveries and orders, components with installation and replacement history, meter readings and measured values, evidence, reports and audit exports, notifications of deadlines and anomalies, the roles Admin, Standard User and Viewer, and AI-supported features (assistant "KAI", analyses of operating and measurement data, calculations, recommendations, for example on maintenance, orders and consumption, reports, text recognition from photos of meters, delivery notes and invoices, transcription of voice notes and shift handovers).

Additional types of data: names and roles of the persons who create, review or approve entries, with timestamps; information on on-call duty and notification settings (name, email address, telephone number, selected types of notification); shift log and handover content; information on maintenance and inspection service providers and suppliers and their contact persons (for example supplier, vehicle, quantity, time);

photos and documents relating to installations, faults, deliveries and invoices; voice recordings and transcripts.

Particularity: Structify Operate runs on the same platform as the other products (data centres in Nuremberg and Falkenstein, § 8(1)). Until they are deleted, data from the previous version of Structify Operate are additionally held by the former development and hosting service Lovable Cloud (Schedule 3); they are not migrated. The AI features use the AI providers listed in Schedule 3 (Anthropic; for transcription, OpenAI). Structify Operate does not issue control commands to installations and does not intervene in their operation; recommendations of the AI are only implemented after review and approval by an authorised person. This excludes automatic notifications according to fixed rules, for example when set thresholds are exceeded or in the case of unprocessed faults: in such cases, Structify Operate creates tickets without prior approval, marks them as „eskaliert“ ("escalated") and notifies the persons entered for this purpose by the Controller in the application and by email; the AI merely formulates explanations and message texts and does not decide whether a notification is triggered. Viewers have read-only access to the extent released by the Admin.

E. Structify Property

Purpose: management of real estate for property management companies and for owners who manage their own property: properties, units and tenancies, move-in and move-out, rent accounts, incoming payments and bank import, dunning, deposits, service charge and heating cost statements, meter readings, handover reports, tickets for maintenance and renovation, maintenance deadlines, document filing, letters and incoming mail, letting with prospective tenants, and AI-assisted reading of documents.

Additional categories of data subjects: tenants and persons living in their household, to the extent named in contracts or reports; prospective tenants; owners; tradespeople, service providers and their contact persons; persons present and witnesses at handovers.

Additional types of data: contract data of tenancies (start and end, rent, advance payments, deposit, type of contract, agreements for example on keeping pets); bank details, account transactions and payments; dunning notices and outstanding amounts; consumption and billing data; meter readings and meter photos; handover reports with photos, room conditions, keys and signatures; the note that, and which, identity document was inspected at a handover (without a copy of the document); information from prospective tenants from enquiries and self-disclosures; invoices from tradespeople and service providers; correspondence and incoming mail.

Particularity: Structify Property runs on separate servers of the Platform in data centres of Hetzner Online GmbH in Germany (Schedule 3). Reading documents (tenancy agreements, invoices, meter photos and paper handover reports) can be switched off per Controller and is switched off for a new account; it uses the AI provider Anthropic listed in Schedule 3. The result only pre-fills input fields; nothing is saved until an authorised person has reviewed and accepted it, and their decision is recorded. E-invoices (XRechnung, ZUGFeRD) are read on Structify's servers without an AI provider. The file uploaded for reading is deleted after no more than 7 days and the result read from it after no more than 30 days; information accepted into the records is retained. Further services relating to Structify Property, for example for sending letters or retrieving bank accounts, will only be used by Structify once they are listed in Schedule 3.

Schedule 2 – Technical and Organisational Measures (Article 32 GDPR)

Structify takes in particular the following measures and develops them further in line with the state of the art.

1. Confidentiality

- **Physical access:** operation exclusively in data centres of Hetzner Online GmbH in Nuremberg and Falkenstein (Schedule 3) with physical access control; Structify does not operate its own server rooms.
- **Access to the servers:** the servers operated by Structify are administered exclusively by SSH key, with no password access; the database and administration interfaces are not publicly accessible (access only internally or, for the backup server, via an encrypted private network); firewall at provider and server level; automatic security updates.
- **Access to user accounts:** login only after authentication; protection of the login and of the „Passwort vergessen“ ("forgot password") function against automated attacks. Two-factor authentication is available for all user accounts (one-time codes in accordance with TOTP or security keys and passkeys in accordance with the WebAuthn standard). Setting it up is voluntary and expressly recommended; accounts without a second factor receive a notice. Once a second factor has been set up, it is requested as a mandatory step at login. The Controller's users decide whether to set it up; the Controller may require its users to do so by instruction, but technical enforcement per organisation is not provided for (§ 4(5)). A second factor is mandatory for the accounts of Structify's platform administration; their logins are logged on the server side. Device pairing by a QR code that can be redeemed only once (valid for 5 minutes); device trust for at most 30 days, for test and demo accounts at most until the end of the test phase, revocable at any time.
- **Data access:** tenant separation at database level (Row Level Security): each organisation sees only its own data; role-based authorisation concept within the organisation; access to project content only for members of the respective project; administrative access by Structify only on a need-to-know basis and logged.
- **Separation:** separate processing of test, showroom and production data through separate organisations.

2. Integrity

- **Input control:** logging of security-relevant operations; immutable audit logs for operations relevant to billing and retention.
- **Transfer control:** transmission only via encrypted connections (TLS); connection of external services only via authenticated interfaces.

3. Availability, Resilience and Restoration

- Operation of the database on a server managed by Structify in the Nuremberg data centre of Hetzner Online GmbH; file storage in the provider's object storage in the Falkenstein data centre with versioning (overwritten or deleted files can be restored for 30 days).
- Continuous backup of the database: archiving of every change and a daily full backup, each encrypted before storage, on separate storage in the Falkenstein data centre; retention of seven daily and four weekly backup states.
- In addition, hourly backup of the database on a backup server managed by Structify with separate storage space (Storage Box) in the Falkenstein data centre; tiered retention: hourly backup states for 48 hours, daily for 35 days, weekly for 12 weeks, monthly for 6 months. File storage is mirrored every hour; deleted or overwritten files are retained there for 90 days.
- The backup copies are encrypted before storage (database: BorgBackup with AES; file storage: rclone crypt with AES, including file and folder names). Only encrypted data are held in the backup storage; the keys remain with Structify. In addition, daily snapshots of the backup storage.
- Daily images of the servers created by the hosting provider (seven states, held by the provider in Germany, not encrypted by Structify). The encrypted disk of the database (No. 4) is not included in

these images; however, they may contain remnants of the database from deleted files on the system disk. The images are deleted automatically after seven days.
- Restoration is made to an existing backup state. No commitment is made to point-in-time restoration to any given minute.
- Weekly automatic check of the backups for completeness and readability; automatic alerting of the management in the event of missing or failed runs.
- Restore tests every quarter; tests on 26 and 27 September 2026 with complete restoration of the database and the file storage into an isolated environment and on 5 October 2026 with a restoration of the continuous database backup into an isolated environment (all check values identical).
- **Recovery times (committed, from becoming aware of the loss):** partial loss (individual records, tables, files) no more than 2 hours; total loss of the database no more than 8 hours until the Platform can be used again in a web browser. Target maximum data loss: one hour. Excluded are apps distributed via app stores that, following a total loss, require a new version to be reviewed by the store operator, periods during which the infrastructure provider is itself unavailable on a large scale, and the loss of access to the account with the infrastructure provider (for example as a result of suspension or termination by the provider); since the backup copies are currently held by the same provider, no committed recovery time applies in that case.
- Deletions take effect in backup copies as these expire (at the latest after six months); in the event of a restoration, previously deleted data are not reactivated.
- **Final backup of the former database service:** Before the data were deleted at the former provider, Structify stored the state as at the migration on 6 October 2026 in encrypted form in the object storage in the Falkenstein data centre, exclusively as proof that the data were taken over completely. The database parts will be deleted on 6 April 2027 at the latest and the files on 4 January 2027 at the latest.

4. Encryption

- Transport encryption (TLS) for data transmission over public networks; the backup server is connected via an encrypted private network.
- Encryption of all backup copies created by Structify before storage; the keys remain with Structify.
- Additional encryption of particularly sensitive stored secrets, for example access keys to connected services.
- Encryption of the disk on which the database is stored (full-disk encryption with LUKS2, AES-256 in XTS mode) since 7 October 2026. So that the database server can start without manual intervention, the key is stored with access protection on the system disk of this server and is therefore also contained in its daily images (No. 3); the encryption therefore protects the database primarily against access to the disk outside the running server, not against access that also covers these images.
- Not additionally encrypted are the system disks of the servers (operating system, programs and log data) and the object storage for the file storage; they are located in access-protected data centres in Germany (No. 1).

5. Review and Further Development

- regular internal security reviews, in particular of the access rules and tenant separation;
- automated checks that verify central security requirements (including access rules at database level) before every release;
- adjustment of the measures on the basis of the results.

6. Sub-processors

- selection according to the level of data protection and security; contracts in accordance with Article 28 GDPR; in the case of a third-country connection, standard contractual clauses and an assessment of the consequences of the transfer (§ 8); contractual exclusion of AI training for AI providers.

Schedule 3 – Sub-processors

Basis for transfers. To the extent that a sub-processor listed below processes data in a third country or access from a third country cannot be ruled out, Structify bases the transfer on the standard contractual clauses adopted by the European Commission (Commission Implementing Decision (EU) 2021/914), **Module Three** (Structify as processor to the sub-processor), with a documented assessment of the consequences of the transfer (§ 8). Certification under the EU-U.S. Data Privacy Framework is stated in addition for all certified providers; the basis remains the standard contractual clauses and the assessment. Status of the list: 8 October 2026. Processing for which Structify itself is the controller (for example the website, protection of the login, embedded content, approaching potential customers) is not processing on behalf of the Controller; such processing and the standard contractual clauses applicable to it (Module Two) are described in the Privacy Policy.

Engaged on a permanent basis

Sub-processor	Service	Data location	Third country and basis
Hetzner Online GmbH, Industriestr. 25, 91710 Gunzenhausen, Germany	hosting of the Platform: servers on which Structify itself operates the database, authentication, server functions and real-time service and delivers the applications; object storage for the file storage; data backup (backup server and separate storage for exclusively encrypted backup copies); web hosting for Structify's email mailboxes, for example for support by email	Nuremberg and Falkenstein, Germany	no third country
Anthropic PBC, USA (contracting entity in the EEA: Anthropic Ireland, Limited)	AI analysis of text, images and documents, assistant "KAI", suggestions, full-text extraction from documents for search; in Structify Operate additionally analyses, calculations and recommendations; in Structify Property reading of tenancy agreements, invoices, meter photos and handover reports to pre-fill input fields (Schedule 1 Section E)	USA	USA. SCC Module Three; no DPF
OpenAI, L.L.C., USA (contracting entity in the EEA: OpenAI Ireland Ltd.)	transcription of voice recordings, including in Structify Operate	USA	USA. SCC Module Three; no DPF
Plus Five Five, Inc. ("Resend"), USA	sending of system and notification emails	USA	USA. SCC Module Three; additionally DPF-certified

Only when the respective feature is used

Sub-processor	Service	Data location	Third country and basis
Oneflow AB, Stockholm, Sweden	electronic signature of documents, including the data of the signatories	EU (Ireland, backup in Sweden)	no third country

Former sub-processors

Structify no longer uses the following providers. They are listed for as long as data may still be held by them or if the termination took place recently.

Provider	Former service	Status
Supabase Pte. Ltd., Singapore	database, authentication, file storage and server functions (data location Frankfurt am Main) until the migration to Hetzner on 6 October 2026	Projects deleted on 7 October 2026. The final backup is held in encrypted form exclusively by Hetzner in Falkenstein (Schedule 2 No. 3).
Vercel Inc., USA	delivery of the web application until 7 October 2026	Projects deleted on 7 October 2026; no further processing.
RunPod, Inc., USA	computing power for walkable 3D tours generated from site inspection videos	Feature discontinued; Structify no longer transfers any data to RunPod. Any data from earlier processing that may still be held there will be deleted.
IONOS SE, Montabaur, Germany	Structify's email mailboxes, for example for support by email, until the move to Hetzner on 6 October 2026	Mailboxes deleted on 8 October 2026; no longer in operation. Structify keeps emails from the period up to 6 October 2026 in the audit-proof email archive of IONOS SE solely to comply with its own statutory retention obligations (Section 257 of the German Commercial Code (HGB), Section 147 of the German Fiscal Code (AO); § 10(4)); to that extent, Structify itself is the controller and IONOS is not a sub-processor. Deletion after the retention period has expired (Privacy Policy G8); no third country.
Lovable Cloud	hosting of the previous version of Structify Operate	Data from the previous version are held there until they are deleted; they are neither migrated nor used any further.

Not sub-processors

- **Stripe** (Stripe Payments Europe, Ltd., Ireland) processes payments as an independent controller. Card data are not stored in the Platform.
- Services that the Controller connects itself and to which it transmits data into **its own accounts** (for example calendar services or its own code and storage repositories) do not act as sub-processors of Structify; the transfer takes place on the Controller's instructions (§ 4(1)).
- Services for which Structify itself is the controller, for example the help voice assistant in the help section of the application, which serves Structify's support, the booking of appointments for meetings with Structify (Cal.com) and the protection of the login pages against automated attacks (Cloudflare Turnstile), are described in the Privacy Policy; Module Two of the standard contractual clauses applies there to transfers to third countries.

Changes to this list are made in accordance with § 5. The current version is available at structify.solutions/rechtliches.