MASTER REGISTRATION AGREEMENT

This **MASTER REGISTRATION AGREEMENT** (this “**Master Registration Agreement**”, together with the Service Terms, and Order Form(s), the “**Agreement**”), is between the applicable Turnitin Contracting Party specified in Section 27 below (“**Turnitin**”, “**we**”, “**us**” or “**our**”), and the individual or legal entity licensing the Services under the Agreement and/or an applicable Order Form (“**Customer**”,“**you**”, or“**your**”) and governs your access to and use of the Services. Turnitin and Customer are each, individually, a “**Party**”, and collectively, the “**Parties**” to the Agreement. Capitalized terms used but not defined in this Master Registration Agreement have the meanings set forth in Section 28 (Definitions).

**Background**. Turnitin has developed a suite of proprietary solutions designed for educational institutions to promote academic integrity, streamline exam assessment processes, and promote originality in academic work. These solutions include advanced technology for test assessments, proctoring, scoring, and recording, as well as tools for detecting potential unoriginal content by comparing texts against resources which may include but are not limited to: (1) internet resources; (2) Turnitin’s proprietary database of texts; and (3) our proprietary Artificial Intelligence (“AI”) detector. Customer is likewise committed to upholding academic integrity and promoting original work and seeks to subscribe to select Services offered by Turnitin, subject to the terms of the Agreement.

TERMS AND CONDITIONS

# Order Forms; Payment; Taxes.

## Order Forms. You will subscribe to the applicable Service by executing an Order Form which will define: (i) the Term; and (ii) the applicable Services you have licensed from us**.** Each Order Form is governed by the Agreement. You are responsible for providing complete and accurate billing, tax, and contact information to Turnitin.

## Fees/Payment. You will pay the total amount due within thirty (30) days of receipt of an invoice. In addition to the total amount due under the invoice, payments not received within thirty (30) days may accrue a late fee (“**Late Fee**”) if specified on an applicable Order Form. Turnitin reserves the right to suspend access to the applicable Service in the event of untimely payment as outlined in section 13. We also reserve the right to pursue legal action for non-payment.

## Taxes.  Each Party will be responsible, as required under Applicable Law, for identifying and paying all taxes and other governmental fees and charges (and any penalties, interest, and other additions thereto) that are imposed on that Party upon or with respect to the transactions and payments under the Agreement. All fees payable by you are exclusive of Indirect Taxes, except where Applicable Law requires otherwise. We may charge and you will pay applicable Indirect Taxes that we are legally obligated or authorized to collect from you. You will provide such information to us as reasonably required to determine whether we are obligated to collect Indirect Taxes from you. We will not collect, and you will not pay, any Indirect Tax for which you furnish us a properly completed exemption certificate or a direct payment permit certificate for which we can claim an available exemption from such Indirect Tax. If you possess a valid exemption certificate from certain taxes, please email such certificate to us at ar@turnitin.com. All payments made by you to us under the Agreement will be made free and clear of any deduction or withholding, as required by law. If any such deduction or withholding (including cross-border withholding taxes) is required on any payment, you will pay such additional amounts as are necessary so that the net amount received by us is equal to the amount then due and payable under the Agreement. We will provide you with such tax forms as are reasonably requested in order to reduce or eliminate the amount of any withholding or deduction for taxes in respect of payments made under this Agreement.

# License Grant and Right to Use Services

During the Term of the Agreement and subject to the Customer’s compliance with the terms and conditions of the Agreement, Turnitin hereby grants to the Customer a limited, non-exclusive, revocable, non-transferable, non-assignable, non-sublicensable, non-commercial, royalty-free license. This license permits the Customer’s Authorized Users to access and use the Services purchased pursuant to the Order Form(s) solely for the Customer’s own internal purposes. This license grant is subject to the additional license terms applicable to each Service (a) in the Service Terms available at www.turnitin.com/service-terms; and (b) in the chart below:

|  |
| --- |
| 1. **– Additional Services License Terms**
 |
| **Turnitin Service** | **Additional License Terms/Restrictions** |
| **Turnitin Feedback Studio, Turnitin Feedback Studio with Originality, Turnitin Similarity, Originality, OC, OC+, and SimCheck** | The license granted for Turnitin Feedback Studio, Turnitin Feedback Studio with Originality, Turnitin Similarity, Originality, Originality Check, Originality Check +, SimCheck and any of their add-on features shall extend to Customer’s Authorized Users, but only for their use in classes offered through Institution, and does not cover partner institutions unless otherwise agreed. |
| **iThenticate Service** | The license granted for the iThenticate Service extends to Authorized Users, but only for faculty research (i.e., grant proposals, general research, and supplemental course materials) produced in connection with Customer. Customer is responsible for ensuring that its Authorized Users comply with the terms of the Agreement.  |
| **Gradescope Service** | The license granted for the Gradescope Service includes the right to access, use, reproduce, distribute, publicly perform, and display the Gradescope Service as set forth in the Agreement and the Order Form. This license extends to Authorized Users. |
| **ExamSoft Service**  | Turnitin grants to Customer during the Term a non-exclusive, non-transferable, limited right, without right of sublicense, for all Authorized Users to: (a) access, use and display the ExamSoft Services from the Site; (b) access and use the Assessment Administration Services; (c) display, manipulate, and print, where enabled, the Authorized User Data, and if applicable, the Proctoring Reports in the course of using the Services; (d) access, use, display and print the applicable User Documentation solely in connection with the Portal Access Services; and (e) if applicable, permit Authorized Users to download and/or use the examinee testing software only for the purpose of taking assessments. |

# Enforcement for Authorized Users.

You shall ensure that all your Authorized Users comply with the terms and conditions of the Agreement, including, without limitation, with your obligations set forth in Sections 4 (Acceptable Use Policy; EULA) and 9 (Restrictions; Other Obligations). You shall promptly notify Turnitin of any suspected or alleged violation of the terms and conditions of the Agreement and shall cooperate with Turnitin with respect to: (a) investigation by Turnitin of any suspected or alleged violation of the Agreement; and (b) any action by Turnitin to enforce the terms and conditions of the Agreement.

# Acceptable Use Policy; EULA.

## AUP. You agree to comply with Turnitin’s Acceptable Use Policy (“**AUP**”), which is incorporated into this Agreement by reference and sets forth the acceptable and prohibited uses of the Services. The AUP can be found at [www.turnitin.com/acceptable-use-policy](https://www.google.com/url?q=https://www.turnitin.com/acceptable-use-policy&source=gmail-imap&ust=1706563564000000&usg=AOvVaw3Uwqr426YZIOsXm2nUguiO). Turnitin reserves the right to update the AUP from time to time at its discretion. You shall ensure that your Authorized Users are aware of and comply with the AUP. In the event of any violation of the AUP by you or your Authorized Users, Turnitin may, at its sole discretion, suspend or terminate access to the Services, in addition to any other remedies available under the Agreement or at law. You shall be liable for violation of the terms and conditions of this Agreement by any of your Authorized Users.

## EULA. Authorized Users will be required to accept our EULA prior to being granted access to any Services as set forth in the Service Terms.

# Turnitin Data Usage Rights.

## Customer License for Provisions of Services. Customer grants Turnitin, its Affiliates, and its third-party vendors (a) to provide the Services in accordance with the Agreement and any applicable Order Form; (b) to a non-exclusive, royalty-free, transferable, and sublicensable license to access, use, reproduce, modify, adapt, publish, translate, create derivative works from, distribute, and display Customer Content and Authorized User Data as necessary for Turnitin (c) to create benchmarks assessing Customer and Customer-based performance and Service utilization; (d) to offer the Customer suggestions; (e) to engage in uses otherwise required by Applicable Law, such as making disclosures to law enforcement pursuant to investigations; and (f) to create Anonymized, Aggregated, and/or De-Identified Data from Customer Content. Customer shall have sole responsibility for the accuracy, quality, integrity, legality, reliability, and appropriateness of all Authorized User Data and any information Customer provides relating to any Authorized Users and for obtaining and maintaining requisite copyright or other intellectual property rights relating to any such data such that Customer can grant the rights provided in this Agreement to Turnitin.

## Customer License for Product Development. Provided that any usage by Turnitin and its Affiliates is in an Anonymized, De-Identified and/or Aggregated manner that does not identify Customer or any of its Authorized Users, Customer grants Turnitin and its Affiliates a perpetual, irrevocable, non-exclusive, royalty-free, transferable, and sublicensable license to use Customer Data, Authorized User Data, and Submissions (in whole or in part) for the purposes of developing, enhancing, or further refining Turnitin’s existing products and services and developing new products and services, including those that leverage artificial intelligence. This license is subject to Turnitin’s compliance with its confidentiality obligations under the Agreement and all Applicable Laws, including privacy laws.

## Aggregated, Anonymized, and/or De-Identified Data. Upon creation, Turnitin shall own all right, title, and interest to any Aggregated, Anonymized, and/or De-Identified Data, and Turnitin may use, disclose, reproduce, distribute, display, perform, create derivative works from, and otherwise exploit Aggregated, Anonymized, and/or De-Identified Data for any lawful purposes, including, but not limited to, improving its existing products and services, developing new products and services, and for research, marketing, and promotional purposes, provided that such use does not directly or indirectly identify Customer or any Authorized User and is not prohibited by Applicable Data Protection Laws.

## Required Consents. Customer represents and warrants that it will comply with and has provided all required notices and obtained all necessary consents and authorizations from its Authorized Users, as required by Applicable Law, to grant Turnitin the licenses set forth in this Section 5.

# Service Terms.

The Service Terms apply to specific Services and provide additional terms and conditions governing your use of those Services. These Service Terms are available at www.turnitin.com/service-terms and are incorporated herein by reference. Your access to and use of the applicable Services are subject to the relevant Service Terms, in addition to the terms and conditions of the Agreement.

# Reports and Source Database.

With respect to any Services that include reports evaluating textual sources, AI writing content and the database of source documents (“**Source Database**”), you agree (a) to maintain any Turnitin notices (including legal notices relating to Turnitin’s proprietary rights such as copyright and trademark notices) and disclaimers on the reports; (b) to exercise independent professional judgment in, and to assume sole and exclusive responsibility for, determining the actual existence of plagiarism in submitted papers, acknowledging and understanding that the reports are only tools for detecting textual similarities between compared works and/or writing likely generated by AI and do not determine conclusively the existence of plagiarism; (c) that any disclosure of a report to any third party is at the your own risk; and (d) that for papers stored in the Source Database, you authorize and instruct Turnitin to retain such papers for the purpose of using them as source material to detect unoriginal text in other papers in the future, including after the Term of the Agreement, unless your Turnitin administrator makes a written request to us to delete such papers.

# Turnitin Obligations.

Turnitin agrees to: (a) use industry standards to protect the security of accounts, passwords, and the Source Database; (b) comply with the then-current Turnitin Policies, which are incorporated herein by reference; and (c) use reasonable efforts to make reports available online for a period of one hundred and eighty (180) days after the set end date for each class, with subsequent access, as available, to be provided via request to your account representative.

# Restrictions; Other Obligations.

## Restrictions. You and your Authorized Users may use the Services solely for the purposes expressly permitted by the Agreement. Neither you nor any Authorized User shall (or shall attempt to): (a) use the Services for purposes other than your internal use; (b) reverse engineer, decompile, disassemble, modify or create works derivative of the Services; (c) assign, sublicense, rent, timeshare, loan, lease or otherwise transfer the Services, or directly or indirectly permit any third party to use or copy the Services; (d) use the Services for purposes of (i) benchmarking or competitive analysis of the Services, (ii) developing, using or providing a competing software product or service, or (iii) any other purpose that is to our detriment or commercial disadvantage; (e) probe, scan, penetrate or test the vulnerability of the Services or breach the Services’ security or authentication measures, whether actively or passively; (f) impersonate or misrepresent us, any of our employees, another user, or any other person or entity (including without limitation, by using email addresses associated with any of the foregoing); or (g) introduce any programs that contain viruses, worms, and/or Trojan horses or any other computer code, files, or programs designed to interrupt, destroy, or limit the functionality of the Services. You shall maintain the confidentiality of any passwords associated with the use of the Services in strict confidence and shall not share such passwords with any third party. For clarity, you may not share user credentials with any third-party without Turnitin’s prior written consent.

## Other Obligations. You shall be solely responsible for all use of the Services made with your passwords. Additionally, you: (a) must use the Services in accordance with Turnitin’s then-current Documentation; (b) shall not remove any proprietary notices (e.g., copyright and trademark notices) from either the Services, Documentation, content, or reports provided by Turnitin; (c) shall ensure your use of the Services complies with all Applicable Laws; (d) abide by all Turnitin Policies provided on the Turnitin Site (<https://www.turnitin.com/>); and (e) shall not (i) use the Services to store or transmit infringing, libelous, or otherwise unlawful or tortious material, or to store or transmit material in violation of third-party privacy rights, (ii) use the Services to store or transmit Malicious Code, (iii) interfere with or disrupt the integrity or performance of the Services or third-party data contained therein, or (iv) attempt to gain unauthorized access to the Services or its related systems or networks.

# Professional Services.

If an Order Form includes the provision of certain professional services (which typically include implementation, training with respect of the use of the Services, or assistance in creating Outputs (as defined below)) (“**Professional Services**”), then such services shall be provided in accordance with the Statement of Work to be attached to the Order Form (“**SOW**”). The Professional Services shall be provided remotely (and not at Customer’s site), unless otherwise agreed in writing between the Parties in the SOW. The Professional Services may be performed by a third party if mutually agreed in the SOW.

# Telecommunications and Internet Services.

You acknowledge and agree that your and your Authorized Users’ use of the Services is dependent upon access to telecommunications and Internet services. You are solely responsible for acquiring and maintaining all telecommunications and Internet services and other hardware and software required to access and use the Services, including, without limitation, any and all costs, fees, expenses, and taxes of any kind related to the foregoing. Turnitin is not responsible for any loss or corruption of data, lost communications, or any other loss or damage of any kind arising from any such telecommunications and Internet services.

# Privacy and Data Protection; Security.

## Collection/Processing of Personal Data**.** Solely to the extent necessary for Turnitin’s provision of the Services to Customer, Customer (in its capacity as Data Controller) may from time to time provide or make available access to Personal Data contained in Customer Content to Turnitin (in its capacity as a Data Processor). Turnitin’s collection, use, processing, and disclosure of Personal Data in connection with the Services will be subject to and in compliance with the Data Processing Agreement available at www.turnitin.com/dpa (“**DPA**”) and as described in its Privacy Policies available at https://help.turnitin.com/Privacy\_and\_Security/Privacy\_and\_Security.htm or <https://examsoft.com/privacy-policy> or (as may be amended and/or updated from time to time by Turnitin in its sole discretion).

## Customer’s Undertakings. Customer acknowledges and agrees that Personal Data and information may be transferred outside of the United States or any other jurisdiction where Customer, its third-party vendors, and users are located. Customer shall be solely responsible for providing all required notices, obtaining all consents, opt-ins, and authorizations, and providing and managing all opt-outs as may be required by all Applicable Data Protection Laws, for the collection, disclosure, transfer, storage and processing of Personal Data and/or Sensitive Personal Data by Turnitin according to Customer’s instructions under this Agreement. When information or data is provided by Customer, Customer shall also have the sole responsibility for accuracy, quality, integrity, reliability, appropriateness, and copyright permission.

## Security. Turnitin shall have in place—and shall comply with—documented written information security policies and procedures, periodically reviewed, covering the administrative, physical, and technical safeguards in place to protect against unauthorized access to or acquisition of Personal Data. Such policies and procedures will include encryption of data, where practicable, virus detection, and firewall utilization.

# Suspension of Access.

## In addition to any Service specific suspension rights set forth in the Service Terms, we may, in our sole discretion, also suspend your or any Authorized User’s access to the Services (i) in order to prevent damage to, or degradation of, the Services; (ii) to comply with Applicable Laws, court order, or other governmental requests; (iii) to otherwise protect us from potential legal liability; (iv) if we believe that your or any Authorized User’s use of the Services is causing immediate and ongoing financial, physical, or reputational harm to us or others (including our customers); or (v) to address a breach of any Turnitin Policy or the Agreement, including, but not limited to, failure to timely pay amounts due and payable for use of the Services. Subject to the foregoing, we shall use reasonable efforts to provide you with notice prior to or promptly following any suspension of the Services. We shall use commercially reasonable efforts to restore access to the Services as soon as it has determined that the event giving rise to suspension has been resolved unless we have elected to terminate the Agreement for breach. You agree that Turnitin will not be liable to you or to any third party for any suspension of any Service under such circumstances as described in this Section 13.

# Return of ExamSoft Data.

Upon request by Customer within ninety (90) days of the termination of an Order Form for ExamSoft Services, Turnitin shall provide access to ExamSoft Services for the sole purpose of permitting Customer to download Authorized User Data, Test Data, and Proctoring Reports using ExamSoft’s standard features and processes. After such 90-day period, Turnitin will have no obligation to maintain or provide Customer access to Authorized User Data or any other relevant data or reports and may thereafter, unless legally prohibited, delete all such data and reports in Turnitin’s Systems or otherwise in Turnitin’s possession or under its control. In the event of expiration or termination of an Order Form for ExamSoft Services, Turnitin shall not use Personal Data, Test Data, or Proctoring Reports related to those Services that have not been deleted, except as otherwise permitted by the Agreement.

# Proprietary Rights; Ownership.

## Turnitin Ownership. Subject to 15.2 (Customer/Student Ownership), Turnitin or its Affiliates, as the case may be owns (a) all rights in and to the Services, including the underlying software and technology (including all Intellectual Property Rights therein or thereto), all as may be updated, improved, modified or enhanced from time to time; (b) all trademarks, service marks, trade names and other statutory or common law intellectual property or other proprietary rights related to the Services; and (c) with the exception of Output (which is owned by Customer), all other reports and all materials created by the Services (including the format of any such reports but excluding the Personal Data of Customer or any Authorized User). With the exception of the limited license granted to Customer in Section 2 (Right to Use Services; License Grant), nothing contained in the Agreement shall be construed as granting Customer, any Authorized Users, or any other third party any right, title, or interest in or to Turnitin’s or its Affiliates’, as the case may be, Intellectual Property Rights whether expressly, by implication, estoppel, or otherwise. All rights in such items are expressly reserved to Turnitin or its Affiliates, as the case may be.

## Customer/Student Ownership: As between the Parties and subject to Sections 5.2 (Customer License for Product Development); 5.3 (Aggregated, Anonymized, and/or De-Identified Data); and 15.3 (Feedback), (a) Customer owns the Authorized User Data, Test Data, and Proctoring Data and acts as the Controller for any Personal Data contained therein; and (b) Students own the Submissions.

## Feedback.All right, title and interest in the Services and any other Turnitin materials furnished or made available hereunder, and all modifications and enhancements thereof, and all suggestions, ideas and feedback proposed by Customer regarding Turnitin, LLC, its Affiliates, or the Services, including all copyright rights, patent rights and other intellectual property rights in each of the foregoing, belong to and are retained solely by Turnitin, LLC, or its Affiliates, as the case may be. Customer hereby does and will irrevocably assign to Turnitin all evaluations, ideas, feedback and suggestions made by Customer to Turnitin regarding the Services (collectively, “**Feedback**”) and all Intellectual Property Rights in the Feedback.

# FERPA.

To the extent Customer or Customer Content is subject to the Family Educational Rights and Privacy Act (“**FERPA**”), Customer designates Turnitin a “school official” within the meaning of FERPA 34 CFR Section 99.31. Turnitin will remain under the direction of Customer with respect to the use and maintenance of personally identifiable information and education records, as those terms are defined in FERPA 34 CFR Section 99.3, and Turnitin may use personally identifiable information and education records only as set forth under the Agreement and in compliance with Applicable Law.

# Insurance.

Turnitin will maintain the current applicable commercial general liability and cyber liability insurance limits as presented in any certificates of insurance (evidence of coverage only) (“**Turnitin COIs**”) provided to you, and will ensure that such coverage extends to Turnitin, with the limits therein not materially decreasing during the Term. Upon your written request during the Term, we will provide you with the then-current Turnitin COIs.

# Support.

We will provide reasonable email and phone support to you via your sole appointed primary account administrator during our normal support hours.

# Term and Termination

## Term.

### Term for Non-Governmental Customers. With the exception of any customers who are governmental entities (which are governed by Section 19.1.2), the initial term of the Agreement (“**Initial Term**”) commences on the start date specified in the Order Form and continues until terminated in accordance with this Section 19.1.1 or as otherwise set forth in the Agreement. If the Initial Term is not perpetual, the Agreement remains in effect for the duration set forth in the Order Form. Following the Initial Term, the Agreement automatically renews for successive one (1) year periods (each, a “**Renewal Term”**, and collectively with the Initial Term, the “**Term**”) unless either Party provides the other Party with written notice of termination at least ninety (90) days prior to the end of the then-current Term. Each Renewal Term shall incorporate and is subject to our then-current pricing. Your administrator will receive reminders regarding renewal requirements when logging into the Services before the Term expires.

### Term for Governmental Customers. This section applies only to customers who are governmental customers or state institutions. For any governmental customers or state institutions, the Initial Term will be as specified in the Order Form; however, the automatic renewal of the Agreement for each Renewal Term is contingent upon the continued need and the availability of adequate appropriations from the relevant government authority. If any of these conditions are not met, the governmental customer or state institution may terminate the Agreement without penalty by providing written notice to us at least ninety (90) days prior to the end of the then-current Term. For clarity, termination is strictly tied to the appropriations from the state and not any budgetary changes made by the governmental customer or state institution. Each Renewal Term shall incorporate and is subject to our then-current pricing.

## Termination.

### Turnitin Immediate Right of Termination. Turnitin shall have the right to immediately terminate the Agreement or any Order Form(s) by giving written notice to Customer if Customer or any of its Authorized Users does or attempts to do any of the following: (a) decodes, decompiles, reverse engineers, merges, modifies, translates, attempts to defeat or disable the Services, or otherwise alters the Services in any form; (b) reproduces, duplicates or copies Services or creates derivative works based on Services, transfers, resells or grants any other rights of any kind for any copy of Services; (c) uses the Services for purposes of: (i) benchmarking or competitive analysis of the Services; (ii) developing, using or providing a competing software product or service; or (iii) any other purpose that is to Turnitin’s detriment or commercial disadvantage; (iv) probes, scans, penetrates or tests the vulnerability of the Services or breaches the Services’ security or authentication measures, whether actively or passively; (v) impersonates or misrepresents Turnitin, any Turnitin personnel, another user, or any other person or entity (including without limitation, by using email addresses associated with any of the foregoing); (vi) introduces any Malicious Code or other programs designed to interrupt, destroy, or limit the functionality of the Services; (vii) fails, within thirty (30) days, after receipt of written notice from Turnitin, to immediately discontinue the distribution or use of software or Services that infringe any copyright of Turnitin; or (viii) Uses the Services in any manner that breaches the terms of the Agreement or fails to follow the operating instructions provided by Turnitin; or (ix) fails, within thirty (30) days, after receipt of written notice from Turnitin, to pay any fees due and payable pursuant to the Agreement; or (x) if Customer becomes or is declared insolvent or bankrupt, is the subject of any proceedings relating to its liquidation, insolvency, or for the appointment of a receiver or similar officer for it, or makes an assignment for the benefit of any creditors.

### Mutual Termination for Material Breaches. If either Party is in material breach of the Agreement and fails to cure such breach within thirty (30) days after written notice thereof, the non-breaching Party may terminate the Agreement by subsequent written notice to the breaching Party. Notwithstanding the foregoing, if Turnitin is terminating the Agreement due to Customer’s failure to pay any amounts due, Turnitin may terminate the Agreement if Customer has not cured the breach within (5) business days after receipt of notice of the breach from Turnitin.

### Termination Due to Third Party Service Providers. In the event our ability to provide the Services is dependent upon a third-party provider of services, either used by you or us (in each case, “**Third-Party Services**”), and that third-party is unwilling or unable to provide the Third Party Services, we reserve the right to terminate that particular Service by written notification to you (which notification, notwithstanding 26.8 (Notice) may be delivered by telephone or electronic communication), or suspend the affected Service until such time as the third-party service provider becomes capable or willing to provide the Third-Party Services.

### Rights and Obligations Upon Termination. Upon expiration or termination of the Agreement, subject to Section 19.2.5 (Use of ExamSoft Beyond Expiration) and Section 19.2.6 (Survival), Customer’s and its Authorized Users’ right to access and use the Services shall immediately terminate, Customer and its Authorized Users shall immediately cease all use of the Services, and each Party shall return or destroy and make no further use of the other Party’s Confidential Information, materials, or other items (and all copies thereof).

### No Refunds. Except as provided in Section 1.10 of the Service Terms, and Sections 12 (Privacy and Data Protection; Security) and 26.12 (Modifications to Turnitin Policies) herein, no Order Form from Customer may be canceled or terminated by Customer, and in no other termination event shall Customer be owed a refund of prepaid fees. For clarity, Customer may not cancel or terminate any fees owed under the Agreement or any Order Form for its convenience, whether payment terms require Customer to make a single payment in full or multiple payments during the Term.

### Use of ExamSoft Beyond Expiration Date. In the event the Parties have not renewed the ExamSoft Services beyond the then-current Term, but Customer desires to continue to use the ExamSoft Services, Turnitin reserves the right to permit Customer to continue to access and use the ExamSoft services pursuant to Section 14; provided however, the fees applicable to Customer’s usage for the ExamSoft Services shall automatically increase by 20% during any such post-expiration usage period.

### Survival. Sections 5 (Turnitin Data Usage Rights); 7 (Reports and Source Database); 15 (Proprietary Rights; Ownership); 19.2.4 (Rights and Obligations upon Termination) through 19.2.7 (Survival); and 20 (Confidentiality) shall survive any expiration or termination of the Agreement, regardless of the reason for such termination, and shall continue in full force and effect thereafter.

# Confidentiality.

## Customer’s Use of Turnitin’s Confidential Information**.** Customer may (a) use Turnitin’s Confidential Information only in connection with Customer’s use of the Services as expressly permitted by the Agreement; and (b) use the Turnitin Content solely as expressly permitted under the Agreement.

## Turnitin’s Use of Customer’s Confidential Information. To the extent Customer submits Confidential Information to the Service(s), Turnitin may use Customer’s Confidential Information only as necessary to perform the Services in accordance with the Agreement and as otherwise expressly permitted by the Agreement.

## Mutual Confidentiality Obligations. Each Party will take all reasonable measures to prevent the disclosure, dissemination, or unauthorized use of the other Party’s Confidential Information, including, at a minimum, those measures they take to protect their own confidential information of a similar nature. The receiving Party’s obligations under this Section shall not apply to information that: (a) is or becomes publicly available without breach of this Agreement; (b) is lawfully obtained from a third party without a duty of confidentiality; (c) is independently developed by the receiving Party without reference to the disclosing Party’s Confidential Information; or (d) is required to be disclosed by law, regulation, or court order, provided that the receiving Party gives the disclosing Party prompt written notice of such requirement and reasonably cooperates with the disclosing Party’s efforts to contest or limit the scope of the required disclosure. Each Party’s obligations related to the other Party’s Confidential Information (except for trade secrets) shall survive for five (5) years following the expiration or termination of the Agreement. For any Confidential Information that constitutes a trade secret under Applicable Law, the receiving Party’s confidentiality obligations shall survive for as long as such information remains a trade secret under Applicable Law.

# Warranty and Disclaimer.

## Warranty. Service Specific warranties (when and if applicable) are set forth in the Service Terms. In addition, during the Term, Turnitin warrants that (a) to the best of its knowledge, the Services (excluding any Customer Content and Third-Party Content) do not infringe the Intellectual Property Rights of any third party; and (b) it shall use reasonable efforts to provide the Services and support as set forth herein and as described on the Site and published Documentation. If the Services are found to be defective or not in compliance with the warranties set forth in this Section 21, Turnitin’s sole obligation, and Customer’s exclusive remedy, shall be for Turnitin to use commercially reasonable efforts to repair or replace (at Turnitin’s option) the defective Services at no additional cost to Customer unless exclusive remedy is specified in Service Terms. Customer acknowledges that the Services are limited in scope by a finite database of material for comparison, a search process that might not have indexed the material used to create the submitted work, and non-access to certain proprietary databases of written work. Customer also acknowledges that reports indicate the possibility of textual matches only, and the actual determination of plagiarism is subject to Customer’s professional judgment.

## Warranty Disclaimer. EXCEPT AS SET FORTH IN SECTION 21.1 ABOVE, THE SERVICES (INCLUDING THE REPORTS) ARE PROVIDED ON AN “AS IS” AND “AS AVAILABLE” BASIS. TURNITIN SPECIFICALLY DISCLAIMS ALL WARRANTIES OF ANY KIND, WHETHER EXPRESS, IMPLIED OR STATUTORY, INCLUDING BUT NOT LIMITED TO ANY WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, QUIET ENJOYMENT, QUALITY OF INFORMATION, NON-INFRINGEMENT AND TITLE. NO WARRANTY IS MADE THAT THE SERVICES WILL BE TIMELY, SECURE OR ERROR-FREE. IN JURISDICTIONS NOT ALLOWING THE LIMITATION OR EXCLUSION OF CERTAIN WARRANTIES, TURNITIN’S WARRANTY SHALL BE LIMITED TO THE GREATEST EXTENT PERMITTED BY APPLICABLE LAW.

## Risks Associated with Internet Use. THE SERVICES ARE ACCESSED AND USED OVER THE INTERNET. CUSTOMER ACKNOWLEDGES AND AGREES THAT TURNITIN DOES NOT OPERATE OR CONTROL THE INTERNET AND THAT VARIOUS RISKS ARE ASSOCIATED WITH ITS USE, INCLUDING BUT NOT LIMITED TO: (I) THE POTENTIAL FOR MALICIOUS CODE AND OTHER VIRUSES, WORMS, OR OTHER UNDESIRABLE DATA OR SOFTWARE; AND (II) THE POSSIBILITY OF UNAUTHORIZED USERS (E.G., HACKERS) ATTEMPTING TO OBTAIN ACCESS TO OR CAUSE DAMAGE TO CUSTOMER’S DATA, COMPUTERS, OR NETWORKS. TURNITIN SHALL NOT BE RESPONSIBLE FOR ANY SUCH ACTIVITIES OR CONSEQUENCES RESULTING FROM THE USE OF THE INTERNET IN CONNECTION WITH THE SERVICES.

# Limitation of Liability.

## WAIVER OF DAMAGES. EXCEPT FOR CLAIMS RELATING TO TURNITIN’S GROSS NEGLIGENCE OR WILLFUL MISCONDUCT (THE “**EXCLUDED CLAIMS**”), NEITHER TURNITIN, ITS AFFILIATES, NOR LICENSORS WILL BE LIABLE FOR ANY INDIRECT, SPECIAL, INCIDENTAL, CONSEQUENTIAL, EXEMPLARY OR PUNITIVE DAMAGES (INCLUDING, BUT NOT LIMITED TO, LOSS OF PROFITS, REVENUES, CUSTOMERS, OPPORTUNITIES, GOODWILL, USE, OR DATA), EVEN IF TURNITIN HAS BEEN ADVISED AS TO THE POSSIBILITY OF SUCH DAMAGES.

## NO LIABILITY FOR CERTAIN CLAIMS. EXCEPT FOR (A) THE EXCLUDED CLAIMS; (B) OR IN CASE OF BREACH OF SECTION 20.2 (TURNITIN’S USE OF CUSTOMER’S CONFIDENTIAL INFORMATION) OR 20.3 (MUTUAL CONFIDENTIALITY OBLIGATIONS), OR (C) TURNITIN’S OBLIGATION TO INDEMNIFY CUSTOMER UNDER SECTION 23.2, AND REGARDLESS OF THE TYPE OF CLAIM OR THE NATURE OF THE CAUSE OF ACTION, TO THE EXTENT ALLOWED BY APPLICABLE LAW, CUSTOMER AGREES THAT IN NO EVENT WILL TURNITIN OR ITS AFFILIATES, OFFICERS, EMPLOYEES, AGENTS OR LICENSORS, BE LIABLE FOR: (I) ANY DECISION MADE OR ACTION TAKEN OR NOT TAKEN IN RELIANCE UPON ANY INFORMATION AND/OR OUTPUT OR OTHER REPORTS PROVIDED OR OTHERWISE ACCESSED IN CONNECTION WITH THE SERVICES; OR (II) FOR ANY LIABILITY ARISING FROM CUSTOMER’S DISCLOSURE OF ANY SUCH REPORTS OR OUTPUT TO ANY THIRD PARTY.

## LIABILITY CAP. EXCEPT FOR (A) THE EXCLUDED CLAIMS; (B) IN CASE OF BREACH OF SECTION 20.2 (TURNITIN’S USE OF CUSTOMER’S CONFIDENTIAL INFORMATION) OR 20.3 (MUTUAL CONFIDENTIALITY OBLIGATIONS); OR (C) TURNITIN’S OBLIGATION TO INDEMNIFY CUSTOMER UNDER SECTION 23.2 (INDEMNIFICATION BY TURNITIN), AND TO THE EXTENT ALLOWED BY APPLICABLE LAW, TURNITIN AND ITS AFFILIATES, OFFICERS, EMPLOYEES, AGENTS OR LICENSORS’ TOTAL CUMULATIVE LIABILITY ARISING UNDER OR RELATED TO THIS AGREEMENT AND THE SERVICES, WHETHER IN CONTRACT, TORT OR OTHERWISE, WILL NOT EXCEED THEGREATER OF THE AMOUNTS PAID TO TURNITIN BY CUSTOMER UNDER THE AGREEMENT DURING THE TWELVE (12) MONTHS IMMEDIATELY PRECEDING THE EVENT GIVING RISE TO THE LIABILITY*,* OR $25,000. SOME JURISDICTIONS DO NOT ALLOW THE LIMITATION OR EXCLUSION OF LIABILITY FOR INCIDENTAL OR CONSEQUENTIAL DAMAGES. IN THOSE JURISDICTIONS, TURNITIN’S LIABILITY UNDER THE AGREEMENT SHALL BE LIMITED TO THE GREATEST EXTENT PERMITTED BY APPLICABLE LAW. THE LIMITATION OF LIABILITY AND LIABILITY CAP SHALL APPLY EVEN IF THE EXPRESS WARRANTIES SET FORTH ABOVE FAIL THEIR ESSENTIAL PURPOSE.

## Third-Party Products. In connection with the Services, Turnitin may make available to Authorized Users or Customer or may separately license certain third-party products (collectively, the “**Third-Party Products**”). Except as otherwise provided in the third-party licensor’s license agreement, if any, accompanying the Third-Party Products, Customer shall have a limited, non-transferable (except to a successor entity), non-exclusive license to use the Third-Party Products solely in connection with the Services.

## EXCEPT AS OTHERWISE PROVIDED IN THE THIRD-PARTY LICENSOR’S LICENSE AGREEMENT, IF ANY, ACCOMPANYING THE THIRD-PARTY PRODUCTS, THE THIRD-PARTY PRODUCTS ARE PROVIDED “AS-IS”, WITHOUT WARRANTIES OF ANY KIND AND TURNITIN AND THE THIRD-PARTY LICENSOR DISCLAIM ALL WARRANTIES WITH RESPECT TO THE THIRD-PARTY PRODUCTS, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, TITLE, MERCHANTABILITY, AND FITNESS FOR A PARTICULAR PURPOSE. IN NO EVENT WILL TURNITIN OR ANY THIRD-PARTY LICENSOR BE LIABLE TO INSTITUTION, INSTRUCTORS, STUDENTS, OR ANY THIRD-PARTY FOR ANY DIRECT, INDIRECT, PUNITIVE, EXEMPLARY, INCIDENTAL, SPECIAL, OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE THIRD-PARTY PRODUCTS, EVEN IF THEY HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES OR LOSSES.

# Indemnification.

## Indemnification by Customer. To the extent allowed by Applicable Law, Customer shall indemnify, defend, and hold harmless Turnitin, its Affiliates, officers, directors, employees, agents, and licensors (collectively, “**Turnitin Indemnified Parties**”) from any and all claims, losses, damages, liabilities, settlements, and expenses (including but not limited to reasonable attorneys’ fees and all related costs) (collectively, “**Losses**”) incurred by Turnitin Indemnified Parties as a result of any claim, lawsuit, demand, cause of action, or proceeding brought by a third party relating to or arising from: (a) Customer’s or any Authorized User’s breach of its restrictions or obligations under the Agreement; or (b) Customer’s decision not to follow Turnitin’s strong recommendations set forth in Section 2 (Turnitin Feedback Studio/Similarity/SimCheck Services) of the Service Terms available at www.turnitin.com/service-terms.

## Indemnification by Turnitin. To the extent allowed by Applicable Law, Turnitin shall indemnify, defend, and hold harmless Customer and its affiliates, officers, directors, employees, agents, and licensors (collectively, “**Customer Indemnified Parties**”) from Losses incurred by Customer’s Indemnified Parties as a result of any claim, lawsuit, demand, cause of action, or proceeding brought by a third party alleging that (i) Customer’s licensed use of the Services, as permitted hereunder, infringes the U.S. patent or copyrights of that third party, or; (ii) Turnitin has violated any state or federal privacy law relating to information provided by Customer hereunder. Turnitin shall have no obligation to indemnify Customer under this Section to the extent the infringement claim arises from (i) any content or other intellectual property provided by Customer or any other third party, including third party content contained in the Source Database; (ii) Customer’s failure to use the Services in accordance with the Agreement; or (iii) any matter for which Customer is obligated to indemnify Turnitin hereunder.

## Indemnification Procedures. To qualify for the foregoing indemnity obligation, the Party seeking indemnity must: (i) give the indemnify Party prompt written notice of any Claim; and (ii) allow the indemnifying Party to control, and fully cooperate with the indemnifying Party in, the defense and all related negotiations.

## Governing Law and Dispute Resolution. The Agreement is governed by Applicable Law in accordance with Section 27 (Contracting Party; Applicable Law), and unless otherwise set forth in an Order Form, the Parties consent to the exclusive personal jurisdiction of the applicable jurisdiction detailed in Section 27 (Contracting Party; Applicable Law).

# Accessibility.

While the parties agree the standards are evolving under the law, Turnitin Services target compliance with Web Content Accessibility Guidelines 2.0 (with the exception of ExamSoft, which conforms with version 2.1), Level AA. Areas of non-conformance, and Voluntary Product Accessibility Templates, are available on the Turnitin website. If a Student user of the Services raises a complaint regarding the accessibility of the Services to accessibility@turnitin.com , Turnitin shall use commercially reasonable efforts to resolve such complaint at no additional cost to the Customer. If Turnitin is unable to provide a satisfactory resolution, Customer’s sole remedy and Turnitin’s sole liability shall be for Customer to terminate the Agreement with thirty (30) days’ written notice to Turnitin. In such case, Customer shall receive a refund of prepaid fees, prorated to the date of termination.

## Other Provisions. Except as provided herein, all amendments or modifications to the Agreement must be agreed by an authorized signatory of each Party. A Party’s failure to insist upon or enforce strict performance of any provision of the Agreement shall not be construed as a waiver of any provision or right.

## Third-Party Beneficiaries. Except as set forth in Section 23 (Indemnification), the Agreement does not create any third-party beneficiary rights in any individual or entity that is not a party to the Agreement.

## Changes to Services. Turnitin reserves the right, in its sole discretion, to make any changes to the features and functionalities of the Services that it deems necessary or useful to: (a) maintain or enhance: (i) the quality or delivery of Services to its customers, (ii) the competitive strength of or market for Turnitin’s services; (iii) the Services’ cost efficiency or performance; (b) to comply with Applicable Laws; or (c) as otherwise determined by Turnitin as commercially necessary.

## Equitable Relief. Each Party acknowledges that a breach by the other Party of any confidentiality or proprietary rights provision of the Agreement may cause the non-breaching Party irreparable damage, for which the award of damages would not be adequate compensation. Consequently, the non-breaching Party may institute an action to enjoin the breaching Party from any and all acts in violation of those provisions, which remedy shall be cumulative and not exclusive, and a Party may seek the entry of an injunction enjoining any breach or threatened breach of those provisions, in addition to any other relief to which the non-breaching Party may be entitled at law or in equity.

# Representations and Warranties.

Each Party represents and warrants to the other Party that: (a) it has full power and authority to enter into and perform the Agreement, (b) the execution and delivery of the Agreement has been duly authorized, and (c) entering into the Agreement does not violate any Applicable Law.

# Miscellaneous

## Controlling Documents. Except as otherwise provided herein, in the event of any conflict between the terms of the Agreement and the terms of any subsequent agreement, including, without limitation, any Turnitin Policies, SOWs or other documents, the terms of the Agreement will control, unless the Parties expressly agree in any applicable Order Form or SOW that such Order Form or SOW should control.

## Severability. If any provision of the Agreement is held by a court of competent jurisdiction to be illegal, invalid or unenforceable, the remaining provisions will remain in full force and effect and the offending provision shall be modified by the minimum extent required to render the provision enforceable.

## Waiver. The waiver from time to time by a Party of any of their rights or their failure to exercise any remedy will not operate or be construed as a continuing waiver of the same or of any other of such Party’s rights or remedies provided in the Agreement.

## Relationship of the Parties. The Parties are operating as independent contractors, and nothing in the Agreement will be construed as creating a partnership, franchise, joint venture, employer-employee, or agency relationship between the Parties. Neither Party will have the power to bind the other or to incur obligations on the other’s behalf without such other Party’s prior written consent.

## Language. All communications and notices made or given pursuant to the Agreement must be in the English language. If we provide a translation of the English language version of the Agreement, the English language version of the Agreement will control if there is any conflict.

## Assignment. Except as expressly provided in the Agreement, neither the Agreement nor any obligations under it may be assigned or delegated by either party without the prior written consent of the other party, except that Turnitin may assign the Agreement, in whole or in part, without consent to (a) any Affiliate or subsidiary of Turnitin; (b) an acquirer of all or substantially all of the assets or equity of Turnitin; or (c) a successor by merger. Any change of control of Customer is considered an assignment for the purposes of this Section.

## Headings. Headings in the Agreement are provided for the convenience of the parties only and will have no substantive effect.

## Notice. Any notice, authorization, designation, request or instruction under or in connection with the Agreement, to be effective, will be in writing and will be deemed duly given or served upon delivery, addressed, if to Turnitin, to contracts@turnitin.com; and if to Customer, to the email address as set forth in the applicable invoice. Either Party may notify the other in the foregoing manner of any other address to which such communications are to be addressed under the Agreement.

## Force Majeure. Neither Party will be liable for any loss, damage, delay or failure of performance resulting directly or indirectly from any cause which is beyond its reasonable control, including but not limited to acts of God, riots, pandemics (but excluding COVID-19), civil disturbances, wars, states of belligerency or acts of the public enemy (a “**Force Majeure Event**”). If any Force Majeure Event occurs, the Party delayed or unable to perform will give immediate notice to the other Party, and, if the delay continues for more than thirty (30) days, the Party affected by the other’s delay or inability to perform may elect to: (i) terminate the Agreement or the applicable Order Form, (ii) suspend the Agreement or the applicable Order Form for the duration of the Force Majeure Event, or (iii) resume performance of the Agreement or the applicable Order Form once the Force Majeure Event ceases with an option for the affected Party to extend the period of the Agreement or the applicable Order Form up to the length of time of the Force Majeure Event. As to any other delay, time is of the essence as to performance under the Agreement.

## Publicity. Except as set forth below, neither Party will use the name of the other Party in any news release, public announcement, advertisement or other form of publicity without securing the prior written consent of the other. Notwithstanding the foregoing, Turnitin may use and reference Customer’s name as a subscriber to the Services in connection with truthful advertising or promotion of the Services.

## Remedies Cumulative. Except as limited under the Agreement, the rights and remedies afforded to each Party under the Agreement are in addition to any other rights or remedies, at law or in equity or otherwise.

## Modifications to Turnitin Policies. Turnitin may modify any Turnitin Policies at any time by posting a revised version on the Site or by otherwise notifying you in accordance with Section 26.8 (Notice). The modified terms will become effective upon posting or, if you are notified pursuant to Section 26.8 (Notice), within thirty (30) days after your receipt of the notice. By continuing to use the Services or Turnitin Content after the effective date of any such modifications, you agree to be bound by the modified terms. It is your responsibility to check the Site regularly for modifications to the Turnitin Policies. In the event that you do not agree to the revised Turnitin Policies, you may terminate the Agreement by giving thirty (30) days written notice, and we will refund you the pro-rated amount of any prepaid annual subscription fees, calculated from the date of such termination. Continued use of the Services shall constitute your acceptance of revisions to the Turnitin Policies.

## Complete Agreement. The Agreement and all exhibits therein (including any other terms incorporated by reference) contain the entire agreement of the parties and supersedes any and all prior agreements, understandings and communications between Turnitin and Customer with respect to the subject matter of the Agreement. Except as set forth in this Section 26.13 (Complete Agreement), no amendment, modification or supplement of any provision of the Agreement will be valid or effective unless made in writing and signed by a duly authorized officer of Turnitin and Customer.

## Non-Exclusive Remedies. Except as set forth in Section 23.2 (Indemnification by Turnitin) and the exercise by either Party of any remedy under the Agreement will be without prejudice to its other remedies under the Agreement or otherwise.

## Counterparts. The Agreement may be executed in counterparts, each of which shall be deemed an original, but all of which together shall be deemed to be one and the same agreement. A signed copy of the Agreement delivered by e-mail or other means of electronic transmission shall be deemed to have the same legal effect as delivery of an original signed copy of the Agreement.

## Battle of Forms.  Customers purchase, license, and use of Services shall be solely governed by the terms and conditions of the Agreement. Any terms or conditions introduced by Customer either directly, indirectly by way of reference or otherwise are hereby explicitly rejected and shall not apply. The Parties agree that any additional or differing terms or conditions in any other document or arrangement not forming part of the Agreement, including but not limited to any letter or terms of engagement or the like, purchase order, invoice, acknowledgment, delivery receipt, confirmation or other delivery or acceptance document issued by or on behalf of Customer shall be void, and of no force or effect to the extent such are in breach of or contradiction with the Agreement.

# Contracting Party; Applicable Law.

|  |
| --- |
| **Turnitin Products** |
| **Account Country** | **Turnitin Contracting Party** | **Turnitin Contracting Party Address** | **Applicable Law / Applicable Jurisdiction** |
| Indonesia | PT Turnitin Education Indonesia | Level 38 Tower A 88 Office Tower,Kota Kasablanka, Jl. Casablanca Raya Kav. 88Kel, Menteng Dalam Jakarta Kec.TebetKota Adm. 12870Indonesia | Indonesia |
| Japan | Turnitin Japan, LLC  | Link Square Shinjuku 16F,5 Chome 27-5 Sendagaya,Shibuya-ku Tokyo 151-0051 Japan | Japan / Singapore (SIAC) |
| All LATAM Countries | Turnitin Mexico S. de R.L. de C.V  | Avenida Vasconcelos 755 Pte. ED Plaza Avanta, 3rd floor, interior A, Col. Del Valle, C.P. 66220, San Pedro Garza García, Nuevo León, 66220, Mexico | Mexico / Mexico City |
| India, Bangladesh, Nepal, Bhutan, Sri Lanka, Maldives | Turnitin India Pvt Ltd | Suite #1603, Floor 16, Max Towers, Sector - 16BNoida, Uttar Pradesh 201301 India | India / Delhi |
| Any other country that is not listed in the table above  | Turnitin, LLC | 2101 Webster St., Ste 1900 Oakland, CA 94612 USA | New York, NY |
| **ExamSoft Products** |
| **Account Country** | **Turnitin Contracting Party** | **Turnitin Contracting Party Address** | **Applicable Law / Applicable Jurisdiction** |
| UK | Liftupp Ltd | Liftupp Ltd.6th floor, Wellbar Central36 GallowgateNewcastle Upon Tyne NE1 4TDUnited Kingdom | United Kingdom |
| India | Turnitin India Pvt Ltd | Suite #1603, Floor 16, Max Towers, Sector - 16BNoida, Uttar Pradesh 201301 India | India / Delhi |
| All other country that is not listed in the table above | Examsoft Worldwide LLC | 2101 Webster St., Ste 1900 Oakland, CA 94612 USA | New York, NY |

# Definitions.

In addition to other terms defined elsewhere in the Agreement, the following terms, when capitalized, will have the following meanings:

“Account Country” is the country associated with Customer’s Services account based on Customer’s billing address on the Order Form, for the purposes of the table in Section 27.

“Affiliate” means a legal entity that directly or indirectly owns, controls, is owned by or is under common ownership or control with a Party.

“Aggregated Data” or “Aggregated” means information that relates to a group or category of Data Subjects, from whom individual Data Subject identities have been removed, that is not linked or reasonably linkable to any Data Subject.

“Anonymized Data” or “Anonymized” means information that does not relate to an identified or identifiable natural person or Personal Data rendered anonymous in such a manner that the Data Subject is not or no longer identifiable.

“Applicable Laws” means all federal, state, local, international and foreign laws, rules, regulations, directives, orders and ordinances of the jurisdiction in the table listed in Section 27.

“Applicable Data Protection Laws” means all worldwide data protection and privacy laws and regulations applicable to the personal data in question, including, where applicable, (i) General Data Protection Regulation 2016/679 (“GDPR”); (ii) Directive 2002/58/EC; (iii) any applicable national implementations of (i) and (ii); (iii) in respect of the United Kingdom, any applicable national legislation that replaces or converts in domestic law the GDPR or any other law relating to data and privacy as a consequence of the United Kingdom leaving the European Union; and (iv) California Consumer Privacy Act of 2018 (California Civil Code §§ 1798.100–1798.199) (“CCPA”); in each case, as may be amended, superseded or replaced.

“Assessment Administration” means assessment administration, including but not limited to authoring, proctoring, scoring, and recording of assessments using the ExamSoft Services.

“Authorized User(s)” means any individual or entity to whom Customer has granted access and use of the Services, in accordance with the terms of this Agreement, this includes, but is not limited to, administrators, Instructors, Students, investigators, publishers, and researchers.

“Authorized User Data” means information that the Authorized User inputs into the Services, including without limitation, Personal Data, written text or materials, assessment questions, answers, and other assessment content.

“Authorized User Documentation” means the written instructions and specifications, user manuals, user guides, technical manuals, release notes, and online help files regarding use of the Services, and any other materials prepared in connection with any Service, correction, or enhancement, and shall include any updated versions as may be provided by ExamSoft from time to time (a) in the course of providing the Services; or (b) as part of any online tutorials or help files provided with the Services.

“Authorized User Portal” means a webpage(s) on the Site that Customer makes available to particular Authorized Users to access and use the Portal Services.

“Confidential Information” means all non-public information, data, or materials of a confidential or proprietary nature of a party including, without limitation, any trade secrets, functional and technical specifications, SOC 2 reports, HECVAT information, designs, drawings, analysis, research, processes, computer programs, algorithms, methods, “know how” and other technical information, sales and marketing research, materials, plans, and other business information, accounting and financial information, personnel records, information concerning the products, services and business of a party and any other information: (a) that the disclosing party marks as confidential or proprietary; or (b) that due to its character or nature, a reasonable person in a like position and under like circumstances would treat as confidential. Confidential Information does not include information that (a) is or becomes publicly available without breach of the Agreement by a Party; (b) was rightfully in a Party’s possession without any confidentiality obligations prior to its disclosure by the other Party; (c) is received by a Party from a third party without breach of any obligation of confidentiality; or (d) is independently developed by a Party without reference to or use of the other Party’s Confidential Information.

“Control” (including the term “controlled by”) means the possession, directly or indirectly, of the power to direct or cause the direction of the management and policies of a person, whether through the ownership of voting securities, by contract or otherwise.

“Controller” means the Party, which alone or jointly with others, determines the purposes and means of processing of Personal Data.

“Customer Content” means any and all data, information, materials, and content provided or submitted by Customer, or on the Customer’s behalf, to Turnitin in connection with the Services, including but not limited to Authorized User Data, Submissions, Output, and any other content related to the Customer’s use of the Services.

“Data Subject” means any identified or identifiable natural person.

“De-Identified Data” or “De-Identified” means information that cannot reasonably be used to infer information about, or otherwise be linked to, a particular consumer provided that the business that possess the information: (a) takes reasonable measures to ensure that the information cannot be associated with a Data Subject; and (b) publicly commits to maintain and use the information in deidentified form and not to attempt to reidentify the information, except that the business may attempt to reidentify the information solely for the purpose of determining whether its deidentified processes satisfy the requirements of Applicable Data Protection Laws.

“Documentation” means the electronic documentation for technical and use requirements for any Service available through the Site.

“Effective Date” means the date identified as such in the applicable Order Form.

“End User License Agreement” or “EULA” means the agreement between Authorized Users and Turnitin or its Affiliates that outlines the terms and conditions of Authorized Users’ access to and use of the software and associated Services.

“Force Majeure Event” has the meaning given to it in Section 26.9.

“Indirect Taxes” means applicable taxes and duties, including, without limitation, VAT, service tax, GST, excise taxes, sales and transactions taxes, and gross receipts tax.

“Instructor” means any individual employed or otherwise engaged by Customer as a teacher, professor, lecturer, or in a similar educational capacity, who is authorized by Customer to access and use the Services in accordance with the terms and conditions set forth in the Agreement.

“Intellectual Property Rights” means all the intellectual property and other proprietary rights, protected or protectable, under the laws of the United States, any foreign country or any political subdivision thereof, including, without limitation: (a) all trade names, trade dress, trademarks, service marks, logos, and other identifiers; (b) copyrights, moral rights (including rights of attribution and rights of integrity); (c) all trade secrets, inventions, discoveries, devices, processes, designs, techniques, trade secrets, ideas, know-how and other confidential or proprietary information, whether or not reduced to practice; (d) all domestic and foreign patents and the registrations, applications, renewals, extensions and continuations (in whole or in part) thereof; and (e) all goodwill associated therewith and all rights and causes of action for infringement, misappropriation, misuse, dilution or unfair trade practices associated with (a) through (d) above.

“Malicious Code” means viruses, worms, time bombs, Trojan horses, malware, spyware and other malicious code, files, scripts, agents or programs designed to: (a) damage, destroy or alter any software, hardware or data stored therein; (b) reveal, damage, destroy or alter any data; (c) disable any computer program automatically; or (d) permit unauthorized access to any software, hardware or data stored therein

“Order Form” means any written order or quote for Services, whether in physical or electronic form, that is executed by both Turnitin and Customer. Each Order Form is effective upon signing by both Parties and is subject to and governed by the terms and conditions of the Agreement, which are incorporated by reference.

“Output” means any data, results, or materials generated or produced by Customer as a direct and specific outcome of using the Services, excluding any data, intellectual property, or Confidential Information owned or controlled by Turnitin or its Affiliates, and any enhancements, modifications, or derivative works of the Services or Turnitin’s Confidential Information. Output includes Proctoring Reports.

“Personal Data” means any information that identifies, relates to, describes, is reasonably capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular individual and also includes any information that meets the definition of “personal data”, “personal information”, “personally identifiable information”, “nonpublic personal information” or any similar term in Applicable Data Protection Legislation.

“Portal Services” means those Services provided to Authorized Users to enable such Authorized Users’ access to and use of the Authorized User Portal.

“Processor” means the Party which processes Personal Data on behalf of the Controller.

“Proctoring Data” means all data, information, and materials collected, generated, or processed during the proctoring of assessments, including without limitation, audio, video, screen recordings, photographs, identity authentication information, and any other data related to the monitoring and evaluation of the integrity and authenticity of the assessment process.

“Proctoring Reports” means the records, summaries, analysis, or other reports generated by the proctoring or monitoring features of any Service, which provides information about a Student’s conduct and performance during an assessment to evaluate whether any such assessments have flagged exam integrity and related issues.

“Product” means the products, services, and software applications that Turnitin provides to Customer and Authorized Users, as applicable.

“Sensitive Personal Data” includes, but is not limited to,Personal Data that reveals a person’s social security number, driver’s license, state identification card number, passport number; account login information, financial account, debit card, or credit card in combination with a security or access code or credentials for accessing the account; precise geolocation; racial or ethnic origin, religious or philosophical beliefs or union membership; contents of a consumers’ mail, email, and/or text message unless to the intended recipient; genetic data; biometric information for the purpose of uniquely identifying an individual; health information; and/or information relating to an individual’s sex life or sexual orientation.

“Service(s)” means each of the services made available by Turnitin or any of its Affiliates including those web services described in the Service Terms. Services do not include any Third-Party Content.

“Service Terms” means the specific rights and restrictions applicable to particular Services, which can be found at www.turnitin.com/service-terms. (and any successor or related locations designated by Turnitin). Turnitin reserves the right to update the Service Terms at its discretion from time to time.

“Site” means the Turnitin website and Authorized User Portals that Turnitin makes available to Customer, its administrators and Instructors, and Students from time to time to access and use certain Portal Services in accordance with the terms of the Agreement.

“Site Terms” means the terms of use of the Site located at https://www.turnitin.com/ (and any successor or related locations designated by Turnitin), as may be updated by Turnitin from time to time.

“Student” means any of Customer’s examinees who (i) install any portion of the ExamSoft Services on personal computer equipment; or (ii) download at least one assessment; or (iii) utilize portions of the ExamSoft Services to take an assessment on equipment provided by Customer; or (iv) take an assessment manually using paper but whose test results are later processed by the ExamSoft Services for processing and analysis by Customer; or (v) any examinee whose performance is otherwise assessed using ExamSoft Services (e.g., with rubrics).

“Submissions” means any written works, documents, or other materials submitted by Authorized Users to the Services for the purpose of examining, detecting, and preventing academic misconduct, including, but not limited to plagiarism in accordance with the terms and conditions set forth in the Agreement.

“Support Services” means the ongoing support and maintenance services that are provided by Turnitin to Customer (including its Authorized Users) for the Services.

“Systems” means the hardware and software platforms, owned, or used by ExamSoft and/or its licensors, in the course of providing the Services.

“Term” has the meaning given to it in Section 19.1.

“Test Data” means information that ExamSoft collects from Students for the purpose of Assessment Administration, including, but not limited to makes and models of computers used by Students, device identification number, types and versions of software used by Students and Software performance related information, Student biometric video and audio recordings, and other assessment-related data.

“Third-Party Content” means any technology, software, data, information, documents, or other materials made available to Customer by any third party on the Site or in conjunction with the Services.

“Turnitin Content” means all data, information, materials, and content that Turnitin provides or makes available through the Services, including without limitation, the Source Database, algorithms, software, tools, templates, text, graphics, images, and any other intellectual property or proprietary information owned or licensed by Turnitin, but excluding Customer Content, Authorized User Data, Test Data, Output or Third-Party Content.

“Turnitin Policies” means all policies of Turnitin applicable to the Services, including its Privacy Policy, Turnitin Service Terms, and Acceptable Use Policy.

“Updates” means bug or error fixes, patches, modifications, enhancements, updates, upgrades, corrections, replacement and successor products, new versions, and new releases.

**Acknowledged and agreed**, as of the Effective Date:

|  |  |
| --- | --- |
| **Turnitin, LLC** | **[Institution]** |
| Signature: [turnitinLlcSignerSignature\_kq7ORYX] | Signature: [counterpartySignerSignature\_h3GCaoX] |
| Print Name: [turnitinLlcSignerName\_zHT6baZ] | Print Name: Ing. Martina Větrovská \_nnKaED7] |
| Print Title: [turnitinLlcSignerTitle\_RbpG7nA] | Print Title: [c bursar ounterpartySignerTitle\_BMCb3kc] |
| Date: [turnitinLlcSignerDateField\_0MTrEBn] | Date: [counterpartySignerDateField\_siSPx3a] |
| 2101 Webster St Ste 1900Oakland CA 94612 USA |  |

**ERDF KVALITA ZČU - UK 02 - Turnitin software license for UWB - Conditions of Contract**

1. **Identification of the contracting authority** (Purchaser)

**University of West Bohemia**

Primary Contact: xxx, e-mail: xxx

Registered Address: Univerzitní 8, 301 00 Plzeň, Czech Republic

Registration No.: 49777513 Tax ID: CZ49777513

1. **Subject-matter of the performance:**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|   | **Product name** | **Service Start Date** | **Service End Date** | **Number of Licences** |
| 1 | Turnitin Feedback Studio | 01.05.2025 | 30.04.2026 | 1255 |
| 2 | Turnitin Originality | 01.05.2025 | 30.04.2026 | 1255 |
| 3 | Online Training | 01.05.2025 | 30.04.2026 |   |
| 4 | Turnitin Feedback Studio | 01.05.2026 | 30.04.2027 | 1255 |
| 5 | Turnitin Originality | 01.05.2026 | 30.04.2027 | 1255 |
| 6 | Online Training | 01.05.2026 | 30.04.2027 |   |
| 7 | Turnitin Feedback Studio | 01.05.2027 | 30.04.2028 | 1255 |
| 8 | Turnitin Originality | 01.05.2027 | 30.04.2028 | 1255 |
| 9 | Online Training | 01.05.2027 | 30.04.2028 |   |
| 10 | Turnitin Feedback Studio | 01.05.2028 | 30.04.2029 | 1255 |
| 11 | Turnitin Originality | 01.05.2028 | 30.04.2029 | 1255 |

1. **Price/Payment conditions:**
2. corresponding to the supplier's tender submitted in the tendering procedure
3. payment is due net thirty (30) days from the date of invoice
4. a late payment fee of up to two percent (2 %) per month
5. the tax document/invoice must be marked with the project registration number, i.e. CZ.02.02.01/00/23\_023/0008982
6. **Necessary provisions in the contract required by the contracting authority:**

**Rules of the grant provider- the contract shall contain the following provisions required by the grant provider:**

1. The Purchaser notifies [the Seller] and the Seller acknowledges that the Subject of Purchase is to be paid from the earmarked funds provided from the budget of the European Union for the implementation of the approved project (hereinafter referred to as the "Grant") and the Purchaser is obliged to ensure that no part of the Grant is provided to persons who are in a conflict of interest or who are subject to international sanctions within the meaning of Act No. 69/2006 Coll., on Implementation of International Sanctions, or other restrictions set by the Grant Provider, or that such persons do not become the final beneficiaries of any part of the Grant.
2. The Seller undertakes to ensure that, in the period between the conclusion of this Contract and its complete fulfilment, its beneficial owner under Act No. 37/2021 Coll., on Registration of Beneficial Owners, does not become a person:
3. who is subject to international sanctions under Act No. 69/2006 Coll.,
4. who has a conflict of interest within the meaning of Section 2, subsection 1 (c) of Act No. 159/2006 Coll., on Conflicts of Interest[[1]](#footnote-1).
5. The Seller is obliged to keep all documentation related to the subject of performance, including accounting documents, at least ten (10) years from the full performance of the Contract, unless a longer period is stipulated by law.
6. The Seller shall, at least for the period for which it is obliged to keep the documentation according to this Contract, cooperate in the performance of inspections and financial control pursuant to Act No. 255/2012 Coll., on Inspection (Inspection Code), and Act No. 320/2001 Coll., on Financial Control in Public Administration, and is also obliged to provide the required information and documentation related to the performance of this Contract to employees or representatives of the authorized bodies (i.e., to the grant provider or its intermediary body, the Ministry of Finance, the European Commission, the European Court of Auditors, the Supreme Audit Office, the authorized financial administration body or another authorized state administration body); furthermore, the Seller is obliged to create conditions for the above-mentioned persons to carry out inspections and audits related to the performance of this Contract and to cooperate in carrying out the inspections and audits.
7. The Seller undertakes to compensate the Purchaser for damages (including the reduction or non-provision of the Grant) resulting from a breach of the Seller's obligation under paragraph 2, 3 or 4.
8. The Purchaser is entitled to withdraw from the Contract in the event of a breach of the Seller's obligations under paragraph 5.

**DATA PROCESSING AGREEMENT**

**v.xx.xx.2023**

This Data Processor Agreement (**“DPA”**) is entered into as of September 1, 2024 between:

**Turnitin, LLC**, 2101 Webster St., Ste 1900, Oakland, CA 94612 USA (the **“Processor”**); and

**University of West Bohemia**, **Univerzitní 2732/8, Plzeň 301 00, Czech Republic** (the **“Controller”**);

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

**Recitals**

Whereas:

* Controller has entered into an Agreement with Processor pursuant to which Processor performs certain services on Controller’s behalf, which are described more fully below in Section 9;
* Processor’s provision of the services and performance of its obligations under the Agreement require that Processor process Personal Data on behalf of Controller;
* 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 Master 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;

“**Applicable Data Protection Law(s)**” means all applicable data protection laws, rules, regulations, orders, ordinances, regulatory guidance, and industry self-regulations, including but not limited to GDPR, the UK GDPR, and the California Consumer Privacy Act.

“**Controller**” means an entity that, alone or jointly with others, determines the purposes for and means of Processing. “Controller” has the same meaning as “Business,” as that term is defined under Applicable Data Protection Law.

“**Data Subject**” means an identified or identifiable natural person and has the same meaning as “Consumer,” as that term is defined under Applicable Data Protection Law.

“**De-Identified Data**” means data that cannot reasonably be used to infer information about, or otherwise be linked to, a Data Subject or as that term is otherwise defined under Applicable Data Protection Law.

**“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 or other Applicable Data Protection Laws and shall include “personal information”, “personally identifiable information”, “nonpublic personal information”, and similar terms under Applicable Data Protection Laws;

**“Process”** or **“Processing”** means any operation or set of operations performed on Personal Data, whether or not by automated means, including, but not limited to, accessing, collecting, recording, organizing, structuring, using, storing, transferring, retaining, disclosing, selling, sharing, deleting, and destroying Personal Data..“**Processor**” means a natural or legal person that processes Personal Data on a Controller’s behalf. “Processor” has the same meaning as “Service Provider,” as that term is defined under Applicable Data Protection Law.

“**Security Breach**” means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Personal Data Processed by Processor.

“**UK Addendum**” refers to the UK’s International Data Transfer Addendum to the EU SCCs, available at https://ico.org.uk/media/for-organisations/documents/4019539/international-data-transfer-addendum.pdf.

Any terms not otherwise defined herein, shall have the meaning specified in the Agreement and if not defined in the Agreement, shall have the meaning provided in Applicable Data Protection Laws.

The Parties agree as follows:

**1. General**

1.1 Customer is a Controller and Turnitin is a Processor with respect to the Processing of Personal Data to provide the Services contemplated under the Agreement. The Processor undertakes to Process Personal Data on behalf of the Controller, for the business purposes described in Section 9 below, pursuant to the terms and conditions of this DPA and solely on the instructions of the Controller, unless otherwise required by applicable law. The Processor shall Process the Personal Data lawfully, with due care and in accordance with the Applicable Data Protection Laws.

1.2 Except as expressly permitted by Applicable Data Protection Law, Processor shall not retain, use, disclose, or otherwise Process Personal Data (i) for any purposes other than those specified in the Agreement and in this DPA; (ii) for any commercial purpose other than the specific business purposes specified in the Agreement and the DPA, including to provide services to a different business; and (iii) outside the direct business relationship between Controller and Processor, including to combine or update Personal Data with information received from or on behalf of another source or collected from Processor’s own interactions with a Data Subject.

1.3 The Processor shall limit Personal Data collection, use, retention, and disclosure to activities reasonably necessary and proportionate to achieve the Processing set out in this DPA and the Agreement and not Process the Personal Data in a manner incompatible with those purposes.

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

1.5 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.

1.6 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. The Processor shall not “sell” or “share” Personal Data, as Applicable Data Protection Law defines those terms.

1.7 With respect to any De-Identified Data that Processor Processes under the Agreement: (i) take reasonable measures to ensure that such data cannot be associated with a Data Subject; (ii) Process such data only in a de-identified fashion; (iii) not attempt to re-identify such data; (iv) contractually obligate any recipients of such data to comply with this section; and (v) publicly commit to complying with this section, such as through a prominent disclosure in its privacy policy, on its website, or similar means.

1.8 The Processor shall reasonably cooperate with and assist Controller in complying with Applicable Data Protection Law including, but not limited to, assisting with data protection impact assessments and consultations with regulatory bodies.

1.9 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 Subprocessors**

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 Processor its general written consent to the use of third-party sub-processors in the provision of the services.

2.2 In the event the Processor engages third-party sub-processors for the provision of the services, the Processor warrants it has a written agreement with the relevant third-party sub-processor which shall include any mandatory provisions required under Applicable Data Protection Laws.

2.3 The Processor is responsible for the acts and omissions of its sub-processors with respect to their processing of Personal Data under the Agreement.

**3.  Security**

3.1 Processor shall have in place appropriate technical and organisational measures as required by Applicable Data Protect Laws 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 a copy of its written information security policy relating to the protection of Personal Data.

**4. Obligation to report Security Breaches**

4.1 In the event of a Security Breach, the Processor shall notify the Controller promptly after the Security Breach 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 Security Breach, the Processor shall reasonably provide to the Controller all relevant and necessary information relating to the Security Breach to enable Controller to fulfill its legal obligations to respond to the Security Breach. The Processor warrants that the information provided will be complete and correct to the best of its knowledge.

4.3 At the Controller’s request, the Processor shall reasonably cooperate 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 outside the EEA) take place only within the USA. Processor will adhere 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 promptly 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:

1. the name and address of the Processor;
2. the purposes for which the Processor processes the Personal Data;
3. the Personal Data categories processed by the Processor;
4. the countries to which the Personal Data are transferred;
5. 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*:* | Processingof 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 Controlleris 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 Processorconfirms that it:

(a)processes thePersonal 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 Czech Republic.

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 Czech Republic.

Signed for and on behalf of **Processor**

[turnitinLlcSignerSignature\_6hedPnu]

Print name: [turnitinLlcSignerName\_JbbuAl0]

Signed for and on behalf of **Controller**

[counterpartySignerSignature\_gzhAJju]

Print name: [c Ing. Martina Větrovská, bursar ounterpartySignerName\_Xs2YQsY]

**ANNEX A**

**STANDARD CONTRACTUAL CLAUSESSECTION I**

*Clause 1*

### ***Purpose and scope***

1. 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)[[2]](#footnote-2) for the transfer of personal data to a third country.
2. The Parties:
	1. 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
	2. 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”).

1. These Clauses apply with respect to the transfer of personal data as specified in Annex I.B.
2. The Appendix to these Clauses containing the Annexes referred to therein forms an integral part of these Clauses.

*Clause 2*

### ***Effect and invariability of the Clauses***

1. 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.
2. 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***

1. Data subjects may invoke and enforce these Clauses, as third-party beneficiaries, against the data exporter and/or data importer, with the following exceptions:
	1. Clause 1, Clause 2, Clause 3, Clause 6, Clause 7;
	2. 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);
	3. Clause 9 - Module Two: Clause 9(a), (c), (d) and (e); Module Three: Clause 9(a), (c), (d) and (e);
	4. Clause 12 - Module One: Clause 12(a) and (d); Modules Two and Three: Clause 12(a), (d) and (f);
	5. Clause 13;
	6. Clause 15.1(c), (d) and (e);
	7. Clause 16(e);
	8. Clause 18 - Modules One, Two and Three: Clause 18(a) and (b); Module Four: Clause 18.
2. Paragraph (a) is without prejudice to rights of data subjects under Regulation (EU) 2016/679.

*Clause 4*

### ***Interpretation***

1. Where these Clauses use terms that are defined in Regulation (EU) 2016/679, those terms shall have the same meaning as in that Regulation.
2. These Clauses shall be read and interpreted in the light of the provisions of Regulation (EU) 2016/679.
3. These Clauses shall not be interpreted in a way that conflicts with rights and obligations provided for in Regulation (EU) 2016/679.

*Clause 5*

***Hierarchy***

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

*Clause 6*

***Description of the transfer(s)***

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

*Clause 7 - Optional*

***Docking clause***

1. 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.
2. 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.
3. 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.

* 1. **Instructions**
1. 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.
2. The data importer shall immediately inform the data exporter if it is unable to follow those instructions.

## **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.

## **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.

## **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.

## **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).

## **Security of processing**

1. 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.
2. 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.
3. 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.
4. 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.

## **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.

## **Onward transfers**

The data importer shall only disclose the personal data to a third party on documented instructions from the data exporter. In addition, the data may only be disclosed to a third party located outside the European Union[[3]](#footnote-3) (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:

* + 1. 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;
		2. 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;
		3. 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
		4. 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.

## **Documentation and compliance**

1. The data importer shall promptly and adequately deal with enquiries from the data exporter that relate to the processing under these Clauses.
2. 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.
3. 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.
4. 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.
5. 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***

1. 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.
2. 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.[[4]](#footnote-4) 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.
3. 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.
4. 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.
5. 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***

1. 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.
2. The data importer shall assist the data exporter in fulfilling its obligations to respond to data subjects’ requests for the exercise of their rights under Regulation (EU) 2016/679. In this regard, the Parties shall set out in Annex II the appropriate technical and organisational measures, taking into account the nature of the processing, by which the assistance shall be provided, as well as the scope and the extent of the assistance required.
3. In fulfilling its obligations under paragraphs (a) and (b), the data importer shall comply with the instructions from the data exporter.

*Clause 11*

### ***Redress***

1. 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.
2. 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.
3. 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:
	1. 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;
	2. refer the dispute to the competent courts within the meaning of Clause 18.
4. 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.
5. The data importer shall abide by a decision that is binding under the applicable EU or Member State law.
6. 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***

1. 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.
2. 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.
3. 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.
4. 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.
5. 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.
6. 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.
7. The data importer may not invoke the conduct of a sub-processor to avoid its own liability.

*Clause 13*

### ***Supervision***

1. 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.
2. 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***

1. 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.
2. The Parties declare that in providing the warranty in paragraph (a), they have taken due account in particular of the following elements:
	1. 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;
	2. the laws and practices of the third country of destination– including those requiring the disclosure of data to public authorities or authorising access by such authorities – relevant in light of the specific circumstances of the transfer, and the applicable limitations and safeguards[[5]](#footnote-5);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.
	3. 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.
3. 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.
4. The Parties agree to document the assessment under paragraph (b) and make it available to the competent supervisory authority on request.
5. 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).
6. Following a notification pursuant to paragraph (e), or if the data exporter otherwise has reason to believe that the data importer can no longer fulfil its obligations under these Clauses, the data exporter shall promptly identify appropriate measures (e.g. technical or organisational measures to ensure security and confidentiality) to be adopted by the data exporter and/or data importer to address the situation 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***

## **Notification**

1. 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:
	1. 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
	2. 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.
2. 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.
3. 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.).
4. 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.
5. 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.

## **Review of legality and data minimisation**

1. 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).
2. 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.
3. 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***

1. The data importer shall promptly inform the data exporter if it is unable to comply with these Clauses, for whatever reason.
2. 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).
3. The data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses, where:
	1. 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;
	2. the data importer is in substantial or persistent breach of these Clauses; or
	3. 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.

1. 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.
2. 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 [Czech Republic] (*specify Member State*).

*Clause 18*

### ***Choice of forum and jurisdiction***

1. Any dispute arising from these Clauses shall be resolved by the courts of an EU Member State.
2. The Parties agree that those shall be the courts of [Czech Republic] *specify Member State*).
3. 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.
4. The Parties agree to submit themselves to the jurisdiction of such courts.

**APPENDIX**

**ANNEX I**

* 1. **LIST OF PARTIES**

**Data exporter(s):**

Name: **University of West Bohemia**

Address: Univerzitní 2732/8, Plzeň 301 00, Czech Republic

Contact person’s name, position and contact details: xxx, e-mail: xxx[counterpartySignerName\_F0BPWOp]\_\_\_[counterpartySignerTitle\_L1rdfZ3]\_\_\_\_[counterpartySignerEmail\_hHzEwgT]

Activities relevant to the data transferred under these Clauses: \_Textual comparison services, storage,

use, database compilation, grading

Signature and date: [counterpartySignerSignature\_2yENBcd]\_\_\_\_\_\_[counterpartySignerDateField\_PJwO7JH]

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 | 6th 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 - 16BNoida, Uttar Pradesh 201301India | Processing of data in India (Customer Support) |
| Turnitin Netherlands B.V. | Stadsplateau 73521 AZUtrecht, Netherlands | Processing of data in the Netherlands (Customer Support) |
| UKU Group Ltd. | SP Hall28-A Stepana Bandery AvenueOffice 302Kyiv, 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 UKDPO@turnitin.com

Signature and date: [turnitinLlcSignerSignature\_0r6K5r9] [turnitinLlcSignerDateField\_Dj3TydA]

## **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.

## **COMPETENT SUPERVISORY AUTHORITY**

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

*Office for Personal Data Protection (UOOU) - https://uoou.gov.cz/en.*

**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
1. **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.
1. **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.
1. **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.
1. **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.
1. **Measures for the protection of data during transmission:**
* All data is encrypted in transit using the technical measures described in section 1 herein.
1. **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.
1. **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.
1. **Measures for ensuring events logging:**
* Centralized logging infrastructure consolidates all relevant events for human and programmatic consumption and processing.
1. **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.
1. **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.
1. **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.
1. **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.
1. **Measures for ensuring data quality:**
* Turnitin only processes the data provided by the Controller. Data rectification is always available via Customer Support.
1. **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.
1. **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.
1. **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**

19.1Turnitin 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”** programson 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.

**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
1. **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/>

Please see our pricing for Turnitin Feedback Studio with Originality and Online Training.

|  |
| --- |
| ERDF KVALITA ZČU - UK 02 - Turnitin software license for UWB |
| **Annex 3 of TD - Table for determining the tender price** |
|  |  |  |  |  |  |  |
|  | **Product name** | **Service Start Date** | **Service End Date** | **Number of Licences** | **Price in EUR excl. VAT** |  |
| 1 | Turnitin Feedback Studio | 5/1/2025 | 4/30/2026 | 1255 | 5,542.70 € |  |
| 2 | Turnitin Originality | 5/1/2025 | 4/30/2026 | 1255 | 1,149.54 € |  |
| 3 | Online Training | 5/1/2025 | 4/30/2026 |  | 500.00 € |  |
| 4 | Turnitin Feedback Studio | 5/1/2026 | 4/30/2027 | 1255 | 5,930.69 € |  |
| 5 | Turnitin Originality | 5/1/2026 | 4/30/2027 | 1255 | 1,230.01 € |  |
| 6 | Online Training | 5/1/2026 | 4/30/2027 |  | 500.00 € |  |
| 7 | Turnitin Feedback Studio | 5/1/2027 | 4/30/2028 | 1255 | 6,345.83 € |  |
| 8 | Turnitin Originality | 5/1/2027 | 4/30/2028 | 1255 | 1,316.11 € |  |
| 9 | Online Training | 5/1/2027 | 4/30/2028 |  | 500.00 € |  |
| 10 | Turnitin Feedback Studio | 5/1/2028 | 4/30/2029 | 1255 | 6,790.04 € |  |
| 11 | Turnitin Originality | 5/1/2028 | 4/30/2029 | 1255 | 1,408.24 € |  |
| **Total price (max 31500 EUR excl. VAT)** | **31,213.16 €** |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  | **Product Descriptions:** |  |  |  |  |  |
|  | Turnitin Feedback Studio (check for similarity and streamline feedback and grading essays) |
|  | Turnitin Originality (comprehensive protection against plagiarism, AI writing detection) |
|  | Online Training |

To access the .xlsx version, please see *07 -Turnitin\_Tender Price Table\_ERDF KVALITA ZČU.xlsx*.

1. List of public officials according to Section 2 subsection 1 (c) of the Conflict of Interest Act can be downloaded here - https://justice.cz/web/msp/seznam-vf [↑](#footnote-ref-1)
2. 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 […]. [↑](#footnote-ref-2)
3. 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 [↑](#footnote-ref-3)
4. This requirement may be satisfied by the sub-processor acceding to these Clauses under the appropriate Module, in accordance with Clause 7. [↑](#footnote-ref-4)
5. 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. [↑](#footnote-ref-5)