

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 current agreements 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 (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. To complete and execute the Addendum, the Customer must:

1. Fill in the information requested on the signature page and sign where indicated. **The Addendum must be signed by the same Customer entity that executed the Agreement for the RR Services.**
2. Scan and send the completed and signed Addendum to Research Research by email to rrGDPRAddendum@exlibrisgroup.com.

EFFECTIVE DATE

This Addendum shall enter into force and become legally binding upon Research Research's receipt of the Addendum validly completed and signed by Customer or a signed Agreement incorporating this Addendum by reference.

CONTACT FOR ADDITIONAL INFORMATION

Any question related to execution of this Addendum should be directed to your Research Research sales contact.

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 (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 processing, on the RR Services, 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, 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.

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 processes in 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. 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, unless required to do so by Union or relevant Member State law and (ii) have committed to maintain the confidentiality of any personal data.
- 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 no less protective of personal data than those imposed on Data Processor in this Addendum; and (b) where any such processor 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 processor's obligations.

- 6.2 Data Controller hereby authorises Data Processor to engage affiliates (under common ownership with Data Processor) 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 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 sub-processors and to adjust the processing roles of the listed sub-processors. Data Processor shall inform Data Controller of any intended adjustment of processing roles and/or addition of sub-processors after the date of execution of this Addendum, thereby giving Data Controller the opportunity to object to such adjustment and/or addition. 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 10 business days after receipt of Data Processor's notice 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 may use 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

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 set forth above), including certain countries outside the EEA. With respect to transfers of personal data to a sub-processor located outside of the EEA, Data Processor shall in advance of any such transfer ensure that such countries are recognised by the European Commission 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.

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

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.

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 To the extent audits of data security are undertaken by Data Processor and/or the data center provider from time-to-time by engaging, at their own expense, duly qualified third parties to audit and certify Data Processor's relevant operations and/or data centers, Data Processor shall make available to Data Controller the security certifications evidencing same.

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 and 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.

[END OF PAGE]

DATA PRIVACY OFFICER OR CONTACT PERSON

The parties' respective data privacy officer ("DPO") or contact person for data protection enquiries is:

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:

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: Ofer Mosseri

Title: Director

Date: 12/02/2019

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;
- d) Security doors (electronic door opener, ID reader);
- e) 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 that ensure that persons entitled to use a data processing system gain access only to such personal data as they are entitled to accessing 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 of 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]