## Data Processing Addendum

This Data Processing Addendum together with all attachments and appendices ("DPA") forms part of the Master Services Agreement (or similar agreement under which Services are provided to Hyland) ("Services Agreement") between Service Provider (or similar term under the Services Agreement) and Hyland and is incorporated therein by reference.

1. **DEFINITIONS**

Any capitalized term not defined herein shall have the meaning given to that term under the Services Agreement.

- 1. "Controller", "Processor", "Processing", and "Supervisory Authority" have the same meanings as in Article 4 of the GDPR.
  2. "Data Subject" means the subject of Personal Data.
  3. "Data Protection Law" means: (i) EU Regulation 2016/679 (General Data Protection Regulation) (the "GDPR"); (ii) EU Directive 2002/58/EC (the "ePrivacy Directive"); (iii) after European Union law no longer applies in the United Kingdom, the data protection laws of the relevant territories of the United Kingdom; and (iv) any and all applicable national data protection laws made under or pursuant to (i), (ii) or (iii), in each case as may be amended or superseded from time to time.
  4. "EU Model Clauses" means standard contractual clauses adopted or approved by the European Commission for transfers under the GDPR (and if more than one set of such clauses may apply to a transfer, the most recent such set).
  5. "Hyland" means Hyland Software, Inc. on behalf of itself and its affiliates. The term affiliates shall be deemed to include any parent company, subsidiary, affiliate of, or entity controlled by (including beneficial control), controlling or under common control with Hyland.
  6. "Personal Data" means any information received by Service Provider from, or received or created on behalf of, Hyland relating to an identified or identifiable natural person located in the European Economic Area, the UK or Switzerland. An "identifiable natural person" is one who can be identified, directly or indirectly, in particular, by reference to an identification number, location data, an online identifier or to one or more factors specific to the physical, psychological, genetic, mental, economic, cultural or social identity of the natural person.
  7. "Personal Data Breach" means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Personal Data transmitted, stored or otherwise Processed when that Personal Data is in the possession of Service Provider or its agents or subcontractors.
  8. "Required By Law" means that a statute, regulation, court order, or legal process, enforceable in a court of law, mandates the conduct.
  9. "Sensitive Personal Data" means Personal Data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, data concerning health, sex life, or sexual orientation, genetic data and biometric data when Processed for the purpose of uniquely identifying a natural person, and also includes information about criminal history.
  10. "Sub-processor" means an entity that processes Personal Data at the request of Service Provider.

1. **SERVICE PROVIDER'S PROCESSING OF PERSONAL DATA**
   1. Nature and Purpose of Processing of Personal Data. Service Provider agrees to Process Personal Data solely in accordance with **Appendix A.**
   2. Duration of Processing. Service Provider shall Process Personal Data only during the term of the Services Agreement.
   3. Violation Of Data Protection Law. Service Provider will immediately notify Hyland if Service Provider becomes aware that Service Provider's compliance with a term or condition of this

DPA has violated, violates, or will violate Service Provider's or Hyland's obligations under applicable law.

2. **CROSS-BORDER DATA TRANSFERS**
    1. Service Provider will not transfer Personal Data outside of the European Economic Area, which term shall include the United Kingdom ("EEA") (but only for so long as transmission of personal data from the EEA to the United Kingdom is not considered as a transfer to a third country under European Union law), unless it has taken such measures as are necessary to ensure the transfer is in compliance with Data Protection Law. Such measures may include (without limitation) transfers to any country or territory and/or sector that is at the time subject to a current finding by the European Commission of adequate protection, to a recipient that has achieved binding corporate rules authorization in accordance with Data Protection Law, or under any derogation permitted by Data Protection Law.

    2. To the extent that Service Provider transfers Personal Data outside the EEA in connection with the Services provided under the Services Agreement, and such transfer is not covered by any measure set forth in Section 3.1, the relevant transfer shall be governed by the appropriate EU Model Clauses, with the data importer being the Service Provider or other approved Sub-Processor and, as appropriate:
        1. the data exporter being Hyland and the governing law being that of where the applicable Hyland entity is established;

or

- 1. the data exporter being the applicable Hyland customer and the governing law being that of where the applicable customer is located;

and the remaining details required under the EU Model Clauses being deemed completed as appropriate with the information set out in this DPA (including without limitation the Appendix) and the Services Agreement. In the event of any conflict or inconsistency among or between the terms and conditions of any such EU Model Clauses and this DPA and/or the Services Agreement, the terms of the EU Model Clauses shall prevail.

- 1. Sections 3.1 and 3.2 shall apply equally to any transfers made from the United Kingdom to a recipient outside the United Kingdom in a territory and/or sector that has not been designated under Data Protection Laws as ensuring an adequate level of protection, with references in those clauses to EU Model Clauses being read as references to standard data protection clauses specified under Data Protection Laws as providing appropriate safeguards for transfers, and such clauses shall be deemed completed with the information stated in Sections 3.1 and 3.2 mutatis mutandis as appropriate.

    2. Where Personal Data originating in Switzerland is Processed by Service Provider (including a Sub-processor) outside Switzerland in a territory and sector that has not been designated as ensuring an adequate level of protection pursuant to Swiss laws Sections 3.1 and 3.2 shall apply mutatis mutandis but with the amendments stated in the Addendum hereto.

1. **SERVICE PROVIDER'S SAFEGUARDS FOR PERSONAL DATA**
    1. Confidentiality Of Personal Data. Service Provider will maintain the confidentiality of all Personal Data. Service Provider will require employees responsible for Processing Personal Data to sign a confidentiality agreement prohibiting the disclosure of Personal Data to any third party except as permitted by this DPA or as Required By Law.

    2. Physical, Technical And Organizational Safeguards. Service Provider shall maintain a comprehensive written information privacy and security program that includes reasonable and appropriate measures to protect against reasonably foreseeable risks to the security, confidentiality, integrity and resilience of Personal Data, which risks could result in the unauthorized disclosure, use, alteration, destruction or other compromise of the Personal Data, including a Personal Data Breach. Such program shall comply with Article 32 of the GDPR and local laws concerning the protection of Personal Data and shall include the measures set forth in the Services Agreement and such measures shall not be materially reduced during the Term of the Services Agreement. Service Provider will regularly monitor, test, and update its information security program. Service Provider shall also maintain in accordance with good

industry practice, measures to protect Personal Data from interception such as: (i) network protections intended to deny attackers the ability to intercept or access Personal Data; and (ii) anonymization or other measures to deny attackers the ability to read intelligible Personal Data, including encryption in transit between Service Provider and any third party, as permitted by this Agreement. Service Provider will provide Hyland with such information concerning its information security program as Hyland may reasonably request from time to time.

3. Reporting Personal Data Breaches. Service Provider shall report to Hyland any Personal Data Breach of which it becomes aware. Service Provider will make such report orally to Hyland within 24 hours of Service Provider's becoming aware of the incident followed by a report in writing (e-mail is acceptable) within 24 hours of the initial oral report. The written report shall include, at a minimum subject to the availability of necessary information, the following: (1) a description of the incident; (2) the date that the incident occurred; (3) the date that Service Provider became aware of the incident; (4) the identity and last known mailing address of each affected Data Subject; (5) the approximate number of affected Personal Data records involved; (6) the affected categories of Personal Data, including Sensitive Personal Data, if any, for each affected Data Subject that was affected; (7) the approximate number of Data Subjects affected; (8) an identification of any law enforcement agency or Supervisory Authority that has been contacted about the incident and contact information for the relevant official; (9) a description of the steps that have been, or will be, taken to mitigate the incident; (10) a description of the steps that have been, or will be, taken to prevent a recurrence; (11) the likely consequences of the Personal Data Breach; and (12) contact information for the person at Service Provider principally responsible for responding to the Personal Data Breach.

4. Service Provider will update the written report periodically as new information becomes available. All reports required by this provision shall be made to: Hyland Legal Department, Attn: Privacy Officer, 28500 Clemens Rd. Westlake, Ohio 44145, 440-788-5000, privacy@hyland.com. Service Provider acknowledges that its determination that a particular set of circumstances constitutes a Personal Data Breach shall not be binding on Hyland.

5. Mitigation Of Damages By Service Provider And Cooperation in Investigation. Service Provider agrees to take, at its own expense, measures reasonably necessary to mitigate any harmful effect of a Personal Data Breach. Service Provider agrees to cooperate, at its own expense, with Hyland in its investigation of any Personal Data Breach. Service Provider will reimburse Hyland for all imputed and out-of-pocket costs reasonably incurred by Hyland in connection with the Personal Data Breach, including, but not limited to, costs related to provision of notices to affected Data Subjects and to any services offered to affected Data Subjects.

6. Notifications Related To A Personal Data Breach. Service Provider acknowledges that Hyland shall determine (1) whether and when to notify any Controller (if applicable) or Supervisory Authority and which Supervisory Authority to notify; (2) who will provide notice to Data Subjects with respect to any Personal Data Breach; (3) the content of any such notice(s); (4) the timing for, and method of, delivery of any such notice(s); and (5) the products or services, if any, to be offered to affected Data Subjects. Service Provider shall not disclose the fact that a Personal Data Breach has occurred or any details related to a Personal Data Breach to any third party without Hyland's written consent, unless otherwise Required By Law.

7. Third Party Access Requests. In the event Service Provider receives a non-compulsory request from any third party, including without limitation, any law enforcement, regulatory, judicial or governmental authority, for disclosure of or access to Personal Data, Service Provider will not disclose or provide such access unless instructed to do so by Hyland. In the event Service Provider receives a compulsory order issued at the request of any third party, including without limitation any law enforcement, regulatory, judicial or governmental authority for disclosure of or access to Personal Data, Service Provider will prior to any disclosure or provision of access:
    1. promptly notify Hyland of such order, unless prohibited by law, and, if so prohibited from notifying Hyland, seek to obtain the right to waive such prohibition in favor of promptly communicating to Hyland as much information as possible; and

    2. inform the third party that: (i) Service Provider is a Processor of such transferred

Personal Data and that Hyland has not authorised the disclosure of Personal Data to the third party; and (ii) any and all requests or demands for disclosure of or access to such transferred Personal Data should therefore be notified to or served upon Hyland; and

3. Only disclose such transferred Personal Data to the extent Service Provider is legally required to do so in accordance with an applicable lawful process, and prior to any such transfer, use reasonable efforts to challenge the scope or validity of any order that Service Provider reasonably believes to be overly broad.

8. Service Provider will maintain, in accordance with good industry practice, measures to protect Personal Data from interception such as: (a) network safeguards intended to deny attackers the ability to access Personal Data; and (b) other measures to deny attackers the ability to read intelligible Personal Data, including encryption in transit between Service Provider to Hyland and from Service Provider to any Sub-Processor.

2. **SERVICE PROVIDER'S ASSISTANCE WITH AUDITS AND DATA SUBJECT REQUESTS**
    1. Availability Of Records Of Processing. Service Provider shall promptly, after a reasonable request from Hyland, make available to Hyland all information necessary to demonstrate the Controller's compliance with the obligations established by Article 28 of the GDPR.

    2. Information Technology Audits. Service Provider will permit Hyland, directly or through a contractor, to conduct site audits of the information technology and information security controls for all facilities used to Process Personal Data so that Hyland can ensure that Service Provider provides the appropriate level of security for the Personal Data.

    3. Requests For Impact Assessment Information. Service Provider shall promptly provide the information requested by Hyland to assist in conducting a data protection impact assessment pursuant to Articles 35 and 36 of the GDPR.

    4. Requests Directed to Service Provider. Service Provider agrees to assist Hyland in responding to a request from a Data Subject to exercise any of his/her rights as provided for under the GDPR. In the event a Data Subject submits such a request with respect to the Data Subject's Personal Data, Service Provider agrees to comply with the request within 5 business days of receiving the request from Hyland. Service Provider will immediately provide Hyland with any requests concerning Personal Data that are sent directly to Service Provider from parties other than Hyland.

3. **SERVICE PROVIDER'S SUB-PROCESSORS**
    1. Consent To Processing By Sub-Processors. Service Provider will not disclose Personal Data to any third party without Hyland's prior written consent. In the event that Hyland consents to Service Provider's disclosure of Personal Data to a Sub-processor, Service Provider shall remain responsible for, and remain liable to, Hyland for, the acts and omissions of such Sub-processor as if they were Service Provider's own acts and omissions.

    2. Sub-processors' Physical, Technical And Administrative Safeguards. Service Provider shall obtain reasonable assurances, in writing, from any Sub-processor to whom Service Provider discloses Personal Data. Such assurances shall include at least the following: that the sub-processor (1) will comply with substantially the same restrictions and conditions on Processing of Personal Data that this DPA imposes on Service Provider, including the restrictions on cross-border data transfers; (2) will implement reasonable and appropriate physical, technical and organizational safeguards to protect Personal Data in compliance with Article 32 of the GDPR; and (3) will notify Service Provider within 24 hours of becoming aware of any Personal Data Breach involving Personal Data.

1. **SERVICE PROVIDER'S OBLIGATIONS UPON TERMINATION OF THE SERVICE AGREEMENT**
    1. Return Or Destruction Of Personal Data. Upon Hyland's written instruction, Service Provider shall return or destroy Personal Data. If Hyland directs Service Provider to destroy the Personal Data, Service Provider shall do so in a manner reasonably intended to prevent recovery of the

Personal Data and shall certify to the same in writing.

2. Service Provider's Retention Of Personal Data. If local law requires Service Provider to retain a copy of any Personal Data, then Service Provider shall (1) notify Hyland of such requirement, (2) extend the protections of this DPA to the retained Personal Data and (3) limit further Processing of the retained Personal Data to those purposes Required By Law for as long as Service Provider maintains the Personal Data.

3. Survival. Service Provider's obligations and duties under this DPA with respect to Personal Data shall survive the termination of the Services Agreement and of this DPA and shall continue for as long as the Personal Data remains in the possession of Service Provider or of its Sub-processors.

2. **MISCELLANEOUS TERMS**
    1. Indemnification. Service Provider shall defend and indemnify Hyland, its parent and subsidiary corporations, officers, directors, employees and agents for any and all claims, charges, inquiries, investigations, costs, reasonable attorneys' fees, monetary penalties, and damages incurred by Hyland and/or its parent or subsidiary corporations, officers, directors, employees and agents resulting from (1) any Processing of Personal Data not permitted by the Services Agreement and this DPA, (2) any Personal Data Breach involving Personal Data in the possession, custody or control of Service Provider or its sub-processors, in the event such Personal Data Breach results in the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Personal Data.

    2. Indemnification Process. The foregoing indemnification obligations are conditioned upon Hyland: (1) notifying Service Provider promptly in writing of any claim, charge, inquiry, or investigation as described in Section VII.A above; (2) reasonably cooperating and assisting in defense of such claim, charge, inquiry, or investigation; and (3) giving sole control of the defense and any related settlement negotiations to Service Provider with the understanding that Service Provider may not settle any claim in a manner that admits guilt or otherwise prejudices Hyland, without Hyland's consent.

    3. Construction. This DPA supersedes any inconsistent provisions in the Services Agreement and/or other existing agreements between the Hyland and Service Provider with respect to Service Provider's obligation to safeguard Personal Data.

**APPENDIX A**

| | |
|---|---|
| **Subject Matter and During of the Processing** | The subject matter of the Processing is Service Providers provision of Services under the Services Agreement.<br><br>The duration of the Processing is the term of the Services Agreement, and any exit period, if applicable. |
| **Nature and Purpose of the Processing** | The purpose of the Processing is to provide the Services as set forth in the Services Agreement.<br><br>The nature of the Processing may include, but is not limited to, collection, recording, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction. |
| **Type of Personal Data Processed** | The Personal Data transferred may concern the following categories of data subjects:<br><br>***Employees*** - Past, potential, present and future staff of Hyland (including job candidates, volunteers, agents, independent contractors, interns, temporary and casual workers).<br><br>***Vendors*** - Past, present and potential advisors, consultants, vendors, contractors, subcontractors and other professionals engaged by Hyland and related staff. |

| | |
|---|---|
| | ***Website visitors*** – Individuals who visit any Hyland owned or operated website.<br><br>***Hyland Customers or End Users (collectively, "Customers")*** – (a) Past, present and potential Customers of Hyland, and (b) data subjects whose Personal Data is uploaded or provided by Customers to Hyland during use of Hyland's services or products. |
| **Categories of Personal Data Processed** | The Personal Data transferred may concern the following categories:<br><br>***Employees***<br><br>Identification data: civil/marital status; first and last name; photograph; date and place of birth; nationality; corporate identifier; gender.<br><br>Contact details: address; telephone number (fixed and mobile); email address; fax number; emergency contact information.<br><br>Employment details: job title; company name; grade, occupation code; geographic location; employee performance and evaluation data; employee discipline information; information regarding previous roles and employment; employee benefits information such as election decisions, leave requests, authorization/declination, health insurance company.<br><br>National identifiers: national ID/passport number; tax ID; government identification number; driver's license, visa or immigration status.<br><br>Academic and professional qualifications: degrees; titles; skills; language proficiency; training information; employment history; CV/résumé.<br><br>Financial data: bank account number; IBAN number; bank details including bank name, bank code, sort code; salary and compensation data; bonuses; pension qualification information; payroll data; tax class; tax office name.<br><br>IT related data: computer ID; user ID and password; domain name; IP address; log files; software and hardware inventory; software usage pattern tracking information (i.e., cookies and information recorded for operation and training purposes).<br><br>Lifestyle: hobbies; social activities; holiday preferences.<br><br>***Vendors***<br><br>Identification data: first and last name; date of birth; place of birth; nationality; photograph; vendor ID.<br><br>Contact details: address; professional email address; professional telephone number (including mobile telephone number).<br><br>Professional details: job title; employer; academic and professional qualifications; data related to transactions involving goods and services.<br><br>National identifiers: tax ID; government identification number.<br><br>Financial data: bank account number; bank details.<br><br>***Website visitors***<br><br>IT-related data: unique device identifiers, dynamic and static Internet Protocol addresses, as well as other information, such as browser characteristics, language preferences, operating system details, referring URLs, length of visits, and pages viewed.<br><br>***Customers, potential Customers and/or their staff, each as applicable***<br><br>Contact information (including name, physical address, e-mail and telephone numbers); Employer; Job title; Login credentials; Account profile, including interests and photograph; Applications for Hyland's educational opportunities, including name, contact information, references, programming |

| | |
|---|---|
| | experience, and application essays; Dietary preferences and restrictions; Order information for trainings courses; Training records including courses taken, certifications completed, and scores and grades; Questions, feedback, comments and other postings, including through https://community.hyland.com; Other information the Customer chooses to provide; Information provided by third parties: data relating to the Customer, potential Customer or staff having clicked on a Hyland advertisement posted on a third party website; Information provided by third parties, where a Customer attends a Hyland event sponsored by a third party: including name, e-mail address, and phone number; Versions of Hyland Group company software used and how the software is being used (what functions, how often etc.); bank account number; bank details; credit card details; purchasing history; return history; cancellation history; and Personal Data submitted by a Customer in the course of the Customer's use of Hyland's Services or during the performance of Services under the Service Agreement. |
| **Categories of Sensitive Personal Data Processed** | No collection of any sensitive data by a Service Provider is anticipated other than employee data required to provide Services in connection with valid employment purposes or to the extent required by applicable law. Such collection will only concern limited sensitive data, for example, health-related information for the purpose of managing employee absences, or disabilities in order to provide access to our premises. |

**ADDENDUM TO Data processing agreemeNT (PERSONAL DATA ORIGINATING IN SWITZERLAND)**

**Changes to Agreement:**

For Switzerland the following definition in the **Agreement** is amended as follows:

*"Data Protection Law(s)" shall also include the applicable privacy laws of Switzerland.*

*Any references to the GDPR shall be replaced by the corresponding provisions of Applicable Privacy Law(s), as amended from time to time.*

**Changes to EU Model Clauses:**

With regard to the EU Model Clauses the following amendments shall apply for Switzerland:

EU STANDARD CONTRACTUAL CLAUSES CONTROLLER TO CONTROLLER (2004/915/EC)

The definitions shall be amended as follows:

**Definition:**

*"personal data" shall mean any information relating to an identified or identifiable natural person or legal entity ("data subject"); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity;*

*"special categories of data/sensitive data", "process/processing", "controller", "processor" and "supervisory authority/authority" shall have the same meaning as in the Swiss Federal Act on Data Protection of 19 June 1992, as amended from time to time ("DPA") (whereby the "authority" shall mean the competent data protection authority in the territory in which the data exporter is established);*

*"Member States" shall mean for Switzerland, Switzerland.*

**Clause II Obligations of the data importer:**

Insert a new Clause II (i) as follows:

*II (i) It will not disclose or transfer the personal data to a third party data controller located outside Switzerland unless it notifies the data exporter about the transfer; and*

*(i) the third party data controller processes the personal data in accordance with guidelines of the authority finding that a third*

*country provides adequate protection; or*

*(ii) the third party data controller becomes a signatory to these Clauses or another data transfer agreement approved by a competent authority in Switzerland.*

**ANNEX A**

Paragraph 5 Annex A shall be deleted and replaced with:

*Rights of access, rectification, deletion and objection: As provided in Articles 5 to 8 of the DPA, as amended from time to time data subjects must, whether directly or via a third party, be provided with the personal information about them that an organisation holds, except for requests which are manifestly abusive, based on unreasonable intervals or their number or repetitive or systematic nature, or for which access need not be granted under the law of the country of the data exporter [rest of provision remains unchanged].*

EU STANDARD CONTRACTUAL CLAUSES CONTROLLER TO PROCESSOR

The definitions shall be amended as follows:

**Clause 1 Definitions:**

*"personal data" shall mean any information relating to an identified or identifiable natural person or legal entity ("data subject"); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity;*

*"special categories of data/sensitive data", "process/processing", "controller", "processor" and "supervisory authority" shall have the same meaning as in the Swiss Federal Act on Data Protection of 19 June 1992, as amended from time to time ("DPA") (whereby the "authority" shall mean the competent data protection authority in the territory in which the data exporter is established);*

*the "data importer" means the processor who agrees to receive from the data exporter personal data intended for processing on his behalf after the transfer in accordance with his instructions and the terms of the Clauses and who is not subject to a third country's system ensuring adequate protection within the meaning of Article 6 DPA;*

*the "applicable data protection law" means the legislation protecting the fundamental rights and freedoms of individuals and, in particular, their right to privacy with respect to the processing of personal data applicable to a data controller in the country in which the data exporter is established;*

*"Member States" shall mean for Switzerland, Switzerland.*

**Clause 4 Obligations of the Data Exporter:**

Clause 4 (a) and (b) will be deleted and Clause 4 (a) will be replaced with:

*The data exporter agrees and warrants:*

1. *that the processing, including the transfer itself, of the personal data has been and will continue to be carried out in accordance with the relevant provisions of the applicable data protection law (and, where applicable, has been notified to the relevant Authorities* of the country where the data exporter is established) and does not violate the relevant provisions of that country.

**Clause 9 Governing Law**

Clause 9 shall be deleted and replaced with:

*The Clauses shall be governed by the law of the country in which the data exporter is established. In case the processor is not in the territorial scope of Article 3 GDPR, the processor shall be affected by contractual obligations, but not regulated by the GDPR.*

**Clause 11 Subprocessing**

Clause 11 shall be deleted and replaced with:

*The provisions relating to data protection aspects for subprocessing of the contract referred to in paragraph 1 shall be governed by the law of the country in which the data exporter is established, namely the DPA and its implementing Ordinance,*

*as amended from time to time.*