DATA PROCESSING AGREEMENT

RECITALS

Whereas:

- Controller needs to have Personal Data processed by Processor for the purpose of the performance of the Agreement;
- The general provisions from this DPA apply for all processing of Personal Data in the performance of the Agreement, and in the event of a conflict between those terms, this DPA shall apply;

DEFINITIONS

"AGREEMENT" shall mean either the Processor's Registration Agreement previously entered into by the Parties or an alternative agreement entered into by the Parties in relation to the provision of Processor's services to the Controller;
"GDPR" shall mean the General Data Protection Regulation (Regulaton (EU) 2016/679 of the European Parliament and of the Council);
"Personal Data" shall have the meaning defined in the GDPR;
"Processing" shall have the meaning defined in the GDPR.

Any terms not otherwise defined herein, shall have the meaning specified in the Agreement.

The Parties agree as follows:

1. General

1.1 The Processor undertakes to process Personal Data in accordance with Regulation (EU) 2016/679 of the European Parliament and of the Council 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) (hereinafter "GDPR") on the terms and conditions of this DPA on the instructions of the Controller. The Processor shall process the Personal Data lawfully, by means of a transparent procedure with due care and in accordance with the GDPR from 25 May 2018.

1.2 The Processor shall only effect Processing to the extent necessary to provide its services to the Controller as described in the Agreement.

1.3 Only employees who need access to Personal Data to contribute to the operation of the services will have such access to that Personal Data.

1.4 Subject to instructions received from the Controller, the Processor shall not retain Personal Data made available to it in the context of the Agreement any longer than is necessary (i) for the performance of the Agreement; or (ii) to comply with any of its statutory obligations.

1.5 The Processor shall only process the Personal Data on and in accordance with the instructions of the Controller. The Processor will not process the Personal Data for its own benefit, for the benefit of third parties (other than when the Institution has selected standard database repository settings), and/or for its own purposes or advertising purposes or other purposes, notwithstanding any of its obligations to the contrary under mandatory law.

1.6 The Processor is obligated to promptly inform the Controller regarding any changes in the performance of the Agreement affecting its obligations hereunder, so that the Controller can monitor its compliance.

2. Use of Third-Party Suppliers

2.1 Only third-parties necessary in the provision of the Services may process Personal Data for the strictly limited purposes of providing the services to the Controller. The third parties currently involved are Microsoft Bing (https://www.bing.com/) and SDL (https://www.sdl.com/). Processor confirms that it has in place written contracts with Microsoft Bing and SDL that satisfy the requirements of Art.28 GDPR. Processor shall inform the Controller in advance of any changes to these suppliers and shall communicate the specific purpose and duration of the involvement of such third parties in the processing of personal data. The Controller subsequently provides its written consent to the use of third-party suppliers in the provision of the services. In the event that a new third-party is engaged by Processor from 25 May 2018, Processor shall notify the Controller to give them the opportunity to object to the engagmement of that third-party. Processor confirms that no other third-party processors have access to the Personal Data of the Controller.

2.2 In the event the Processor engages third-party suppliers for the provision of the services, the Processor warrants it has a written agreement with the relevant third-party supplier which shall include the mandatory provisions of Article 28(3) GDPR from 25 May 2018, such third-parties may only be engaged by Turnitin if they are GDPR compliant.

2.3 The Processor indemnifies the Controller from and against all claims by third-parties asserted against the Controller due to a breach of the obligations under this DPA regarding the processing of Personal Data that is attributable to the Processor or third-party suppliers engaged by the Processor.

3. Security

3.1 Processor shall have in place appropriate technical and organisational measures pursuant to Article 32 GDPR with regard to data security, including appropriate data centre security measures. Such non-exhaustive measures are described in Annex A.

3.2 On request, the Processor shall promptly provide the Controller written information relating to the security of Personal Data.

4. Obligation to report data breaches

4.1 In the event of a: (i) loss of Personal Data, or (ii) breach of the security measures described in Annex A resulting in compromise of Personal Data, or (iii) disclosure of personal data that breaches of confidentiality; the Processor shall notify the Controller promptly after the incident was first discovered. The Processor shall take all commercially reasonable measures to prevent or limit unauthorised and unlawful processing, without prejudice to any right the Controller might have to other measures.

4.2 In the event of a breach, the Processor shall provide to the Controller all relevant and necessary information relating to the breach within 24 hours since of the breach. The Processor warrants that the information provided will be complete and correct.

4.3 At the Controller's request, the Processor shall cooperate appropriately in informing the competent authorities.

5. Audit

5.1 The Processor warrants that it undergoes periodic third-party penetration testing of its network, and utilizes the resulting reports to make changes to its Services as it deems necessary.

5.2 The Processor shall submit to and comply with commercially reasonable audits by Controller during the Term. If it is established during such an audit that the Processor has failed to comply with the provisions of the Agreement and the DPA, the Processor shall take all commercially reasonable measures to remediate such failure.

6. Data Transfer

6.1 The Processor warrants that any processing of Personal Data in connection with the performance of the Agreement performed by or for the Processor, including the third-parties engaged by it, will (when transferred outside the EEA) take place only within the United States of America. Processor has Privacy Shield certification which is recognised by the European Commission as being an adequate mechanism for data transfer to the USA (more detailed information can be found at www.privacyshield.gov), and will adhere to the standard EU model clauses on data transfer incorporated at Annex B.

6.2 Personal Data will only be transmitted in encrypted form, using proprietary and secure encryption technology.

7. Investigation Requests

7.1 If the Processor receives a request or order from a supervisory authority, government agency or investigation, prosecution or national security agency to provide (access to) Personal Data, the Processor shall immediately notify the Controller. When handling the request or order, the Processor shall observe all of the Controller's lawful instructions (including the instruction to leave the handling of the request or order in full or in part to the Controller) and provide appropriate cooperation.

8. Informing Data Subjects

8.1 The Processor shall cooperate appropriately so that the Controller can comply with its legal obligations in the event that a Data Subject exercises its rights under GDPR concerning the processing of Personal Data.

8.2 If a Data Subject, in relation to the execution of its applicable rights, contacts the Processor directly, the Processor shall not substantively respond unless expressly instructed otherwise by the Controller, but shall immediately report this to the Controller, with a request for further instructions.

8.3 If, in the context of the Agreement, the Processor offers the Service directly to end users whose Personal Data are processed, the Processor is required to inform the end user about the following in an easily accessible and permanently available manner:

a. the name and address of the Processor;
b. the purposes for which the Processor processes the Personal Data;
c. the Personal Data categories processed by the Processor;
d. the countries to which the Personal Data are transferred;
e. the right to access, correct and delete the Personal Data.

The Processor shall notify the Controller where this information is published.

9. Article 28(3) GDPR Compliance

9.1 The following applies to the processing by the Processor:

Subject matter of the processing*:*	Processing of submissions (student or academic papers or proposed published texts) and their associated personal data pursuant to the purpose described below.
Duration of the processing*:*	For the period of the processing instructed by the Data Processor only.
Nature of the processing*:*	Textual comparison services, database compilation.
Purpose of the processing*:*	To allow the Processor's customers (academic institutions / publishers) to detect potential plagiarism in the academic / publishing sectors.
Type of personal data*:*	Generally names, email addresses, student IDs, submission content.
Categories of Data Subjects*:*	Students, account administrators, instructors, authors.
Obligations of the Controller:	The Data Controller is obliged to comply with its general obligations under the GDPR, in particular to process the personal data it collects in accordance with Articles 5 and 6, and to comply with Articles 13, 14, 24, 30 and 32, and to comply with any actionable rights of the data subject.
Rights of the Controller*:*	The Controller may exercise its rights against the Data Processor under the GDPR, in particular under Articles 28 and 32.

9.2 The Processor confirms that it:

(a) processes the Personal Data only on documented instructions from the Controller, including with regard to transfers of Personal Data to a third party or an international organisation, unless required to do so by Union or Member State law to which the Processor is subject; in such a case, the Processor shall inform the Controller of that legal requirement before processing, unless that law prohibits such information on important grounds of public interest;

(b) ensures that persons authorised to process the Personal Data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality;

(c) takes all measures required pursuant to Article 28 and 32;

(d) shall not engage another processor in the performance of its obligations under the Agreement;

(e) taking into account the nature of the processing, assists the Controller by utilising appropriate technical and organisational data protection measures, insofar as this is possible, for the fulfilment of the Controller's obligation to respond to requests for exercising the data subject's rights laid down in Chapter III of GDPR;

(f) assists the Controller in ensuring compliance with the obligations pursuant to Articles 32 to 36 taking into account the nature of processing and the information available to the Processor;

(g) at the choice of the Controller, deletes or returns all the Personal Data to the Controller after the end of the provision of services relating to processing, and deletes existing copies unless Union or Member State law requires storage of the Personal Data; and

(h) makes available to the Controller all information necessary to demonstrate compliance with the obligations laid down in Article 28 and allow for and contribute to audits, including inspections, conducted by the Controller or another auditor mandated by the Data Controller.

10. Changes

10.1 If either Party makes a material change to the Personal Data to be processed or to the processing, the parties shall consult on amending the arrangements made in this DPA.

10.2 Such changes can never have the effect that the Parties cannot comply with applicable laws and regulations relating to Personal Data.

11. Term and Termination

11.1 The term of the DPA is equal to the term of the Agreement or the duration of processing, whichever is longer. The DPA cannot be terminated separately from the Agreement.

11.2 In the event of written request from the Controller during the Term or upon termination of the Agreement, the Processor shall delete and destroy Personal Data and certify such destruction in writing.

11.3 Any Party may, without undue delay, withdraw from this Agreement if there is a substantial breach of Articles 2, 3, 4, 5 and 9 of this Agreement. Effects of withdrawal shall take effect on the date of delivery to the other Party.

11.4 This Agreement shall enter into force on the date of signature by the last Party below and becomes effective on the date of its publication in the Register of Contracts under Act. No. 340/2015 Coll., On the Special Conditions for the Effectiveness of Certain Contracts, the Publishing of such Contracts and the Registry of Contracts (The Act of the Register of Contracts), as amended. The Parties agree that the Controller will ensure the publication of this Agreement under the preceding sentence.

12. Governing Law and Dispute Resolution

12.1 Performance of this DPA shall be governed by the laws of the Netherlands.

12.2 Any dispute which might arise between the Parties in connection with the DPA shall be submitted to the competent court in Amsterdam.

ANNEX A: TECHNICAL & ORGANISATIONAL MEASURES

1 Introduction

Processor, as a part of its services, collects and maintains data to fulfill its contractual obligations to Controller. To accomplish this, Processor has created a set of standard operating procedures and measures that enable secure, reliable operation of the Processor services.

2 Privacy Shield Certification

Processor is Privacy Shield certified. Privacy Shield is recognised by the European Commission as being an adequate mechanism for data transfers outside the EEA. Processor's certification can be viewed at www.privacyshield.gov/list

Note: there is no data transfer outside the EEA for Processor's 'Ephorus' product.

3 Technical Measures

Pursuant to Article 32 GDPR, Processor utilises the following technical measures to ensure data security:

3.1 Processor's services are designed with security and high availability in mind. Processor's services operate across several hundred servers and thousands of disk drives, using load balancers, custom software, and other techniques to automatically distribute load and maintain redundant copies of data at all times.

3.2 Processor currently operates its customer-facing services out of two primary datacenters in Sacramento and Santa Clara, California, USA.

3.3 Processor may also operate equipment in other smaller datacenters in the United States or European Union for networking and data redundancy reasons. Each datacenter has N+1 redundancy for power and cooling systems, and access is limited to Turnitin's staff and approved contractors who need access to perform their work duties. Our private corporate network provides secure, redundant connectivity between our offices and our datacenters.

3.4 SOC2 compliance was awarded to our technical infrastructure in May 2018 and proof of certification can be provided upon request.

3.5 Other technical measures include:

- Intrusion detection systems;
- File integrity monitors;
- Network security scanners;
- Security event monitoring;
- Sophisticated firewalls;
- Encryption of all data (in transit and at rest) submitted to the services using a proprietary, one-way hash method providing pseudonymisation;
- SSL network security;
- Employee device encryption and central management;
- Periodic third-party penetration testing of Processor's network.

4 Organisational Measures

4.1 Processor has appointed a Data Protection Officer voluntarily who can be contacted at DPO@turnitin.com and has appointed a Chief Security Officer to assist the Data Protection Officer with their role and to continuously monitor Processor's data security practices.

4.2 Processor has instigated an ongoing programme of GDPR awareness training within its organisation and receives Executive level support for data protection initiatives.

4.3 Processor has adopted the following non-exhaustive policies in relation to GDPR compliance to assist the Controller with its obligations:

- Data Breach Notification Policy;
- Data Protection Policy;
- Data Retention Policy;
- Data Subject Access Request Policy; and
- Privacy Policy available at: https://guides.turnitin.com/Privacy_and_Security#EU_Data_Protection_and_GDPR_Compliance

Annex B: Standard EU Model Clauses

The Standard Contractual Clauses for the transfer of personal data to processors outside the European Economic Area (New Processor Clause), last updated February 2010, are hereby incorporated into this Agreement by reference, amended as follows:

AMENDMENTS TO STANDARD CONTRACTUAL CLAUSES FOR THE TRANSFER OF PERSONAL DATA

Data Exporters shall mean the Controller.

Data Importer shall mean the Processor.

With reference to clause 9 of the Standard Contractual Clauses for the transfer of personal data to processors established in third countries under Directive 95/46/EC, the Governing Law is the law of England and Wales.

With reference to Appendix 1:

The Data Exporter is:

The academic institution using the services of the Data Importer as described immediately below.

The Data Importer is:

A provider of services to the academic and private sectors, to assess uploaded textual intellectual property for originality. Clients use the service as a form of plagiarism prevention and copyright protection and personal data relating to the authors of works is transferred to and stored by the data importer in the United States.

The Personal Data transferred concern the following categories of data subjects:

Individual authors and users of the services.
Individuals who wish to receive commercial information.

The personal data transferred fall within the following categories of data:

Name, title, email address, institution name - all required.
Mailing address, phone number and fax number - optional.

The personal data transferred fall within the following categories of sensitive personal data:

Not applicable unless sensitive Personal Data is contained within a submission's content, in which case it is processed lawfully under Art.9 GDPR.

The personal data transferred will be subject to the following basic processing activities:

Creation and maintenance of user profile, responses to service queries, comparison checks.