> **Informative translation.** The Slovak version is binding; in case of any conflict the Slovak version prevails.

Data Processing Agreement (DPA)

Contracting parties

Controller:
The User whose identification details (business name, registered office, company ID, tax ID, representative) are kept in its User account in the SureDocs Redact application — filled in at registration from public registers (company ID lookup) and supplemented by data not available from the registers.
The current data of the specific Controller and the date/person of confirmation of this Agreement are available in its printable confirmation of the Terms of Use in SureDocs (Dashboard → Orders).
(the "Controller")

Processor:
InnovativeIT, s.r.o.
Registered office: Častkovce 61, 916 27 Častkovce, Slovak Republic
Registered in the Commercial Register of the District Court Trenčín, section: Sro, file no. 47355/R
Company ID (IČO): 56427689 | Tax ID (DIČ): 2122313380 | VAT ID: SK2122313380
Represented by: Ing. Pavol Žiška, managing director
E-mail: info@innovativeit.sk
(the "Processor" or "SureDocs")

Preamble

The Controller and the Processor conclude this Data Processing Agreement (the "Agreement") in accordance with Art. 28 of Regulation (EU) 2016/679 of the European Parliament and of the Council on the protection of natural persons with regard to the processing of personal data (GDPR).

The Processor provides the Controller with the SureDocs Redact service — automated anonymisation of personal data in documents. In providing this service, the Processor processes personal data exclusively on behalf of and according to the instructions of the Controller.

Article 1 — Subject of the Agreement

1.1 The subject of this Agreement is to regulate the rights and obligations of the contracting parties when processing personal data in connection with the use of the SureDocs Redact service.

1.2 This Agreement is an integral part (Annex No. 1) of the Terms of Use of the SureDocs Redact service and takes effect upon acceptance of the Terms of Use.

1.3 This Agreement is concluded in electronic form. The Controller expresses its explicit consent to its entire wording by ticking the relevant box at registration for the Service — an Agreement concluded in this way is as binding for both parties as an agreement signed by hand or with a qualified electronic signature; a separate paper/electronic signed copy is not required.

Article 2 — Scope, nature and purpose of processing

Purpose of processing:
Automatic detection, classification and anonymisation of personal data in documents uploaded by the Controller to the Service, in order to fulfil the Controller's obligations under the GDPR and other data protection regulations.

Nature of processing:

- Reading the document content (text extraction / OCR)
- Analysis of the text by an artificial intelligence model
- Identification and classification of personal data
- Generation of the anonymised output
- Writing an approval record to the audit log

Types of personal data processed (depending on the content of the uploaded documents):

- Names and surnames of natural persons
- Permanent/temporary residence addresses
- Telephone numbers and e-mail addresses
- Bank account numbers (IBAN)
- Birth numbers and identity document numbers
- Dates of birth
- Other identifiers of natural persons

Categories of data subjects:
Natural persons whose personal data are contained in documents uploaded by the Controller (customers, employees, contracting parties, etc.).

Duration of processing:
For the duration of the contractual relationship between the parties or, where applicable, for the period necessary to fulfil legal obligations.

Article 3 — Obligations of the Processor

The Processor undertakes to:

3.1 Process only on instructions
Process personal data only on documented instructions from the Controller, including with regard to transfers of personal data to third countries, unless required to do so by EU or Member State law; in such a case the Processor shall inform the Controller of that legal requirement before processing, unless that law prohibits such information.

3.2 Confidentiality
Ensure that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

3.3 Security measures
Take all measures required under Art. 32 GDPR, including:

- Encryption of data in transit (TLS/HTTPS)
- An automated local filter for special categories of data under Art. 9 GDPR: the text of the document (for scans and photos after it is read locally) is evaluated on the Processor's server before it is sent to any sub-processor, and on clear signs of health data the document is not sent and is refused; the filter is not 100 % reliable and does not replace the Controller's obligation under Art. 4.2
- Temporary processing of documents in the working memory of the server and in its temporary copy (an internal database on the same server, reachable only locally, kept for at most 12 hours, 4 hours for the API, and deleted when the session ends), without permanent storage of the content after the session ends; for automatic analysis, data are sent to the

selected sub-processor (Art. 6) exclusively via its API, again without permanent storage on its side after processing is completed

- Access control to the production environment
- Regular testing of system security (internal code review, automated CI checks; the Processor currently holds no external security certification such as ISO 27001/SOC 2 and has not undergone a formal penetration test — details and context in the internal document `dpia_lia_interne_posudenie.md` Part C)

The optional **SureDocs Print driver** component (a locally installed virtual printer) accepts print jobs exclusively on `127.0.0.1` (it is not reachable from the network), and the document remains only locally on the User's computer until the User confirms it for processing in the application's review window — only then is it sent to the SureDocs server via the same route (`/v1/api/jobs`) as a regular API integration. It is therefore not a separate data flow outside this Agreement, only an alternative way of handing over a document for processing.

3.4 Sub-processors
The current list of sub-processors is set out in Annex 1 — by accepting it, the Controller grants **general written authorisation** within the meaning of Art. 28(2) GDPR. The Processor informs the Controller of planned changes (a new sub-processor or its replacement) by e-mail at least **14 days in advance**. The Controller has the right to raise a reasoned objection within **7 days** of this notice; if it does not raise an objection within this period, it is deemed to agree with the change.

3.5 Assistance to the Controller
Taking into account the nature of the processing, assist the Controller by appropriate technical and organisational measures in fulfilling the Controller's obligation to respond to requests for exercising the data subject's rights.

3.6 Assistance with obligations under Art. 32–36 GDPR
Assist the Controller in ensuring compliance with the obligations under Art. 32–36 GDPR (security, breach notification, impact assessment, prior consultation). The formal obligation to carry out an impact assessment (DPIA, Art. 35) lies with the Controller — beyond this assistance, the Processor has itself internally assessed the risk of its own processing (scope, data categories, sub-processors) as part of due diligence; the record of this assessment is the internal document `dpia_lia_interne_posudenie.md`.

3.7 Deletion or return of data
At the choice of the Controller, delete or return all personal data after the end of the provision of the Service and delete existing copies, unless EU or Member State law requires their storage.

3.8 Audit and inspection
Make available to the Controller all information necessary to demonstrate compliance with the obligations laid down in this Article and allow for and contribute to audits and inspections conducted by the Controller or another auditor mandated by the Controller. The Controller may carry out an audit **at most once per calendar year**, after prior written notice at least **30 days in advance** (outside this period only in the event of a reasonable suspicion of a serious breach). The Processor is entitled to reimbursement from the Controller of the costs actually incurred in assisting with the audit according to its current hourly rates.

3.9 Immediate notification
Immediately inform the Controller if, in its opinion, an instruction infringes the GDPR or other EU or Member State data protection provisions.

Article 4 — Obligations of the Controller

The Controller undertakes to:

4.1 By uploading documents to the Service, confirm that it has a lawful basis for processing the personal data contained in those documents.

4.2 Ensure that the uploaded documents DO NOT CONTAIN special categories of personal data under Art. 9 GDPR (health records, biometric data, genetic data, data relating to criminal convictions) — this prohibition is absolute and without exception (consistent with Art. 5(b) of the Terms of Use); the Processor does not and cannot grant consent to it.

4.3 Inform the Processor of any instructions, requirements or changes that could affect the processing of personal data.

4.4 Ensure that approval of the anonymisation in the application is carried out only by authorised persons with the appropriate powers.

Article 5 — Transfers to third countries

5.1 The Controller acknowledges that, depending on the selected AI backend, the content of documents may be transferred to third countries:

Backend	Contracting party	Infrastructure	Legal basis for transfer
Claude (Anthropic)	Anthropic Ireland, Limited (EU contracting party for customers in the EEA/CH/UK)	Global/worldwide (Google Cloud, AWS, Microsoft Azure)	Standard Contractual Clauses (SCC)
Mistral	Mistral AI SAS	France (EU)	Not required (EU)
Ollama	—	Local (User's device)	Not required

5.2 The Processor shall ensure that every sub-processor in a third country is bound by appropriate safeguards within the meaning of Art. 46 GDPR (Standard Contractual Clauses or another suitable mechanism).

5.2a Transfer Impact Assessment: The Controller acknowledges that US authorities (in particular under Section 702 FISA and Executive Order 12333) may under certain circumstances request access to data processed by providers headquartered or with infrastructure in the USA, even though standard contractual clauses exist. The Processor has identified this risk and adopted the following mitigating measures:

- the processing time of a document at the AI sub-processor is short (in the order of seconds to a few minutes in normal operation) and it is not permanent storage — this reduces, but does not exclude, the likelihood of the data being intercepted during the active processing window (see also Art. 8.1 and the exception for trust & safety monitoring);
- since June 2026 Anthropic has been certified under the EU-US Data Privacy Framework — an additional legal mechanism alongside the Standard Contractual Clauses (Art. 45 GDPR);
- the User can avoid a transfer to the USA entirely by choosing the **Mistral** (EU) or **Ollama** (local processing) backend — see Art. 5.3.

The Processor does not declare that technical measures (e.g. temporary processing without permanent storage of the content) prevent third-country public authorities from accessing the data during active processing — such a declaration would be unfounded. A User processing documents with particularly sensitive content should consider the Mistral or Ollama backend.

5.3 The Controller can minimise transfers to third countries by choosing the **Mistral** (EU) or **Ollama** (local) backend in the application settings.

Article 6 — Sub-processors

Annex 1 — Approved sub-processors

Sub-processor	Registered office	Purpose	Data category	Link to DPA

Anthropic Ireland, Limited (contracting party for EEA/CH/UK customers; outside the EEA Anthropic, PBC)	Ireland (EU) — processing on global infrastructure (Google Cloud/AWS/Azure)	AI text analysis (Claude backend)	Document content (text)	anthropic.com/legal/data-processing-addendum
Mistral AI SAS	Paris, France (EU)	AI text analysis (Mistral backend, default for paying organisations)	Document content (text)	legal.mistral.ai/terms/data-processing-addendum
Google Ireland Limited (Google Cloud)	EU (Document AI region `eu`)	OCR of scanned/ photographed pages (Document AI)	Document content (page image)	cloud.google.com/terms/data-processing-addendum
Supabase Pte. Ltd	Singapore (contracting party) — database physically in the EU (Ireland). Legal basis for transfer: Standard Contractual Clauses (SCC) integrated in the sub-processor's DPA.	Authentication, user database, audit log	Account, billing/ organisation metadata, processing audit log (NOT document content)	supabase.com/legal/customer-resources/data-processing-addendum
Stripe Payments Europe, Limited	Ireland (EU) — contracting party for InnovativeIT. Data are nevertheless transferred to Stripe, LLC (USA) — certified under the EU-US Data Privacy Framework.	Payments and billing (hosted Stripe Checkout page)	Organisation name, billing e-mail — **never the card number**	stripe.com/legal/dpa
Websupport, s.r.o.	Bratislava, Slovakia (EU)	Sending e-mails (SMTP — invitations, notifications)	Recipient's e-mail address, e-mail content	websupport.sk/obchodne-podmienky (PART B, point 16.11 et seq. — processing agreement with the User under Art. 28 GDPR)
Hetzner Online GmbH	Germany (EU)	Hosting of the web application server	Infrastructure (SureDocs does not communicate with them via API)	hetzner.com/AV/DPA_en.pdf (Data Processing Agreement under Art. 28 GDPR, concluded in the Hetzner customer account)

Cloudflare, Inc.	USA (contracting party) — global edge network, transfer covered by Standard Contractual Clauses (SCC) integrated in the sub-processor's DPA	Reverse tunnel (Cloudflare Tunnel) in front of the production server — DDoS/bot protection, TLS termination	IP address and HTTP metadata (headers, request path) of passing requests — NOT document content	cloudflare.com/cloudflare-customer-dpa

The Processor shall ensure that sub-processors are bound by the same data protection obligations as apply to the Processor under this Agreement. In accordance with Art. 28(4) GDPR, the Processor remains fully liable to the Controller for the proper performance of the data protection obligations by the sub-processors.

Note — public register lookups (not sub-processors within the meaning of Art. 28): When verifying a company ID during registration/renewal, SureDocs calls public register APIs (RPO of the Statistical Office of the SR, ŽRSR and RMNO of the Ministry of Interior of the SR, Financial Administration of the SR, ARES CZ). Only the company ID is sent; the response consists mostly of public register data of THIRD entities (business name, address, legal form), not personal data of the Controller's customers — in this respect there is no processing of personal data on behalf of the Controller and these services are deliberately NOT in the table above. **Exception:** if the register also returns the name of the statutory body/managing director (a natural person) for the given company ID, SureDocs further processes this name as personal data — the legal basis and retention are set out in the table "What data we collect" below (name of the statutory body), not in this note.

Article 7 — Personal data breach

7.1 In the event of a personal data breach (security breach), the Processor informs the Controller **without undue delay** after becoming aware of the breach.

7.2 The notification contains: a description of the nature of the breach, the categories and number of data subjects concerned, the contact details of the responsible person, a description of the likely consequences, and a description of the measures taken to remedy it.

7.3 The Controller is responsible for fulfilling the notification obligation towards the supervisory authority (for a Slovak Controller the ÚOOÚ SR; otherwise the competent supervisory authority) within the statutory period of 72 hours under Art. 33 GDPR.

Article 8 — Retention policy and deletion

8.1 The content of uploaded documents is not stored permanently — it is processed in the working memory of the server and in its temporary copy (Art. 3.3), which is deleted after processing is completed or the session ends and expires after 12 hours at the latest (4 hours for the API). Traces of the temporary copy may remain in the technical journal and the database snapshot on the server's disk until the system overwrites them automatically (usually days to weeks). Exception: AI sub-processors (Anthropic, Mistral) may, in accordance with their own trust & safety policies and independently of the no-training agreement, retain inputs/outputs for a short time for the purpose of abuse monitoring — as a rule up to 30 days, and in exceptional cases of a detected breach of their terms of use also longer (see Terms of Use Art. 2.2b).

8.2 The audit log (record of approval of the anonymisation) contains: file name, SHA-256 hash of the original, name of the approver, timestamp, number of anonymised fields, backend used. The audit log **does not contain** the document content.

8.2a The audit log serves to demonstrate compliance under Art. 5(2) and Art. 30 GDPR (an internal record of processing activity) — it does not constitute a qualified electronic seal or any other legally qualified time/integrity certification, unless expressly agreed otherwise between the parties.

8.3 Audit log records are kept for **3 years (36 months)** from their creation and are then automatically deleted.

8.4 The User's registration data are deleted within **90 days** after the account is cancelled, unless their retention is required by law (e.g. accounting documents — 10 years).

Article 9 — Final provisions

9.1 This Agreement is governed by the law of the Slovak Republic and the relevant EU regulations, in particular the GDPR.

9.2 In the event of a conflict between this Agreement and the Terms of Use, this Agreement prevails as regards the protection of personal data.

9.3 Amendments to this Agreement are valid only in written form (including acceptance by e-mail).

9.4 If any provision of this Agreement is invalid, the remaining provisions remain in force.

9.5 This Agreement takes effect upon acceptance of the Terms of Use of the SureDocs Redact service — in electronic form under Art. 1.3, without the need for a paper or qualified electronic signature.

9.6 This agreement may also be made available in translation into other languages. The translation is for information only; in the event of any conflict between the Slovak version and the translation, the Slovak version always prevails. The User's consent applies to the Slovak version; the accepted Slovak version is stored as the official document in the User's account (Dashboard → Orders) together with the translation the User had displayed when consenting.

Privacy Policy

> In this document SureDocs is the **controller** (users' registration data). The processing of document content is governed by the DPA above.

Who we are

InnovativeIT, s.r.o., Častkovce 61, 916 27 Častkovce, Slovak Republic, Company ID: 56427689
Contact: privacy@suredocs.eu (data subject requests, personal data protection)
Data Protection Officer (DPO): the controller currently has no appointed data protection officer; for data protection matters please contact the Provider directly at the contact above.

What data we collect

Data	Purpose	Legal basis	Retention
E-mail	Registration, communication	Contract (Art. 6(1)(b))	For the duration of the account + 90 days
Name (optional)	Personalisation	Consent	Until withdrawn
Audit log records	Evidence of approvals	Legitimate interest	3 years (36 months)
Name of a removed approver	Tracing the name behind a stamp after the account is deleted	Legitimate interest	3 years (36 months)
IP address, access log	Network security, prevention of abuse and cyber attacks, fault diagnostics	Legitimate interest	90 days

Payment records	Accounting	Legal obligation	10 years
Name of the organisation's statutory body/managing director (from a public register)	Verifying that the person carrying out the registration is authorised to represent the organisation	Legitimate interest (the data are part of a publicly available register, Art. 6(1)(f))	For the duration of the contractual relationship — tied to the organisation's record, removed when it is deleted

The IP address and access log are recorded as a technically necessary part of operating the web server (as with any web service) — this is neither a cookie nor a tracking mechanism, and the record is created regardless of the choice in the cookie banner. SureDocs currently does not use optional (analytics) cookies. In production, requests to SureDocs pass through Cloudflare (reverse tunnel, see Annex 1) — Cloudflare as a sub-processor processes the same IP/HTTP metadata on its own edge infrastructure under its DPA, independently of SureDocs' 90-day retention.

For items based on "legitimate interest", a balancing test has been carried out — the record is in the internal document `dpia_lia_interne_posudenie.md` Part B.

Your rights

You have the right to: access · rectification · erasure · restriction of processing · portability · objection · complaint to a supervisory authority (in Slovakia the ÚOOÚ SR — dataprotection.gov.sk; or the supervisory authority of your Member State).

Send your request to: privacy@suredocs.eu — we will reply within 30 days.