Standard Contractual Clauses

For the purposes of Article 28(3) of Regulation 2016/679 (the GDPR)

between

Customer Entity Name Specified in the Order Form
(the data controller)

and

Keepit A/S
Per Henrik Lings Allé 4, 7th floor, 2100 Copenhagen OE, Denmark
(the data processor)

each a 'party'; together 'the parties'

HAVE AGREED on the following Contractual Clauses (the Clauses) in order to meet the requirements of the GDPR and to ensure the protection of the rights of the data subject.

1. Table of Contents

2. Preamble

1. These Contractual Clauses (the Clauses) set out the rights and obligations of the data controller and the data processor, when processing personal data on behalf of the data controller.

2. The Clauses have been designed to ensure the parties' compliance with Article 28(3) of Regulation 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).

3. In the context of the provision of the Services, the data processor will process personal data on behalf of the data controller in accordance with the Clauses.

4. The Clauses shall take priority over any similar provisions contained in other agreements between the parties.

5. Four appendices are attached to the Clauses and form an integral part of the Clauses.

6. Appendix A contains details about the processing of personal data, including the purpose and nature of the processing, type of personal data, categories of data subject and duration of the processing.

7. Appendix B contains the data controller's conditions for the data processor's use of sub-processors and a list of sub-processors authorised by the data controller.

8. Appendix C contains the data controller's instructions with regards to the processing of personal data, the minimum security measures to be implemented by the data processor and how audits of the data processor and any sub-processors are to be performed.

9. Appendix D contains provisions for other activities which are not covered by the Clauses.

10. The Clauses along with appendices shall be retained in writing, including electronically, by both parties.

11. The Clauses shall not exempt the data processor from obligations to which the data processor is subject pursuant to the General Data Protection Regulation (the GDPR) or other legislation.

3. The rights and obligations of the data controller

1. The data controller is responsible for ensuring that the processing of personal data takes place in compliance with the GDPR (see Article 24 GDPR), the applicable EU or Member State[1] data protection provisions and the Clauses.

2. The data controller has the right and obligation to make decisions about the purposes and means of the processing of personal data.

[1] References to "Member States" made throughout the Clauses shall be understood as references to "EEA Member States".

3. The data controller shall be responsible, among other, for ensuring that the processing of personal data, which the data processor is instructed to perform, has a legal basis.

4. The data processor acts according to instructions

1. The data processor shall process personal data only on documented instructions from the data controller, unless required to do so by Union or Member State law to which the processor is subject. Such instructions shall be specified in appendices A and C. Subsequent instructions can also be given by the data controller throughout the duration of the processing of personal data, but such instructions shall always be documented and kept in writing, including electronically, in connection with the Clauses.

2. The data processor shall immediately inform the data controller if instructions given by the data controller, in the opinion of the data processor, contravene the GDPR or the applicable EU or Member State data protection provisions.

5. Confidentiality

1. The data processor shall only grant access to the personal data being processed on behalf of the data controller to persons under the data processor's authority who have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality and only on a need to know basis. The list of persons to whom access has been granted shall be kept under periodic review. On the basis of this review, such access to personal data can be withdrawn, if access is no longer necessary, and personal data shall consequently not be accessible anymore to those persons.

2. The data processor shall at the request of the data controller demonstrate that the concerned persons under the data processor's authority are subject to the abovementioned confidentiality.

6. Security of processing

1. Article 32 GDPR stipulates that, taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the data controller and data processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk.

   The data controller shall evaluate the risks to the rights and freedoms of natural persons inherent in the processing and implement measures to mitigate those risks. Depending on their relevance, the measures may include the following:
   a. Pseudonymisation and encryption of personal data;

   b. the ability to ensure ongoing confidentiality, integrity, availability and resilience of processing systems and services;

   c. the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident;

d. a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.

2. According to Article 32 GDPR, the data processor shall also – independently from the data controller – evaluate the risks to the rights and freedoms of natural persons inherent in the processing and implement measures to mitigate those risks. To this effect, the data controller shall provide the data processor with all information necessary to identify and evaluate such risks.

3. Furthermore, the data processor shall assist the data controller in ensuring compliance with the data controller's obligations pursuant to Articles 32 GDPR, by *inter alia* providing the data controller with information concerning the technical and organisational measures already implemented by the data processor pursuant to Article 32 GDPR along with all other information necessary for the data controller to comply with the data controller's obligation under Article 32 GDPR.

   If subsequently – in the assessment of the data controller – mitigation of the identified risks require further measures to be implemented by the data processor, than those already implemented by the data processor pursuant to Article 32 GDPR, the data controller shall specify these additional measures to be implemented in Appendix C.

7. Use of sub-processors

1. The data processor shall meet the requirements specified in Article 28(2) and (4) GDPR in order to engage another processor (a sub-processor).

2. The data processor shall therefore not engage another processor (sub-processor) for the fulfilment of the Clauses without the prior general written authorisation of the data controller.

3. The data processor has the data controller's general authorisation for the engagement of sub-processors. The data processor shall inform in writing the data controller of any intended changes concerning the addition or replacement of sub-processors at least thirty (30) calendar days in advance, thereby giving the data controller the opportunity to object to such changes prior to the engagement of the concerned sub-processor(s). Longer time periods of prior notice for specific sub-processing services can be provided in Appendix B. The list of sub-processors already authorised by the data controller can be found in Appendix B.

4. Where the data processor engages a sub-processor for carrying out specific processing activities on behalf of the data controller, the same data protection obligations as set out in the Clauses shall be imposed on that sub-processor by way of a contract or other legal act under EU or Member State law, in particular providing sufficient guarantees to implement appropriate technical and organisational measures in such a manner that the processing will meet the requirements of the Clauses and the GDPR.

   The data processor shall therefore be responsible for requiring that the sub-processor at least complies with the obligations to which the data processor is subject pursuant to the Clauses and the GDPR.

5. A copy of such a sub-processor agreement and subsequent amendments shall – at the data controller's request – be submitted to the data controller, thereby giving the data controller the opportunity to ensure that the same data protection obligations as set out in the Clauses are imposed on the sub-processor. Clauses on business related issues that do not affect the legal data protection content of the sub-processor agreement, shall not require submission to the data controller.

6. The processor shall agree a third-party beneficiary clause with the sub-processor whereby – in the event the processor has factually disappeared, ceased to exist in law or has become insolvent – the controller shall have the right to terminate the sub-processor contract and to instruct the sub-processor to erase or return the personal data.

7. If the sub-processor does not fulfil his data protection obligations, the data processor shall remain fully liable to the data controller as regards the fulfilment of the obligations of the sub-processor. This does not affect the rights of the data subjects under the GDPR – in particular those foreseen in Articles 79 and 82 GDPR – against the data controller and the data processor, including the sub-processor.

8. Transfer of data to third countries or international organisations

1. Any transfer of personal data to third countries or international organisations by the data processor shall only occur on the basis of documented instructions from the data controller and shall always take place in compliance with Chapter V GDPR.

2. In case transfers to third countries or international organisations, which the data processor has not been instructed to perform by the data controller, is required under EU or Member State law to which the data processor is subject, the data processor shall inform the data controller of that legal requirement prior to processing unless that law prohibits such information on important grounds of public interest.

3. Without documented instructions from the data controller, the data processor therefore cannot within the framework of the Clauses:

    a. transfer personal data to a data controller or a data processor in a third country or in an international organization

    b. transfer the processing of personal data to a sub-processor in a third country

    c. have the personal data processed in by the data processor in a third country

4. The data controller's instructions regarding the transfer of personal data to a third country including, if applicable, the transfer tool under Chapter V GDPR on which they are based, shall be set out in Appendix C.6.

5. The Clauses shall not be confused with standard data protection clauses within the meaning of Article 46(2)(c) and (d) GDPR, and the Clauses cannot be relied upon by the parties as a transfer tool under Chapter V GDPR.

9. Assistance to the data controller

1. Taking into account the nature of the processing, the data processor shall assist the data controller by appropriate technical and organisational measures, insofar as this

is possible, in the fulfilment of the data controller's obligations to respond to requests for exercising the data subject's rights laid down in Chapter III GDPR.

This entails that the data processor shall, insofar as this is possible, assist the data controller in the data controller's compliance with:

a. the right to be informed when collecting personal data from the data subject
b. the right to be informed when personal data have not been obtained from the data subject
c. the right of access by the data subject
d. the right to rectification
e. the right to erasure ('the right to be forgotten')
f. the right to restriction of processing
g. notification obligation regarding rectification or erasure of personal data or restriction of processing
h. the right to data portability
i. the right to object
j. the right not to be subject to a decision based solely on automated processing, including profiling

2. In addition to the data processor's obligation to assist the data controller pursuant to Clause 6.3., the data processor shall furthermore, taking into account the nature of the processing and the information available to the data processor, assist the data controller in ensuring compliance with:

   a. The data controller's obligation to without undue delay and, where feasible, not later than 72 hours after having become aware of it, notify the personal data breach to the competent supervisory authority of the data controller, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons;

   b. the data controller's obligation to without undue delay communicate the personal data breach to the data subject, when the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons;

   c. the data controller's obligation to carry out an assessment of the impact of the envisaged processing operations on the protection of personal data (a data protection impact assessment);

   d. the data controller's obligation to consult the competent supervisory authority of the data controller, prior to processing where a data protection impact assessment indicates that the processing would result in a high risk in the absence of measures taken by the data controller to mitigate the risk.

3. The parties shall define in Appendix C the appropriate technical and organisational measures by which the data processor is required to assist the data controller as well as the scope and the extent of the assistance required. This applies to the obligations foreseen in Clause 9.1. and 9.2.

10. Notification of personal data breach

1. In case of any personal data breach, the data processor shall, without undue delay after having become aware of it, notify the data controller of the personal data breach.

2. The data processor's notification to the data controller shall, if possible, take place within 72 hours after the data processor has become aware of the personal data breach to enable the data controller to comply with the data controller's obligation to notify the personal data breach to the competent supervisory authority, cf. Article 33 GDPR.

3. In accordance with Clause 9(2)(a), the data processor shall assist the data controller in notifying the personal data breach to the competent supervisory authority, meaning that the data processor is required to assist in obtaining the information listed below which, pursuant to Article 33(3)GDPR, shall be stated in the data controller's notification to the competent supervisory authority:

    a. The nature of the personal data breach including where possible, the categories and approximate number of data subjects concerned and the categories and approximate number of personal data records concerned;

    b. the likely consequences of the personal data breach;

    c. the measures taken or proposed to be taken by the controller to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.

4. The parties shall define in Appendix C all the elements to be provided by the data processor when assisting the data controller in the notification of a personal data breach to the competent supervisory authority.

11. Erasure and return of data

1. On termination of the provision of personal data processing services, the data processor shall be under obligation at the controller's choice either (i) to delete all personal data processed on behalf of the data controller and certify to the data controller that it has done so, or (ii) to return all the personal data to the data controller and delete existing copies unless Union or Member State law requires storage of the personal data.

12. Audit and inspection

1. The data processor shall make available to the data controller all information necessary to demonstrate compliance with the obligations laid down in Article 28 and the Clauses and allow for and contribute to audits, including inspections, conducted by the data controller or another auditor mandated by the data controller.

2. Procedures applicable to the data controller's audits, including inspections, of the data processor and sub-processors are specified in appendices C.7. and C.8.

3. The data processor shall be required to provide the supervisory authorities, which pursuant to applicable legislation have access to the data controller's and data processor's facilities, or representatives acting on behalf of such supervisory authorities, with access to the data processor's physical facilities on presentation of appropriate identification.

13. The parties' agreement on other terms

1. The parties may agree other clauses concerning the provision of the personal data processing service specifying e.g. liability, as long as they do not contradict directly or indirectly the Clauses or prejudice the fundamental rights or freedoms of the data subject and the protection afforded by the GDPR.

14. Commencement and termination

1. The Clauses shall become effective on the date of both parties' signature of an agreement for the provisioning of the Services of which these Clauses are an integral part.

2. Both parties shall be entitled to require the Clauses renegotiated if changes to the law or inexpediency of the Clauses should give rise to such renegotiation.

3. The Clauses shall apply for the duration of the provision of personal data processing services. For the duration of the provision of personal data processing services, the Clauses cannot be terminated unless other Clauses governing the provision of personal data processing services have been agreed between the parties.

4. If the provision of personal data processing services is terminated, and the personal data is deleted or returned to the data controller pursuant to Clause 11.1. and Appendix C.4., the Clauses may be terminated by written notice by either party.

5. Signature

   On behalf of the data controller

Name	Customer Entity Name Specified in the Order Form
Signature	Executed either by online click-through, by signature together with the Terms of Service, or by separate signature.

   On behalf of the data processor

Name	Keepit A/S
Signature	Executed upon the Customer's online click-through acceptance, or by signature together with the Terms of Service, or by separate signature.

15. Data controller and data processor contacts/contact points

1. The parties may contact each other using the following contacts/contact points:

2. The parties shall be under obligation continuously to inform each other of changes to contacts/contact points.

Name, Position, E-mail address of the data controller:
Entered and kept up to date by the data controller within the Services

Name, Position, E-mail address of the data processor:
Entity Name: Keepit A/S
Address: Per Henrik Lings Allé 4, 7th floor, 2100 Copenhagen OE, Denmark
Att.: Data Protection Officer
E-mail address: dpo@keepit.com

Appendix A Information about the processing

As part of Keepit's provision of Services to the Customer, Keepit will be processing personal data on behalf of the Customer.

A.1. The purpose of the data processor's processing of personal data on behalf of the data controller is:

Providing backup services whereby the data controller can create and maintain data backup of certain cloud solutions used by the data controller at his discretion and initiative, and whereby the data controller restore data back to where the data originally resided or download data using the export/restore tools offered.

A.2. The data processor's processing of personal data on behalf of the data controller shall mainly pertain to (the nature of the processing):

Providing a technical cloud-based solution that enables the data controller to perform backup, recover and restoration of their data cf. A.1., by making available data centers and technical solutions for extracting and creating data backup, at the data processor's data centers.

The personal data will be subject to several processing activities, including but not limited to: any operation or set of operations performed on personal data or on sets of personal data, 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. Such processing is carried out on an ongoing basis for the duration of the data controller's use of the Services.

The data processor only processes data by automatic means and stores the data of the data controller in data processor's own data centers designated by the data controller. The data processor does not access and is not familiar with the content of the data controller's backup data, unless the data controller specifically instructs the data processor to gain access hereto.

A.3. The processing includes the following types of personal data about data subjects:

Data may consist of any types of personal data about data subjects. It is entirely dependent of the data controller's types of data and their use of the backup services.

Personal data stored may contain any kind of 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, etc.) as defined in GDPR article 9.

A.4. Processing includes the following categories of data subject:

The backup data may contain any categories of data subjects, and it is solely determined, changed, and controlled by the data controller. Data subjects may be customers, employees, patients, professionals, minors, etc.

A.5. The data processor's processing of personal data on behalf of the data controller may be performed when the Clauses commence. Processing has the following duration:

The data controller can configure its own data retention rules within the Services. Data Retention refers to the amount of time a data object remains in the backup after being deleted from the data controller's cloud solutions covered by the Services.

At termination the data processor will retain all data processed under these Clauses for 30 days after the deletion of the data controller's account or termination thereof. This "deletion retention" will ensure that the data controller's access to personal data can be reestablished after any conceivable targeted attack against the data controller's primary data and backup

data. After expiration of the retention period, the data processor will delete all records of the data controller's personal data without undue delay.

Appendix B Authorised sub-processors

B.1. Approved sub-processors

On commencement of the Clauses, the data controller authorises the engagement of the following sub-processors:

Name	Location	Role
Keepit Poland Sp. z o.o. (Wholly-owned EU based affiliate of Keepit A/S)	Poland	Supporting Keepit's delivery of customer support services.

The data controller shall on the commencement of the Clauses authorize the use of the abovementioned sub-processors for the processing described for that party. The data processor shall not be entitled – without prior notice to the data controller – to engage a sub-processor for a 'different' processing than the one which has been agreed upon or have another sub-processor perform the described processing

B.2. Prior notice for the engagement or change of sub-processors

In case of engagements, change or disengagements of sub-processors, the data processor will notify the data controller directly in writing about such change with thirty (30) calendar days' notice cf. point 7.3 of the Clauses.

The data controller will have twenty-five (25) calendar days to object to the change in writing to the data processor. The objection of the data controller must be well-founded. Absence of any objections from the data controller shall be deemed a consent to the sub-processing.

In addition to notifying the data controller directly in writing about such changes, the processor will notify the change on its website, at www.keepit.com/data-processing-agreement/.

Appendix C Instruction pertaining to the use of personal data

C.1. The subject of/instruction for the processing

The data processor's processing of personal data on behalf of the data controller shall be carried out by the data processor performing the following:

The Terms of Service along with the data controller's configuration and use of the Services constitute the data controller's documented instructions to the data processor for purpose of providing backup services as described in i) these Clauses including appendices, particularly Appendix A, ii) the Terms of Service and data controller's configuration regarding the data processor's provision of the services.

C.2. Security of processing

The level of security shall take into account that the processing involves a large volume of personal data including personal data subject to Article 9 GDPR on 'special categories of personal data' which is why a 'high' level of security has been established.

The data processor shall hereafter be entitled and under obligation to make decisions about the technical and organizational security measures that are to be applied to create the necessary (and agreed) level of data security. The data processor may update the technical and organizational measures from time to time, as long as the updated measures do not decrease the overall protection of personal data.

The data processor has described its current technical and organizational measures in a separate document "Keepit Technical and Organizational Measures". Data Processor may update the technical and organizational measures from time to time, so long as the updated measures do not decrease the overall protection of personal data.

C.3. Assistance to the data controller

The data processor shall insofar as this is possible – within the scope and the extent of the assistance specified below – assist the data controller in accordance with Clause 9.1. and 9.2. by implementing the following technical and organisational measures:

Taking into account the nature of the processing, the information available and insofar it is possible, the data processor provides reasonable assistance to the data controller by appropriate technical and organizational measures for the fulfilment of the data controller's obligation to respond to requests for exercising the data subject's rights laid down in GDPR Chapter III.

The data processor shall be compensated for the time devoted in relation to the assistance with responses to requests regarding the data subject's rights. The compensation shall be agreed upon separately.

The data processor must assist the data controller in ensuring compliance with any of the data controller's obligations pursuant to GDPR Articles 32-36. The data processor is entitled to receive separate compensation regarding such assistance.

C.4. Storage period/erasure procedures

Upon termination of the provision of personal data processing services, the data processor shall either delete or return the personal data in accordance with Clause 11.1., unless the data controller – after the signature of the contract – has modified the data controller's original choice. Such modification shall be documented and kept in writing, including electronically, in connection with the Clauses.

The data controller can configure its own retention rules within the Services and thereby determine storage period and erasure procedures.

C.5. Processing location

Processing of the personal data under the Clauses cannot be performed at other locations than the following without the data controller's prior written authorisation:

Processing of personal data will take place in the data processor's data center as designated by the data controller at the data controller's configuration of the services or as set out in the agreement between the data processor and the data controller as the case may be.

The data processor's support organization may occasionally, as part of an ongoing support issue with the data controller, be requested by the data controller to access personal data. The request and the granting of access will be logged. Technical and organizational measures are in place to limit access to personal data, and all support activities that requires access to personal data will be performed by designated personnel located within EU.

C.6. Instruction on the transfer of personal data to third countries

Data processor does currently not transfer personal data to third countries.

If the data controller does not in the Clauses or subsequently provide documented instructions pertaining to the transfer of personal data to a third country, the data processor shall not be entitled within the framework of the Clauses to perform such transfer.

C.7. Procedures for the data controller's audits, including inspections, of the processing of personal data being performed by the data processor

The data processor will on yearly basis obtain an independent third-party audit concerning the data processor's compliance.

The parties have agreed that the following type of audit is sufficient for compliance purposes:

SOC2 audit and ISO 27001:2022 certification.

The data processor will conduct independent third-party audits of its organizational procedures, security, and assets on a yearly basis as part of its SOC2 audit. The audit report of the most recent audit can be requested by the data controller free of charge.

The data processor may, at its discretion, discontinue its SOC2 in favor of another relevant audit.

The processor is ISO 27001:2022 certified and can provide the certification upon request.

The data controller may at its own expense contest the scope and/or methodology of the report 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.

Based on the results of such an audit/inspection, the data controller may request further measures to be taken to ensure compliance with the GDPR, the applicable EU or Member State data protection provisions and the Clause.
The parties have further agreed that the data controller may carry out on-site audits at the data processor's premises located at Per Henrik Lings Allé 4, 7th floor, 2100 Copenhagen OE, Denmark.

C.8. Procedures for audits, including inspections, of the processing of personal data being performed by sub-processors

The data processor 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.

Where the sub-processor forms part of the data processor's organization, including by being an affiliate of the data processor, 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 section C.8. In such case, a separate or individual audit report for each entity shall not be required.

The parties have agreed that either of the following is sufficient for compliance purposes:
SOC 2 audit and/or ISO 27001 certification.

The SOC 2 audit and/or ISO 27001 certification shall upon request be submitted to the data controller for information.

Appendix D The parties' terms of agreement on other subjects

The Clauses, including all appendices and schedules, form an integral part of and are incorporated into Keepit's Terms of Service. Except as expressly set out in the Clauses, the Terms of Service shall govern the parties' contractual relationship, including but not limited to limitation of liability, ownership of data, acceptable use of the Service, confidentiality, and other commercial terms.