

GDPR DATA PROCESSING ADDENDUM

Research Research Services

PURPOSE OF THIS ADDENDUM

In the course of providing access to Research Research's Professional News, funding database and related services to customers (the "**RR Services**"), Research Research Limited ("**Research Research**") may process personal data (as defined below) submitted by customers to the RR Services.

The purpose of this Data Processing Addendum is to incorporate the data processing terms set forth below into agreement(s) for the provision of RR Services (the "**Agreement**") between Research Research and the customer identified below ("**Customer**"). These data processing terms are required by the 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, including, as applicable, as implemented or adopted under the laws of the United Kingdom (the "**General Data Protection Regulation**" or "**GDPR**") to govern processing by Research Research of personal data of Customer's data subjects.

CUSTOMER EXECUTION OF ADDENDUM

This Addendum has been signed on behalf of Research Research and relevant affiliates thereof and may be signed on behalf of Customer either electronically (currently DocuSign) or manually in accordance with the instructions below. **The Addendum must be signed by the same Customer entity that executed the Agreement for the RR Services.** To complete and execute the Addendum:

1. **Electronic Signature:** A Customer that wishes to sign electronically and has not received an e-mail from Research Research requesting such signature should send a request to rrGDPRAddendum@exlibrisgroup.com with the full name of the Customer institution. Customer will receive the Addendum (or a link to the Addendum) via e-mail and Customer must follow the step-by-step instructions provided by DocuSign to fill in the requested information and electronically sign the Addendum. Research Research may also make available the option for Customers to initiate the electronic signature process directly from Research Research's and/or its affiliate's website.
2. **Manual Signature:** Customers preferring to sign this Addendum manually must:
 - a. fill in the Customer information requested on the page below entitled "ADDENDUM SIGNATURE PAGE";
 - b. sign where indicated on the "ADDENDUM SIGNATURE PAGE";
 - c. scan and send the completed and signed Addendum to Research Research by email to rrGDPRAddendum@exlibrisgroup.com.

RESEARCH RESEARCH ENTITY

This Addendum is entered into between Customer and Research Research Limited or the Research Research Limited affiliate that is the party to the Agreement(s) ("**Research Research**").

EFFECTIVE DATE

This Addendum shall enter into force and become legally binding upon receipt by Research Research of this Addendum completed, unchanged and signed by Customer or, with respect to each new Agreement that incorporates this Addendum by reference, upon execution of such new Agreement.

CONTINUITY OF THE AGREEMENT(S)

The terms of the Agreement remain unmodified except to the extent expressly modified herein and/or in a prior amendment signed by both parties.

[END OF PAGE]

DATA PROCESSING TERMS

This Addendum, together with the Agreement (as defined below), constitutes the contract governing the processing by processor as contemplated under paragraph 3 of Article 28 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, including, as applicable, as implemented or adopted under the laws of the United Kingdom (the “**General Data Protection Regulation**” or “**GDPR**”). Customer shall be and act as the “controller” (as defined in the GDPR) of all personal data (as defined below) and shall comply with its obligations as the controller under the GDPR. Research Research shall be and act as the “processor” (as defined in the GDPR) and will comply with the requirements of the processor under the GDPR with respect to the processing, on the RR Services (as defined below), of personal data covered by the GDPR. This Addendum shall not be construed to impose any obligations beyond those required by the GDPR itself. Capitalised terms used herein and not defined herein shall have the meaning ascribed to them in the Agreement.

1. Definitions

- 1.1 “**Agreement**” means the Research Research License Agreement(s) or other contract(s) pursuant to which Research Research grants Customer a subscription/license to Research Research’s cloud-based service. This Addendum is incorporated in and forms a part of the Agreement.
- 1.2 “**Data Controller**” means Customer, as controller under the GDPR.
- 1.3 “**Data Processor**” means Research Research or the Research Research affiliate that is the party to the Agreement, as processor under the GDPR.
- 1.4 “**personal data**”, “**personal data breach**”, “**processing**”, and “**data subject**” shall have the meaning specified for each term in the GDPR.
- 1.5 “**Standard Contractual Clauses**” means the agreement attached hereto as Schedule 2 authorised pursuant to Regulation (EU) 2016/679 of the European Parliament and the Council approved by European Commission Implementing Decision (EU) 2021/914 of 4 June 2021 on Standard Contractual Clauses for the transfer of personal data to processors established in third countries which do not ensure an adequate level of data protection.

2. Processing Details

2.1 Subject-matter and duration of the processing

The subject-matter of the processing includes the provision to Data Controller of access to a cloud-based funding database and/or news service and related functionality and services specified in the Agreement (“**RR Services**”) and related implementation, support and other services described in the Agreement. The duration of the processing shall be the term of the Agreement and a reasonable and limited period of time following its expiration or other termination (see Section 10 below (Return or Deletion)), all as further described herein and in the Agreement.

2.2 Purpose of the processing

The purpose of the intended processing of personal data is for the provision to Data Controller of the RR Services and related services described in the Agreement and the performance of Data Processor’s obligations under the Agreement.

2.3 Nature of the processing

The nature of the processing shall be to provide to Data Controller the RR Services pursuant to the Agreement, as further specified in the RR Services product documentation and as further instructed by Data Controller in its use of the RR Services. Data Processor may also provide related implementation, support and other services to the extent described in the Agreement or other written order or instruction by Data Controller.

2.4 Type of personal data

- (a) The subject of the processing shall be personal data types consistent with the purposes described in Section 2.2 above and may, as applicable, include the following types of personal data, along with other categories as described in the RR Services product documentation:
 - Basic user and researcher information, including
 - First and last names
 - Email addresses
 - Job title
 - Faculty/department affiliation
 - Federated authentication identifiers

- Institutional identification numbers
- Discipline areas and research interests
- Basic staff and staff contact information
- Staff related usage information, including records of staff operations and activity
- Research activity
- Saved searches and bookmarks
- General usage information, including connection data (e.g., IP addresses)

- (b) Data Controller agrees not to provide or upload for processing in the RR Services any personal data types that are not required by the RR Services personal data fields. Without limiting the foregoing, in no event shall Data Controller process in the RR Services (a) special categories of data described in Article 9(1) of the GDPR, (b) payment card information or personal financial records, or (c) any other data prohibited by the Agreement or the GDPR. Data Controller determines which personal data it uploads to the RR Services and shall have sole responsibility for the accuracy, quality, and legality of personal data processed in the RR Services and the means by which Data Controller acquired personal data.

2.5 Categories of Data Subjects

The categories of data subjects shall be determined by Data Controller in compliance with the relevant RR Services subscription/license and may include, without limitation, Data Controller's faculty, students, administrators, researchers, employees, visitors and alumni.

3. **Data Controller instructions**

Data Processor shall process personal data only within the scope of Data Processor's obligations under the Agreement and the GDPR, according to documented instructions of Data Controller. This Addendum and the relevant terms of the Agreement constitute documented instructions of Data Controller with respect to the processing of personal data under the GDPR and, to the extent applicable, the Standard Contractual Clauses, including, without limitation, Clause 5(a) thereof. Data Controller shall be responsible for having all necessary rights to collect and process and to allow collection and processing of all personal data contemplated hereunder.

4. **Confidentiality obligations of Data Processor personnel**

Data Processor shall take reasonable steps to ensure that only authorised personnel have access to personal data. All personnel of Data Processor engaged in the processing of personal data (i) will process personal data only in accordance with the Agreement and this Addendum, except as may be required by Union or relevant Member State law or law of member state of the EEA, Switzerland or the United Kingdom, as the case may be, and (ii) have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

5. **Technical and organisational measures**

- 5.1 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, Data Controller and Data Processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, including inter alia as appropriate:

- the pseudonymisation and encryption of personal data;
- the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;
- the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident;
- a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.

- 5.2 In assessing the appropriate level of security, account shall be taken of the risks that are presented by processing, in particular from accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data transmitted, stored or otherwise processed.

- 5.3 The technical and organisational measures are set out in more detail in the Schedule 1 to this GDPR Addendum. Data Processor shall, upon request, provide Data Controller with information regarding the technical and organisational measures referred to in Schedule 1.

6. **Subprocessors**

- 6.1 Data Processor will ensure that: (a) any subprocessor it engages to process personal data under the Agreement on its behalf does so only on the basis of a written contract which imposes on such subprocessor data protection obligations as a whole no less protective of personal data than those imposed on Data Processor in this Addendum;

and (b) where any such subprocessor engaged by Data Processor fails to fulfil its data protection obligations, Data Processor shall remain fully liable to Data Controller for the performance of that other subprocessor's obligations.

- 6.2 Data Controller hereby authorises Data Processor to engage affiliates (under common ownership with Data Processor) as specified below to participate in performance of Data Processor's obligations with respect to processing of personal data under the Agreement and this Addendum and to transfer personal data to such affiliates for such purpose. The specified affiliates and any other subprocessors, their respective jurisdictions of organisation and description of their activities, together with publication of replacements or additions of subprocessors and a mechanism by which Data Controller may subscribe to receive prior notifications of such replacements and additions, are set forth on the Ex Libris website, currently at <https://knowledge.exlibrisgroup.com>.
- 6.3 Data Controller hereby provides Data Processor with a general written authorisation to employ other subprocessors. Data Processor shall inform Data Controller of any intended changes concerning the addition or replacement of sub-processors after the date of execution of this Addendum in the manner set forth above, thereby giving Data Controller the opportunity to object to such changes. If Data Controller has a reasonable basis to object to Data Processor's use of a new sub-processor, Data Controller shall so notify Data Processor in a written notice that includes an explanation of the grounds for objection within thirty (30) days after receipt of Data Processor's notification regarding such new sub-processor. In the event Data Controller so objects, Data Processor will use reasonable efforts to work in good faith with Data Controller to find an acceptable, reasonable, alternate approach. If Data Processor is unable to make available such an alternative approach within a reasonable period of time, which shall not exceed sixty (60) days, Data Controller may terminate the applicable RR Services which cannot be provided without the use of the objected-to new sub-processor, without penalty or liability for either party, by providing written notice to Data Processor within thirty (30) days.
- 6.4 In addition, Data Processor uses data center facilities provided by unaffiliated third parties. The relevant data center providers and the respective locations of the data centers, if any, are listed on the Ex Libris website, currently at <https://knowledge.exlibrisgroup.com>.

7. Data Transfer

- 7.1 Data Controller acknowledges and accepts that the provision of the RR Services under the Agreement requires the transfer of personal data to, and processing by, sub-processors in Third Countries (as defined in Section 7.2 below). With respect to transfers of personal data to a sub-processor located outside of the European Union, the EEA, Switzerland and the United Kingdom, Data Processor shall in advance of any such transfer ensure that such countries are recognised by the European Commission, member state of the EEA, Switzerland or the United Kingdom, as the case may be, as providing an adequate level of data protection or that a mechanism is in place to provide appropriate safeguards and enforcement of personal data protection in compliance with the requirements of the GDPR or the laws and regulations of the EEA member state, Switzerland or the United Kingdom, as the case may be, applicable to the processing of personal data under the Agreement ("Other Data Processing Laws").
- 7.2 The Standard Contractual Clauses provide a mechanism for safeguarding transfers of personal data outside the European Union, EEA, Switzerland or the United Kingdom, as applicable, to processors established in third countries which are not recognised by such jurisdictions, as applicable, as providing an adequate level of protection (a "Third Country"). Where the Data Processor hereunder is established in such a Third Country, unless and until the Data Processor has adopted an alternative mechanism recognised under the GDPR or Other Data Processing Laws, as applicable, for the lawful transfer of personal data to such country, the Standard Contractual Clauses will apply to personal data that is transferred to such Data Processor in such country (and only to such personal data).
- 7.3 The Data Controller hereby authorizes the Data Processor to replace and/or amend Schedule 2, as appropriate, with the most recent version of the Standard Contractual Clauses applicable to the data transfer as required under the GDPR or Other Data Processing Laws, as applicable. The Data Processor will inform the Data Controller accordingly with reasonable prior notice of any changes to Schedule 2.

8. Rights of Data Subjects

- 8.1 Data Processor shall provide Data Controller with instructions regarding the use, by Data Controller and/or its authorised users, of procedures or tools within the RR Services to allow Data Controller to access, rectify, erase, and block personal data relating to data subjects that is stored on the RR Services, and to export such personal data in a structured, commonly used and machine-readable format.
- 8.2 If Data Processor receives a request from Data Controller's data subject to exercise one or more of its rights under the GDPR, Data Processor will redirect the data subject to make its request directly to Data Controller. In addition, to the extent Data Controller, in its use of the RR Services, does not have the ability to address a data subject request, Data Processor shall upon Data Controller's request provide reasonable assistance in responding to such

data subject request to the extent Data Processor is legally permitted to do so and the response to such data subject request is required under the GDPR.

9. Assistance to Data Controller

- 9.1 Taking into account the nature of processing and the information available to Data Processor, Data Processor shall provide such assistance to Data Controller as Data Controller reasonably requests in relation to Data Controller's compliance with the obligations pursuant to Articles 32 to 36 of the GDPR. Data Controller shall cover all reasonable costs incurred by Data Processor in connection with its provision of such assistance.
- 9.2 With regard to point (h) of the first subparagraph of Article 28(3) of the GDPR, Data Processor shall immediately inform the Data Controller if, in its opinion, an instruction infringes the GDPR or other Union or Member State data protection provisions.

10. Return or deletion of personal data after expiration or termination of Agreement

After the expiration or other termination of the Agreement or a RR Services subscription, Data Processor shall, at the choice of Data Controller made in a written notice received by Data Processor within 30 days after such expiration or termination, provide or make available for download Data Controller's personal data held on the relevant RR Service, and shall, after such period, delete existing copies of all personal data unless Union or Member State law requires storage of the personal data. Unless otherwise agreed or required by applicable law, deletion of personal data shall be completed within 120 days following the later of (a) termination of the relevant RR Services subscription and (b) if requested by Data Controller as set forth above, providing or making available for download the personal data.

11. Rights of Data Controller to audit

- 11.1 Data Processor shall make available to Data Controller all information necessary to demonstrate compliance with the obligations laid down in Article 28 of the GDPR and allow for and contribute to audits, including inspections, conducted by Data Controller or another auditor mandated by Data Controller. For the avoidance of doubt, the cost of any such audit or inspection shall be paid by Data Controller, except as noted in Section 11.2.
- 11.2 Audit of data security shall be undertaken by Data Processor and/or the data center provider engaging, at their own expense, a duly qualified third party to audit relevant data centers on an annual basis, and making available to Data Controller, at all times, an SSAE 16 or SSAE 18 Report or comparable third party information security assessment report regarding the data centers, along with any other available security and privacy certifications.
- 11.3 If and to the extent Data Controller requires an additional audit or inspection to meet its obligations under the GDPR that would involve on-site access to a data center where personal data of other customers of Data Processor may be stored, Data Controller agrees that such audit or inspection shall be conducted at Data Controller's expense by a mutually acceptable independent third party. Data Controller shall also reimburse Data Processor for any time expended for any such on-site audits or inspections at Data Processor's then-current professional services rates, which shall be made available to Data Controller upon request. Before the commencement of any such on-site audit or inspection, Data Controller and Data Processor shall mutually agree upon the scope, timing, and duration of the audit or inspection in addition to such reimbursement rate. Data Controller agrees that it and its third party auditor shall keep the contents and results of any such audits confidential, subject to any applicable legal obligations under the GDPR to disclose same to the relevant supervisory authorities. Audits of the facilities of third party subprocessors indicated in the subprocessor list maintained in accordance with Section 6.2 may be subject to additional or different audit terms.

12. Data Protection Officer

Data Processor and its affiliates have appointed a data protection officer or a primary contact for data privacy-related matter. The appointed person may be reached at dpo@exlibrisgroup.com or such other address as published by Data Processor from time-to-time and further information regarding such person can be found on Research Research's parent company public website, currently at <https://knowledge.exlibrisgroup.com>.

13. Notification in the event of a personal data breach

Data Processor shall notify Data Controller without undue delay after becoming aware of a personal data breach.

14. Conflicting Terms

In the event of any conflict or inconsistency between the provisions of this Addendum and any prior terms or agreements between the parties with respect to the processing of personal data, including, without limitation, prior data processing agreement(s), the provisions of this Addendum shall prevail.

ADDENDUM SIGNATURE PAGE**DATA PRIVACY OFFICER OR CONTACT PERSON**

The parties' respective data privacy officers ("DPO") or contact persons for data protection enquiries are:

Research Research	Customer (Please complete)
DPO/Contact for data protection enquiries	DPO/Contact for data protection enquiries
Privacy Team	Name/Role: _____
Email: dpo@exlibrisgroup.com	Email: _____

The parties' authorized signatories have duly executed this Addendum and, to the extent the Standard Contractual Clauses are applicable, such execution shall be deemed to constitute signature and acceptance of the Standard Contractual Clauses attached hereto as Schedule 2, including their Appendices and, with respect to an exporter located in the United Kingdom, the attached UK Addendum to EU Standard Contractual Clauses.

CUSTOMER INFORMATION AND SIGNATURE

Customer (current complete legal name): _____

Customer current address: _____

Former name of Customer as it appears on the Agreement (if different): _____

Customer signature: _____

Printed Name: _____

Title: _____

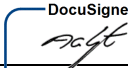
Date: _____

RESEARCH RESEARCH SIGNATURE**Research Research Limited**

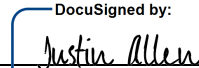
By: _____
 Name: Justin Allen
 Title: Director
 Date: 24 October 2022

DocuSigned by:
Justin Allen
6D40263DC92C4A8...

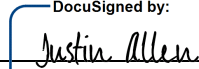
Ex Libris (Deutschland) GmbH
Tasköprüstraße 1, 22761 Hamburg

By:  DocuSigned by:
EDAC3A784545418...
Name: Andrew Wright
Title: Director
Date: 02 November 2022

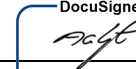
Ex Libris (UK) Limited
70 St. Mary Axe, London EC3A 8BE

By:  DocuSigned by:
6D40263DC92C4A8...
Name: Justin Allen
Title: Director
Date: 24 October 2022

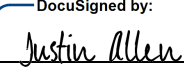
Ex Libris (France) SARL
Parc d'Affaires SILIC, 24 Rue Saarinen, 94568
RUNGIS Cedex

By:  DocuSigned by:
6D40263DC92C4A8...
Name: Justin Allen
Title: Director
Date: 24 October 2022

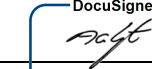
Ex Libris Italy S.R.L
Via Cartiera 4 – 40037 Sasso Marconi (Bo)

By:  DocuSigned by:
EDAC3A784545418...
Name: Andrew Wright
Title: Director
Date: 02 November 2022

Ex Libris Ltd.
Malha Technological Park, Alon Building, Jerusalem
9695102, Israel

By:  DocuSigned by:
6D40263DC92C4A8...
Name: Justin Allen
Title: Director
Date: 24 October 2022

Ex Libris (Scandinavia) A/S
c/o Plesner, Amerika Plads 37, DK-2100 Copenhagen

By:  DocuSigned by:
EDAC3A784545418...
Name: Andrew Wright
Title: Director
Date: 02 November 2022

SCHEDULE 1 TO DATA PROCESSING ADDENDUM

Technical and Organisational Measures

Further to the general principles set out in Section 5 of the Addendum, the below reflects Data Processor's current technical and organisational measures. Data Processor may change these from time to time so long as Data Processor does not materially decrease the overall security of the RR Services during a Subscription term. Changes will be published in the security and product documentation available on Ex Libris' website, currently at <https://knowledge.exlibrisgroup.com>.

1. Pseudonymisation of personal data/Encryption of personal data

Measures, including encryption, are used to ensure that personal data cannot be read, copied, modified or deleted without authorisation during electronic transmission or transport, and that the target entities for any transfer of personal data by means of data transmission facilities can be established and verified.

2. Ability to ensure the ongoing confidentiality and integrity of processing systems and services

2.1 Measures to prevent unauthorised persons from gaining physical access to data processing systems for processing or using personal data:

- a) Definition of persons who are granted physical access;
- b) Electronic access control;
- c) Alarm device or security service outside service times; Security doors (electronic door opener, ID reader);
- d) Implementation of measures for on-premises security (e.g. intruder alert/notification).

2.2 Measures to prevent that unauthorised persons use data processing equipment:

- a) Definition of persons who may access data processing equipment.
- b) Password protection of personal computers.

2.3 Measures to ensure that persons entitled to use a data processing system gain access only to such personal data as they are entitled to access in accordance with their access rights:

- a) Implementation of access rights for respective personal data and functions;
- b) Requirement of identification vis-à-vis the data processing system (e.g., via ID and authentication);
- c) Implementation of policy on access- and user-roles;
- d) Evaluation of protocols in case of damaging incidents.

2.4 Measures such as logging of data entry, to ensure that it is possible to check and ascertain whether personal data have been entered into, altered or removed from personal data processing systems and if so, by whom:

2.5 Measures to ensure that personal data processed on behalf of others are processed in compliance with Data Controller's instructions, including training of Data Processor personnel and documentation of Data Controller support requests.

2.6 Measures to ensure that data collected for different purposes can be processed separately such as the use of logical separation of data of each of Data Processor's clients.

3. Ability to ensure the availability and resilience of processing systems and services

Measures to ensure that personal data is protected against accidental destruction or loss:

- a) Realisation of a regular backup schedule;
- b) Safe storage of data backups;
- c) Implementation and regular control of emergency power systems and overvoltage protection systems.

4. Ability to restore the availability to access personal data in a timely manner in the event of a physical or technical incident

Measures to ensure that personal data can be restored in a timely manner in the event of accidental destruction or loss:

- a) Implementation of an emergency plan;
- b) Protocol on the initiation of crisis- and/or emergency management.

5. Procedures for regular testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing

- a) Regular review of any IT security related certifications;
- b) Monitoring by the Data Protection Officer, if designated, and IT review concerning the compliance with the determined processes and requirements for the configuration and operation of the systems.

[END OF PAGE]

SCHEDULE 2 TO DATA PROCESSING ADDENDUM

STANDARD CONTRACTUAL CLAUSES

Controller to Processor

SECTION I

Clause 1

Purpose and scope

- (a) The purpose of these standard contractual clauses is to ensure compliance with the requirements 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 (General Data Protection Regulation) for the transfer of data to a third country.
 - (b) The Parties:
 - (i) the natural or legal person(s), public authority/ies, agency/ies or other body/ies (hereinafter 'entity/ies') transferring the personal data, as listed in Annex I.A (hereinafter each 'data exporter'), and
 - (ii) the entity/ies in a third country receiving the personal data from the data exporter, directly or indirectly via another entity also Party to these Clauses, as listed in Annex I.A (hereinafter each 'data importer')
- have agreed to these standard contractual clauses (hereinafter: 'Clauses').
- (c) These Clauses apply with respect to the transfer of personal data as specified in Annex I.B.
 - (d) The Appendix to these Clauses containing the Annexes referred to therein forms an integral part of these Clauses.

Clause 2

Effect and invariability of the Clauses

- (a) These Clauses set out appropriate safeguards, including enforceable data subject rights and effective legal remedies, pursuant to Article 46(1) and Article 46(2)(c) of Regulation (EU) 2016/679 and, with respect to data transfers from controllers to processors and/or processors to processors, standard contractual clauses pursuant to Article 28(7) of Regulation (EU) 2016/679, provided they are not modified, except to select the appropriate Module(s) or to add or update information in the Appendix. This does not prevent the Parties from including the standard contractual clauses laid down in these Clauses in a wider contract and/or to add other clauses or additional safeguards, provided that they do not contradict, directly or indirectly, these Clauses or prejudice the fundamental rights or freedoms of data subjects.
- (b) These Clauses are without prejudice to obligations to which the data exporter is subject by virtue of Regulation (EU) 2016/679.

Clause 3

Third-party beneficiaries

- (a) Data subjects may invoke and enforce these Clauses, as third-party beneficiaries, against the data exporter and/or data importer, with the following exceptions:
 - (i) Clause 1, Clause 2, Clause 3, Clause 6, Clause 7;

- (ii) Clause 8.1(b), 8.9(a), (c), (d) and (e);
- (iii) Clause 9(a), (c), (d) and (e);
- (iv) Clause 12(a), (d) and (f);
- (v) Clause 13;
- (vi) Clause 15.1(c), (d) and (e);
- (vii) Clause 16(e);
- (viii) Clause 18(a) and (b).

(b) Paragraph (a) is without prejudice to rights of data subjects under Regulation (EU) 2016/679.

Clause 4

Interpretation

- (a) Where these Clauses use terms that are defined in Regulation (EU) 2016/679, 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.
- (c) These Clauses shall not be interpreted in a way that conflicts with rights and obligations provided for in Regulation (EU) 2016/679.

Clause 5

Hierarchy

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

Clause 6

Description of the transfer(s)

The details of the transfer(s), and in particular the categories of personal data that are transferred and the purpose(s) for which they are transferred, are specified in Annex I.B.

Clause 7 - Optional

Not used

SECTION II – OBLIGATIONS OF THE PARTIES

Clause 8

Data protection safeguards

The data exporter warrants that it has used reasonable efforts to determine that the data importer is able, through the implementation of appropriate technical and organisational measures, to satisfy its obligations under these Clauses.

8.1 Instructions

- (a) The data importer shall process the personal data only on documented instructions from the data exporter. The data exporter may give such instructions throughout the duration of the contract.
- (b) The data importer shall immediately inform the data exporter if it is unable to follow those instructions.

8.2 Purpose limitation

The data importer shall process the personal data only for the specific purpose(s) of the transfer, as set out in Annex I.B, unless on further instructions from the data exporter.

8.3 Transparency

On request, the data exporter shall make a copy of these Clauses, including the Appendix as completed by the Parties, available to the data subject free of charge. To the extent necessary to protect business secrets or other confidential information, including the measures described in Annex II and personal data, the data exporter may redact part of the text of the Appendix to these Clauses prior to sharing a copy, but shall provide a meaningful summary where the data subject would otherwise not be able to understand the its content or exercise his/her rights. On request, the Parties shall provide the data subject with the reasons for the redactions, to the extent possible without revealing the redacted information. This Clause is without prejudice to the obligations of the data exporter under Articles 13 and 14 of Regulation (EU) 2016/679.

8.4 Accuracy

If the data importer becomes aware that the personal data it has received is inaccurate, or has become outdated, it shall inform the data exporter without undue delay. In this case, the data importer shall cooperate with the data exporter to erase or rectify the data.

8.5 Duration of processing and erasure or return of data

Processing by the data importer shall only take place for the duration specified in Annex I.B. After the end of the provision of the processing services, the data importer shall, at the choice of the data exporter, delete all personal data processed on behalf of the data exporter and certify to the data exporter that it has done so, or return to the data exporter all personal data processed on its behalf and delete existing copies. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit return or deletion of the personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process it to the extent and for as long as required under that local law. This is without prejudice to Clause 14, in particular the requirement for the data importer under Clause 14(e) to notify the data exporter throughout the duration of the contract if it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under Clause 14(a).

8.6 Security of processing

- (a) The data importer and, during transmission, also the data exporter shall implement appropriate technical and organisational measures to ensure the security of the data, including protection against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access to that data (hereinafter '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 purpose(s) of processing and the risks involved in the processing for the data subjects. The Parties shall in particular consider having recourse to encryption or pseudonymisation, including during transmission, where the purpose of processing can be fulfilled in that manner. In case of pseudonymisation, the additional information for attributing the personal data to a specific data subject shall, where possible, remain under the exclusive control of the data exporter. In complying with its obligations under this paragraph, the data importer shall at least implement the technical and organisational measures specified in Annex II. The data importer shall carry out regular checks to ensure that these measures continue to provide an appropriate level of security.

- (b) The data importer shall grant access to the personal data to members of its personnel only to the extent strictly necessary for the implementation, management and monitoring of the contract. It shall ensure that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.
- (c) In the event of a personal data breach concerning personal data processed by the data importer under these Clauses, the data importer shall take appropriate measures to address the breach, including measures to mitigate its adverse effects. The data importer shall also notify the data exporter without undue delay after having become aware of the breach. Such notification shall contain the details of a contact point where more information can be obtained, a description of the nature of the breach (including, where possible, categories and approximate number of data subjects and personal data records concerned), its likely consequences and the measures taken or proposed to address the breach including, where appropriate, measures to mitigate its possible adverse effects. Where, and in so far as, it is not possible to provide all 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.
- (d) The data importer shall cooperate with and assist the data exporter to enable the data exporter to comply with its obligations under Regulation (EU) 2016/679, in particular to notify the competent supervisory authority and the affected data subjects, taking into account the nature of processing and the information available to the data importer.

8.7 Sensitive data

Where the transfer 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 (hereinafter 'sensitive data'), the data importer shall apply the specific restrictions and/or additional safeguards described in Annex I.B.

8.8 Onward transfers

The data importer shall only disclose the personal data to a third party on documented instructions from the data exporter. In addition, the data may only be disclosed to a third party located outside the European Union ⁽¹⁾ (in the same country as the data importer or in another third country, hereinafter 'onward transfer') if the third party is or agrees to be bound by these Clauses, under the appropriate Module, or if:

- (i) the onward transfer is to a country benefitting from an adequacy decision pursuant to Article 45 of Regulation (EU) 2016/679 that covers the onward transfer;

- (ii) the third party otherwise ensures appropriate safeguards pursuant to Articles 46 or 47 Regulation of (EU) 2016/679 with respect to the processing in question;
- (iii) the onward transfer is necessary for the establishment, exercise or defence of legal claims in the context of specific administrative, regulatory or judicial proceedings; or
- (iv) the onward transfer is necessary in order to protect the vital interests of the data subject or of another natural person.

Any onward transfer is subject to compliance by the data importer with all the other safeguards under these Clauses, in particular purpose limitation.

8.9 Documentation and compliance

- (a) The data importer shall promptly and adequately deal with enquiries from the data exporter that relate to the processing under these Clauses.
- (b) The Parties shall be able to demonstrate compliance with these Clauses. In particular, the data importer shall keep appropriate documentation on the processing activities carried out on behalf of the data exporter.
- (c) The data importer shall make available to the data exporter all information necessary to demonstrate compliance with the obligations set out in these Clauses and at the data exporter's request, allow for 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 audit, the data exporter may take into account relevant certifications held by the data importer.
- (d) The data exporter may choose to conduct the audit by itself or mandate an independent auditor. Audits may include inspections at the premises or physical facilities of the data importer and shall, where appropriate, be carried out with reasonable notice.
- (e) The Parties shall make the information referred to in paragraphs (b) and (c), including the results of any audits, available to the competent supervisory authority on request.

Clause 9

Use of sub-processors

- (a) The data importer has the data exporter's general authorisation for the engagement of sub-processor(s) from an agreed list. The data importer shall specifically inform the data exporter in writing of any intended changes to that list through the addition or replacement of sub-processors at least 30 days in advance, thereby giving the data exporter sufficient time to be able to object to such changes prior to the engagement of the sub-processor(s). The data importer shall provide the data exporter with the information necessary to enable the data exporter to exercise its right to object.
- (b) Where the data importer engages a sub-processor to carry out specific processing activities (on behalf of the data exporter), it shall do so by way of a written contract that provides for, in substance, the same data protection obligations as those binding the data importer under these Clauses, including in terms of third-party beneficiary rights for data subjects. The Parties agree that, by complying with this

Clause, the data importer fulfils its obligations under Clause 8.8. The data importer shall ensure that the sub-processor complies with the obligations to which the data importer is subject pursuant to these Clauses.

- (c) The data importer shall provide, at the data exporter's request, a copy of such a sub-processor agreement and any subsequent amendments to the data exporter. To the extent necessary to protect business secrets or other confidential information, including personal data, the data importer may redact the text of the agreement prior to sharing a copy.
- (d) The data importer shall remain fully responsible to the data exporter for the performance of the sub-processor's obligations under its contract with the data importer. The data importer shall notify the data exporter of any failure by the sub-processor to fulfil its obligations under that contract.
- (e) The data importer shall agree a third-party beneficiary clause with the sub-processor whereby – in the event the data importer has factually disappeared, ceased to exist in law or has become insolvent – the data exporter shall have the right to terminate the sub-processor contract and to instruct the sub-processor to erase or return the personal data.

Clause 10

Data subject rights

- (a) The data importer shall promptly notify the data exporter of any request it has received from a data subject. It shall not respond to that request itself unless it has been authorised to do so by the data exporter.
- (b) The data importer shall assist the data exporter in fulfilling its obligations to respond to data subjects' requests for the exercise of their rights under Regulation (EU) 2016/679. In this regard, the Parties shall set out in Annex II the appropriate technical and organisational measures, taking into account the nature of the processing, by which the assistance shall be provided, as well as the scope and the extent of the assistance required.
- (c) In fulfilling its obligations under paragraphs (a) and (b), the data importer shall comply with the instructions from the data exporter.

Clause 11

Redress

- (a) The data importer shall inform data subjects in a transparent and easily accessible format, through individual notice or on its website, of a contact point authorised to handle complaints. It shall deal promptly with any complaints it receives from a data subject.
- (b) In case of a dispute between a data subject and one of the Parties as regards compliance with these Clauses, that Party shall use its best efforts to resolve the issue amicably in a timely fashion. The Parties shall keep each other informed about such disputes and, where appropriate, cooperate in resolving them.
- (c) Where the data subject invokes a third-party beneficiary right pursuant to Clause 3, the data importer shall accept the decision of the data subject to:

- (i) lodge a complaint with the supervisory authority in the Member State of his/her habitual residence or place of work, or the competent supervisory authority pursuant to Clause 13;
 - (ii) refer the dispute to the competent courts within the meaning of Clause 18.
- (d) The Parties accept that the data subject may be represented by a not-for-profit body, organisation or association under the conditions set out in Article 80(1) of Regulation (EU) 2016/679.
 - (e) The data importer shall abide by a decision that is binding under the applicable EU or Member State law.
 - (f) The data importer agrees that the choice made by the data subject will not prejudice his/her substantive and procedural rights to seek remedies in accordance with applicable laws.

Clause 12

Liability

- (a) Each Party shall be liable to the other Party/ies for any damages it causes the other Party/ies by any breach of these Clauses.
- (b) The data importer shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages the data importer or its sub-processor causes the data subject by breaching the third-party beneficiary rights under these Clauses.
- (c) Notwithstanding paragraph (b), the data exporter shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages the data exporter or the data importer (or its sub-processor) causes the data subject by breaching the third-party beneficiary rights under these Clauses. This is without prejudice to the liability of the data exporter and, where the data exporter is a processor acting on behalf of a controller, to the liability of the controller under Regulation (EU) 2016/679 or Regulation (EU) 2018/1725, as applicable.
- (d) The Parties agree that if the data exporter is held liable under paragraph (c) for damages caused by the data importer (or its sub-processor), it shall be entitled to claim back from the data importer that part of the compensation corresponding to the data importer's responsibility for the damage.
- (e) Where more than one Party is responsible for any damage caused to the data subject as a result of a breach of these Clauses, all responsible Parties shall be jointly and severally liable and the data subject is entitled to bring an action in court against any of these Parties.
- (f) The Parties agree that if one Party is held liable under paragraph (e), it shall be entitled to claim back from the other Party/ies that part of the compensation corresponding to its/their responsibility for the damage.
- (g) The data importer may not invoke the conduct of a sub-processor to avoid its own liability.

Clause 13**Supervision**

- (a) [Where the data exporter is established in an EU Member State:] The supervisory authority with responsibility for ensuring compliance by the data exporter with Regulation (EU) 2016/679 as regards the data transfer, as indicated in Annex I.C, shall act as competent supervisory authority.

[Where the data exporter is not established in an EU Member State, but falls within the territorial scope of application of Regulation (EU) 2016/679 in accordance with its Article 3(2) and has appointed a representative pursuant to Article 27(1) of Regulation (EU) 2016/679:] The supervisory authority of the Member State in which the representative within the meaning of Article 27(1) of Regulation (EU) 2016/679 is established, as indicated in Annex I.C, shall act as competent supervisory authority.

[Where the data exporter is not established in an EU Member State, but falls within the territorial scope of application of Regulation (EU) 2016/679 in accordance with its Article 3(2) without however having to appoint a representative pursuant to Article 27(2) of Regulation (EU) 2016/679:] The supervisory authority of one of the Member States in which the data subjects whose personal data is transferred under these Clauses in relation to the offering of goods or services to them, or whose behaviour is monitored, are located, as indicated in Annex I.C, shall act as competent supervisory authority.

- (b) The data importer agrees to submit itself to the jurisdiction of and cooperate with the competent supervisory authority in any procedures aimed at ensuring compliance with these Clauses. In particular, the data importer agrees to respond to enquiries, submit to audits and comply with the measures adopted by the supervisory authority, including remedial and compensatory measures. It shall provide the supervisory authority with written confirmation that the necessary actions have been taken.

SECTION III – LOCAL LAWS AND OBLIGATIONS IN CASE OF ACCESS BY PUBLIC AUTHORITIES

Clause 14**Local laws and practices affecting compliance with the Clauses**

- (a) The Parties warrant that they have no reason to believe that the laws and practices in the third country of destination applicable to the processing of the personal data by the data importer, including any requirements to disclose personal data or measures authorising access by public authorities, prevent the data importer from fulfilling its obligations under these Clauses. This is based on the understanding that laws and practices that respect the essence of the fundamental rights and freedoms and do not exceed what is necessary and proportionate in a democratic society to safeguard one of the objectives listed in Article 23(1) of Regulation (EU) 2016/679, are not in contradiction with these Clauses.
- (b) The Parties declare that in providing the warranty in paragraph (a), they have taken due account in particular of the following elements:
- (i) the specific circumstances of the transfer, including the length of the processing chain, the number of actors involved and the transmission channels used; intended onward transfers; the type of recipient; the purpose of processing; the categories and format of the transferred personal data; the economic sector in which the transfer occurs; the storage location of the data transferred;

- (ii) the laws and practices of the third country of destination– including those requiring the disclosure of data to public authorities or authorising access by such authorities – relevant in light of the specific circumstances of the transfer, and the applicable limitations and safeguards ⁽²⁾;
 - (iii) any relevant contractual, technical or organisational safeguards put in place to supplement the safeguards under these Clauses, including measures applied during transmission and to the processing of the personal data in the country of destination.
- (c) The data importer warrants that, in carrying out the assessment under paragraph (b), it has made its best efforts to provide the data exporter with relevant information and agrees that it will continue to cooperate with the data exporter in ensuring compliance with these Clauses.
 - (d) The Parties agree to document the assessment under paragraph (b) and make it available to the competent supervisory authority on request.
 - (e) The data importer agrees to notify the data exporter promptly if, after having agreed to these Clauses and for the duration of the contract, it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under paragraph (a), including following a change in the laws of the third country or a measure (such as a disclosure request) indicating an application of such laws in practice that is not in line with the requirements in paragraph (a).
 - (f) Following a notification pursuant to paragraph (e), or if the data exporter otherwise has reason to believe that the data importer can no longer fulfil its obligations under these Clauses, the data exporter shall promptly identify appropriate measures (e.g. technical or organisational measures to ensure security and confidentiality) to be adopted by the data exporter and/or data importer to address the situation. The data exporter shall suspend the data transfer if it considers that no appropriate safeguards for such transfer can be ensured, or if instructed by the competent supervisory authority to do so. In this case, the data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses. If the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise. Where the contract is terminated pursuant to this Clause, Clause 16(d) and (e) shall apply.

Clause 15

Obligations of the data importer in case of access by public authorities

15.1 Notification

- (a) The data importer agrees to notify the data exporter and, where possible, the data subject promptly (if necessary with the help of the data exporter) if it:
 - (i) receives a legally binding request from a public authority, including judicial authorities, under the laws of the country of destination for the disclosure of personal data transferred pursuant to these Clauses; such notification shall include information about the personal data requested, the requesting authority, the legal basis for the request and the response provided; or
 - (ii) becomes aware of any direct access by public authorities to personal data transferred pursuant to these Clauses in accordance with the laws of the country of destination; such notification shall include all information available to the importer.
- (b) If the data importer is prohibited from notifying the data exporter and/or the data subject under the laws of the country of destination, the data importer agrees to use its best efforts to obtain a waiver of the prohibition, with a view to communicating as much information as

possible, as soon as possible. The data importer agrees to document its best efforts in order to be able to demonstrate them on request of the data exporter.

- (c) Where permissible under the laws of the country of destination, the data importer agrees to provide the data exporter, at regular intervals for the duration of the contract, with as much relevant information as possible on the requests received (in particular, number of requests, type of data requested, requesting authority/ies, whether requests have been challenged and the outcome of such challenges, etc.).
- (d) The data importer agrees to preserve the information pursuant to paragraphs (a) to (c) for the duration of the contract and make it available to the competent supervisory authority on request.
- (e) Paragraphs (a) to (c) are without prejudice to the obligation of the data importer pursuant to Clause 14(e) and Clause 16 to inform the data exporter promptly where it is unable to comply with these Clauses.

15.2 Review of legality and data minimisation

- (a) The data importer agrees to review the legality of the request for disclosure, in particular whether it remains within the powers granted to the requesting public authority, and to challenge the request if, after careful assessment, it concludes that there are reasonable grounds to consider that the request is unlawful under the laws of the country of destination, applicable obligations under international law and principles of international comity. The data importer shall, under the same conditions, pursue possibilities of appeal. When challenging a request, the data importer shall seek interim measures with a view to suspending the effects of the request until the competent judicial authority has decided on its merits. It shall not disclose the personal data requested until required to do so under the applicable procedural rules. These requirements are without prejudice to the obligations of the data importer under Clause 14(e).
- (b) The data importer agrees to document its legal assessment and any challenge to the request for disclosure and, to the extent permissible under the laws of the country of destination, make the documentation available to the data exporter. It shall also make it available to the competent supervisory authority on request.
- (c) The data importer agrees to provide the minimum amount of information permissible when responding to a request for disclosure, based on a reasonable interpretation of the request.

SECTION IV – FINAL PROVISIONS

Clause 16

Non-compliance with the Clauses and termination

- (a) The data importer shall promptly inform the data exporter if it is unable to comply with these Clauses, for whatever reason.
- (b) In the event that the data importer is in breach of these Clauses or unable to comply with these Clauses, the data exporter shall suspend the transfer of personal data to the data importer until compliance is again ensured or the contract is terminated. This is without prejudice to Clause 14(f).
- (c) The data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses, where:

- (i) the data exporter has suspended the transfer of personal data to the data importer pursuant to paragraph (b) and compliance with these Clauses is not restored within a reasonable time and in any event within one month of suspension;
- (ii) the data importer is in substantial or persistent breach of these Clauses; or
- (iii) the data importer fails to comply with a binding decision of a competent court or supervisory authority regarding its obligations under these Clauses.

In these cases, it shall inform the competent supervisory authority of such non-compliance. Where the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise.

- (d) Personal data that has been transferred prior to the termination of the contract pursuant to paragraph (c) shall at the choice of the data exporter immediately be returned to the data exporter or deleted in its entirety. The same shall apply to any copies of the data. The data importer shall certify the deletion of the data to the data exporter. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit the return or deletion of the transferred personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process the data to the extent and for as long as required under that local law.
- (e) Either Party may revoke its agreement to be bound by these Clauses where (i) the European Commission adopts a decision pursuant to Article 45(3) of Regulation (EU) 2016/679 that covers the transfer of personal data to which these Clauses apply; or (ii) Regulation (EU) 2016/679 becomes part of the legal framework of the country to which the personal data is transferred. This is without prejudice to other obligations applying to the processing in question under Regulation (EU) 2016/679.

Clause 17

Governing law

These Clauses shall be governed by the law of the EU Member State in which the data exporter is established. Where such law does not allow for third-party beneficiary rights, they shall be governed by the law of another EU Member State that does allow for third-party beneficiary rights. The Parties agree that this shall be the law of the Republic of Ireland.

Clause 18

Choice of forum and jurisdiction

- (a) Any dispute arising from these Clauses shall be resolved by the courts of an EU Member State.
- (b) The Parties agree that those shall be the courts of the EU Member State in which the data exporter is established.
- (c) A data subject may also bring legal proceedings against the data exporter and/or data importer before the courts of the Member State in which he/she has his/her habitual residence.
- (d) The Parties agree to submit themselves to the jurisdiction of such courts.

APPENDIX

ANNEX I

A. LIST OF PARTIES

Data exporter(s): *[Identity and contact details of the data exporter(s) and, where applicable, of its/their data protection officer and/or representative in the European Union]*

Name: Customer/Data Controller as set forth in the GDPR Data Processing Addendum (“DPA”).

Address: As set forth in the DPA.

Contact person’s name, position and contact details: As set forth in the DPA.

Activities relevant to the data transferred under these Clauses:

The processing of personal data by data importer pursuant to the Agreement.

Signature and date: Please see the signature page to the DPA.

Role: Controller.

Data importer(s): *[Identity and contact details of the data importer(s), including any contact person with responsibility for data protection]*

Name: Data Processor under the DPA

Address: Address and Contact Information for such Data Processor as set forth in the DPA

Contact person’s name, position and contact details: As set forth in the DPA.

Activities relevant to the data transferred under these Clauses: The processing of personal data by data importer pursuant to the Agreement.

Signature and date: Please see the signature page to the DPA.

Role: Processor

B. DESCRIPTION OF TRANSFER

Categories of data subjects whose personal data is transferred

As specified in the DPA.

Categories of personal data transferred

As specified in the DPA.

Sensitive data transferred (if applicable) and applied restrictions or safeguards that fully take into consideration the nature of the data and the risks involved, such as for instance strict purpose limitation,

access restrictions (including access only for staff having followed specialised training), keeping a record of access to the data, restrictions for onward transfers or additional security measures.

If and to the extent specified in the DPA.

The frequency of the transfer (e.g. whether the data is transferred on a one-off or continuous basis).

Continuous basis.

Nature of the processing

As specified in the DPA.

Purpose(s) of the data transfer and further processing

As specified in the DPA.

The period for which the personal data will be retained, or, if that is not possible, the criteria used to determine that period

As specified in the DPA.

For transfers to (sub-) processors, also specify subject matter, nature and duration of the processing

As specified in the DPA.

C. COMPETENT SUPERVISORY AUTHORITY

Identify the competent supervisory authority/ies in accordance with Clause 13

Where the data exporter is established in an EU Member State: The supervisory authority of that EU Member State shall act as competent supervisory authority.

Where the data exporter is not established in an EU Member State, but falls within the territorial scope of application of Regulation (EU) 2016/679 in accordance with its Article 3(2) and has appointed a representative pursuant to Article 27(1) of Regulation (EU) 2016/679: The supervisory authority of the Member State in which such representative is established shall act as competent supervisory authority.

Where the data exporter is not established in an EU Member State, but falls within the territorial scope of application of Regulation (EU) 2016/679 in accordance with its Article 3(2) without however having to appoint a representative pursuant to Article 27(2) of Regulation (EU) 2016/679: The Data Protection Commission of the Republic of Ireland shall act as competent supervisory authority.

ANNEX II

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

Description of the technical and organisational measures implemented by the data importer(s) (including any relevant certifications) to ensure an appropriate level of security, taking into account the nature, scope, context and purpose of the processing, and the risks for the rights and freedoms of natural persons.

Technical and organisational measures as specified in the DPA.

UK ADDENDUM TO EU STANDARD CONTRACTUAL CLAUSES

Standard Data Protection Clauses to be issued by the Commissioner under S119A(1) Data Protection Act 2018

International Data Transfer Addendum to the EU Commission Standard Contractual Clauses

VERSION B1.0, in force 21 March 2022

This Addendum has been issued by the Information Commissioner for Parties making Restricted Transfers. The Information Commissioner considers that it provides Appropriate Safeguards for Restricted Transfers when it is entered into as a legally binding contract.

Part 1: Tables

Table 1: Parties

<p>Start date</p>	<p>This Addendum shall start upon the date of the importer’s signature on the DPA (as defined below) or, with respect to an agreement that incorporates the DPA by reference, upon the date of such agreement.</p> <p>In this Addendum, the term “DPA” refers to the GDPR Data Processing Addendum - to which this Addendum is attached.</p>	
<p>The Parties</p>	<p>Exporter (who sends the Restricted Transfer)</p>	<p>Importer (who receives the Restricted Transfer)</p>

<p>Parties' details</p>	<p>Full legal name: The name of the Data Controller as set forth on the signature pages to the DPA.</p> <p>Trading name (if different): Main address (if a company registered address): The address of the Data Controller as set forth on the signature pages to the DPA.</p> <p>Official registration number (if any) (company number or similar identifier): If applicable, as set forth on the signature pages to the DPA.</p>	<p>Full legal name: The name of the Data Processor as set forth on the signature pages to the DPA.</p> <p>Trading name (if different): Main address (if a company registered address): The address of the Data Processor as set forth on the signature pages to the DPA.</p> <p>Official registration number (if any) (company number or similar identifier): Not applicable.</p>
<p>Key Contact</p>	<p>Full Name (optional): As set forth on the signature page of the DPA.</p> <p>Job Title: As set forth on the signature page of the DPA.</p> <p>Contact details including email: As set forth on the signature page of the DPA.</p>	<p>Full Name (optional): As set forth on the signature page of the DPA.</p> <p>Job Title: As set forth on the signature page of the DPA.</p> <p>Contact details including email: As set forth on the signature page of the DPA.</p>
<p>Signature (if required for the purposes of Section 2)</p>	<p>By _____ Name _____ Title _____ Date _____</p>	<p>By _____ Name _____ Title _____ Date _____</p>

Table 2: Selected SCCs, Modules and Selected Clauses

Addendum EU SCCs		<input checked="" type="checkbox"/> The version of the Approved EU SCCs which this Addendum is appended to, detailed below, including the Appendix Information: Date: The date of the DPA. Reference (if any): Other identifier (if any): Or <input type="checkbox"/> the Approved EU SCCs, including the Appendix Information and with only the following modules, clauses or optional provisions of the Approved EU SCCs brought into effect for the purposes of this Addendum:				
Module	Module in operation	Clause 7 (Docking Clause)	Clause 11 (Option)	Clause 9a (Prior Authorisation or General Authorisation)	Clause 9a (Time period)	Is personal data received from the Importer combined with personal data collected by the Exporter?
1						
2						
3						
4						

Table 3: Appendix Information

“**Appendix Information**” means the information which must be provided for the selected modules as set out in the Appendix of the Approved EU SCCs (other than the Parties), and which for this Addendum is set out in:

Annex 1A: List of Parties: As set forth in Part A of Annex I to the version of the Approved EU SCCs which this Addendum is appended to.

Annex 1B: Description of Transfer: As set forth in Part B of Annex I to the version of the Approved EU SCCs which this Addendum is appended to.

Annex II: Technical and organisational measures including technical and organisational measures to ensure the security of the data: As set forth in Annex II to the version of the Approved EU SCCs which this Addendum is appended to.

Annex III: List of Sub processors (Modules 2 and 3 only): As specified in the DPA.

Table 4: Ending this Addendum when the Approved Addendum Changes

<p>Ending this Addendum when the Approved Addendum changes</p>	<p>Which Parties may end this Addendum as set out in Section 19:</p> <p><input checked="" type="checkbox"/> Importer</p> <p><input checked="" type="checkbox"/> Exporter</p> <p><input type="checkbox"/> neither Party</p>
---	--

Part 2: Mandatory Clauses

Entering into this Addendum

1. Each Party agrees to be bound by the terms and conditions set out in this Addendum, in exchange for the other Party also agreeing to be bound by this Addendum.
2. Although Annex 1A and Clause 7 of the Approved EU SCCs require signature by the Parties, for the purpose of making Restricted Transfers, the Parties may enter into this Addendum in any way that makes them legally binding on the Parties and allows data subjects to enforce their rights as set out in this Addendum. Entering into this Addendum will have the same effect as signing the Approved EU SCCs and any part of the Approved EU SCCs.

Interpretation of this Addendum

3. Where this Addendum uses terms that are defined in the Approved EU SCCs those terms shall have the same meaning as in the Approved EU SCCs. In addition, the following terms have the following meanings:

<p>Addendum</p>	<p>This International Data Transfer Addendum which is made up of this Addendum incorporating the Addendum EU SCCs.</p>
-----------------	--

Addendum EU SCCs	The version(s) of the Approved EU SCCs which this Addendum is appended to, as set out in Table 2, including the Appendix Information.
Appendix Information	As set out in Table 3.
Appropriate Safeguards	The standard of protection over the personal data and of data subjects' rights, which is required by UK Data Protection Laws when you are making a Restricted Transfer relying on standard data protection clauses under Article 46(2)(d) UK GDPR.
Approved Addendum	The template Addendum issued by the ICO and laid before Parliament in accordance with s119A of the Data Protection Act 2018 on 28 January 2022, as it is revised under Section 18.
Approved EU SCCs	The Standard Contractual Clauses set out in the Annex of Commission Implementing Decision (EU) 2021/914 of 4 June 2021.
ICO	The Information Commissioner.
Restricted Transfer	A transfer which is covered by Chapter V of the UK GDPR.
UK	The United Kingdom of Great Britain and Northern Ireland.
UK Data Protection Laws	All laws relating to data protection, the processing of personal data, privacy and/or electronic communications in force from time to time in the UK, including the UK GDPR and the Data Protection Act 2018.
UK GDPR	As defined in section 3 of the Data Protection Act 2018.

4. This Addendum must always be interpreted in a manner that is consistent with UK Data Protection Laws and so that it fulfils the Parties' obligation to provide the Appropriate Safeguards.
5. If the provisions included in the Addendum EU SCCs amend the Approved SCCs in any way which is not permitted under the Approved EU SCCs or the Approved Addendum, such amendment(s) will not be incorporated in this Addendum and the equivalent provision of the Approved EU SCCs will take their place.
6. If there is any inconsistency or conflict between UK Data Protection Laws and this Addendum, UK Data Protection Laws applies.
7. If the meaning of this Addendum is unclear or there is more than one meaning, the meaning which most closely aligns with UK Data Protection Laws applies.

8. Any references to legislation (or specific provisions of legislation) means that legislation (or specific provision) as it may change over time. This includes where that legislation (or specific provision) has been consolidated, reenacted and/or replaced after this Addendum has been entered into.

Hierarchy

9. Although Clause 5 of the Approved EU SCCs sets out that the Approved EU SCCs prevail over all related agreements between the parties, the parties agree that, for Restricted Transfers, the hierarchy in Section 10 will prevail.
10. Where there is any inconsistency or conflict between the Approved Addendum and the Addendum EU SCCs (as applicable), the Approved Addendum overrides the Addendum EU SCCs, except where (and in so far as) the inconsistent or conflicting terms of the Addendum EU SCCs provides greater protection for data subjects, in which case those terms will override the Approved Addendum.
11. Where this Addendum incorporates Addendum EU SCCs which have been entered into to protect transfers subject to the General Data Protection Regulation (EU) 2016/679 then the Parties acknowledge that nothing in this Addendum impacts those Addendum EU SCCs.

Incorporation of and changes to the EU SCCs

12. This Addendum incorporates the Addendum EU SCCs which are amended to the extent necessary so that:
 - a. together they operate for data transfers made by the data exporter to the data importer, to the extent that UK Data Protection Laws apply to the data exporter's processing when making that data transfer, and they provide Appropriate Safeguards for those data transfers;
 - b. Sections 9 to 11 override Clause 5 (Hierarchy) of the Addendum EU SCCs; and
 - c. this Addendum (including the Addendum EU SCCs incorporated into it) is (1) governed by the laws of England and Wales and (2) any dispute arising from it is resolved by the courts of England and Wales, in each case unless the laws and/or courts of Scotland or Northern Ireland have been expressly selected by the Parties.
13. Unless the Parties have agreed alternative amendments which meet the requirements of Section 12, the provisions of Section 15 will apply.
14. No amendments to the Approved EU SCCs other than to meet the requirements of Section 12 may be made.
15. The following amendments to the Addendum EU SCCs (for the purpose of Section 12) are made:
 - a. References to the "Clauses" means this Addendum, incorporating the Addendum EU SCCs;
 - b. In Clause 2, delete the words:

“and, with respect to data transfers from controllers to processors and/or processors to processors, standard contractual clauses pursuant to Article 28(7) of Regulation (EU) 2016/679”;

- c. Clause 6 (Description of the transfer(s)) is replaced with:

“The details of the transfers(s) and in particular the categories of personal data that are transferred and the purpose(s) for which they are transferred) are those specified in Annex I.B where UK Data Protection Laws apply to the data exporter’s processing when making that transfer.”;

- d. Clause 8.7(i) of Module 1 is replaced with:

“it is to a country benefitting from adequacy regulations pursuant to Section 17A of the UK GDPR that covers the onward transfer”;

- e. Clause 8.8(i) of Modules 2 and 3 is replaced with:

“the onward transfer is to a country benefitting from adequacy regulations pursuant to Section 17A of the UK GDPR that covers the onward transfer;”

- f. References to “Regulation (EU) 2016/679”, “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 (General Data Protection Regulation)” and “that Regulation” are all replaced by “UK Data Protection Laws”. References to specific Article(s) of “Regulation (EU) 2016/679” are replaced with the equivalent Article or Section of UK Data Protection Laws;

- g. References to Regulation (EU) 2018/1725 are removed;

- h. References to the “European Union”, “Union”, “EU”, “EU Member State”, “Member State” and “EU or Member State” are all replaced with the “UK”;

- i. The reference to “Clause 12(c)(i)” at Clause 10(b)(i) of Module one, is replaced with “Clause 11(c)(i)”;

- j. Clause 13(a) and Part C of Annex I are not used;

- k. The “competent supervisory authority” and “supervisory authority” are both replaced with the “Information Commissioner”;

- l. In Clause 16(e), subsection (i) is replaced with:

“the Secretary of State makes regulations pursuant to Section 17A of the Data Protection Act 2018 that cover the transfer of personal data to which these clauses apply;”;

- m. Clause 17 is replaced with:

“These Clauses are governed by the laws of England and Wales.”;

- n. Clause 18 is replaced with:

“Any dispute arising from these Clauses shall be resolved by the courts of England and Wales. A data subject may also bring legal proceedings against the data exporter and/or data importer before the courts of any country in the UK. The Parties agree to submit themselves to the jurisdiction of such courts.”; and

- o. The footnotes to the Approved EU SCCs do not form part of the Addendum, except for footnotes 8, 9, 10 and 11.

Amendments to this Addendum

16. The Parties may agree to change Clauses 17 and/or 18 of the Addendum EU SCCs to refer to the laws and/or courts of Scotland or Northern Ireland.
17. If the Parties wish to change the format of the information included in Part 1: Tables of the Approved Addendum, they may do so by agreeing to the change in writing, provided that the change does not reduce the Appropriate Safeguards.
18. From time to time, the ICO may issue a revised Approved Addendum which:
 - a. makes reasonable and proportionate changes to the Approved Addendum, including correcting errors in the Approved Addendum; and/or
 - b. reflects changes to UK Data Protection Laws;

The revised Approved Addendum will specify the start date from which the changes to the Approved Addendum are effective and whether the Parties need to review this Addendum including the Appendix Information. This Addendum is automatically amended as set out in the revised Approved Addendum from the start date specified.

19. If the ICO issues a revised Approved Addendum under Section 18, if any Party selected in Table 4 “Ending the Addendum when the Approved Addendum changes”, will as a direct result of the changes in the Approved Addendum have a substantial, disproportionate and demonstrable increase in:
 - a. its direct costs of performing its obligations under the Addendum; and/or
 - b. its risk under the Addendum,and in either case it has first taken reasonable steps to reduce those costs or risks so that it is not substantial and disproportionate, then that Party may end this Addendum at the end of a reasonable notice period, by providing written notice for that period to the other Party before the start date of the revised Approved Addendum.
20. The Parties do not need the consent of any third party to make changes to this Addendum, but any changes must be made in accordance with its terms.