

# DATA PROCESSING AGREEMENT

## 1. BACKGROUND

- 1.1. As part of Keepit's provision of Services to the Customer, Keepit will be processing Customer Content, which may include personal data, on behalf of the Customer. The purpose of the processing activities is described in the Terms of Service. Accordingly, the Parties have entered into this Data Processing Agreement.

## 2. DEFINITIONS

- 2.1. All capitalized terms used shall have the meaning given to them in the applicable Terms of Service or this Data Processing Agreement:
- 2.2. **Data Processing Agreement** means this agreement on processing of Customer Content, which may include personal data, including any schedules.
- 2.3. **Data Protection Legislation** means all the laws and rules governing the processing and protection of personal data throughout the European Economic Area (EEA) or the United Kingdom (UK) as amended, supplemented and/or modified from time to time, relevant national legislation, the GDPR and, where relevant, the guidelines and rules issued by the Danish Data Protection Agency or other competent supervisory authorities in the EEA or the UK (including the national supervisory authorities).
- 2.4. **GDPR** means 'Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data and repealing Directive 95/46/EC (General Data Protection Regulation)' as amended, supplemented and/or modified from time to time.
- 2.5. **UK GDPR** means the GDPR as incorporated into the law of the United Kingdom under the UK European Union (Withdrawal) Act 2018 and amended by the Data Protection, Privacy and Electronic Communications (Amendments etc.) (EU Exit) Regulations 2019.
- 2.6. The terms '**personal data**', '**special categories of personal data**', '**personal data breach**', '**process/processing**', '**controller**', '**processor**', '**data subject**', '**supervisory authority**' and '**technical and organizational measures**' as used in this Data Processing Agreement shall be understood in accordance with the Data Protection Legislation, including the GDPR.

## 3. PROCESSING OF CUSTOMER CONTENT

- 3.1. The Parties agree that in relation to the GDPR, the Customer acts as the 'data controller' and Keepit as the 'data processor' except for situations where the Customer act as the 'data processor' and Keepit as the 'sub-processor'.
- 3.2. Keepit shall process Customer Content on behalf of the Customer in accordance with the Customer's instruction. The Agreement along with the Customer's configuration and use of the Services constitute Customer's complete and documented instructions to Keepit.
- 3.3. Keepit must ensure that the persons involved in the processing of Customer Content under the Agreement have either committed themselves to confidentiality or are subject to a proper statutory duty of confidentiality, and that they only process Customer Content in compliance with the given instructions and the Data Protection Legislation.
  - 3.3.1. Where the Customer is not subject to the Data Protection Legislation, the Parties acknowledge and accept that the rights and obligations of each Party under of this Data Processing Agreement shall apply mutatis mutandis.
- 3.4. Keepit shall, upon request from the Customer, provide reasonable access to all necessary information in order for the Customer to ensure compliance with the obligations laid down in the Data Protection Legislation.
- 3.5. Keepit must immediately notify the Customer if, in Keepit's opinion, an instruction from the Customer according to this section is contrary to the Data Protection Legislation as required in accordance with GDPR Article 28(3)(h).
- 3.6. In the event Keepit becomes aware of a personal data breach which has led to accidental or malicious destruction, loss, alteration or distribution of Customer Content while processed by Keepit, Keepit will, in accordance with GDPR Article 33(2):
  - Notify the Customer about the incident without undue delay,
  - Investigate the incident and provide the Customer with detailed information about the incident,
  - Take reasonable steps to mitigate the effects and minimize the damage from the incident.
- 3.7. Notification of a security incident will be delivered to a registered contact person with the Customer by any means available (including e-mail).

- 3.8. The Customer is solely responsible for fulfilling any third-party notification obligations, such as GDPR Article 33 or any other applicable law or regulation.
- 3.9. Notification by Keepit of a security incident does not in itself constitute an acknowledgment of any wrongdoing, fault or liability by Keepit.

#### **4. SECURITY MEASURES**

- 4.1. Keepit implements and maintains appropriate organizational and technical measures to protect the Customer Content processed under the Agreement pursuant to GDPR Articles 28(3)(c) and 32. These measures are based on industry best practices such as ISO 27001, ISO27002, NIST SP800-30, NIST SP800-39 and FEMA guidelines.
  - 4.1.1. Keepit has described its current technical and organizational measures in a separate document 'Keepit Technical and Organizational Measures' available upon request. Keepit may update the technical and organizational measures from time to time, so long as the updated measures do not decrease the overall protection of Customer Content.
  - 4.1.2. The Customer is solely responsible for determining if the technical and organizational measures around the Services meet the requirements for the Customer and the Customer Content. This includes, but is not limited to, the GDPR.
- 4.2. Keepit is ISO 27001:2022 certified and can provide the certification upon request.
- 4.3. Keepit will additionally on a yearly basis obtain an independent third-party SOC2 audit concerning Keepit's organizational procedures, security, and assets. The results of the most recent audit can be requested by the Customer. Any facility in which Customer Content is physically located undergoes equivalent or stricter certifications annually as well.
  - 4.3.1. Keepit may, at its discretion, discontinue its SOC2 audit in favor of another relevant audit.
  - 4.3.2. The Customer may at its own expense contest the scope and/or methodology of the audit and may in such cases at its own expense request a new audit/inspection under a revised scope and/or different methodology, agreed by the Parties.
  - 4.3.3. The Customer agrees to exercise its audit right by requesting the most recent audit or a third-party audit as described in Section 4.3.
  - 4.3.4. The parties have further agreed that the Customer, upon prior agreement, may carry out on-site audits at Keepit's premises located at Per Henrik Lings Allé 4, 7th floor, 2100 Copenhagen OE, Denmark.

#### **5. RECORDS OF PROCESSING ACTIVITIES**

- 5.1. Keepit maintains records of processing activities as per GDPR Article 30(2) and makes these records available to the Customer upon request or directly as part of the Services.

#### **6. KEEPIT'S GENERAL OBLIGATIONS**

- 6.1. Keepit shall apply and comply with the Data Protection Legislation and shall not perform its obligations under the Terms of Service and this Data Processing Agreement in such a way, as to cause the Customer to breach any of its obligations under applicable Data Protection Legislation.
- 6.2. Taking into account the nature of the processing, the information available to Keepit and insofar it is possible, Keepit provides reasonable assistance to the Customer by appropriate technical and organizational measures, for the fulfilment of the Customer's obligation to respond to requests for exercising the data subject's rights laid down in GDPR Chapter III.
- 6.3. Keepit must assist the Customer in ensuring compliance with any of the Customer's obligations pursuant to GDPR Articles 32-36.

#### **7. SUB-PROCESSING**

- 7.1. The Customer agrees that Keepit may engage sub-processors. In case of engagements, changes or disengagements of sub-processors, Keepit shall notify the Customer directly in writing about such change with thirty (30) calendar days' notice. The Customer will have twenty-five (25) calendar days to object to the change in writing to Keepit. The objection of the Customer must be well-founded. Absence of any objections from the Customer shall be deemed a consent to the sub-processing.
- 7.2. Keepit warrants and ensures that in case sub-processing is carried out, the sub-processing will be lawful and that any and all sub-processors will undertake and be subject to the same terms and obligations as Keepit as set out in this Data Processing Agreement. Should the sub-processors not comply with their obligations, Keepit shall remain responsible for all acts and omissions of such sub-processors.
- 7.3. A list of Keepit's sub-processors is available at <https://www.keepit.com/data-processing-agreement/>.

- 7.4. Keepit shall on a yearly basis obtain an auditor's report from an independent third party concerning the sub-processor's compliance with the GDPR, the applicable EU or Member State data protection provisions and the Clauses.
- 7.4.1. Where the sub-processor forms part of Keepit's organization, including by being an affiliate of Keepit, such audit may be conducted as a consolidated or group-level audit covering the relevant entities within the organization, provided that the audit sufficiently addresses the sub-processor's compliance with the requirements set forth in this Agreement. In such case, a separate or individual audit report for each entity shall not be required.
- 7.4.2. The parties have agreed that either of the following is sufficient for compliance purposes:
- 7.4.3. SOC 2 audit and/or ISO 27001 certification.
- 7.4.4. The SOC 2 audit and/or ISO 27001 certification shall upon request be submitted to the data controller for information.

## **8. TRANSFERS OF CUSTOMER CONTENT TO A THIRD COUNTRY**

- 8.1. If the Customer uses a Keepit data center within the EU/EEA or the UK Keepit may not transfer nor authorize the transfer of Customer Content to countries outside the EU/EEA or the UK without the prior consent of the Customer. If Customer Content is transferred from a country within the EU/EEA or the UK to a country outside of the EU/EEA or the UK, the Parties shall ensure that the Customer Content is adequately protected in accordance with Chapter V of the GDPR. To achieve this, the Parties shall, unless agreed otherwise, rely on EU and/or ICO approved standard contractual clauses for the transfer of Customer Content including supplementary measures.
- 8.2. If the Customer uses a Keepit data center outside of the EU/EEA or the UK then Keepit's support organization may occasionally, as part of an ongoing support issue with the Customer, request access to the Customer Content. It is the responsibility of the Customer to determine if such access from another country can be granted under applicable laws and regulations, before granting such access and thereby providing Keepit with instruction to process Customer Content. The request and the granting of access will be logged. Technical and organizational measures are in place to limit access to Customer Content.
- 8.3. Any Keepit personnel engaged in the maintenance, support, or processing of Customer Content is instructed and obligated to maintain the confidentiality of Customer Content, including after a termination of the Services.

## **9. DURATION OF DATA PROCESSING**

- 9.1. The provisions of this Data Processing Agreement and the obligations of the Parties shall remain in force, as long as Keepit processes Customer Content on behalf of the Customer under the Agreement. Keepit's processing of personal data on behalf of the controller may be performed when the Agreement commences.
- 9.2. The Customer can configure its own data retention rules within the backup services, in accordance with the Terms of Service.
- 9.3. The Parties agree that upon termination or expiry of the Agreement, Keepit shall, at the choice of the Customer, (i) return all Customer Content processed under the Agreement and any copies thereof to the Customer, or (ii) delete all Customer Content processed under the Agreement and certify to the Customer that this has been done, including for avoidance of doubt, delete such Customer Content from any computer, server, and/or any other storage device or media, unless European Union and/or relevant member state law requires storage of such Customer Content.
- 9.4. Notwithstanding clause 10.2 above, Keepit will retain all Customer Content processed under the Agreement for 30 days after the deletion of the Customer's account or termination thereof. This 'deletion retention period' will ensure that the Customer's access to its Customer Content can be re-established after any conceivable targeted attack against the Customer's primary data and backup data. After expiration of the 'deletion retention' period, Keepit will delete all records of the Customer Content without undue delay.

## Schedule A

## Processing Activities, Categories of Data Subjects and Types of Personal Data

This Schedule forms an integral part of the Agreement.

### 1. PROCESSING ACTIVITIES

- 1.1. Keepit's processing of Customer Content (the nature of the processing) shall mainly pertain to providing a cloud-based solution that enables the Customer to perform backup, recover and restoration of their Customer Content cf. the Terms of Service. Such processing is carried out on an ongoing basis for the duration of the Customer's use of the Services.
- 1.2. Customer Content will be subject to several processing activities, including but not limited to any operation or set of operations performed on Customer Content, solely by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure, or destruction.
- 1.3. Keepit only processes data by automatic means and stores the Customer Content in data centers of the Customer's designation. Keepit does not access and is not familiar with the content of the Customer Content unless Customer specifically instructs Keepit to gain access hereto.

### 2. CATEGORIES OF DATA SUBJECTS

- 2.1. Customer Content may contain any categories of data subjects, and it is solely determined, changed, and controlled by the Customer. Data subjects may be customers, employees, patients, professionals, minors, etc. Keepit has therefore implemented and maintains the level of security as described in Section 4 of the Data Processing Agreement above and Section 3 below.

### 3. TYPES OF PERSONAL DATA

- 3.1. Customer Content may consist of any types of personal data about data subjects. It is entirely dependent of the Customer's type of data and its use of the Services. Customer Content stored by Keepit may contain non-sensitive personal data (such as contact information, bank information, names, addresses, e-mail addresses, information relating to criminal convictions and offences, national identification numbers) or special categories of personal data (such as health data, data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data etc.) as defined in GDPR Article 9. Keepit has therefore implemented and maintains the level of security that takes into account that the processing may involve a large volume of personal data, including personal data subject to GDPR Article 9, which is why a 'high' level of security has been established.