

DOCREVEAL - DATA PROCESSING TERMS

Effective from: 26 September 2026

1. INTRODUCTION

- 1.1 This Data Processing Terms (“**DPT**”) governs the processing of personal data carried out by DocReveal on behalf of the User in the course of providing the Services. The DPT is referred to in Section 13.7 of the **Terms of Service** available at <https://docreveal.ai/assets/documents/legal/docreveal-terms-en.pdf> (the “**Terms**”), forms an integral part of the Agreement, and is concluded together with the Agreement at the moment the User accepts the Terms.
- 1.2 **DocReveal:** DocReveal s.r.o., ID No. (IČO): 29871972, with its registered office at Příčná 1892/4, Nové Město, 110 00 Prague 1, Czech Republic, registered in the Commercial Register maintained by the Municipal Court in Prague under file No. C 453198; e-mail: info@docreveal.org; telephone: +420 605 919 219 (the “**Processor**” or “**DocReveal**”).
- 1.3 **User:** the person who has entered into the Agreement with DocReveal, as identified in that person's account (the “**Controller**” or the “**User**”).
- 1.4 Capitalized terms used but not defined in this DPT have the meaning given to them in the Terms. “**GDPR**” means Regulation (EU) 2016/679. “**Personal Data**” means personal data within the meaning of Article 4(1) GDPR contained in User Data and processed by DocReveal on behalf of the User. “**Data Protection Law**” means the GDPR and any other legislation on the protection of personal data applicable to the processing under this DPT. “**Sub-processor**” means any third party engaged by DocReveal to process Personal Data on behalf of the User.
- 1.5 Notwithstanding the order of precedence set out in Section 13.1 of the Terms, **this DPT prevails over the remaining parts of the Agreement in matters concerning the processing of Personal Data on behalf of the User**; in all other matters the Terms prevail. This DPT does not amend, and shall not be construed as amending, the limitations of liability, the disclaimers or the commercial terms set out in the Terms.

2. ROLES OF THE PARTIES AND SCOPE OF THE DPT

- 2.1 In relation to Personal Data contained in User Data, **the User acts as controller** (or, where the User itself processes such Personal Data on behalf of a third party, as processor) and **DocReveal acts as processor** (or, as the case may be, as sub-processor). This DPT applies exclusively to that processing.
- 2.2 Where DocReveal determines the purposes and means of processing, **DocReveal acts as an independent controller**. This applies in particular to the purposes described in Section C of Part I of the Privacy Policy – e. g. the provision of the Services and administration of the account, payment processing and invoicing and the security of the Services and the prevention and detection of abuse etc. That processing is not governed by this DPT but by the Privacy Policy available at <https://docreveal.ai/assets/documents/legal/docreveal-privacy-en.pdf>.

- 2.3 Where the User acts as a processor for a third-party controller, the User warrants that it has obtained all authorizations necessary to engage DocReveal as a sub-processor and that this DPT satisfies the requirements of the underlying contract. DocReveal owes no obligations to that third-party controller beyond those set out in this DPT, and all its obligations may be exercised exclusively by the User.

3. SUBJECT MATTER, NATURE AND PURPOSE OF THE PROCESSING

- 3.1 **Subject matter of the processing.** The provision of the Services to the User, i.e. the hosting, storage and AI-assisted processing of documents and other unstructured data uploaded by the User and its Authorized Users.
- 3.2 **Nature of the processing.** Collection, recording, organization, structuring, storage, adaptation, retrieval, use (including extraction, classification, indexing and vectorization, construction of search indexes and of graph entities and relationships, semantic search, generation of Outputs, transcription of audio and video, analytics and workflow execution), logging of the queries submitted to the AI Features for audit and security purposes, disclosure by transmission through integrations configured by the User, restriction, erasure and destruction. Conversations with the AI Features are stored in the User's workspace as a conversation history for the retention period set by the User in the Services (by default 365 days from the last activity) or until the User deletes them.
- 3.3 **Purpose of the processing.** The provision, operation, maintenance and security of the Services in accordance with the Agreement.
- 3.4 **Duration of the processing.** DocReveal processes Personal Data for the duration of the Agreement and thereafter only for the period necessary to fulfill the obligations set out in Section 16 of this DPT or to comply with applicable law.
- 3.5 **Content of User Data.** DocReveal does not systematically review, monitor or filter the content of User Data and is under no obligation to do so. The specific content of the Personal Data processed is determined **solely by the User**. This is without prejudice to the assessment of reported content and to voluntary own-initiative investigations under Section 9 of the Terms and Regulation (EU) 2022/2065 (the Digital Services Act). Where DocReveal assesses reported content, carries out voluntary own-initiative investigations, or detects, investigates and prevents security incidents and conduct contrary to the Terms, it does so in order to comply with its own legal obligations and to protect its own legitimate interests; in respect of those operations DocReveal acts as an independent controller in accordance with Section 2.2 of this DPT and the Privacy Policy, and not as a processor on the User's instructions.

4. TYPES OF PERSONAL DATA AND CATEGORIES OF DATA SUBJECTS

- 4.1 **Types of personal data.** Determined solely by the User. The following types of Personal Data are typically processed:
- a) identification data (name, surname, title, date of birth, identification numbers);

- b) contact data (address, e-mail, telephone);
- c) employment and professional data (position, employer, career history in CVs);
- d) economic and transaction data (invoice details, amounts, bank account numbers, payment references, contractual terms);
- e) contract and correspondence content;
- f) images and signatures contained in scanned documents;
- g) voice recordings and their transcripts where speech-to-text is used;
- h) account and access data of Authorized Users;
- i) data derived from User Data by the Services (vector embeddings, search indexes, graph entities and relationships and analytical records);
- j) any other personal data contained in the documents uploaded by the User.

4.2 Categories of data subjects. Persons whose personal data are contained in User Data, as determined solely by the User. Personal Data typically relate to the following categories of data subjects:

- a) the User's employees, contractors and Authorized Users;
- b) the User's customers, clients and their contact persons;
- c) the User's suppliers and business partners and their contact persons;
- d) job applicants;
- e) any other natural persons referred to in the documents processed.

4.3 Special categories of personal data. The Services are not intended for the processing of special categories of personal data or of data relating to criminal convictions and offences. Where such data are nevertheless contained in User Data, this occurs solely as a result of the User's decision, in accordance with Section 6.2 of this DPT. Where such data are present, the following safeguards apply: encryption in transit and at rest, tenant isolation, document-level access control, restriction of DocReveal personnel access to the minimum necessary on the basis of a logged and approved request, and full audit logging of every access. No further restrictions specific to such data are applied, and the User remains responsible for assessing whether these safeguards are adequate to the risk.

5. INSTRUCTIONS OF THE USER

5.1 DocReveal shall process Personal Data **only on the documented instructions of the User**, unless required to do so by Union or Member State law to which DocReveal is subject; in such a case DocReveal shall inform the User of that legal requirement before processing, unless that law

prohibits such information on important grounds of public interest.

5.2 The parties agree that the following constitute **the complete and documented instructions of the User** for the purposes of Article 28(3)(a) GDPR:

- a) this DPT, the Terms and any other part of the Agreement;
- b) the configuration and settings of the Services selected by the User (including workspace, access, integration, retention and export settings);
- c) the User's use of the Services and the actions of its Authorized Users within the Services, including the uploading of documents, the submission of prompts and questions to the AI Features, the running of reveal calls, transcriptions, searches, workflows and analyses, and the export of data;
- d) the Documentation.

5.3 **Any instruction outside the scope of Section 5.2 must be given in writing to info@docreveal.org.** DocReveal shall implement such an instruction where it is technically feasible within the standard functionality of the Services, does not require a modification of the Services, does not infringe Data Protection Law and does not conflict with a legal obligation of DocReveal. DocReveal is entitled to charge for the implementation of any such instruction in accordance with Section 18 of this DPT. Where DocReveal is unable to implement the instruction on those grounds, it shall inform the User without undue delay, and either party may terminate the affected Services by written notice; the User's rights under Section 12 of the Terms are not affected.

5.4 DocReveal shall **immediately** inform the User where, in its opinion, an instruction infringes Data Protection Law. DocReveal is entitled to suspend the performance of the instruction concerned until the instruction is confirmed, amended or withdrawn by the User. DocReveal has no obligation to carry out a legal assessment of the User's instructions or of the lawfulness of the User's processing.

6. OBLIGATIONS AND WARRANTIES OF THE USER

6.1 **The User is solely responsible for the lawfulness of the processing** of Personal Data contained in User Data. The User warrants and undertakes, throughout the term of the Agreement, that:

- a) it has a valid legal basis under Article 6 GDPR (and, where applicable, under Article 9(2) or Article 10 GDPR) for all processing carried out through the Services, including for the disclosure of Personal Data to DocReveal and its Sub-processors and for any transfer outside the EEA;
- b) its instructions and its use of the Services do not infringe Data Protection Law or any other applicable legislation or the rights of any third party;
- c) it will not use the Services in a manner that would make DocReveal a joint controller within the meaning of Article 26 GDPR.

- 6.2 Special categories of Personal Data.** The Services are **not designed or intended** for the processing of special categories of personal data within the meaning of Article 9 GDPR or of personal data relating to criminal convictions and offences within the meaning of Article 10 GDPR. Where the User nevertheless processes such data through the Services, it does so **entirely at its own risk and on its own responsibility**, it warrants that a valid legal basis exists, and it acknowledges that DocReveal (i) does not review the content of User Data in advance and is under no obligation to do so, (ii) applies to them the same technical and organizational measures as to other Personal Data, and (iii) gives no assurances as to the suitability of the Services for such data.
- 6.3 Automated decision-making.** The User shall not use the Services, or Outputs generated by them, as the sole basis for decisions producing legal effects concerning natural persons or similarly significantly affecting them within the meaning of Article 22 GDPR. Compliance with Article 22 GDPR, the provision of meaningful human oversight and the assessment of Outputs remain **exclusively the responsibility of the User**.
- 6.4 Authorized Users and access.** The User is responsible for the administration of access rights to its environment, for the conduct of its Authorized Users, for the protection of login credentials, and for the immediate revocation of access where it is no longer justified. Any access to Personal Data obtained through valid credentials of the User or its Authorized Users is deemed to have been made by the User.

7. OBLIGATIONS OF DOCREVEAL

7.1 DocReveal shall:

- a) process Personal Data only in accordance with Section 5 of this DPT;
- b) ensure that persons authorized to process Personal Data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality (Section 8 of this DPT);
- c) implement the technical and organizational measures set out in Section 9 of this DPT;
- d) comply with the conditions for engaging Sub-processors set out in Section 10 of this DPT;
- e) assist the User with data subject requests in accordance with Section 11 of this DPT;
- f) assist the User, in accordance with Sections 9, 12 and 13 of this DPT, with the obligations under Articles 32 to 36 GDPR, taking into account the nature of the processing and the information available to DocReveal;
- g) delete or return Personal Data in accordance with Section 16 of this DPT;
- h) make available to the User the information necessary to demonstrate compliance with Article 28 GDPR and allow for audits in accordance with Section 14 of this DPT.

- 7.2 DocReveal's obligations under this DPT are limited to the extent expressly set out herein. DocReveal owes **no obligations that are not expressly stated in this DPT or required by mandatory provisions of Data Protection Law.**

8. CONFIDENTIALITY

- 8.1 DocReveal shall ensure that access to Personal Data is limited to those of its personnel who need such access in order to perform the Agreement, that such persons are bound by an obligation of confidentiality of no shorter duration than that set out in Section 5.5 of the Terms, and that they are appropriately trained in the protection of personal data.
- 8.2 The confidentiality obligation does not apply where disclosure is required by law or by a decision of a public authority; in such a case DocReveal shall, to the extent permitted by law, inform the User in advance.

9. SECURITY OF PROCESSING

- 9.1 Taking into account the state of the art, the costs of implementation, the nature, scope, context and purposes of the processing and the risks to the rights and freedoms of natural persons, DocReveal has implemented the technical and organizational measures described below.
- 9.2 DocReveal is entitled to update the measures in Sections 9.4 to 9.6 at any time, provided that the overall level of security is not thereby reduced. The current version of those measures is available in the Security Overview at <https://docreveal.ai/assets/documents/legal/docreveal-security-overview-en.pdf>.
- 9.3 **Organizational measures.** DocReveal has adopted and undertakes to maintain the following organizational measures:
- a) **Information security policies** approved by management, reviewed at least annually.
 - b) **Confidentiality obligations** for all personnel and contractors with access to Personal Data, surviving the end of their engagement.
 - c) **Security awareness training** for personnel with access to Personal Data.
 - d) **Access management** based on the principles of least privilege and need-to-know, with regular review of access rights and immediate revocation on termination of a role.
 - e) **Supplier management** – assessment of sub-processors before engagement and contractual data protection obligations equivalent to those in the DPT.
 - f) **Incident management** – a documented procedure for detecting, classifying, resolving and reporting security incidents and personal data breaches.
 - g) **Change management** – testing and approval of changes before deployment to production.

9.4 Technical measures. DocReveal has adopted and undertakes to maintain the following technical measures:

- a) **Encryption in transit** – TLS 1.2 or higher for all connections between the user and the Services and between the components of the Services.
- b) **Encryption at rest** – encryption of stored data using industry-standard algorithms, with key management through the infrastructure provider's managed key service.
- c) **Tenant isolation** – each customer environment is logically separated from the environments of other customers; access is enforced at the level of the individual document (RBAC/ABAC).
- d) **Authentication** – registration and sign-in exclusively with an e-mail address and a password, with confirmation of registration by e-mail; passwords hashed using a modern algorithm with salt; API keys for integrations stored only in a hashed form; multi-factor authentication for DocReveal's administrative access. Sign-in through third-party identity providers is not offered (Section 2.1 of the Terms).
- e) **Audit trail** – logging of access to and operations performed on data, including the steps of AI processing and the queries submitted to the AI Features, with protection of logs against modification.
- f) **Availability and resilience** – redundant serverless infrastructure of the cloud provider, with a target availability of the Services of at least ninety percent (90%) per calendar month, excluding planned maintenance and events of force majeure (Section 2.10 of the Terms). **DocReveal does not create backups of User Data on behalf of the User** (Section 2.11 of the Terms); the User is responsible for exporting its data or for configuring continuous backups to its own or a third-party environment through the export functions and the integrations available in the web application.
- g) **Network security** – segmentation, firewalls, protection against denial-of-service attacks, and restriction of administrative access.
- h) **Vulnerability management** – regular scanning, patching and dependency updates.
- i) **Pseudonymization and minimization** – separation of identifiers where technically feasible, and a setting that redacts the names of third parties in AI answers, where activated by the User.

10. SUB-PROCESSORS

10.1 Sub-processors. The User hereby grants DocReveal a general written authorization to engage Sub-processors in the processing of Personal Data within the meaning of Article 28(2) GDPR. Where DocReveal engages such a Sub-processor, DocReveal shall ensure that the Sub-processor complies with the same data protection obligations as those set out in this DPT.

- 10.2 Approved Sub-processors.** The Sub-processors that process Personal Data contained in User Data on behalf of the User are listed in the list of Sub-processors available at <https://docreveal.ai/assets/documents/legal/docreveal-subprocessors-en.pdf> (the “Sub-processor List”), which also identifies the optional tools whose providers receive data only when the User or its Authorized Users use the respective tool. By concluding the Agreement, the User approves the Sub-processors listed in the Sub-processor List at that time. Public registers queried through the optional tools on the User’s instruction (such as company, insolvency and VAT registers) receive only the query and are not Sub-processors.
- 10.3** DocReveal shall notify the User of the intended addition or replacement of a Sub-processor at least fourteen (14) days in advance, by e-mail, through the Services or by updating the Sub-processor List referred to in Section 10.2.
- 10.4** The User may object to the addition or replacement of a Sub-processor **within fourteen (14) days** of the notification, by a written objection sent to info@docreveal.org **stating reasonable grounds relating to the protection of personal data**. Objections that are not reasoned, are not based on grounds relating to data protection, or are submitted late shall be disregarded and the Sub-processor shall be deemed approved.
- 10.5** Where the User raises a duly reasoned objection, DocReveal shall assess it and shall use reasonable efforts to make available an alternative arrangement or an additional safeguard. Where no such arrangement is reasonably available, DocReveal may (i) engage the Sub-processor notwithstanding the objection, in which case the User may, as its sole and exclusive remedy, terminate the Agreement or the affected Services by written notice with effect from the end of the then-current Subscription period, or (ii) itself terminate the Agreement or the affected Services on the same terms.
- 11. ASSISTANCE WITH DATA SUBJECT REQUESTS**
- 11.1 Requests of data subjects must be addressed by the data subject to the User.** Where DocReveal receives such a request directly, it shall not respond to it on the merits and shall, without undue delay, refer the data subject to the User and inform the User, unless prohibited by law.
- 11.2** Taking into account the nature of the processing, DocReveal shall assist the User by appropriate technical and organizational measures, insofar as this is possible, in fulfilling the User’s obligation to respond to requests for the exercise of data subjects’ rights. **The User shall primarily use the functionality of the Services**, which enables it to search, access, correct, export and delete Personal Data in its environment without DocReveal’s involvement.
- 11.3** Where the required assistance cannot be provided through the functionality of the Services, DocReveal shall provide it within a reasonable period, as a rule within fourteen (14) days of a written request, and is entitled to charge for it in accordance with Section 18 of this DPT.

12. PERSONAL DATA BREACHES

- 12.1** DocReveal shall notify the User of a personal data breach affecting Personal Data processed on behalf

of the User **without undue delay after becoming aware of it, no later than 48 hours**. The notification shall be sent by e-mail to the address associated with the User's account, or through the Services.

12.2 The notification shall contain the information available to DocReveal at that time, in particular a description of the nature of the breach, the categories and approximate number of data subjects and records concerned, the likely consequences and the measures taken or proposed. Where and insofar as it is not possible to provide the information at the same time, it shall be provided in phases without further undue delay.

12.3 **The obligation to notify a personal data breach to the supervisory authority under Article 33 GDPR and to communicate it to data subjects under Article 34 GDPR rests with the User.** DocReveal shall provide reasonable assistance, taking into account the nature of the processing and the information available to it.

13. ASSISTANCE WITH IMPACT ASSESSMENTS AND PRIOR CONSULTATION

13.1 Taking into account the nature of the processing and the information available to it, DocReveal shall provide the User with reasonable assistance in carrying out a data protection impact assessment under Article 35 GDPR and in any prior consultation with the supervisory authority under Article 36 GDPR.

13.2 **That assistance consists primarily in making available the Documentation, this DPT (including Sections 3, 4, 9 and 10.2) and the Security Overview**, which the parties agree normally contain the information necessary for the User to carry out such an assessment. Where the User demonstrates that this information is insufficient for a specific assessment, DocReveal shall provide such further information as is available to it and as relates to the processing carried out on behalf of the User; such further assistance is chargeable in accordance with Section 18 of this DPT.

14. AUDITS AND INSPECTIONS

14.1 DocReveal shall make available to the User the information necessary to demonstrate compliance with the obligations laid down in Article 28 GDPR. **The parties agree that this obligation is fulfilled primarily** by DocReveal providing, on written request: (i) the current Security Overview and a description of the technical and organizational measures; (ii) copies of, or attestations relating to, the certifications and audit reports of DocReveal's infrastructure providers (in particular ISO/IEC 27001 certificates and SOC 2 Type II reports), to the extent DocReveal is entitled to disclose them; and (iii) a completed standard security questionnaire.

14.2 Where the information provided under Section 14.1 does not enable the User to demonstrate compliance with Article 28 GDPR, the User is entitled to carry out an audit or inspection, subject to all of the following conditions:

- a) the audit is requested in writing at info@docreveal.org at least **thirty (30) days** in advance and the request specifies the scope and the grounds for it;

- b) the audit is carried out no more than **once in any twelve (12) month period**, unless it is required by a binding instruction of a supervisory authority or follows a substantiated personal data breach affecting the User;
- c) the audit takes place during DocReveal's ordinary business hours, does not exceed **one (1) business day**, does not disrupt the operation of the Services and is limited to systems and documentation which relate to the processing of Personal Data on behalf of the User;
- d) the audit is carried out at the User's own cost, and the User shall reimburse DocReveal for the time and costs incurred in accordance with Section 18 of this DPT;
- e) the User shall provide DocReveal with the audit report and shall not disclose it to any third party other than the competent supervisory authority.

14.3 DocReveal may object in writing to an auditor appointed by the User where, in DocReveal's reasonable opinion, the auditor is insufficiently qualified, is not independent, is in a competitive position with DocReveal or is otherwise manifestly unsuitable. In such a case the User shall appoint a different auditor.

15. TRANSFERS OF PERSONAL DATA OUTSIDE THE EEA

15.1 Where Personal Data are transferred to a country outside the EEA, DocReveal shall ensure that the transfer takes place only on the basis of a safeguard under Chapter V GDPR, in particular an adequacy decision of the European Commission (including, where applicable, the EU-U.S. Data Privacy Framework) or the **standard contractual clauses** adopted by Commission Implementing Decision (EU) 2021/914 (the "standard contractual clauses").

16. DELETION AND RETURN OF PERSONAL DATA

16.1 Upon termination of the Agreement, DocReveal shall, **at the User's choice, delete or return** the Personal Data processed on behalf of the User, and shall delete existing copies, unless Union or Member State law requires their further storage. **Where the User itself deletes its account, or where DocReveal terminates the Agreement and deletes the account**, the User shall export the Personal Data it wishes to retain before the deletion takes effect – in the case of Section 12.1 of the Terms, within the fourteen (14) day notice period.

16.2 **The User must communicate its choice in writing before the termination of the Agreement takes effect.** Where the User does not do so, DocReveal shall delete the Personal Data upon the expiry of the period set out in Section 16.3, and the User shall have no claim in respect of that deletion.

16.3 Subject to Section 16.5, deletion shall be carried out within thirty (30) days of the termination of the Agreement, or, where Section 10 of the Terms (switching under the Data Act) applies, upon the expiry of the Additional Access Period under Section 10.12 of the Terms. Where the User deletes its account (workspace), the deletion of the entire workspace – including all Personal Data contained in User Data and all data derived from it, the configuration and the integration credentials – takes effect

immediately and is complete and irreversible (Section 12.3 of the Terms). DocReveal does not keep backups of User Data and cannot restore deleted data; the User must therefore export everything it wishes to retain before the deletion. Technical recovery copies that the cloud infrastructure maintains for operational resilience (such as database point-in-time recovery or previous versions of stored objects) cannot be used to restore data at the User's request and are automatically erased no later than thirty-five (35) days after the deletion.

16.4 Return of Personal Data is effected by means of the standard self-service export tools of the Services in the formats described in the Documentation. DocReveal is not obliged to provide the data in any other format; the standard self-service export is provided free of charge, while any conversion or other assistance is chargeable in accordance with Section 18 of this DPT.

16.5 The obligation to delete does not apply to data whose further storage is required of DocReveal by Union or Member State law, including records that must be retained in order to comply with a legal obligation or with a decision of a public authority. Where such data are retained, DocReveal shall restrict their processing to the purpose for which they are retained and shall continue to protect them in accordance with Section 9 of this DPT.

16.6 DocReveal shall confirm the deletion in writing at the User's written request.

17. AI FEATURES

17.1 Where the User uses AI Features, Personal Data contained in User Data may be processed by AI models.

17.2 **DocReveal does not use User Data or Outputs to train its own or third-party general-purpose AI models.** Where the Services adapt their extraction behavior on the basis of corrections made by the User, that adaptation takes place **only within the User's own tenant environment** and the resulting data are not made available to other customers.

17.3 Outputs are User Data and, where they contain Personal Data, they are processed under this DPT. Given the probabilistic nature of AI Features, **Outputs may contain inaccuracies**; ensuring the accuracy of Personal Data within the meaning of Article 5(1)(d) GDPR, and reviewing Outputs before they are used, is the responsibility of the User.

18. FEES FOR ASSISTANCE

18.1 DocReveal is entitled to charge the User for costs and time reasonably incurred in connection with the performance of any obligation under Sections 5.3, 11.3, 13.2, 14 and 16.4 of this DPT, and in connection with the handling of any request going beyond the standard functionality of the Services.

18.2 Unless agreed otherwise, such assistance is charged on a time-and-material basis at DocReveal's hourly rate of **EUR 100 + VAT** plus costs actually incurred, consistently with the Terms. DocReveal shall inform the User of the anticipated scope of the work before commencing it.

- 18.3 Sections above do not apply to assistance which DocReveal is required to provide free of charge under mandatory provisions of Data Protection Law, nor to activities in respect of which DocReveal may not charge a fee under Section 10.16 of the Terms and Article 29 of Regulation (EU) 2023/2854 (with effect from 12 January 2027).

19. LIABILITY

- 19.1 **The limitations and exclusions of liability set out in Section 7 of the Terms apply to this DPT and to any claim arising out of or in connection with it**, whether based on contract, tort, statute or otherwise, including any claim for reimbursement under Article 82(5) GDPR. All claims of the User under the Agreement and under this DPT taken together are subject to a **single aggregate cap** under Section 7.2 of the Terms.
- 19.2 DocReveal is not liable for any damage, including administrative fines, arising from (i) the User's instructions, (ii) the User's breach of this DPT or of Data Protection Law, (iii) the content of User Data, (iv) the User's configuration of the Services, its access settings or its integrations, or (v) the conduct of the User's Authorized Users.
- 19.3 **The User shall indemnify DocReveal** in accordance with Section 6 of the Terms against any claim, fine, penalty, loss or cost (including reasonably incurred legal costs) arising from the User's breach of this DPT or of Data Protection Law, from the content of User Data, or from any claim of a data subject or of a supervisory authority relating to processing for which the User is responsible as controller.

20. TERM, CHANGES AND FINAL PROVISIONS

- 20.1 This DPT takes effect upon the conclusion of the Agreement and remains in force for as long as DocReveal processes Personal Data on behalf of the User.
- 20.2 **DocReveal may amend this DPT** in the same manner and subject to the same conditions as apply to changes to the Terms.