Data Processing Agreement (Art. 28 GDPR)

Version 1.0, 25 November 2026 – helprange.com/dpa

Customer (the "Controller"): the company or person that uses HelpRange under the HelpRange Terms and Conditions, as identified in its account and billing details (or in the signature block below).

HelpRange (the "Processor"): Wiktor Sierociński, sole proprietorship trading as HelpRange, Topołowa 37, 96-515 Teresin, Poland, NIP (VAT ID) PL5272600509, REGON 147127353, hello@helprange.com.

This Agreement forms part of the HelpRange Terms and Conditions (the "Main Agreement") under which the Processor provides the HelpRange service (secure document sharing, tracked links and virtual data rooms) to the Controller. It applies to every team using HelpRange without a separate signature; a Controller that needs a signed copy can fill in and sign this document and send it to hello@helprange.com, and the Processor countersigns it.

1. Subject, duration, nature and purpose

1.1 Subject: processing of personal data contained in documents the Controller uploads and of personal data of the people the Controller shares documents with ("Recipients"), as needed to provide the service.

1.2 Duration: for the term of the Main Agreement and until deletion under clause 10.

1.3 Nature and purpose: storage, conversion for viewing, display under the access rules the Controller sets (e-mail verification, passcodes, expiry, view and device limits, watermarks, NDA acceptance), recording of views (viewer e-mail, IP address, country, pages and time read), sending one-time codes and notifications, AI answers when the Controller or its Recipients use the AI features, and support.

1.4 Categories of data subjects: the Controller's users (team members); Recipients and data room guests; any person whose data appears in documents uploaded by the Controller.

1.5 Categories of personal data: names, e-mail addresses, IP addresses and approximate location (country), device and browser information, viewing activity, NDA acceptance and e-signature records (name, e-mail, time, IP, browser), questions asked in data room Q&A; or to the AI, and any personal data contained in uploaded documents (determined by the Controller). Special categories (Art. 9 GDPR): only if the Controller uploads them; the Controller is responsible for having a legal basis and for choosing protection settings appropriate to them.

2. Instructions

2.1 The Processor processes personal data only on the documented instructions of the Controller – this Agreement, the Main Agreement and the settings the Controller chooses in the service – unless EU or Member State law requires otherwise; in that case the Processor informs the Controller before processing unless the law prohibits it.

2.2 The Processor informs the Controller immediately if, in its opinion, an instruction infringes data protection law.

3. Confidentiality

Persons authorised by the Processor to process the personal data are bound by confidentiality. HelpRange staff access production data only to operate the service or when the Controller asks for support.

4. Security (Art. 32 GDPR)

The Processor implements the technical and organisational measures in Annex 2 and may update them provided the overall level of protection is not reduced.

5. Subprocessors

5.1 The Controller gives general authorisation to the subprocessors in Annex 3.

5.2 The Processor informs the Controller of any intended addition or replacement of a subprocessor by updating helprange.com/gdpr and this page and by e-mail to the team's administrators at least 30 days in advance. The Controller may object on reasonable data protection grounds; if no solution is found, the Controller may terminate the affected service.

5.3 The Processor imposes on each subprocessor data protection obligations no less protective than this Agreement and remains liable to the Controller for the subprocessor's performance.

6. International transfers

Documents uploaded since the move to Frankfurt are stored in the EU (AWS eu-central-1). Older files, account data, settings, viewing analytics and transactional e-mails are processed in the United States (AWS us-west-2) and some subprocessors are in the US (Annex 3). Such transfers rely on the EU-US Data Privacy Framework where the recipient is certified, otherwise on the EU Standard Contractual Clauses (Commission Implementing Decision (EU) 2021/914), Module 2 (controller to processor) and Module 3 (processor to processor), incorporated by reference.

7. Assistance

7.1 Data subject requests: the Processor forwards requests it receives from Recipients to the Controller without undue delay and helps the Controller answer them, using the service's tools (revoking access, deleting documents, exporting view data) or support.

7.2 The Processor assists the Controller with Art. 32–36 GDPR obligations (security, breach notification, impact assessments, prior consultation) taking into account the nature of processing and the information available to it.

8. Personal data breaches

The Processor notifies the Controller without undue delay, and where possible within 48 hours, after becoming aware of a personal data breach affecting the Controller's data, with the information required by Art. 33(3) GDPR as it becomes available.

9. Audits

The Processor makes available the information necessary to demonstrate compliance with Art. 28 GDPR: this Agreement, the security description at helprange.com/security, the answers in the vendor security questionnaire (helprange.com/vendor-security-assessment-questionnaire) and written answers to reasonable questions. The Processor does not currently hold SOC 2 or ISO 27001 certification. On-site audits: once a year, with 30 days' notice, during business hours, at the Controller's cost, by an auditor bound by confidentiality, without access to other customers' data.

10. Deletion and return

10.1 During the term the Controller can download and delete its documents at any time. A deleted document and its links stop working at once; the document or folder can be restored from the Trash for 30 days, and the stored file is removed 30 days after the deletion.

10.2 At the end of the service, or when an administrator deletes the team, the team's accounts, documents, folders, data rooms, links and stored files are permanently deleted; invoices and payment records are kept as accounting law requires. Data rooms after a paid plan ends are kept read-only for administrators for 18 months unless deleted earlier. A free team inactive for 183 days is deleted after a notice e-mail.

10.3 When a data room is deleted, a record of its evidence (NDA acceptances and signed NDAs, e-signature audit trail, acknowledgements, Q&A;, guests' AI questions, the activity log, guests and the list of documents – not the documents themselves) is kept for the team's administrators for 6 years and then deleted; the team's audit log is kept for 6 years. Both are deleted earlier if the whole team is deleted.

10.4 Exception: content of a team suspended after an abuse report may be kept as evidence.

11. Liability and order of precedence

Liability is governed by the Main Agreement, without prejudice to Art. 82 GDPR. In case of conflict between this Agreement and the Main Agreement concerning personal data, this Agreement prevails.

12. Law and jurisdiction

Polish law; the courts competent for the Processor's registered address.

Controller	**Processor**
_____	_____
Company, name, title, date, signature	Wiktor Sierociński, HelpRange – date, signature

Annex 1 – Description of processing

See clause 1. Retention periods: clause 10 and helprange.com/gdpr ("How long we keep data").

Annex 2 – Technical and organisational measures

- Storage: new uploads in AWS Frankfurt (eu-central-1); older files in AWS Oregon (us-west-2); private buckets.
- Encryption: uploaded documents and the database encrypted at rest with AES-256 (AWS KMS); TLS 1.2+ for every connection (TLS 1.3 preferred).
- Access control in the service: e-mail verification with one-time codes, passcodes, expiry dates, view limits, IP allow-lists, network and device limits, one active session per guest, revoking access at any time; download and print blocking, dynamic watermarks with the viewer's e-mail, screenshot protection, image mode.
- Account security: two-step login (authenticator codes), optional requirement for the whole team, Google / Microsoft sign-in, SSO (SAML 2.0, OpenID Connect) and SCIM 2.0 on the Unlimited plan and Deal Room Pass; password and sign-in e-mail changes confirmed by e-mail (plus the authenticator code when enabled).
- Roles: administrators and members; members see only the folders and data rooms they are given.
- Brute-force limits on passcodes, one-time codes and passwords (per target and per IP address).
- Tenant isolation: every web, API and MCP request is checked against the requesting team and its folders.
- API and AI connectors: OAuth 2.1, tokens stored only as SHA-256 hashes, access tokens expire after 1 hour, refresh tokens after 30 days, revocable at any time.
- Audit trail of views per link, document and data room, exportable to CSV; an audit log of the team's actions (sign-ins, deletions, settings and access changes) kept 6 years.
- Trash: deleted documents and folders can be restored for 30 days; deleted data rooms leave an evidence record for 6 years (clause 10.3).
- Reader guard (detection of copying behaviour) and forwarding alerts.
- Anti-phishing scan of links in uploaded documents; abuse reporting on every shared page.
- No advertising or third-party analytics on recipient pages.
- Payments handled by Stripe; card numbers are never stored by HelpRange.
- Staff access to production data only to operate the service or for support.
- Backups: the database is backed up automatically every day, encrypted, and backups are kept for 7 days (AWS, United States); the database is not reachable from the internet and is protected against accidental deletion.
- Monitoring: application and access logs with alerting on errors; security reports via helprange.com/security#report and /.well-known/security.txt.
- Incidents: assessed without undue delay; affected Controllers are notified as in clause 8.

Annex 3 – Subprocessors

Provider	Purpose	Location
Amazon Web Services (S3)	Storage of uploaded documents	Frankfurt, Germany (new uploads); United States, us-west-2 (older files)
Amazon Web Services (hosting, database)	Application, account data, settings, viewing analytics	United States
Amazon Web Services (SES)	Verification codes and notifications	United States
Stripe	Payments	EU / United States
Anthropic	AI features (document text and question needed for an answer; set-up assistant; phishing/spam check of new accounts' first documents); not used for training	United States
Cloudflare	Certificates and traffic for custom domains	Global
iFirma	Invoicing (billing details)	Poland
Google	"Sign in with Google", if used	United States
Microsoft	"Sign in with Microsoft", if used	United States

Analytics on HelpRange's own website and signed-in app (not on recipient pages) concern HelpRange's own controller data and are not subprocessors of the Controller's data.