

**DATA PROCESSING
AGREEMENT**

v.06.10.2021

This Data Processor Agreement (“**DPA**”) is entered into as of 2.5.2024 between:

Turnitin LLC, 2101 Webster Street, Suite 1900, Oakland CA 94612 USA (the “**Processor**”); and

Hochschule Konstanz HTWG, Alfred-Wachtel-Str. 8, 78462 Konstanz, (the “**Controller**”);
Deutschland

who may be referred to as a “**Party**” or the “**Parties**” as the context so requires.

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 (Regulation (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 on the terms and conditions of this DPA on the instructions of the Controller. The Processor shall process the Personal Data lawfully, with due care and in accordance with the GDPR.

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 Controller provides its general 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 engagement of that third-party.

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, Appendix 2.

3.2 On request, the Processor shall promptly provide to 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, Appendix 2 resulting in compromise of Personal Data; 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. 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 (at least annually), 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 Data Transfers on the Amazon Web Services (AWS) Platform:

6.1.1 The AWS platform stores 100% of submitted content on a localized data centre in the EU (currently in Frankfurt, Germany). Randomized and encrypted sections of such submissions are processed in the USA for comparison purposes. It is not possible to re-compile submissions in the USA from the data that is processed in the USA.

6.2 Data Transfers on non-AWS Platforms:

6.2.2 Non-AWS services are provided exclusively from USA based data centres located in Sacramento and Santa Clara, California.

6.3 Regardless of whether a Service is based on the AWS platform or not, Personal Data will only be transmitted and stored in encrypted form, using proprietary and secure encryption technology on a SOC2 certified infrastructure.

6.4 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 to the USA) take place only subject to the EU Standard Contractual Clauses on data transfer incorporated at Annex A.

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, examination answers or proposed published texts) and their associated personal data pursuant to the purpose described below.
Duration of the processing:	Indefinitely unless instructed in writing by the Controller to delete the Personal Data. The Processor retaining Personal Data (submission content only) allows its Services to improve annually by adding to the database of content against which comparisons are made.
Nature of the processing:	Textual comparison services, storage, use, database compilation, grading.
Purpose of the processing:	To allow the Processor's customers (academic institutions / publishers) to detect potential plagiarism in the academic / publishing sectors, and to allow the streamlining of grading.
Type of personal data:	Generally names, email addresses, student IDs, submission content, examination answers.
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 country 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 32 GDPR;

(d) respects the conditions in paragraphs 2 and 4 of Art.28 GDPR with regard to engaging other processors;

(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 the 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 Controller.

9.3 Where the Processor engages another processor for carrying out specific processing activities on behalf of the Controller, the same data protection obligations as set out in the contract or other legal act between the controller and the processor as referred to in paragraph 3 of Art.28 GDPR shall be imposed on that other processor by way of a contract, in particular providing sufficient guarantees to implement appropriate technical and organisational measures in such a manner that the processing will meet the requirements of the GDPR. Where that other processor fails to fulfil its data protection obligations, the Processor shall remain fully liable to the Controller for the performance of that other processor's obligations.

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.

12. Governing Law and Dispute Resolution

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

12.2 Any dispute between the Parties which cannot be amicably settled without recourse to the courts in connection with the DPA shall be submitted to the competent court in Germany.

Signed for and on behalf of **Processor**


.....

Print name:

Signed for and on behalf of **Controller**



Print name: Dr. Monika Oertner

ANNEX A

STANDARD CONTRACTUAL CLAUSES

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)¹ for the transfer of personal 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

¹ Where the data exporter is a processor subject to Regulation (EU) 2016/679 acting on behalf of a Union institution or body as controller, reliance on these Clauses when engaging another processor (sub-processing) not subject to Regulation (EU) 2016/679 also ensures compliance with Article 29(4) of Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC (OJ L 295 of 21.11.2018, p. 39), to the extent these Clauses and the data protection obligations as set out in the contract or other legal act between the controller and the processor pursuant to Article 29(3) of Regulation (EU) 2018/1725 are aligned. This will in particular be the case where the controller and processor rely on the standard contractual clauses included in Decision [...].

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 - Module One: Clause 8.5 (e) and Clause 8.9(b); Module Two: Clause 8.1(b), 8.9(a), (c), (d) and (e); Module Three: Clause 8.1(a), (c) and (d) and Clause 8.9(a), (c), (d), (e), (f) and (g); Module Four: Clause 8.1 (b) and Clause 8.3(b);
 - (iii) Clause 9 - Module Two: Clause 9(a), (c), (d) and (e); Module Three: Clause 9(a), (c), (d) and (e);
 - (iv) Clause 12 - Module One: Clause 12(a) and (d); Modules Two and Three: Clause 12(a), (d) and (f);
 - (v) Clause 13;
 - (vi) Clause 15.1(c), (d) and (e);
 - (vii) Clause 16(e);
 - (viii) Clause 18 - Modules One, Two and Three: Clause 18(a) and (b); Module Four: Clause 18.
- (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

Docking clause

- (a) An entity that is not a Party to these Clauses may, with the agreement of the Parties, accede to these Clauses at any time, either as a data exporter or as a data importer, by completing the Appendix and signing Annex I.A.
- (b) Once it has completed the Appendix and signed Annex I.A, the acceding entity shall become a Party to these Clauses and have the rights and obligations of a data exporter or data importer in accordance with its designation in Annex I.A.
- (c) The acceding entity shall have no rights or obligations arising under these Clauses from the period prior to becoming a Party.

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 Union² (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;

² The Agreement on the European Economic Area (EEA Agreement) provides for the extension of the European Union's internal market to the three EEA States Iceland, Liechtenstein and Norway. The Union data protection legislation, including Regulation (EU) 2016/679, is covered by the EEA Agreement and has been incorporated into Annex XI thereto. Therefore, any disclosure by the data importer to a third party located in the EEA does not qualify as an onward transfer for the purposes of these clauses.

- (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 thirty (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.³ 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

³ This requirement may be satisfied by the sub-processor acceding to these Clauses under the appropriate Module, in accordance with Clause 7.

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) 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.
- (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 safeguards⁴; 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.

- (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

⁴ As regards the impact of such laws and practices on compliance with these Clauses, different elements may be considered as part of an overall assessment. Such elements may include relevant and documented practical experience with prior instances of requests for disclosure from public authorities, or the absence of such requests, covering a sufficiently representative time-frame. This refers in particular to internal records or other documentation, drawn up on a continuous basis in accordance with due diligence and certified at senior management level, provided that this information can be lawfully shared with third parties. Where this practical experience is relied upon to conclude that the data importer will not be prevented from complying with these Clauses, it needs to be supported by other relevant, objective elements, and it is for the Parties to consider carefully whether these elements together carry sufficient weight, in terms of their reliability and representativeness, to support this conclusion. In particular, the Parties have to take into account whether their practical experience is corroborated and not contradicted by publicly available or otherwise accessible, reliable information on the existence or absence of requests within the same sector and/or the application of the law in practice, such as case law and reports by independent oversight bodies.

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 if appropriate in consultation with the controller. 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 controller or 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 **Germany** (*specify Member State*).

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 **Konstanz** (*specify Member State*).
- (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):

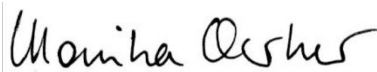
Name: **HTWG Konstanz**

Address: **Alfred-Wachtel-Str. 8, 78462 Konstanz, Germany**

Contact person's name, position and contact details: **Dr. Monika Oertner, Schreibberatung**

Activities relevant to the data transferred under these Clauses: **Schreibberatung**

Signature and date: **2.5.2024**



Role: Controller

Data importers (Turnitin group companies) that accede to these Standard Contractual Clauses in accordance with Clause 7:

Name (Primary Processor)	Address	Activities
Turnitin LLC	2101 Webster Street, Suite 1800, Oakland 94612 CA USA	Processing of data in the USA (Customer Support, Engineering)
Name (group companies)	Address	Activities
Turnitin UK Ltd	6 th Floor, Wellbar Central, 36 Gallowgate, Newcastle upon Tyne, NE1 4TD UK	Processing of data in the UK (Customer Support, Engineering)
Turnitin India Pvt. Ltd.	Suite #1603, Floor 16, Max Towers, Sector - 16B Noida, Uttar Pradesh 201301 India	Processing of data in India (Customer Support)
Turnitin Netherlands B.V.	Stadsplateau 7 3521 AZ Utrecht, Netherlands	Processing of data in the Netherlands (Customer Support)
UKU Group Ltd.	SP Hall 28-A Stepana Bandery Avenue Office 302 Kyiv, Ukraine 04073	Processing of data in Ukraine (Engineering)
ExamSoft Worldwide LLC	5001 LBJ Freeway, Suite 700, Dallas, TX 75244 USA	Processing of data in the USA (Customer Support, Engineering)

Contact person's name, position and contact details: Giles Kerrush, Data Protection Officer - 6th Floor, Wellbar Central, 36 Gallowgate, Newcastle upon Tyne, NE1 4TD UK DPO@turnitin.com

Signature and date:



Hier Text eingeben

B. DESCRIPTION OF TRANSFER

- *Categories of data subjects whose personal data is transferred:*
Students, authors, employees of academic institutions including instructors and administrators.
- *Categories of personal data transferred:*
Names, email addresses, academic ID numbers (if provided by the data exporter), academic submission content and associated online identifiers.
- *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:*
It is possible that sensitive personal data could be processed if a student submits work relating to their own sensitive personal data, but the likelihood is very remote.
- *The frequency of the transfer (e.g., whether the data is transferred on a one-off or continuous basis):*
Dependent on the use of the services by the data exporter and the frequency of their submissions, which is their choice. Generally continuous due to regular submissions during the academic year.
- *Nature of the processing:*
Collection, storage, retrieval, use (in the context of text matching functions), service and product improvement.
- *Purpose(s) of the data transfer and further processing:*
The provision of academic integrity and/or assessment software.
- *The period for which the personal data will be retained, or, if that is not possible, the criteria used to determine that period:*
Storage of the content of submissions is indefinite unless instructed otherwise by the data exporter. The data controller may at any time during or after the service period instruct the data importer(s) to delete such submissions and data.
- *For transfers to (sub-) processors, also specify subject matter, nature and duration of the processing:*
Submission content is processed by sub-processors for textual comparison purposes.

C. COMPETENT SUPERVISORY AUTHORITY

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

.....

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

1. Measures of pseudonymisation and encryption of personal data:

- All data is encrypted in flight using up-to-date HTTPS when traversing public networks;
- Encryption utilises a proprietary, one-way hash method providing pseudonymisation. Decryption keys are isolated from the encryption system.
- Encryption applies to Personal Data that is written into databases that reside in encrypted filesystems (AES-256 cipher), which are backed up continuously (files replicated in N+3 redundancy), the back-ups of which are encrypted in a separate server farm;
- Storage devices are encrypted in accordance with the US Federal Information Processing Standards (FIPS) Publication 140-2

2. Measures for ensuring ongoing confidentiality, integrity, availability and resilience of processing systems and services:

- AICPA's SOC2 certification applies to Turnitin's infrastructure. SOC 2 defines criteria for managing customer data based on five 'trust service principles': security, availability, processing integrity, confidentiality and privacy. Periodic third-party penetration testing is carried out;
- AWS Cloud Security applies to any services hosted on AWS. AWS supports more security standards and compliance certifications than any other offering, including HIPAA, FedRAMP, GDPR, FIPS 140-2, and NIST 800-171, helping Turnitin satisfy compliance requirements for its customers globally;
- SSL network security applies to all relevant domains used in the solution. Other features include intrusion detection systems, file integrity monitors; security event monitoring and sophisticated firewalls;
- Turnitin continuously monitors the US National Vulnerability Database and patches as necessary.

3. Measures for ensuring the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident:

- Databases are backed up continuously. Submissions are replicated five times: 4 on active storage and 1 copy on a back-up server.

4. Processes for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures in order to ensure the security of the processing:

- Periodic third-party penetration testing;
- Programmatic analysis of software code for open-source and proprietary vulnerabilities;
- Policies and processes that enforce segregation of duties and peer-reviews to govern production stability and security;
- Annual or semi-annual incident-response tabletop drills and disaster recovery drills;
- Continuous vulnerability monitoring by multiple third-party tools;
- Host intrusion-detection systems;
- Security, privacy, and availability processes audited by AICPA;

- Periodic internal red-team exercises;
- Weekly vulnerability-scans;
- Monthly company-wide meetings dedicated to information security processes and practices;
- Centralized logging SIEM infrastructure;
- Security response team staffed and responding at all times with tiered-response procedures and programmatic escalation and alerting infrastructure;
- Cloud security posture monitoring;
- Continuous risk aggregation and reporting systems;
- Vendor auditing and supply-chain monitoring for third-party processor security.

5. Measures for user identification and authorisation:

- Employee identity is controlled by a central team, members of which prescribe role identity to an Active Directory system;
- The employee Active Directory system acts as the programmatic source of truth, and federates various levels of authority to security providers that govern systems at varying levels of diligence dependent on the risk those systems pose if identity or credentials were compromised. These systems employ MFA and other sophisticated challenge techniques depending on risk;
- Customer identity is managed by server single-sign on partners as well as our own proprietary identity management framework.

6. Measures for the protection of data during transmission:

- All data is encrypted in transit using the technical measures described in section 1 herein.

7. Measures for the protection of data during storage:

- All data is encrypted at rest using the technical measures described in section 1 herein;
- Any student submissions stored on the AWS platform in the EU will be exclusively stored in the EU.

8. Measures for ensuring physical security of locations at which personal data are processed:

- Access to data centers is limited to staff and approved contractors who need access to perform their duties on Turnitin's behalf to benefit the Controller. Turnitin's private corporate network provides secure, encrypted, and redundant connectivity between Turnitin's offices and its data centers;
- Access to devices that contain Personal Data is restricted to specific, security-trained personnel who may only access these systems in the course of their employment. Access and privilege escalation is monitored and logged for 2 years. Remote access is only possible using cryptographic SSH keys, physical access is restricted to authorized employees via badge access - all server racks have locked cage doors with codes that are only known to Turnitin employees.
- Employee device encryption and central management.

9. Measures for ensuring events logging:

- Centralized logging infrastructure consolidates all relevant events for human and programmatic consumption and processing.

10. Measures for ensuring system configuration, including default configuration:

- Configuration management is deployed on all traditional host-based systems to idempotently define configuration standards.
- System deployment templates are used for all VM and physical infrastructure.
- Container images are designed and stored locally for consistent microservice configuration.

11. Measures for internal IT and IT security governance and management:

- Turnitin's on-call technology team provides 24/7 coverage by monitoring and alerting on any issues or problems with servers, operating systems, network devices (switches/routers) backup systems and server-side performance. Turnitin will notify its customers immediately of any changes to its environment that could adversely impact security.
- Internal governance assessments that measure the likelihood/impact of risk events that may occur within the environment;
- Annual training to measure employees' security readiness concerning protection of information assets, minimization of phishing attempts, and regulatory requirements for sharing personal data. Results from the training are assessed and action plans are developed to address gaps in training;
- Measuring the effectiveness of IT Disaster Recovery with the creation of issue categorization and response timeframes for events that occur based on level of risk severity.

12. Measures for certification/assurance of processes and products:

- Turnitin is SOC2 certified by a third-party auditor, AICPA;
- Qualys™ grades of 'A' apply to all relevant domains;
- Turnitin's infrastructure is compliant with the 'SANS Top 20' security controls as published by the Center for Internet Security Critical Security Controls for Effective Cyber Defense.

13. Measures for ensuring data minimisation:

- Turnitin only processes the data provided by the Controller, which is generally the minimum required to achieve the processing aims.

14. Measures for ensuring data quality:

- Turnitin only processes the data provided by the Controller. Data rectification is always available via Customer Support.

15. Measures for ensuring limited data retention:

- The default retention period is indefinite due to the nature of the services; however data will be deleted upon the instruction of the Controller.

16. Measures for ensuring accountability:

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

- Turnitin has implemented policies on GDPR breach notifications, data retention and data subject access requests;
- Turnitin has instigated an ongoing programme of GDPR awareness training within its organisation and receives Executive level support for data protection initiatives.

17. Measures for allowing data portability and ensuring erasure:

- All data requiring portability is supplied in commonly used, readable formats via email;
- Erasure is managed by the Customer Support and Engineering teams who have over 3 years of experience in GDPR erasure requests/actions;
- Equipment removed for off-site maintenance is sanitized of any personal data in accordance with NIST SP 800-88 Revision 1. Turnitin sanitizes or destroys media containing Personal Data in accordance with NIST SP 800-88 Revision 1 before disposal or re-use.

18. Sub-Processors

- For details of the technical and organisational measures that sub-processors utilize, refer to Annex III.

19. Additional Safeguards further to *Schrems II* applicable to transfers to the USA

19.1 Turnitin has assessed the impact of the Foreign Intelligence Surveillance Act S.702, “**FISA 702**”; Executive Order 12333, “**EO12333**”; the Clarifying Lawful Overseas Use of Data Act, “**CLOUD Act**”, and the “**PRISM**” and “**UPSTREAM**” programs on transfers of Personal Data to Turnitin in the United States. As noted below, Turnitin has determined that given the safeguards provided under the Standard Contractual Clauses and this Appendix 2, Personal Data transferred to Turnitin pursuant to the Standard Contractual Clauses is afforded an adequate level of protection under EU data protection law.

19.1A On 7 October 2022, the US passed into law an Executive Order on Enhancing Safeguards for United States Intelligence Activities, intended to address the concerns in the case of *Schrems II*. In particular, the Executive Order:

- provides that US intelligence activities shall be ‘*necessary*’ and ‘*proportionate*’ to a ‘*validated intelligence priority*’;
- defines the steps to be taken for the handling of personal data collected through signals intelligence;
- establishes a mechanism for non-US data subjects to seek review of intelligence activities; and
- creates a ‘Data Protection Review Court’ to review qualifying complaints.

19.2 **FISA 702** sets forth processes and conditions for U.S. intelligence agencies to lawfully collect from **electronic communication service providers** information relating to non-U.S. persons who are reasonably believed to be outside the United States. Turnitin is **not** an ‘electronic communications service provider’ as per 50 U.S.C. § 1881. At the time of the 2013 Edward Snowden leaks regarding the scope of FISA 702 surveillance, fewer than 10 companies were reported as receiving FISA 702 directives; all of those companies provided electronic communications services aimed at facilitating the exchange of communications between users of the services. Turnitin has no such

communications functionality and has not received a request to provide information pursuant to FISA 702. If Turnitin receives a directive pursuant to FISA 702, it shall resist and, as permitted by law, inform its data exporters in accordance with the Standard Contractual Clauses.

- 19.3 **EO12333** authorizes and governs surveillance activities by U.S. intelligence agencies. EO12333 provides no mechanism or process for the U.S. government to compel entities to assist the government in surveillance activities, therefore Turnitin is not legally required to cooperate with U.S. intelligence agencies seeking to conduct foreign intelligence surveillance pursuant to EO12333. Turnitin shall resist any requests issued pursuant to EO12333. Furthermore, EO12333 cannot compel data importers to provide decryption keys which would allow the US Government to decrypt Turnitin's encrypted data as set out in section 1 herein, and such decryption keys shall not be provided by Turnitin. EO12333 works by exploiting vulnerabilities in telecommunications infrastructure over which Turnitin data is not passed. Restrictions were placed upon the use of EO12333 in 2014 by Presidential Policy Directive 28 (PPD28).
- 19.4 **The CLOUD Act** establishes a framework via which U.S. law enforcement may obtain from U.S.-based cloud providers information stored outside the United States provided that the information is relevant to an ongoing criminal investigation. And to obtain contents of communications that have been stored for 180 days or less, U.S. law enforcement must obtain from a judge a warrant supported by probable cause. The CLOUD Act does not authorize bulk collection of information, and the Court of Justice of the European Union has never raised concerns regarding the U.S. regime for criminal investigations.
- 19.5 **PRISM and UPSTREAM:** both these programs operate under FISA 702, which we consider to be non-applicable in terms of potential access to Turnitin data.
- 19.6 Turnitin undertakes to adopt appropriate measures to protect the personal data received under the Standard Contractual Clauses from the data exporter ("**SCC Personal Data**") in accordance with the requirements of EU data protection law, including by implementing appropriate technical and organizational safeguards, such as encryption or similar technologies described in sections 2 and 3 herein to protect personal data against any interference that goes beyond what is necessary in a democratic society to safeguard national security, defence and public security.
- 19.7 In the event that Turnitin receives from a U.S. government authority a legally binding request for access to the SCC Personal Data, such as a court order, Turnitin will promptly notify the data exporter of such request to enable the data exporter to intervene and seek relief from such disclosure, unless Turnitin is otherwise prohibited from providing such notice, such as a prohibition under criminal law to preserve the confidentiality of a law enforcement investigation. If Turnitin is so prohibited:
- It will use its reasonable best efforts to obtain the right to waive this prohibition in order to communicate as much information as it can and as soon as possible, and be able to demonstrate that it did so.
 - In the event that, despite having used its reasonable best efforts, Turnitin is not permitted to notify the data exporter, it will make available on an annual basis general information on the requests it received to the data exporter and/or the competent supervisory authority of the data exporter.
 - It will work with the data exporter to oppose any such request for access.
- 19.8 In the event of a legally binding request such as a court order, for access to the SCC Personal Data by a public authority, Turnitin will:

- not make any disclosures of the SCC Personal Data to any public authority that are determined to be massive, disproportionate and indiscriminate in a manner that it would go beyond what is necessary in a democratic society; and
- upon request from the data exporter, provide general information on the requests from public authorities it received in the preceding 12-month period relating to SCC Personal Data.

19.9 On 10 July 2023 the European Commission adopted an adequacy decision (Decision C (2023) 4745) which confirmed that the European Commission viewed the US as a country with adequate safeguards for the legally valid transfer of personal data pursuant to Art.45 GDPR. Turnitin has self-certified to the new Data Privacy Framework.

ANNEX III – LIST OF SUB-PROCESSORS

The controller has authorised the use of the following sub-processors: **(Note: these are not applicable to the Gradescope service, where no sub-processors are used)**

1. Microsoft BING

- Contact: Microsoft Privacy, Microsoft Corporation, One Microsoft Way, Redmond, Washington 98052, USA. Telephone: +1 (425) 882 8080
- Processing description: The Microsoft BING functionality is a web-crawler that compares submission content against internet-based resources.
- Technical & Organisational Measures:
 - Turnitin and Microsoft are party to a data processing agreement compliant with Art.28 GDPR available at: <https://aka.ms/DPA>; Turnitin and Microsoft are party to the Standard Contractual Clauses incorporated therein;
 - Microsoft is SOC1, SOC2 and SOC3 compliant, and is ISO/IEC 22301, 27001, 27017, 27018, 27701 and 9001 certified;
 - Microsoft complies with applicable data protection laws, including applicable security breach notification laws;
 - For further information see <https://privacy.microsoft.com/en-gb/privacystatement>;
 - Microsoft is certified under the EU-US Data Privacy Framework.

2. SDL Limited (part of the RWS group)

- Contact: SDL Limited, New Globe House, Vanwall Business Park, Vanwall Road, Maidenhead SL6 4UB, United Kingdom. Attention: Data Privacy Officer Tel: +44 (0) 1628 760610 Email: privacy@sdl.com;
- Processing description: Machine translation for multi-lingual submission comparison (if this feature is present in the services provided).
- Technical & Organisational Measures:
 - Turnitin and SDL are party to a data processing agreement compliant with Art.28 GDPR; and Turnitin and SDL are party to the Standard Contractual Clauses;
 - SDL is SOC2 and SOC3 compliant, and is ISO/IEC 27001 certified;
 - For further information see <https://www.rws.com/legal/security/>

3. AWS (Amazon Web Services)

- Contact: <https://aws.amazon.com/contact-us/compliance-support/>
- Processing Description: AWS provides cloud-based storage for submissions made through the service.
- Technical & Organisational Measures: see https://aws.amazon.com/privacy/?nc1=f_pr
- AWS is certified under EU-US Data Privacy Framework.
- For compliance programs see: <https://aws.amazon.com/compliance/programs/>

