Data Processing Agreement

in accordance with Art. 28 GDPR

between

You and the entity you represent, ordering Business Products from ResearchGate,

the Controller in the sense of Art. 28 GDPR, hereinafter referred to as the "**Controller**"

and

ResearchGate GmbH
Chausseestrasse 20
10115 Berlin
Germany,

the Processor in the sense of Art. 28 GDPR, hereinafter referred to as "**ResearchGate**".

Preamble

The Controller has selected ResearchGate to act as a service provider in accordance with Art. 28 of Regulation (EU) 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation, "**GDPR**").

This Data Processing Agreement, including all Annexes (hereinafter referred to collectively as the "**DPA**"), specifies the data protection obligations that apply to parties to any of the following types of agreement: Framework Agreement, Service Agreement (as defined in the ResearchGate Business Service Terms (https://www.researchgate.net/business-service-terms)) and/or a ResearchGate Purchase Order
(hereinafter referred to as the "**Principal Agreement**").

This DPA is concluded when the Controller signs the Framework Agreement or ResearchGate Purchase Order.

1. Scope and definitions

(1) The following provisions shall apply to all data processing that can be subject to a Data Processing Agreement according to Art. 28 GDPR, undertaken by ResearchGate on behalf of the Controller under Art. 28 GDPR, which ResearchGate performs pursuant to that agreed herein and the Principal Agreement.

(2) "Processing" and "personal data" shall mean what Art. 4 GDPR provides.

ResearchGate GmbH
Chausseestr. 20
10115 Berlin, Germany
www.researchgate.net

Registered Seat
Berlin, Germany
HR B 232771 B
VAT-ID DE258434568

Managing Directors
Dr. Ijad Madisch
Dr. Sören Hofmayer

A proud affiliate of
ResearchGate Corporation
350 Townsend St #754
San Francisco, CA 94107, USA

(3) Lead Collection, means Lead Collection and Events as defined in the Principal Agreement.

(4) *Job Application,* means Job Posts, Job Bundles, and/or Job Subscriptions as defined in the Principal Agreement.

2. Subject matter and duration of the data processing

(1) ResearchGate shall process the personal data relevant for this DPA only on behalf of the Controller. ResearchGate shall process the relevant personal data in accordance with the instructions of the Controller.

(2) The data processing shall be:

Carrying out "Lead Collection" in accordance with the Principal Agreement and/or

Carrying out Collecting Job Applications in accordance with the Principal Agreement.

ResearchGate may process data for a wholly separate and unrelated purpose while acting in its independent role as "Controller" of the ResearchGate website/platform. The herein agreed data processing for Controller only affects the specific processing executed for and on behalf of Controller and/or that results in a specific output created for and on behalf of the Controller. For example, an individual's email address may be used to create an account on ResearchGate's website and, as a wholly separate matter, that same email address may be entered by the individual into a webform created for the Controller. In such case, the subject matter of this DPA is only the processing of the email address when entered into the Controller's webform.

(3) The duration of this DPA corresponds to the duration of the Principal Agreement, unless ResearchGate terminates the DPA. ResearchGate may terminate this DPA at any time, with a termination period of three months to the end of the month.

3. Nature and purpose of the data processing

The nature and purpose of the processing of personal data by ResearchGate is:

Lead Collection	**Job Applications**
• ResearchGate creates a webform for the Controller. This webform, displayed to internet users who visit ResearchGate's website, enables users to enter their personal data and provide their consent for specific purposes.	• ResearchGate creates a webform for the Controller, as part of a Job Post that may also be promoted on Controller's website. This webform, displayed to internet users who visit ResearchGate's website, may enable users to enter their personal data, attach application documents such as CVs, reference

• The data entered is not sent to the Controller directly but is sent to ResearchGate's systems first. • As per the Controller's instructions and insofar as applicable, ResearchGate might transfer the relevant data to Controller by a) "CRM forward" (meaning the data is automatically forwarded to the Controller's own CRM system), b) SFTP lead forwarder (CSV forwarder that exports the data to an SFTP server of Controller)or c) an Excel sheet with the data, provided in bulk. • Generally, when users enter their data and grant consent, they will receive "materials" (which may include, for example, posters, whitepapers, studies, current research, product descriptions, survey results, access to webinars, video recordings, etc) by email or direct download. Such materials are provided by the Controller. If the user is to receive the materials by email, such email will be sent to the user by ResearchGate. • The Controller can also choose to include in the same webform, a checkbox asking users for consent to receive commercial emails from the Controller. • The Controller can also request that the webform include further query fields and/or checkboxes. • When users submit the completed webform and provide the necessary consents, the data is stored in ResearchGate's systems.	letters, cover letters, and provide their consent for specific purposes. • The data entered is not sent to the Controller directly but is sent to ResearchGate's systems first. • ResearchGate will display the webform to logged-in members of its platform (website visitors with a ResearchGate account who are logged-in) and to website visitors who are not logged-in or do not have an account. • When users submit the completed webform and provide the mandatory consent, all data provided is stored in ResearchGate's systems • The data will then be made available to Controller within their "Recruiter Account" on ResearchGate's website and also by sending an email to Controller. • ResearchGate will delete the application documents six months after these have been uploaded by the applicant, the applicant's profile will also be deleted from the Recruiter account at the same time

4. Categories of data subjects

The categories of individuals affected by the processing of personal data under this DPA ("data subjects") include:

- Website visitors, which may include individuals who have an account with ResearchGate's professional social network, or individuals who don't have an account.

5. Types of personal data

The following types of personal data shall be processed under this DPA:

Lead Collection

- Personal master data (name, email address)
- Personal data that the Controller additionally asks ResearchGate to include in the webform

Job Applications:

- Job application documents (e.g. curriculum vitae, occupation, qualification, certificates, photos) including personal master data (e.g. name, title, academic degree, date of birth) and contact details (email address, phone number, postal address)

6. Rights and duties of the Controller

(1) The Controller is solely responsible for assessing the lawfulness of the data processing and for safeguarding the rights of data subjects.

(2) The Controller shall notify ResearchGate immediately of any errors or irregularities detected in relation to the processing of personal data by ResearchGate.

(3) The Controller may issue instructions concerning the nature, scale, and method of data processing. When requested by the Controller, ResearchGate shall confirm verbal instructions in writing or in text form (e.g. by email).

(4) The Controller can authorize dedicated persons to issue instructions. ResearchGate shall be notified of such persons in writing or in text form. In the event of changes to the persons authorized to issue instructions, the Controller must immediately notify ResearchGate of this change in writing or in text form, naming the new person(s) in each case.

7. Duties of ResearchGate

(1) Data processing

ResearchGate shall process personal data specified under Paragraph 5 of this DPA in accordance with this DPA and in accordance with the Controller's instructions.

(2) Data subjects' rights

a. Insofar as possible and insofar as personal data specified under Paragraph 5 of this DPA are affected, ResearchGate shall, within its technical and organizational capabilities, assist the Controller in complying with the rights of data subjects according to Chapter 3 GDPR.

b. If a data subject contacts ResearchGate directly with regard to any data subject rights, it is ResearchGate's sole responsibility to forward the enquiry to Controller.

(3) Monitoring duties

ResearchGate shall organize its business and operations in such way that the data processed on behalf of the Controller is secured to the extent necessary in each case and protected from unauthorized access by third parties.

a. ResearchGate has appointed a Data Protection Officer:
Data Protection Officer
ResearchGate GmbH
Chausseestr. 20
10115 Berlin, Germany
privacy@researchgate.net

(4) Information duties

a. ResearchGate will inform the Controller immediately if, in its opinion, an instruction issued by the Controller violates legal regulations. In such cases, ResearchGate shall be entitled to suspend execution of the relevant instruction until it is confirmed or changed by the Controller. However, ResearchGate is under no obligation to perform a comprehensive legal examination with respect to Controller's instructions.

b. Taking into account the nature of processing and the information available to ResearchGate, ResearchGate shall assist the Controller to comply with the obligations of Articles 32 to 36 GDPR.

c. In the event that ResearchGate establishes or reasonably believes that relevant personal data processed by ResearchGate has, due to a breach of security, led to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored or otherwise processed on behalf of the Controller, ResearchGate shall promptly, and without undue delay, however not later than seventy-two hours after becoming aware of the relevant facts, inform the Controller by email. ResearchGate shall also inform the Controller via email of the following information, without delay as such information becomes available:

    i. the nature of the personal data breach, including, where possible, the categories and approximate number of affected data subjects and

categories and approximate number of affected personal data records;

ii. the likely consequences of the personal data breach;

iii. measures taken or proposed to be taken by ResearchGate to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects; and

iv. any other reasonably available information that could help the Controller independently assess any of the above.

(5) Location of processing

ResearchGate's physical servers are located in Canada.

Apart from that the processing of the data shall in principle take place in the territory of the Federal Republic of Germany, in a member state of the European Union or in another contracting state of the Agreement on the European Economic Area. Any transfer to a third country will only take place if the requirements of Art. 44 et seq. GDPR are fulfilled.

(6) Deletion of personal data after termination of the Principal Agreement

Subject to other agreements such as in Paragraph 3 above, after termination of the Principal Agreement, ResearchGate shall delete or return the personal data processed on behalf of the Controller as soon as the Controller decides whether ResearchGate shall delete or return the data. ResearchGate will also delete existing copies, provided that the deletion of this data does not conflict with any statutory obligations of ResearchGate.

8. Monitoring rights of the Controller

(1) The Controller shall be entitled to carry out an inspection to the extent required to determine ResearchGate's compliance with the provisions on data protection and the contractual agreements, either independently or by using a third party. Such an inspection must take place during normal business hours and not disrupt ResearchGate's business operations or endanger security measures. The Controller must provide at least 8 weeks' written notice of its intention to carry out such an inspection and undertake the inspection solely at its own expense. ResearchGate shall offer the necessary support to carry out the inspection.

(2) The Controller may also request copies of existing industry-standard certifications of ResearchGate's systems, current attestations, or reports from an independent body (such as an auditor, external data protection officer or external data protection auditor), or self-assessments carried out by ResearchGate.

(3) ResearchGate shall inform the Controller of any inspection measures carried out by the supervisory authority to the extent that such measures or requests concern data processing operations carried out by ResearchGate on behalf of the Controller.

9. Sub-processing

(1) The Controller authorizes ResearchGate to make use of sub-processors in accordance with the following subsections in this Paragraph 9 of this DPA. This authorization shall constitute a general written authorization according to Art. 28 (2) GDPR.

(2) ResearchGate currently works with the sub-processors specified in Annex 2 and the Controller hereby agrees to their appointment.

(3) ResearchGate shall be entitled to appoint new sub-processors or replace sub-processors named in Annex 2 ResearchGate shall inform the Controller in advance of any intended change regarding the appointment or replacement of other sub-processors. The Controller may object to an intended change.

(4) The objection to the intended change must be lodged with ResearchGate within 2 weeks after receipt of the information regarding the intended change. In the event of an objection, ResearchGate may, at its own discretion, either provide the service without the intended change or propose an alternative sub-processor and coordinate it with the Controller. Insofar as the provision of the service is unreasonable for ResearchGate without the intended modification - for example, due to the associated disproportionate costs for ResearchGate – or where the parties are unable to agree on an alternative sub-processor, the Controller and ResearchGate may terminate this DPA as well as the Principal Agreement with a notice period of one month to the end of the month.

(5) Where ResearchGate engages a sub-processor for carrying out specific processing activities (on behalf of the controller), it shall do so by way of a contract which imposes on the sub-processor, in substance, the same data protection obligations as the ones imposed on the data processor in accordance with this DPA. ResearchGate is liable to the Controller for all acts and omissions of other sub-processors it appoints.

10. Confidentiality

(1) ResearchGate is obliged to maintain confidentiality when processing data for the Controller.

(2) In fulfilling its obligations under this DPA, ResearchGate undertakes to employ only employees or other agents who are committed to confidentiality in the handling of personal data and who have been appropriately familiarized with the requirements of data protection.

(3) Insofar as the Controller is subject to other confidentiality provisions, it shall inform ResearchGate accordingly. ResearchGate shall oblige its employees to observe these confidentiality rules in accordance with the requirements of the Controller insofar as provided to ResearchGate.

11. Technical and organizational measures

(1) The technical and organizational measures described in Annex 1 are agreed upon as appropriate. ResearchGate may update and amend these measures provided that the level of protection is not significantly reduced by such updates and/or changes.

(2) ResearchGate shall observe the principles of due and proper data processing in accordance with Art. 32 in conjunction with Art. 5 (1) GDPR. ResearchGate shall undertake appropriate measures to safeguard the data and security of the processing, taking into account the costs of implementation of such measures; the nature, scope, context, and purposes of processing; and the risk of varying likelihood and severity for the rights and freedoms of natural persons.

12. Liability/Indemnification

(1) ResearchGate shall be liable to the Controller for any damage caused in the performance of the services under this DPA by wilful or gross negligent breach of applicable statutory data protection obligations on the part of ResearchGate. ResearchGate shall not be obliged to pay any compensation when ResearchGate has processed the data relevant to this DPA solely in accordance with the instructions of the Controller and has complied with its obligations arising from the GDPR specifically directed towards processors.

(2) The Controller shall indemnify ResearchGate against all claims for damages asserted against ResearchGate based on the Controller's breach of its own obligations under this DPA or under applicable data protection and security regulations.

13. Applicability of standard data protection clauses

(1) In circumstances of Art. 46 (1) GDPR, the Processor exporting personal data to the Controller in a third country without an adequacy decision of the European Commission, the parties additionally agree in accordance with Art. 46 (2) c) to conclude standard data

protection clauses in their then current form as applicable.

(2) For the application of the Standard Data Protection Clauses as per the "COMMISSION IMPLEMENTING DECISION on standard contractual clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679" from 4 June 2021, the Parties agree to conclude "Module four": Transfer processor to controller" in the following form. The parties also agree that these Standard Contractual Clauses shall always prevail over of this DPA. Also, nothing in this DPA shall be interpreted as directly or indirectly contradictory to the Standard Contractual Clauses.

a) Clause 7 Docking Clause will be incorporated

b) Clause 8 will be Clause 8 of Module Four: Transfer processor to controller

c) There will be no Clause 9

d) Clause 10 will be Clause 10 of Module Four: Transfer processor to controller.

e) Clause 11 will be:

> 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.

f) Clause 12 will be Clause 12 of MODULE FOUR: Transfer processor to controller

g) There will be no Clause 13, Clause 14, and Clause 15

h) Clause 16 d) will be Clause 16 d) of MODULE FOUR: Transfer processor to controller

i) Clause 17 will be:

> Governing law These Clauses shall be governed by the law of a country allowing for third-party beneficiary rights. The Parties agree that this shall be the law of Germany.

j) Clause 18 will be:

> Choice of forum and jurisdiction Any dispute arising from these Clauses shall be resolved by the courts of Germany

k) With regard to Annex 1:

> This DPA's Processor is Data exporter. This DPA's Controller is Data importer. Name and addresses are such of the Principal Agreement. Contact person's name, position and contact details are also such of the Principal Agreement.
>
> Categories of data subjects: see Paragraph 4 of this DPA
>
> Categories of personal data transferred: see Paragraph 5 of this DPA
>
> No sensitive data will be transferred.

Frequency of the transfer: continuous, for duration of Principal Agreement

Nature of processing and Purpose of data transfer: Paragraph 3 of this DPA

Retention period: see Paragraph 7 (6) of this DPA

14. Miscellaneous

(1) In case of contradictions between the provisions contained in this DPA and provisions contained in the Principal Agreement, the provisions of this DPA shall prevail.

(2) Amendments and supplements to this DPA shall be subject to the mutual consent of the contracting parties, with specific reference to the provisions of this DPA to be amended. Verbal side agreements do not exist and shall also be excluded for any subsequent changes to this DPA.

(3) This DPA is exclusively subject to the laws of the Federal Republic of Germany. Any dispute arising from this DPA shall be resolved by the courts of Germany.

(4) In the event that access to the data which the Controller has transmitted to ResearchGate for data processing is jeopardized by third-party measures (such as measures taken by an insolvency administrator, seizure by revenue authorities, etc.), ResearchGate shall notify the Controller of such without undue delay.

Schedule of Annexes

Annex 1 Technical and organizational measures taken to ensure the security of processing

Annex 2 Sub-processors pursuant to Paragraph 9 of this Data Processing Agreement

Annex 1

Technical and organizational measures to ensure the security of processing

These terms form part of the DPA and describe the technical and organizational measures of ResearchGate.

Security Standards

ResearchGate has agreed to employ appropriate technical and organizational measures designed to protect against unauthorized or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data. ResearchGate's technical and organizational measures shall cover the following areas:

(1) Information Security Policies and Standards. ResearchGate will maintain information security policies, standards, and procedures. These policies, standards, and procedures shall be kept up to date, and revised whenever relevant changes are made to the information systems that use or store personal data. These policies, standards, and procedures shall be designed and implemented to:

a. prevent unauthorized persons from gaining physical access to personal data processing systems (e.g. physical access controls);

b. prevent personal data processing systems from being used without authorization (e.g. logical access controls);

c. ensure that Data Personnel gain access only to such personal data as they are entitled to access (e.g. in accordance with their access rights) and that, in the course of processing or use and after storage, personal data cannot be read, copied, modified or deleted without authorization (e.g. data access controls);

d. ensure that personal data cannot be read, copied, modified, or deleted without authorization during electronic transmission, transport or storage, and that the recipients of any transfer of personal data by means of data transmission facilities can be established and verified (e.g. data transfer controls);

e. ensure the establishment of an audit trail to document whether and by whom personal data has been entered into, modified, or removed from personal data processing (e.g. entry controls);

f. ensure that personal data is processed solely in accordance with Controller's instructions (e.g. control of instructions);

g. ensure that personal data is protected against accidental destruction or loss (e.g. availability controls);

h. ensure that personal data collected for different purposes can be processed separately (e.g. separation controls);

i. ensure that personal data maintained or processed for different customers is processed in logically separate locations (e.g. data segregation);

j. ensure that all systems that process personal data are subject to a secure software developmental lifecycle; and

k. ensure that all systems that process personal data are the subject of a vulnerability management program that includes, without limitation, internal and external vulnerability scanning with risk rating findings and formal remediation plans to address any identified vulnerabilities.

(2) Physical Security.

a. General. ResearchGate will maintain commercially reasonable security systems at all ResearchGate sites at which an information system that uses or stores personal data is located ("Processing Locations") and will reasonably restrict access to such Processing Locations.

b. Data Centers. In addition to the requirements above for, for any data centers, meaning any Processing Locations that primarily contain electronic equipment used to process, store, and/or transmit digital information ("Data Centers"), ResearchGate will prevent unauthorized access through enhanced physical security measures, including at a minimum, 24x7 onsite staff, biometric scanning, and security camera monitoring.

(3) Organizational Security.

ResearchGate will maintain information security policies and procedures addressing:

a. Data Disposal. Procedures for when media are to be disposed or reused have been implemented to prevent any subsequent retrieval of any personal data stored on media before they are withdrawn from ResearchGate's inventory or control.

b. Data Minimization. Procedures for when media are to leave the premises at which the files are located as a result of maintenance operations have been implemented to prevent undue retrieval of personal data stored on media.

c. Data Classification. Policies and procedures to classify sensitive information assets, clarify security responsibilities, and promote awareness for all employees have been implemented and are maintained.

d. Incident Response. All personal data security incidents are managed in accordance with appropriate incident response procedures.

e. Encryption. Data at transfer is encrypted. Sensitive data at rest is stored using industry standard encryption mechanisms and strong cipher suites (AES 265-bit is recommended).

(4) Network Security.

a. ResearchGate maintains information security policies and procedures addressing network security.

b. ResearchGate secures its networks employing a defense-in-depth approach that utilizes commercially available equipment and industry standard techniques, including, without limitation, firewalls, access control lists, and routing protocols.

(5) Access Control (Governance).

a. ResearchGate governs access to information systems that process personal data.

b. Only authorized staff of ResearchGate can grant, modify, or revoke access to an information system that processes personal data.

c. User administration procedures are used by ResearchGate to: (i) define user roles and their privileges; (ii) govern how access is granted, changed, and terminated; (iii) address appropriate segregation of duties; and (iv) define the requirements and mechanisms for logging/monitoring.

d. All Data Personnel are assigned unique user IDs.

e. Access rights are implemented adhering to the "least privilege" approach.

f. ResearchGate implements commercially reasonable physical and technical safeguards to create and protect passwords.

(6) Virus and Malware Controls. ResearchGate protects personal data from malicious code and installs and maintains anti-virus and malware protection software.

(7) Employees.

a. ResearchGate has implemented and maintains an information security awareness program to train all employees about their security obligations. This program amongst other things, includes training about data classification obligations, physical security controls, security practices, and security incident reporting. The program is mandatory and must be completed once a year.

b. ResearchGate has implemented and maintains a data protection awareness program to train all employees amongst other things about types/categories of data; authorization procedure, justifications to use data, data processing agreements. The program is mandatory and must be completed once a year.

c. ResearchGate has clearly defined roles and responsibilities for employees.

d. ResearchGate employees are required to strictly follow established security policies and procedures. Disciplinary process is applied if employees fail to adhere to relevant policies and procedures.

e. ResearchGate shall take reasonable steps to ensure the reliability of any employees, agents or contractors who may process personal data.

(8) Business Continuity. ResearchGate implements disaster recovery and business resumption plans. Business continuity plans are tested and updated to ensure that they are up to date and effective.

Annex 2

Sub-processors pursuant to Paragraph 9 Data Processing Agreement

ResearchGate currently works with the following subcontractors and the Controller hereby agrees to their appointment.

Company: Cloudflare Inc.

Data processing activity: distributing server load, blocking bots and crawlers, security queries

Location: USA

Company: Aptum Technologies UK Ltd

Data processing activity: Server Hosting

Location: Hosting location is Toronto, Canada

Company: OVH

Data processing activity: Backup on remote location

Location: Canada

Company: Amazon Web Services EMEA SARL

Data processing activity: DNS web services

Location: Europe

Company: Google Ireland Limited

Data processing activity: Analytics and Cloud

Location: Europe

Company: Salesforce Inc.

Data processing activity:

CRM

Location: Hosting location is Germany

Company: Salesloft Inc.

Data processing activity: Sales enablement software

Location: USA