LEGAL

Privacy Policy

Core Section and Modules M1 to M5

Version 2.0 · valid from 8 October 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.

Privacy Policy

Structify Solutions UG (haftungsbeschränkt)
Version 2.0 · valid from 8 October 2026

The German version prevails.

This Privacy Policy applies to all Structify products and to our website. It consists of a **Core Section**, which applies to everyone, and of **Modules** for individual products and occasions:

Module	For whom
M1 Structify in the browser and for macOS and Windows	Users of the application in the browser and of the desktop app
M2 Structify for iOS and Android	Users of the app for iOS and Android
M3 Structify Operate	Users of the digital operations log
M4 Website	Visitors to structify.solutions
M5 Approaching potential customers, partners and investors	Persons whom we approach on our own initiative for business purposes

In addition, the **AI Transparency Statement** describes how we use artificial intelligence.

Core Section

G1 Controller and contact

Structify Solutions UG (haftungsbeschränkt)
Gartenstraße 8, 92348 Berg, Germany
represented by its Managing Directors Tim Rosen and Felix König
Local Court (Amtsgericht) of Nuremberg, HRB 46012

Data protection enquiries: **datenschutz@structify.solutions**
General enquiries: info@structify.solutions · Support: support@structify.solutions

We have not appointed a data protection officer because there is no legal obligation to do so (Article 37 GDPR, Section 38 of the German Federal Data Protection Act (BDSG)).

G2 Two roles: who is responsible for your data?

Data	Structify's role	Who informs you
Our Customers' content in the products, such as project and installation data, photos, recordings, tickets, defects, documents, minutes and any information contained therein about employees, project participants and third parties	**Processor** (Article 28 GDPR). We process this content only on the Customer's instructions, on the basis of the Data Processing Agreement.	the Customer as controller, in its own privacy information
Access, usage, contract, billing, security and support data, data of website visitors, prospective customers and sales contacts	**Controller**	Structify, in this Privacy Policy

This Privacy Policy provides full information about the second row. For the first row, it describes what happens technically. If, as a project participant, you have questions about content that a Customer

processes via Structify, please contact that Customer; if your enquiry reaches us, we will forward it and support the Customer.

G3 Customers, contracts, invoices and payments

Data: company name, address, contact persons, VAT identification number, booked User Seats, modules and terms, invoice, payment and accounting data, confirmations of contract documents with time and version.

Purposes and legal bases: conclusion and performance of the contract (Article 6(1)(b) GDPR); compliance with legal obligations, in particular bookkeeping, retention and verification of the VAT identification number (Article 6(1)(c) GDPR in conjunction with Section 147 of the German Fiscal Code (AO), Section 257 of the German Commercial Code (HGB) and Section 14 of the German VAT Act (UStG)); proof that the contract documents were incorporated (Article 6(1)(f) GDPR).

Payment: Payments are processed by Stripe (Stripe Payments Europe, Ltd., Ireland) as an independent controller. You enter card details in a Stripe payment environment; we do not receive complete card details, only information on the payment status. Stripe's privacy notice additionally applies.

Recipients: For bookkeeping and accounting, we use the accounting software Lexware (Haufe-Lexware GmbH & Co. KG, Germany) as a processor. Our tax advisers, who are bound by professional secrecy, receive billing documents.

G4 AI assistance for internal tasks

For internal development and administrative tasks, for example the further development and operation of our software, the handling of enquiries and the preparation of documents, we use an AI assistant from Anthropic PBC, USA ("Claude"). In doing so, personal data for which we ourselves are responsible may be processed, for example information from customer accounts, from our CRM system and from our correspondence.

Role of Anthropic: We use the assistant via subscriptions for which Anthropic does not offer a data processing agreement. Anthropic therefore processes the data as a controller in its own right in accordance with its own terms and privacy notices; according to these, the controller for users in the European Economic Area is Anthropic Ireland, Limited, Dublin. We have switched off the use of our inputs to improve Anthropic's models in all subscriptions we use. We only enter the data that is necessary for the respective task.

Legal basis: Article 6(1)(f) GDPR; our legitimate interest lies in the efficient development of our products and administration of our company.

Third country: The data is also processed in the USA. According to its own information, Anthropic bases transfers to the USA on the standard contractual clauses of the European Commission; Anthropic is not certified under the EU-U.S. Data Privacy Framework.

G5 Support and communication

Support: If you contact us by e-mail or via the application, we process your details to handle your request (Article 6(1)(b) GDPR, otherwise point (f)). Our e-mail mailboxes are operated by Hetzner Online GmbH, Gunzenhausen, Germany (web hosting), as a processor. E-mails from the period up to 6 October 2026 are additionally kept by our former e-mail provider IONOS SE in an e-mail archive that we now use only to comply with statutory retention obligations (G6, G8). We pre-sort support requests that you submit in the application using an AI model from Anthropic PBC, USA (contracting entity in the EEA: Anthropic Ireland, Limited): it suggests the category, subject and urgency; the requests are handled by humans. Anthropic

acts as our processor in this respect; we base the transfer to the USA on the EU standard contractual clauses, Module Two (G7).

Checking of invoice attachments: We automatically check PDF attachments of e-mails received in certain of our mailboxes, in particular at info@structify.solutions, using an AI model from Anthropic PBC, USA (contracting entity in the EEA: Anthropic Ireland, Limited), to determine whether they are invoices; invoices identified in this way are entered into our accounting (G3). In the process, personal data from the attachment may be processed, for example names and contact details of senders. Anthropic acts as our processor in this respect. The legal basis is Article 6(1)(f) GDPR; our legitimate interest is the complete and efficient recording of our incoming invoices. We base the transfer to the USA on the EU standard contractual clauses, Module Two (G7).

Help voice assistant: In the help area of the application, you can voluntarily speak to our help assistant (support assistant) by voice. It is an AI system, not a human. We operate it for our own purpose of helping you with questions about using Structify; we are the controller for this processing, even if you use Structify for your company. During the conversation, your voice and the content of the conversation are transferred to Retell AI, Inc., USA, which operates the voice dialogue as our processor and, for this purpose, uses the language model of OpenAI, L.L.C., USA, as its sub-processor. We then pre-sort the conversation transcript with Anthropic in the same way as a written support request (see Support). The legal basis is Article 6(1)(b) GDPR, otherwise point (f). We base the transfer to the USA on the EU standard contractual clauses, Module Two (G7). If you do not use the assistant, no voice data is transferred to these providers.

System e-mails: We send invitations, login and security notices, notifications and invoices, as well as confirmations of and replies to enquiries submitted via our website, via Plus Five Five, Inc. ("Resend"), USA, as a processor (third country: see G7).

Appointment booking: If you book a meeting with us, we use the booking service Cal.com, Inc., USA. The appointment data (name, e-mail address, time, the information you provide about the occasion) is transferred to Cal.com in the process. The booking calendar is loaded only when you open it and give your consent (Article 6(1)(a) GDPR, Section 25(1) of the German Telecommunications Digital Services Data Protection Act (TDDDG)); the processing of the appointment data is based on Article 6(1)(b) GDPR.

G6 Recipients

Within Structify, only the persons who need access for their tasks are given access. External recipients are:

Processors for our own processing operations (Article 28 GDPR): Hetzner Online GmbH (Germany; servers for the database, website and applications, data backup and e-mail mailboxes in the Nuremberg and Falkenstein data centres), Plus Five Five, Inc. ("Resend", USA; system e-mails and e-mails from our CRM system), Cloudflare, Inc. (USA; protection of the login, M1.1), Cal.com, Inc. (USA; appointment booking), Retell AI, Inc. (USA; help voice assistant, G5, with OpenAI, L.L.C., USA, as sub-processor), Anthropic PBC (USA; checking of invoice attachments and pre-sorting of support requests, G5, as well as AI-supported analyses in our CRM system, M4.3 and M5), Haufe-Lexware GmbH & Co. KG (Germany; accounting), for approaching potential customers, partners and investors Apify Technologies s.r.o. (Czech Republic) and Instantly (USA, including the sending mailboxes "Instantly AirMail") (M5).

Sub-processors for our Customers' content: the service providers listed in the Data Processing Agreement (Schedule 3). The list is publicly available at structify.solutions/rechtliches/avv and is kept up to date there.

Independent controllers: Stripe (payments), Anthropic for the internal AI assistance (G4), Google for diagnostic data of the barcode recognition in the Android app (M2.1), the OpenStreetMap Foundation (map sections, M1.6), our tax advisers, operators of app stores (distribution of the apps), authorities and courts, insofar as we are legally obliged to disclose data.

Former service providers: Until the migration to our own servers at Hetzner on 6 October 2026, we used Supabase Pte. Ltd. (Singapore; database and hosting with data location Frankfurt am Main) and, until 7 October 2026, Vercel Inc. (USA; delivery of the website and the web application). Both services have been switched off; we deleted the projects there on 7 October 2026. Beforehand, we stored the data as at the time of the migration as an encrypted final backup at Hetzner in the Falkenstein data centre; it serves only as proof that the data was taken over completely and will be deleted on 7 April 2027 at the latest for the databases and on 5 January 2027 at the latest for files. Our e-mail mailboxes were held by IONOS SE (Montabaur, Germany) until 6 October 2026; we deleted the mailboxes there on 8 October 2026, and they are no longer in operation. IONOS continues to keep e-mails from the period up to 6 October 2026 for us in an audit-proof e-mail archive, exclusively to comply with our statutory retention obligations (Section 257 of the German Commercial Code (HGB), Section 147 of the German Fiscal Code (AO); G3); once the retention period has expired, they will be deleted there (G8). The data location is Germany. Data from the previous version of Structify Operate is additionally held by our former development and hosting service Lovable Cloud until it is deleted; it is not migrated.

Other recipients receive your data only if you or the Customer arrange this, for example by inviting project participants or by sending documents from the application.

G7 Transfers to third countries

Hosting and storage in Germany (EU) on our own servers at Hetzner Online GmbH. For AI analyses (voice, text, images), we use US providers (OpenAI, Anthropic; for the voice assistant, Retell AI) on the basis of data processing agreements and EU standard contractual clauses; for the internal AI assistance, see G4.

In detail:

- **Storage location:** The database is located in the data centre in Nuremberg, the file storage and the encrypted backup copies in the data centre in Falkenstein, in each case at Hetzner Online GmbH.
- **Other service providers based outside the EU:** In addition to the AI providers, we use service providers based in the USA for sending e-mails (Resend), protecting the login (Cloudflare, M1.1), the help voice assistant (Retell AI, G5), appointment booking (Cal.com) and sending e-mails in business development (Instantly, M5).
- **Basis:** We base all these transfers on the **EU standard contractual clauses** (Article 46(2)(c) GDPR, Commission Implementing Decision (EU) 2021/914), namely:
  - on **Module Two** (transfer from a controller to a processor), insofar as we process data for our own purposes, for example when operating our website (M4), for protecting the login (M1.1), for embedded content (M1.6), for support, checking of invoice attachments, the help voice assistant and appointment booking (G5), for enquiries and applications via the website (M4.3, M4.5) and when approaching potential customers, partners and investors (M5);
  - on **Module Three** (transfer from a processor to a sub-processor), insofar as we process content on behalf of our Customers; these sub-processors are listed in Schedule 3 to the Data Processing Agreement.
- **Transfer impact assessment:** For each provider, we have assessed the consequences of the transfer and defined supplementary measures, such as encryption, data minimisation, limited retention periods and the exclusion of AI training.
- **Data Privacy Framework:** Where a provider is certified under the EU-U.S. Data Privacy Framework, we rely on this in addition; this currently applies to Resend, Cloudflare, Atlassian (Loom) and Google (M2.1). In all cases, the standard contractual clauses and our transfer impact assessment remain the basis. Anthropic, OpenAI, Retell AI and Cal.com are not certified under the Data Privacy Framework.

- **Copy:** You can obtain a copy of the standard contractual clauses on request from datenschutz@structify.solutions; they are also published on the website of the European Commission.

A transfer to other third countries takes place only insofar as this Privacy Policy describes it or the law permits it.

G8 Retention period

We store personal data only for as long as is necessary for the purpose or required by law.

Data	Retention period
Account and contract data	for the duration of the contract, then erasure unless there is a statutory retention obligation
Customers' content	until the end of the contract; then 30 days of read-only access for export, followed by erasure (Data Processing Agreement § 10)
Platform server logs with IP address	30 days
Logs of security events (such as logins, pairing of devices, changes to the second factor), including IP address and browser or app identifier	12 months
Website server logs	14 days
Confirmations of contract documents (time, version, person)	for the duration of the contract and thereafter until the limitation period expires, usually three years
Support requests	until resolved, then usually six months, unless there is a statutory retention obligation
Enquiries from prospective customers (contact, demo)	until resolved or until you object, at the latest 24 months after the last contact
Applications not followed by employment (M4.5)	until the application procedure is completed, then no longer than six months
Business development contacts (M5)	at the latest 24 months after the last contact; in the event of an objection, only the information needed to observe it permanently
Invoices and accounting records	eight years; books of account and annual financial statements ten years; commercial and business letters six years
Analysis photos from the AI photo analysis	90 days (your original photos remain unaffected)
Download links for data exports	valid for 48 hours
Intermediate storage of the tickets transferred from PlanRadar (M1.7)	30 days after the transfer has been completed or aborted
Pairing of mobile devices	at most 30 days (for test and demo accounts until the end of the test phase) or until revoked
Raw data for usage statistics (G9)	no longer than 90 days, thereafter only in anonymised form
Backup copies	database in stages up to a maximum of six months; deleted files 90 days
Daily images of our servers created by the hosting provider	seven days
Final backup of the former database service (G6)	databases until 7 April 2027 at the latest, files until 5 January 2027 at the latest

Data	Retention period
E-mails from the period up to 6 October 2026 in the e-mail archive of IONOS SE (G6)	eleven years from archiving (retention period of the audit-proof archive; it includes the statutory retention periods under Section 257 of the German Commercial Code (HGB) and Section 147 of the German Fiscal Code (AO)), then deleted
Verification tokens of the bot protection (M1.1)	no longer than five minutes, single use only
Set-up of a second factor in the app for iOS and Android that has not yet been confirmed (M2.2)	no longer than 24 hours on the device
Entries in the app for iOS and Android not yet transferred after the end of the contract (M2.2)	up to 30 days on the device once the blocking of the app after the end of the contract has been introduced; until then, until they are transferred

G9 Our own use of data

No AI training without consent. We do not use our Customers' content to train AI models unless the Customer's management has expressly switched this on for its organisation. This setting is off by default. As long as we do not offer it, no training takes place. Our AI providers are contractually prohibited from using content for training.

Anonymised usage statistics. We record which functions are used, when and how (usage events with timestamp and technical metrics such as loading times or error codes), but no content. We aggregate this information into anonymous statistics in order to improve the products, secure operations, plan capacity and substantiate our performance figures. We delete the raw data after aggregation, at the latest after 90 days. Insofar as raw data relates to our Customers' content, aggregation takes place on the Customer's instructions under the Data Processing Agreement; insofar as your usage data as a User is concerned, the legal basis is Article 6(1)(f) GDPR (our legitimate interest in improving the products and operating them securely). You can object to this in accordance with G10.

We do **not use advertising trackers, analytics services for advertising purposes or advertising** in our products.

G10 Your rights

You have the right to

- access (Article 15 GDPR),
- rectification (Article 16 GDPR),
- erasure (Article 17 GDPR),
- restriction of processing (Article 18 GDPR),
- data portability (Article 20 GDPR),
- withdraw consent with effect for the future (Article 7(3) GDPR).

In the application, you will find a data export and the option to request deletion of your account under Einstellungen → Datenschutz & DSGVO (Settings → Privacy & GDPR). Otherwise, an informal message to datenschutz@structify.solutions is sufficient.

Right to object (Article 21 GDPR). Where we process your data on the basis of legitimate interests (Article 6(1)(f) GDPR), you may object at any time on grounds relating to your particular situation. We will then no longer process the data unless we can demonstrate compelling legitimate grounds that override your interests, or the processing serves the establishment, exercise or defence of legal claims. **You may object**

to processing for direct marketing purposes at any time without giving reasons; we will then no longer use your data for this purpose.

G11 Complaint to a supervisory authority

You may lodge a complaint with a data protection supervisory authority (Article 77 GDPR), in particular in the country in which you live or work. The authority responsible for us is:

Bavarian State Office for Data Protection Supervision (Bayerisches Landesamt für Datenschutzaufsicht, BayLDA), Promenade 18, 91522 Ansbach, Germany.

Other authorities in our sales territory:

- **Austria:** Austrian Data Protection Authority (Datenschutzbehörde), Barichgasse 40–42, 1030 Vienna.
- **Liechtenstein:** Data Protection Authority of Liechtenstein (Datenschutzstelle Liechtenstein), Kirchstrasse 8, Postfach 684, 9490 Vaduz.
- **Switzerland:** Federal Data Protection and Information Commissioner (FDPIC), Feldeggweg 1, 3003 Bern.

Information for persons in Switzerland. Insofar as the Swiss Federal Act on Data Protection (FADP) applies, the information in this Privacy Policy applies accordingly; your rights then arise from Article 25 et seq. FADP. Under Swiss law, Germany and the EU provide an adequate level of data protection. For transfers to the USA, we use the standard contractual clauses with the adaptations for Switzerland. We have not appointed a representative in Switzerland (Article 14 FADP): we process data of persons in Switzerland neither regularly on a large scale nor with a high risk for the persons concerned. We will review this again if our activities in Switzerland expand.

G12 Obligation to provide data, no automated decision-making

You are not legally obliged to provide us with data. Without account, company and billing details, however, we cannot conclude a contract or set up access.

There is no decision based solely on automated processing, including profiling, that produces legal effects or similarly significant effects (Article 22 GDPR). Our AI features generate suggestions; the decision is made by a human. The only exception is automatic notifications in Structify Operate: they are triggered according to fixed rules, for example when a recorded measured value exceeds a set threshold or a fault remains unprocessed for a defined period, and not by a decision of the AI; the AI only drafts explanations and message texts. These notifications concern the operation of the installations, not decisions about persons, and have no legal or similarly significant effect within the meaning of Article 22 GDPR (details in M3.1).

G13 Data security

We protect data in accordance with the state of the art, in particular through storage in Germany on servers that we manage ourselves (Hetzner Online GmbH, Nuremberg and Falkenstein data centres), encryption in transit, encryption of the database disk and of all backup copies created by us, strict separation of Customer data at database level, protection of the login against automated attacks, two-factor authentication, which is available for all user accounts and which we expressly recommend setting up (it is mandatory for the accounts of our platform administration), logging of security-relevant events and a tiered backup procedure: the database is backed up continuously and additionally every hour, backup states are kept for up to six months and deleted files for 90 days; restoration is made to such a backup state, not to any arbitrary point in time. Our backup copies are encrypted before being stored and are kept separately from the database server in the Falkenstein data centre; the keys remain with us. During a backup run, a server managed by us at the same provider processes the data unencrypted for a short time, exclusively in its main memory. The system disks of the servers and the object storage for the file storage are not

additionally encrypted; in addition, the hosting provider creates daily images of our servers and keeps them for seven days. We check the backups automatically every week and practise restoration every quarter. Erasures take effect in the backups as those backups expire, at the latest after six months. Details are set out in Schedule 2 to the Data Processing Agreement.

G14 Changes to this Privacy Policy

We amend this Privacy Policy when our products, service providers or the legal situation change. It is provided for information and does not require consent. Each version bears the common version number of the legal documents; you can find earlier versions at structify.solutions/rechtliches. We inform you of material changes in the application.

M1 Structify in the browser and for macOS and Windows

M1.1 Account and login

Data: name, business e-mail address, organisation, role, password (only as a hash), information on the second factor, times and circumstances of login. If your company invites you, we initially receive your name and e-mail address from your company (Article 14 GDPR).

Purposes and legal bases: provision of access and functions (Article 6(1)(b) GDPR); if you are not yourself a contracting party but a User of a Customer, the legal basis is our legitimate interest in providing the Platform to the Customer and its Users (Article 6(1)(f) GDPR). Two-factor authentication serves the security of your account (Article 6(1)(b) and (f) GDPR).

Two-factor authentication: We offer two-factor authentication for all user accounts (one-time codes in accordance with TOTP and security keys and passkeys in accordance with the WebAuthn standard). Setting it up is voluntary; we expressly recommend it, because without a second factor, your password is all that unauthorised persons need to access your account. As long as no second factor has been set up for an account, the application points this out. A second factor is mandatory for the accounts of Structify's platform administration.

Protection of the login (Cloudflare Turnstile): To ward off automated login attempts, the guessing of passwords and misuse of the „Passwort vergessen“ ("forgot password") function, we integrate the Turnstile service of Cloudflare, Inc., 101 Townsend St., San Francisco, CA 94107, USA, when you log in and when you reset your password. In the apps for macOS, Windows, iOS and Android, a separate „Sicherheitsprüfung“ ("security check") window opens for this purpose, from the respective version with security check onwards, which loads only this service. According to its own information, Cloudflare processes your IP address, the TLS fingerprint of your connection, the identifier of your browser or the app, as well as the site key and the calling address, in order to distinguish whether the request comes from a human or an automated program. The result is a single-use verification token that is valid for no more than five minutes and is transmitted to our login service together with the login or the reset request. We are the controller for this processing; Cloudflare acts as our processor and, according to its own information, also uses the data under its own responsibility to improve its bot detection. According to the provider, Turnstile does not set any cookies; insofar as it reads information from your browser or device, it does so only in order to provide the secure login you have requested (Section 25(2) No. 2 TDDDG). The legal basis is Article 6(1)(f) GDPR (protection of your account and the Platform against misuse). You can object in accordance with G10; without the bot protection, however, it may not be possible to log in with a password. Transfer to the USA: see G7.

Confirmation of legal documents: We store which version of the Terms of Use and, for persons authorised to represent the Customer, of the General Terms and Conditions you confirmed and when (Article 6(1)(f) GDPR: proof).

M1.3 Server and security logs

When you access the application, we process technical access data (IP address, time, resource accessed, technical error messages) for secure operation, error analysis and the prevention of misuse (Article 6(1)(f) GDPR). We store server logs with IP address for **30 days**. We log security events, such as logins, failed login attempts, changes to the second factor and the pairing of devices, including IP address and browser or app identifier, for **12 months** so that we can investigate security incidents.

M1.4 Cookies and storage in the browser

We use only technically necessary cookies and comparable storage in the browser (for example for the session and your settings). The legal basis is Section 25(2) No. 2 TDDDG and, for further processing, Article 6(1)(b) or (f) GDPR. We load third-party content that is not strictly necessary only after you have given your consent (M1.6).

Fonts: We deliver the application's fonts from our own servers; no data is transferred to font providers when they are loaded.

M1.5 AI features

The application contains AI features, such as the assistant "KAI", the transcription of voice recordings, the analysis of photos and documents, and suggestions for minutes, tickets and reports. If you use these features, the content required for them (texts, recordings, photos, documents, project information) is transferred to and processed by the following providers:

- **Anthropic PBC, USA** (contracting entity in the EEA: Anthropic Ireland, Limited): text understanding, image and document analysis, assistant "KAI";
- **OpenAI, L.L.C., USA** (contracting entity in the EEA: OpenAI Ireland Ltd.): transcription of voice recordings.

Where the content concerns a Customer's data, we process it as a processor and the providers act as sub-processors. We operate the help voice assistant under our own responsibility (G5). Transfer to the USA: see G7. The providers are contractually prohibited from using content for training. We delete analysis photos from the AI photo analysis after 90 days. AI results are labelled. More information can be found in the AI Transparency Statement.

Notice before the first transfer: Before any of your content is transferred to AI services for the first time, we show you a one-time notice. In Structify in the browser, for macOS and Windows and in Structify Operate, you confirm by ticking a checkbox that you have read and taken note of the information on the transfer to AI services, and you click „Zustimmen“ ("Agree"); M2.3 applies to Structify for iOS and Android. **In doing so, you confirm that you have taken note. The legal basis for the transfer is your company's Data Processing Agreement, not consent under Article 6(1)(a) GDPR.** We store your confirmation together with the time and the version (Article 6(1)(f) GDPR: proof). You can revoke it in the settings; the notice will then be shown again before the next transfer.

M1.6 Embedded content

- **Tutorial videos (Loom):** Some tutorial videos come from the Loom service (Loom, Inc., a company of the Atlassian group, USA). The video and the preview image are loaded only when you click „Abspielen“ ("Play"); nothing is retrieved from Loom before that. When you click, your IP address and technical data

are transferred to Loom (Article 6(1)(a) GDPR, Section 25(1) TDDDG). We base the transfer to the USA on the EU standard contractual clauses, Module Two (G7); Atlassian is additionally certified under the Data Privacy Framework.

- **Map section (OpenStreetMap):** If a photo in a project's photo gallery contains location information, you can have the place where it was taken displayed on an OpenStreetMap map. The map is provided by the OpenStreetMap Foundation, St John's Innovation Centre, Cowley Road, Cambridge, CB4 0WS, United Kingdom (registered in England and Wales under number 05912761). The map is loaded only when you click „Karte laden" ("Load map") in the „Standort" ("Location") tab; nothing is retrieved from OpenStreetMap before that. When you click, your browser retrieves the map section directly from the OpenStreetMap Foundation. In the process, your IP address, technical information about your browser and device (browser type, operating system, date and time of retrieval) and the coordinates of the displayed map section are transferred; the place where the photo was taken can be derived from these coordinates. The purpose is to display the place where the photo was taken at your request. The legal basis is our legitimate interest in offering you this map function (Article 6(1)(f) GDPR); since the map is loaded only when you click, you decide yourself whether this transfer takes place. To the best of our knowledge, the embedded map does not set any cookies and does not include any audience measurement. The OpenStreetMap Foundation processes the data under its own responsibility in accordance with its privacy policy (osmfoundation.org/wiki/Privacy_Policy); according to its own information, it stores the access data only temporarily and does not specify a fixed period for this. It delivers the map page and map tiles via a worldwide network of caches; which server responds depends on your location and on the time of the request. For the United Kingdom, there is an adequacy decision of the European Commission (Article 45 GDPR; Commission Implementing Decision (EU) 2021/1772, extended by Commission Implementing Decision (EU) 2025/2574 of 19 December 2025 until 27 December 2031); further safeguards are therefore not required.

M1.7 Other functions

- **Electronic signature:** If your company uses the electronic signature of documents, we use Oneflow AB (Sweden) as a sub-processor for this purpose.
- **Connections to services of your choice:** If your company connects the application to its own accounts with other services, such as calendars or code and storage repositories, we transfer data to the Customer's account on the Customer's instructions. The respective service is responsible for the processing there in accordance with its terms.
- **Data export:** Download links for exports are valid for 48 hours.
- **Data migration from PlanRadar and Capmo:** If your organisation switches from PlanRadar or Capmo to Structify, data from the previous system can be transferred to Structify (data migration). We set up the connection at the request of your organisation. For this purpose, your organisation generates an access key (API token) with the provider, for PlanRadar additionally with the customer ID; depending on the settings at the provider, this key may also include write permissions. We use it exclusively for reading and never write to the previous system; write access is technically blocked in our connection. We store the key in encrypted form. With the access, we check the connection and load the list of projects; in doing so, the provider receives the technical connection data of our server and the key. At the request of your organisation, we also transfer the tickets of a project designated by it into a project of your organisation in Structify: title, description and other form entries, status, priority, form, category or trade, location or plan, due date, creation and completion date as well as the person entered as responsible with their e-mail address, so that we can assign them to a member of the Structify project. For this purpose, we read the user list of your PlanRadar account; only the e-mail addresses of the persons entered as responsible in the transferred tickets are stored. We do not transfer comments, photos and attachments. Until the transfer, these details are held in an intermediate storage, which we delete 30

days after the transfer has been completed or aborted. To map the values of both systems to each other, we send only the labels of status, priority, form and category or trade and the corresponding selection lists of Structify to our AI service (M1.5); beforehand, we filter out labels that look like names, addresses or contact details. We do not send titles, descriptions and other content of the tickets, location and plan names or names and e-mail addresses of the persons involved to the AI. Each start of a transfer requires a new confirmation by an authorised person at Structify and is logged. The providers are PlanRadar GmbH, Schottenring 16/Top DG1, 1010 Vienna, Austria, and Capmo GmbH, Ridlerstraße 39, 80339 Munich, Germany, respectively. They are contractual partners of your organisation; for the content that we retrieve from these systems and transfer to Structify, we act on behalf of your organisation (G2). The legal basis for setting up and storing the access is Article 6(1)(b) GDPR (contract with your organisation); the Data Processing Agreement applies to the transferred content. We store the access until your organisation asks us to remove the connection.

M1.8 Special features of the app for macOS and Windows

The app for macOS and Windows accesses the same Platform as Structify in the browser; M1.1 to M1.7 apply. On the device, the app stores session data (the login encrypted in the operating system's keychain), settings and, temporarily, incomplete entries such as drafts and technical information on uploads that have not yet been completed. The app itself does not create its own crash reports; we process technical error messages as described in M1.3. If you obtain the app via the Mac App Store, Apple processes data relating to the download and updates as an independent controller; we receive aggregated statistics from Apple and, if you have consented in your device settings to sharing analytics data with app developers, crash reports for the app.

M2 Structify for iOS and Android

M1.1 to M1.5 apply accordingly to Structify for iOS and Android. In addition:

M2.1 Permissions on your device

Permission	Data	Purpose
Camera	images; content of a QR code	documentation of defects, construction progress and installations; scanning the QR code for pairing
Microphone	voice recordings and transcripts	voice notes during site inspections, dictation of tickets, suggestions for minutes and tickets
Location (precise, only while in use)	coordinates at the time a photo is taken	assigning photos to a location
Photo library	images selected by you	adding existing photos
Internet	technical connection data	synchronisation with the Platform

The app requests a permission only when you use the function. You can revoke permissions in the operating system at any time. The location is not determined in the background; without location permission, photos are stored without a location. We process the content as the Customer's processor (G2).

Photo metadata: Photos may contain metadata stored by the device, such as the time of capture, the device model or the place where the photo was taken. This metadata is currently transferred and stored together with the photo.

Recognition of the QR code for pairing: The app evaluates the QR code for pairing (M2.4) exclusively on the device, on iOS using the image recognition of the operating system and on Android using the barcode recognition Google ML Kit, which runs on the device as part of the app. Camera images are not transmitted to Google in the process. According to Google, ML Kit sends technical diagnostic and usage data to Google LLC, USA, for example the device model, operating system version, identifier and version of the app, an identifier per installation, performance metrics and error codes; Google uses this data for diagnostics and usage analysis of the feature. The legal basis is Article 6(1)(f) GDPR (our legitimate interest in reliable pairing). Google is certified under the Data Privacy Framework (G7).

M2.2 Storage on the device

The app keeps data captured without a network connection on the device until it has been transferred and deletes it afterwards. Entries that have not yet been transferred are retained even after logging out and are transferred when the same person logs in again. Cached project information is deleted when you log out. Uninstalling the app removes all local data. We do not create backups of local data.

If your company's contract or a test and demo account ends, the app is also blocked (§ 25(6) of the General Terms and Conditions) as soon as we have technically introduced this blocking; until then, the app continues to transfer entries that have not yet been transferred. Once the blocking is in place, entries that have not yet been transferred remain on the device for up to 30 days and are transferred if your company extends the contract during this period.

If you set up a second factor with one-time codes (TOTP) in the app, the app stores the secret key of the factor that has not yet been confirmed in encrypted form in the keychain or keystore of the device so that you can continue the set-up after an interruption. It is deleted after confirmation, when you log out, when the user changes and after 24 hours at the latest.

M2.3 Notice before using AI

Before the first voice recording, the first dictation and the first document upload, the app shows the notice on the transfer to the AI services (Anthropic, OpenAI) in accordance with M1.5; you confirm it with „Zustimmen und weiter“ ("Agree and continue"). **By clicking „Zustimmen und weiter“ ("Agree and continue"), you confirm that you have taken note. The legal basis is your company's Data Processing Agreement, not consent under Article 6(1)(a) GDPR.** The confirmation is stored on the device together with your account identifier, the time and the version of the notice and applies to you on that device. You can revoke it under „Rechtliches & KI-Transparenz“ ("Legal & AI Transparency"); the app will then ask again before the next transfer. Site inspections that are already waiting to be transferred at the time of revocation will still be uploaded, but will only be transcribed once you agree again, unless your company initiates the analysis.

M2.4 Pairing via QR code

If you pair the app with a logged-in session of Structify in the browser, the app generates a random device identifier. We store only its hash, a platform designation (for example „Structify-App (iPhone/iPad)“) and the times of pairing and last use (Article 6(1)(b) and (f) GDPR). The QR code for pairing can be redeemed only once and is valid for 5 minutes. A pairing is valid for at most 30 days, for test and demo accounts at most until the end of the test phase; it is deleted when it expires, when it is revoked or when the password is changed.

M2.5 App stores

Apple distributes the iOS app via the App Store; we provide the Android app as an installation file on our website. If you obtain the app via the App Store, Apple processes data as an independent controller; we receive only aggregated statistics. The app contains no advertising and no advertising trackers.

M3 Structify Operate

M3.1 Digital operations log

Data: account and login data of the Users (name, e-mail address, role Admin, Standard User or Viewer); entries in the operations log with author and timestamp; maintenance tasks and deadlines; faults and tickets; input materials and deliveries with suppliers and their contact persons; components with installation and replacement history; meter readings; photos and records of proof; information on on-call staff and notification settings (name, e-mail address, telephone number, selected types of notification).

Roles: We process the content of the operations log as the operator's processor (G2); account, security and support data as controller in accordance with M1.1 and M1.3.

Viewers: Operators can invite External Parties as Viewers with read-only access. In this case, we receive the name and e-mail address from the operator (Article 14 GDPR).

AI features: Structify Operate contains AI features, such as the assistant "KAI", analyses of operating and measurement data, calculations, recommendations on maintenance, orders and consumption, reports, text recognition from photos of meters, delivery notes and invoices, and the transcription of voice notes and shift handovers. If you use these features, we transfer the content required for them to Anthropic PBC, USA (contracting entity in the EEA: Anthropic Ireland, Limited), and, for transcription, to OpenAI, L.L.C., USA (contracting entity in the EEA: OpenAI Ireland Ltd.). M1.5 applies accordingly, including the notice before the first transfer. Structify Operate does not issue control commands to installations; recommendations are implemented only after an authorised person has reviewed and approved them. Automatic notifications according to fixed rules are excluded from this, for example when set thresholds are exceeded or faults remain unprocessed: in these cases, Structify Operate creates tickets without prior approval, marks them as „eskaliert“ ("escalated") and notifies the persons entered for this purpose in the application and by e-mail; the AI only drafts explanations and message texts. These notifications concern the operation of the installations, not decisions about persons. There is no decision based solely on automated processing (Article 22 GDPR).

Storage location and delivery: Structify Operate runs on our Platform. The database is located in the data centre in Nuremberg, the file storage and the encrypted backup copies in Falkenstein (G7, G13). The application is delivered at operate.structify.solutions from our own servers at Hetzner Online GmbH; we deliver fonts from our own servers. Data from the previous version of Structify Operate is additionally held by our former development and hosting service Lovable Cloud until it is deleted; it is not migrated.

M3.2 Information page on Structify Operate

The information page on Structify Operate does not contain its own contact form. For a demo, it refers to structify.solutions/demo; M4.3 and M4.4 apply there. We deliver fonts from our own servers. M4.1 and M4.2 apply accordingly to visits to the information page.

M4 Website structify.solutions

This Module applies to our website structify.solutions, the information page on Structify Operate and the landing pages that refer to this Privacy Policy.

M4.1 Hosting and server logs

The website is operated on a server managed by us at Hetzner Online GmbH, Industriestr. 25, 91710 Gunzenhausen, in the Nuremberg data centre (Germany); a data processing agreement under Article 28 GDPR is in place with Hetzner. When the website is accessed, technically necessary data is processed: IP address, date and time, page accessed, access status, amount of data transferred, referrer and browser identifier. The legal basis is our legitimate interest in secure operation (Article 6(1)(f) GDPR). The logs are deleted on the server after 14 days. Hetzner creates a daily image of the entire server for us and keeps the seven most recent images; the logs contained in them are deleted when the respective image is replaced, as a rule seven days after it was created. No transfer to third countries takes place in this context. Until 7 October 2026, the website was delivered via Vercel Inc., USA; the projects at Vercel have been deleted (G6).

M4.2 Cookies

On the website, we use only technically necessary cookies, for example to store your decision regarding embedded content (Section 25(2) No. 2 TDDDG). We do not use tracking cookies, analytics services or advertising pixels.

M4.3 Contact and demo requests

If you request a demo via the website or write to us, we process your details (name, e-mail address, company, your message and information about your interest) in order to answer your request, prepare and conduct a demo and manage your request in our CRM system. We store the data in our database on our servers at Hetzner Online GmbH in Germany. We send acknowledgements of receipt and notifications by e-mail via Resend (G5). In our CRM system, we may have enquiries summarised and classified with the support of AI models from Anthropic PBC, USA (contracting entity in the EEA: Anthropic Ireland, Limited); the result is a suggestion, and a human decides how to proceed. Legal bases: Article 6(1)(b) GDPR (pre-contractual measures) and point (f) (management and efficient handling of enquiries). Transfer to the USA: see G7. Retention period: see G8.

M4.4 Appointment booking

If you book an appointment for a demo or a meeting on the website, G5 (Cal.com) applies.

M4.5 Applications

If you apply via our careers page, we process the information and documents that you send us, for example your name, contact details, CV and certificates or references and, if you add them, voice or video recordings, in order to review your application and carry out the application procedure. We store the documents in non-public storage on our servers at Hetzner Online GmbH in Germany; only the persons involved in the selection have access. We send the acknowledgement of receipt and the internal notification via Resend (G5). The legal basis is Article 6(1)(b) GDPR (initiation of an employment relationship) and your consent, which you give in the application form (Article 6(1)(a) GDPR) and which you can withdraw at any time by e-mail to info@structify.solutions. If no employment relationship is established, we delete your

documents no later than six months after the conclusion of the procedure, unless we need them for longer to defend against legal claims.

M4.6 AI images

Some images on the website have been generated with artificial intelligence. The AI Transparency Statement explains which ones.

M5 Approaching potential customers, partners and investors (information under Article 14 GDPR)

This Module applies when we approach you on our own initiative for business purposes without you having provided us with your data yourself: as a contact person of a company that plans, builds or operates installations and could be a customer or partner, or as a potential investor.

Data: name, form of address, position, company, business contact details (e-mail address, telephone number, business address, website), the address of your public professional profile (such as LinkedIn), the industry, size and region of your company, the assignment to a target group, the result of our assessment of whether it makes sense to approach you, and the history of our contact (messages, replies, objections, appointments, notes). We do not process private contact details.

Sources: publicly accessible sources, in particular company websites and legal notices, commercial registers, professional and industry directories and publicly visible profiles on the professional network LinkedIn; in addition, meetings at events, recommendations and our own contact with you.

Purpose and legal basis: We present our products or a possible collaboration or investment to you, document the contact and avoid approaching you more than once. The legal basis is our legitimate interest in initiating business relationships in business-to-business dealings (Article 6(1)(f) GDPR, Recital 47).

E-mails only with your consent: We send you promotional e-mails only if you have expressly consented in advance (Section 7(2) No. 2 of the German Act against Unfair Competition (UWG); in Austria, Section 174 of the Austrian Telecommunications Act 2021 (TKG 2021)). Without consent, we do not approach you by e-mail. We approach you via professional networks such as LinkedIn or by telephone only insofar as competition law permits. Every message contains information on how you can refuse further contact.

Service providers and recipients:

- **Research:** For the automated compilation of publicly accessible information, including from databases with business contact details, we use, where required, the research tool Apify (Apify Technologies s.r.o., Vodičkova 704/36, 110 00 Prague 1, Czech Republic) exclusively via Structify's own account, as a processor.
- **AI-assisted pre-selection:** To assess whether your company belongs to our target group and to summarise public information, we use AI models from Anthropic PBC, USA (contracting entity in the EEA: Anthropic Ireland, Limited), as a processor. The assessment is a suggestion; a human decides whether and how we approach you.
- **Storage:** We store the data in our prospecting system in our database on our servers at Hetzner Online GmbH in Germany; only our management has access.
- **E-mail sending:** If we send you e-mails from our prospecting system with your consent, we use the sending service Resend (G5) for this purpose.
- **E-mail campaigns:** For e-mail campaigns, we have used the Instantly platform (Foo Monk, LLC dba Instantly.ai, 30 N. Gould St., Ste. R, Sheridan, WY 82801, USA) with its included sending mailboxes

"Instantly AirMail", which Instantly operates on its own servers; no campaigns are currently running there. Insofar as contact details and the history of previous campaigns are still stored there, Instantly processes them as our processor. Our other mailboxes are operated by Hetzner Online GmbH (G5).

- **LinkedIn:** Messages that we send you via LinkedIn are processed by LinkedIn Ireland Unlimited Company, Dublin, Ireland, as an independent controller in accordance with its own privacy policy.

Transfers to third countries: Anthropic, Resend and Instantly are based in the USA. We base these transfers on the EU standard contractual clauses, Module Two (G7).

Retention period: as long as a business relationship or investment realistically remains a possibility, at the latest 24 months after our last contact; if a contract is concluded, the periods under G8 apply. If you object, we store only the information needed to observe your objection permanently (suppression list; Article 6(1)(c) in conjunction with Article 21(3) GDPR).

Time of this information: We refer you to this information at the latest when we first contact you.

Your objection: You may object to processing for direct marketing purposes **at any time without giving reasons**, for example with a short reply to our message or by e-mail to datenschutz@structify.solutions. Your other rights are set out in G10 and G11.