EUROPEAN
COMMISSION

Brussels, 4.6.2021
C(2021) 3701 final

ANNEX

ANNEX

to the

COMMISSION IMPLEMENTING DECISION

on standard contractual clauses between controllers and processors under Article 28 (7) of Regulation (EU) 2016/679 of the European Parliament and of the Council and Article 29 (7) of Regulation (EU) 2018/1725 of the European Parliament and of the Council

NOTE: Keepit uses the standard contractual clauses for controller-to-processor relationships prepared by the European Commission (https://ec.europa.eu/info/law/law-topic/data-protection/publications/standard-contractual-clauses-controllers-and-processors_en). These clauses govern the processing of personal data between controllers and processors within the EU/EEA.

These standard contractual clauses should not be mistaken for the standard contractual clauses (SCCs) prepared by the European Commission relating to the transfer of personal data from the EU/EEA to third countries. The SCCs for international data transfers are separate instruments designed specifically to provide appropriate safeguards for cross-border data transfers to jurisdictions outside the EU/EEA that do not benefit from an adequacy decision under Article 45 of the GDPR.

ANNEX

STANDARD CONTRACTUAL CLAUSES

SECTION I

Clause 1

Purpose and scope

(a) The purpose of these Standard Contractual Clauses (the Clauses) is to ensure compliance with Article 28(3) and (4) of 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.

(b) The controllers and processors listed in Annex I have agreed to these Clauses in order to ensure compliance with Article 28(3) and (4) of Regulation (EU) 2016/679 and/or Article 29 (3) and (4) Regulation (EU) 2018/1725.

(c) These Clauses apply to the processing of personal data as specified in Annex II.

(d) Annexes I to IV are an integral part of the Clauses.

(e) These Clauses are without prejudice to obligations to which the controller is subject by virtue of Regulation (EU) 2016/679 and/or Regulation (EU) 2018/1725.

(f) These Clauses do not by themselves ensure compliance with obligations related to international transfers in accordance with Chapter V of Regulation (EU) 2016/679 and/or Regulation (EU) 2018/1725.

Clause 2

Invariability of the Clauses

(a) The Parties undertake not to modify the Clauses, except for adding information to the Annexes or updating information in them.

(b) This does not prevent the Parties from including the standard contractual clauses laid down in these Clauses in a broader contract, or from adding other clauses or additional safeguards provided that they do not directly or indirectly contradict the Clauses or detract from the fundamental rights or freedoms of data subjects.

Clause 3

Interpretation

(a) Where these Clauses use the terms defined in Regulation (EU) 2016/679 or Regulation (EU) 2018/1725 respectively, those terms shall have the same meaning as in that Regulation.

(b) These Clauses shall be read and interpreted in the light of the provisions of Regulation (EU) 2016/679 or Regulation (EU) 2018/1725 respectively.

(c) These Clauses shall not be interpreted in a way that runs counter to the rights and obligations provided for in Regulation (EU) 2016/679 / Regulation (EU) 2018/1725 or in a way that prejudices the fundamental rights or freedoms of the data subjects.

Clause 4

Hierarchy

In the event of a contradiction between these Clauses and the provisions of related agreements between the Parties existing at the time when these Clauses are agreed or entered into thereafter, these Clauses shall prevail.

Clause 5

Docking clause

(a) Any entity that is not a Party to these Clauses may, with the agreement of all the Parties, accede to these Clauses at any time as a controller or a processor by completing the Annexes and signing Annex I.

(b) Once the Annexes in (a) are completed and signed, the acceding entity shall be treated as a Party to these Clauses and have the rights and obligations of a controller or a processor, in accordance with its designation in Annex I.

(c) The acceding entity shall have no rights or obligations resulting from these Clauses from the period prior to becoming a Party.

SECTION II – OBLIGATIONS OF THE PARTIES

Clause 6

Description of processing(s)

The details of the processing operations, in particular the categories of personal data and the purposes of processing for which the personal data is processed on behalf of the controller, are specified in Annex II.

Clause7

Obligations of the Parties

7.1. Instructions

(a) The processor shall process personal data only on documented instructions from the controller, unless required to do so by Union or Member State law to which the processor is subject. In this case, the processor shall inform the controller of that legal requirement before processing, unless the law prohibits this on important grounds of public interest. Subsequent instructions may also be given by the controller throughout the duration of the processing of personal data. These instructions shall always be documented.

(b) The processor shall immediately inform the controller if, in the processor's opinion, instructions given by the controller infringe Regulation (EU) 2016/679 / Regulation (EU) 2018/1725 or the applicable Union or Member State data protection provisions.

7.2. Purpose limitation

The processor shall process the personal data only for the specific purpose(s) of the processing, as set out in Annex II, unless it receives further instructions from the controller.

7.3. Duration of the processing of personal data

Processing by the processor shall only take place for the duration specified in Annex II.

7.4. Security of processing

(a) The processor shall at least implement the technical and organisational measures specified in Annex III to ensure the security of the personal data. This includes protecting the data against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access to the data (personal data breach). In assessing the appropriate level of security, the Parties shall take due account of the state of the art, the costs of implementation, the nature, scope, context and purposes of processing and the risks involved for the data subjects.

(b) The processor shall grant access to the personal data undergoing processing to members of its personnel only to the extent strictly necessary for implementing, managing and monitoring of the contract. The processor shall ensure that persons authorised to process the personal data received have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

7.5. Sensitive data

If the processing involves personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data or biometric data for the purpose of uniquely identifying a natural person, data concerning health or a person's sex life or sexual orientation, or data relating to criminal convictions and offences ("sensitive data"), the processor shall apply specific restrictions and/or additional safeguards.

7.6 Documentation and compliance

(a) The Parties shall be able to demonstrate compliance with these Clauses.

(b) The processor shall deal promptly and adequately with inquiries from the controller about the processing of data in accordance with these Clauses.

(c) The processor shall make available to the controller all information necessary to demonstrate compliance with the obligations that are set out in these Clauses and stem directly from Regulation (EU) 2016/679 and/or Regulation (EU) 2018/1725. At the controller's request, the processor shall also permit and contribute to audits of the processing activities covered by these Clauses, at reasonable intervals or if there are indications of non-compliance. In deciding on a review or an audit, the controller may take into account relevant certifications held by the processor.

(d) The controller may choose to conduct the audit by itself or mandate an independent auditor. Audits may also include inspections at the premises or physical facilities of the processor and shall, where appropriate, be carried out with reasonable notice.

(e) The Parties shall make the information referred to in this Clause, including the results of any audits, available to the competent supervisory authority/ies on request.

7.7. Use of sub-processors

(a) The processor has the controller's general authorisation for the engagement of sub-processors from an agreed list. The processor shall specifically inform in writing the controller of any intended changes of that list through the addition or replacement of sub-processors at least 30 days in advance, thereby giving the controller sufficient time to be able to object to such changes prior to the engagement of the concerned sub-processor(s). The processor shall provide the controller with the information necessary to enable the controller to exercise the right to object.

(b) Where the processor engages a sub-processor for carrying out specific processing activities (on behalf of the controller), it shall do so by way of a contract which imposes on the sub-processor, in substance, the same data protection obligations as the ones imposed on the data processor in accordance with these Clauses. The processor shall ensure that the sub-processor complies with the obligations to which the processor is subject pursuant to these Clauses and to Regulation (EU) 2016/679 and/or Regulation (EU) 2018/1725.

(c) At the controller's request, the processor shall provide a copy of such a sub-processor agreement and any subsequent amendments to the controller. To the extent necessary to protect business secret or other confidential information, including personal data, the processor may redact the text of the agreement prior to sharing the copy.

(d) The processor shall remain fully responsible to the controller for the performance of the sub-processor's obligations in accordance with its contract with the processor. The processor shall notify the controller of any failure by the sub-processor to fulfil its contractual obligations.

(e) 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.

7.8. International transfers

(a) Any transfer of data to a third country or an international organisation by the processor shall be done only on the basis of documented instructions from the controller or in order to fulfil a specific requirement under Union or Member State law to which the processor is subject and shall take place in compliance with Chapter V of Regulation (EU) 2016/679 or Regulation (EU) 2018/1725.

(b) The controller agrees that where the processor engages a sub-processor in accordance with Clause 7.7. for carrying out specific processing activities (on behalf of the controller) and those processing activities involve a transfer of personal data within the meaning of Chapter V of Regulation (EU) 2016/679, the processor and the sub-processor can ensure compliance with Chapter V of Regulation (EU) 2016/679 by using standard contractual clauses adopted by the Commission in accordance with of Article 46(2) of Regulation (EU) 2016/679, provided the conditions for the use of those standard contractual clauses are met.

Clause 8

Assistance to the controller

(a) The processor shall promptly notify the controller of any request it has received from the data subject. It shall not respond to the request itself, unless authorised to do so by the controller.

(b) The processor shall assist the controller in fulfilling its obligations to respond to data subjects' requests to exercise their rights, taking into account the nature of the processing. In fulfilling its obligations in accordance with (a) and (b), the processor shall comply with the controller's instructions

(c) In addition to the processor's obligation to assist the controller pursuant to Clause 8(b), the processor shall furthermore assist the controller in ensuring compliance with the following obligations, taking into account the nature of the data processing and the information available to the processor:

   (1) the 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') where a type of processing is likely to result in a high risk to the rights and freedoms of natural persons;

(2) the obligation to consult the competent supervisory authority/ies 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 controller to mitigate the risk;

(3) the obligation to ensure that personal data is accurate and up to date, by informing the controller without delay if the processor becomes aware that the personal data it is processing is inaccurate or has become outdated;

(4) the obligations in Article 32 Regulation (EU) 2016/679.

(d) The Parties shall set out in Annex III the appropriate technical and organisational measures by which the processor is required to assist the controller in the application of this Clause as well as the scope and the extent of the assistance required.

Clause 9

Notification of personal data breach

In the event of a personal data breach, the processor shall cooperate with and assist the controller for the controller to comply with its obligations under Articles 33 and 34 Regulation (EU) 2016/679 or under Articles 34 and 35 Regulation (EU) 2018/1725, where applicable, taking into account the nature of processing and the information available to the processor.

9.1 Data breach concerning data processed by the controller

In the event of a personal data breach concerning data processed by the controller, the processor shall assist the controller:

(a) in notifying the personal data breach to the competent supervisory authority/ies, without undue delay after the controller has become aware of it, where relevant/(unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons);

(b) in obtaining the following information which, pursuant to Article 33(3) Regulation (EU) 2016/679, shall be stated in the controller's notification, and must at least include:

(1) the nature of the personal data including where possible, the categories and approximate number of data subjects concerned and the categories and approximate number of personal data records concerned;

(2) the likely consequences of the personal data breach;

(3) 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.

Where, and insofar as, it is not possible to provide all this information at the same time, the initial notification shall contain the information then available and further information shall, as it becomes available, subsequently be provided without undue delay.

(c) in complying, pursuant to Article 34 Regulation (EU) 2016/679, with the obligation to communicate without undue delay 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.

9.2 Data breach concerning data processed by the processor

In the event of a personal data breach concerning data processed by the processor, the processor shall notify the controller without undue delay after the processor having become aware of the breach. Such notification shall contain, at least:

(a) a description of the nature of the breach (including, where possible, the categories and approximate number of data subjects and data records concerned);

(b) the details of a contact point where more information concerning the personal data breach can be obtained;

(c) its likely consequences and the measures taken or proposed to be taken to address the breach, including to mitigate its possible adverse effects.

Where, and insofar as, it is not possible to provide all this information at the same time, the initial notification shall contain the information then available and further information shall, as it becomes available, subsequently be provided without undue delay.

The Parties shall set out in Annex III all other elements to be provided by the processor when assisting the controller in the compliance with the controller’s obligations under Articles 33 and 34 of Regulation (EU) 2016/679.

SECTION III – FINAL PROVISIONS

Clause 10

Non-compliance with the Clauses and termination

(a) Without prejudice to any provisions of Regulation (EU) 2016/679 and/or Regulation (EU) 2018/1725, in the event that the processor is in breach of its obligations under these Clauses, the controller may instruct the processor to suspend the processing of personal data until the latter complies with these Clauses or the contract is terminated. The processor shall promptly inform the controller in case it is unable to comply with these Clauses, for whatever reason.

(b) The controller shall be entitled to terminate the contract insofar as it concerns processing of personal data in accordance with these Clauses if:

(1) the processing of personal data by the processor has been suspended by the controller pursuant to point (a) and if compliance with these Clauses is not restored within a reasonable time and in any event within one month following suspension;

(2) the processor is in substantial or persistent breach of these Clauses or its obligations under Regulation (EU) 2016/679 and/or Regulation (EU) 2018/1725;

(3) the processor fails to comply with a binding decision of a competent court or the competent supervisory authority/ies regarding its obligations pursuant to these Clauses or to Regulation (EU) 2016/679 and/or Regulation (EU) 2018/1725.

(c) The processor shall be entitled to terminate the contract insofar as it concerns processing of personal data under these Clauses where, after having informed the controller that its instructions infringe applicable legal requirements in accordance with Clause 7.1 (b), the controller insists on compliance with the instructions.

(d) Following termination of the contract, the processor shall, at the choice of the controller, delete all personal data processed on behalf of the controller and certify to the controller that it has done so, or, return all the personal data to the controller and delete existing copies unless Union or Member State law requires storage of the personal data. Until the data is deleted or returned, the processor shall continue to ensure compliance with these Clauses.

ANNEX I LIST OF PARTIES

Controller(s)

Customer Entity Name: Specified in the Order Form

Custumer Entity Address: Specified in the Order Form

Conteact Person of the Controller

Name: Entered and kept up to date by the Controller within the Services

E-mail address: Entered and kept up to date by the Controller within the Services

DPO / Compliance Officer / Compliance Team (if appointed) of the Controller

Att.: Entered and kept up to date by the Controller within the Services

E-mail address: Entered and kept up to date by the Controller within the Services

Processor(s)

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

ANNEX II: DESCRIPTION OF THE PROCESSING

Purpose(s) for which the personal data is processed on behalf of the controller

The purpose of the processor's processing of personal data on behalf of the controller is to provide backup services whereby the controller can create and maintain data backup of certain cloud solutions used by the controller at their discretion and initiative, and whereby the controller can restore data back to where the data originally resided or download data using the export/restore tools offered.

The Clauses, the Terms of Service along with the controller's configuration and use of the backup services constitute the controller's documented instructions to the processor for the purpose of providing the backup services.

Nature of the processing

The processors processing of the controller's data shall mainly pertain to providing a cloud-based backup solution cf. the Terms of Service. 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, 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 controller's use of the Services.

The processor does not access and is not familiar with the content of the backup data unless the controller specifically instructs the processor to gain access hereto.

Categories of data subjects whose personal data is processed

The backup data may contain any categories of data subjects, and it is solely determined, changed, and controlled by the controller. Data subjects may be customers, employees, patients, professionals, minors, etc. The processor has therefore implemented and maintains the level of security as described in Annex III.

Categories of personal data processed

The backup data may consist of any types of personal data about data subjects. It is entirely dependent of the controller's type of data and their use of the backup services. Personal data stored by the processor 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. The processor 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.

Assistance to the controller

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

The processor must assist the controller in ensuring compliance with any of the controller's obligations pursuant to GDPR Articles 32-36.

Processing location

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

Processing of controller's data will take place in the data centers designated by the controller, cf. the Terms of Service.

The processor's support organization may occasionally, as part of an ongoing support issue with the controller, be requested by the 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.

Duration of the processing, storage and deletion

The processor's processing of personal data on behalf of the controller may be performed when the Clauses commence.

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

Upon termination or expiry of the Terms of Service and Clasues, the processor shall in accordance with Clause 10 (d), at the choice of the controller either, (i) return all backup data, including personal data, processed under the Terms of Service and the Clauses and any copies thereof to the controller or (ii) delete all backup data, including personal data, processed under the Terms of Service and the Clauses and certify to the controller that this has been done, including for avoidance of doubt, delete such backup data 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 backup data.

Notwithstanding the abovementioned, the processor will retain all data processed under the Terms of Service and Clauses for 30 days after the deletion of the controller's account or termination thereof. This "deletion retention" will ensure that the controller's access to personal data can be reestablished after any conceivable targeted attack against the controller's primary data and backup data. After expiration of the retention period, the processor will delete all records of the controller's personal data without undue delay.

Instruction on the transfer of personal data to third countries

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

Miscellaneous

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.

ANNEX III TECHNICAL AND ORGANISATIONAL MEASURES INCLUDING TECHNICAL AND ORGANISATIONAL MEASURES TO ENSURE THE SECURITY OF THE DATA

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

The 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 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 processor has described its current technical and organizational measures in a separate document, "*Keepit Technical and Organizational Measures".*

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

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

The parties have agreed that the following is sufficient for compliance purposes: SOC2 audit and ISO 27001:2022 certification.

The 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 controller free of charge.

The 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 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 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 Clauses.

The parties have further agreed that the controller may carry out on-site audits at the processor's premises located at Per Henrik Lings Allé 4, 7th floor, 2100 Copenhagen Ø.

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 controller for information.

ANNEX IV: LIST OF SUB-PROCESSORS

On commencement of the Clauses, the controller authorizes 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 controller shall on the commencement of the Clauses authorize the use of the abovementioned sub-processors for the processing described for that party.

Prior notice for the engagement or change of sub-processors

In case of engagements, changes or disengagements of sub-processors, the processor shall notify the controller directly in writing about such change with thirty (30) calendar days' notice. The controller will have twenty-five (25) calendar days to object to the change in writing to the processor. The objection of the controller must be well-founded. Absence of any objections from the controller shall be deemed a consent to the sub-processing.

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