Privileged & Confidential

GLOBAL DATA PROCESSING SCHEDULE

This Global Data Processing Schedule ("DPA Schedule") forms a part of the Hyland Master Agreement or any other agreement between Customer and Hyland (the "Agreement") which incorporates this DPA Schedule by reference.

1. DEFINITIONS

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

"Adequacy Determination" means a final determination by a Regulator that the laws of a third country provide an adequate level of protection for Personal Data when that Personal Data is transferred from the jurisdiction of the governmental authority to a third country.

"Customer Personal Data" means any Personal Data submitted by or on behalf of Customer to Hyland for the performance of Services.

"Data Protection Law(s)" means any applicable law, regulation, legislation, or directive applicable to the Processing of Personal Data.

"Data Subject" means an identified or identifiable natural person as defined by applicable Data Protection Law.

"EU SCCs" means the Commission Implementing Decision (EU) 2021/914 establishing Standard Contractual Clauses for data transfers to third countries.

"Personal Data" means any individually identifiable information relating to a Data Subject which is protected under applicable Data Protection Law.

"Personal Data Breach" means a breach of security leading to the accidental or unlawful destruction, loss, alteration, disclosure or access to Customer Personal Data.

"Processing" means any operation or set of operations which is performed on Personal Data or on sets of Personal Data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

"Regulator" means the competent supervisory authority or regulatory body under applicable Data Protection Law.

"Services" means technical support services, professional services, services relating to Hyland's hosted offering, or other applicable services provided by Hyland to Customer as defined in the Hyland Master Agreement.

"Sub-Processor," means an entity that Processes Personal Data at the request of Hyland.

2. HYLAND'S PROCESSING OF PERSONAL DATA

2.1 Instructions for Processing Personal Data. Hyland shall only Process Customer Personal Data for the purposes of performing its obligations under the Hyland Master Agreement and in accordance with **Appendix A**, unless otherwise required by law. Each Party shall comply with the obligations that apply to it under the Data Protection Laws.

2.2 Duration of Processing. Hyland shall Process Personal Data only for the duration set out in **Appendix A**.

3. HYLAND'S SAFEGUARDS FOR PERSONAL DATA

3.1 Physical, Technical And Organizational Safeguards. Maintain appropriate technical and organizational security measures designed to protect Customer Personal Data from accidental or unlawful destruction, loss, alteration, disclosure, or access, as more fully described in **Appendix B**.

3.2 Processing By Sub-Processors. Hyland shall only engage those Sub-Processors, listed at https://community.hyland.com/en/connect/hyland-sub-processor-list (as may be updated by Hyland from time to time without amendment of this DPA). Hyland has entered into a written agreement with each Sub-Processor containing data protection obligations to protect Customer Personal Data no less protective of Data Subjects than those required by applicable Data Protection Law. Hyland shall remain liable to Customer for the acts or omissions of its Sub-Processors. Hyland shall provide Customer notification of any new sub-processors that Hyland intends to engage by updating such webpage, to which Customer can subscribe, with the new sub-processor's details. Where such rights are granted by applicable Data Protection Law, Customer may object to any such new Sub-Processor solely on reasonable grounds relating to data protection concerns by notifying Hyland (in accordance with this DPA) of its objection and grounds within 10 days after receipt of Hyland's notice. In the event of such an objection, Hyland may elect to not engage such Sub-Processor to Process Customer Personal Data. If Hyland continues use of such Sub-Processor after Customer's reasonable objection, then Customer may elect to immediately (without prejudice to accrued fees or other rights under the Hyland Master Agreement) suspend or terminate the portions of the Hyland Master Agreement affected by the use of such Sub-Processor upon notice to Hyland.

3.3 Confidentiality of Personal Data. Hyland shall treat Customer Personal Data as confidential and ensure that Hyland's personnel (including independent contractors) who have access to the Customer Personal Data: (i) have entered into appropriate contractually binding confidentiality undertakings; (ii) are informed of the confidential nature of Customer Personal Data; and (iii) have received appropriate training related to Customer Personal Data;

3.4 Information Technology Audits. Hyland will permit Customer audits in accordance with the Hyland Master Agreement. If the Hyland Master Agreement does not address Customer audits, then where such rights are granted by applicable Data Protection Law, at the Customer's reasonable request but no more than once per annum, Hyland shall permit Customer to conduct an audit of Hyland's security and privacy policies and records in relation to the Processing of Customer Personal Data and such other evidence as Customer may reasonably request to demonstrate Hyland's compliance with the requirements of this DPA. To the extent that Customer elects to conduct an audit at Hyland's physical facility, such audit shall be limited to the physical areas where Processing of Customer Personal Data occurs. Customer is prohibited from distributing or publishing the results of such audit to any third party (except to a competent supervisory authority) without Hyland's prior written approval. At Hyland's election and upon prior notice, Customer shall reimburse Hyland's reasonable costs in relation to any such request at Hyland's then-current professional services rates (rates list available on request). All such audits shall be subject to the Parties' confidentiality obligations. Should Customer retain an independent third party to perform an audit, the Parties agree that: (i) prior to such audit, the independent third party and Hyland shall directly enter into appropriate confidentiality provisions; and (ii) any reports or Hyland information collected during such audit can only be used for Customer internal use.

3.5 Return or Destruction of Personal Data. Hyland shall delete or return Customer Personal Data in accordance with the Hyland Master Agreement. If the Hyland Master Agreement does not address the deletion of return of Customer Personal Data, then at the Customer's written direction, Hyland shall arrange for the prompt and safe return and/or secure permanent destruction of all Customer Personal Data in Hyland's possession and control, together with all copies (if any) within 28 days of such direction and, where requested by the Customer, certify that such destruction has taken place. Hyland shall continue to extend the protections set forth in this DPA to such Customer Personal Data pending such return and/or destruction.

3.6 Requests Directed to Hyland. To the extent legally permitted, Hyland will notify Customer without undue delay (and in any event within forty-eight (48) hours) following its receipt of: (a) any actual or purported request from (or on behalf of) a Data Subject exercising his rights under Data Protection Laws ("Data Subject Request"); or (b) any correspondence or communication from a Regulator ("Regulator Correspondence"). Unless otherwise required by applicable law, Hyland shall not disclose any Customer Personal Data in response to any such request without Customer's prior written direction.

3.7 Requests For Privacy Impact Assessment Information. At Customer's reasonable request and to the extent Customer does not otherwise have access to the relevant information, Hyland shall provide Customer with reasonable cooperation and assistance necessary to assist Customer to fulfil any obligation on Customer under Data Protection Laws to conduct a privacy impact assessment or data protection impact assessment regarding Customer's use of the Services. At Hyland's election and upon prior notice, Customer shall reimburse Hyland's reasonable costs in relation to any such request at Hyland's then-current professional services rates (rates list available on request).

3.8 Reporting Personal Data Breach. Hyland will notify the Customer without undue delay upon becoming aware of a Personal Data Breach. Hyland will take reasonable efforts to identify the cause of such Personal Data Breach and take the steps that Hyland deems necessary and reasonable to remediate the cause of the Personal Data Breach. In relation

to such Personal Data Breach, Hyland shall further assist Customer, taking into account the information available to Hyland and the nature of its Processing, with Customer's Personal Data Breach notification obligations under Data Protection Laws. Any notification by Hyland under this subsection shall not be construed as an admission of fault by Hyland.

4. CUSTOMER OBLIGATIONS FOR PERSONAL DATA

4.1 Customer shall, where required to do so by applicable Data Protection Law, make third party notification(s) in an objective manner that does not intentionally or unreasonably bring Hyland into disrepute or otherwise tarnish the reputation of Hyland.

4.2 Customer shall ensure it is not subject to any prohibition or restriction which would: (i) prevent or restrict it from disclosing or transferring the Customer Personal Data to Hyland; (ii) prevent or restrict it from granting Hyland access to the Customer Personal Data; and/or (iii) prevent or restrict Hyland from Processing the Customer Personal Data, in each case as required for Hyland to perform the Services.

4.3 Customer shall ensure that all fair processing notices have been given (and, as applicable, consents obtained) and are sufficient in scope to enable Hyland to Process the Customer Personal in accordance with the Data Protection Laws.

4.4 Customer shall ensure that Customer Personal Data disclosed or transferred to Hyland is only the minimum amount necessary to perform the Services.

4.5 Customer shall ensure implement and maintain reasonable technical and organizational security measures sufficient to prevent unauthorized access to the Services through Customer's information systems.

4.6 Customer shall have sole responsibility for the accuracy, quality, and legality of the Customer Personal Data provided to Hyland and the means by which Customer acquired the Customer Personal Data.

5. JURISDICTION-SPECIFIC TERMS

5.1 The Parties acknowledge that certain jurisdictions require the Parties to provide additional protections for Personal Data through written contract terms. Such jurisdiction-specific terms are contained in the following addenda and are incorporated by reference into this DPA. Each Addendum, to the extent applicable, is binding on the Parties as follows:

5.1.1 Addendum I (EEA & Switzerland): Addendum I applies when (a) Customer is (i) located in the European Economic Area ("EEA") or Switzerland, or (ii) contracting on behalf of any member of its corporate group located in the EEA or Switzerland; and (b) Hyland Processes Personal Data from a country not subject to an Adequacy Determination.

5.1.2 Addendum II (UK): Addendum II applies when (a) Customer is (i) located in the United Kingdom ("UK"), or (ii) contracting on behalf of a member of its corporate group located in the UK; and (b) Hyland Processes the Personal Data from a country not subject to an Adequacy Determination.

5.1.3 Addendum III (California, USA): Addendum III applies when Customer, or a member of its corporate group is subject to the California Privacy Rights Act ("CPRA").

6. TERM AND TERMINATION

6.1 Term. This DPA shall have a term commencing on the Effective Date and will terminate automatically upon the termination or expiration of all the Hyland Master Agreement.

6.4 Effect. Upon termination of this DPA, Hyland shall return or destroy any Customer Personal Data as set forth above.

7. GENERAL PROVISIONS

7.1 Modification. The Parties agree to amend this DPA from time to time as may be necessary to permit the Parties to remain in compliance with applicable Data Protection Laws.

7.2 Conflict. This DPA supersedes any inconsistent provision in Hyland Master Agreement, and/or other existing

agreements between the Hyland and Customer with respect to the Parties' obligations to comply with Data Protection Laws with respect to Customer Personal Data. If there is any conflict between this DPA, the Hyland Master Agreement(s), and the terms of an applicable Addendum, the terms of the applicable Addendum shall prevail regarding the Personal Data subject to that Addendum.

ADDENDUM I

EEA

The parties agree that transfers of Customer Personal Data from the European Union or Switzerland (collectively the "EEA") shall be governed by the appropriate EU SCCs (as supplemented by this DPA), which are incorporated herein by reference.

The Parties further agree that the EU SCCs shall be completed as follows:

- Module 2 shall apply unless Customer is a Processor in which case Module 3 will apply.
- Clause 7, the optional docking clause will not apply.
- Clause 9(a), Option 2 will apply. Customer authorizes Hyland to engage Sub-Processors as set forth in this DPA.
- Clause 11, the optional redress language will not apply.
- Clause 17, Option 1 will apply, and the EU SCCs shall be governed by the law specified in the Hyland Master Agreement, provided that law is an EU Member State recognizing third party beneficiaries, otherwise the laws of the Netherlands shall apply.
- Under Clause 18(b), disputes will be resolved before the courts specified under the Hyland Master Agreement, provided those courts are in an EU Member State recognizing third party beneficiaries, otherwise those courts shall be the courts of the Netherlands.
- Annex I of the EU SCCs shall be deemed completed with the information set out in Appendix A.
- Annex II of the EU SCCs shall be deemed completed with the information set out in Appendix B.
- Annex III of the EU SCCs shall be deemed completed with the applicable information set out in Appendix A.

In relation to Personal Data that is protected by the Swiss Federal Act on Data Protection, the EU SCCs will apply as completed herein and as adapted below:

- The Swiss Federal Data Protection and Information Commissioner ("Swiss DPA") is the exclusive supervisory authority, and each reference to a "supervisory authority" shall be understood to be a reference to the Swiss DPA.
- The term "member state" will not be interpreted in such a way as to exclude Data Subjects in Switzerland from the possibility of enforcing their rights in their place of habitual residence (Switzerland) in accordance with Clause 18 and the choice of law in Clause 17 shall be the applicable Swiss law.
- References to the GDPR and EU SCCs shall include equivalent provisions of the Swiss Federal Act on Data Protection.

Signatures to the Agreement shall constitute all necessary signatures to the EU SCCs, including the Appendices attached thereto.

Addendum II

United Kingdom

Part 1: Tables

TABLE 1: Parties		
Start date	Effective Date as defined in the Agreement.	
The Parties	Exporter (who sends the Restricted Transfer)	Importer (who receives the Restricted Transfer)
Parties' details	Full legal name: Trading name (if different): Main address (if a company registered address): Official registration number (if any) (company number of similar identifier):	Full legal name: Hyland Trading name (if different): n/a Main address (if a company registered address): As specified in the Agreement Official registration number (if any) (company number of similar identifier):
Key Contact	Full Name (optional): Job Title: Contact Details including email:	Full Name (optional): Job Title: Global Privacy Officer Contact Details including email: privacy@hyland.com
Signature (if required for purposes of Section 2)	Signatures to the Agreement shall constitute all necessary signatures to this Addendum II.	Signatures to the Agreement shall constitute all necessary signatures to this Addendum II.

TABLE 2: Selected SCCs, Modules, and Selected Clauses	
Addendum EU SCCs	The version of the Approved EU SCCs which this Addendum is appended, including the Appendix Information.

TABLE 3: Appendix Information	
"Appendix Information" means the information which must be provided for the selected modules as set out in the Appendix of the Approved EU SCCs (other than the Parties), and which for this Addendum is set out in.	
Annex 1A: List of Parties:	As described in the Agreement, Appendix A
Annex 1B: Description of Transfer:	As described in the Agreement, Appendix A

Annex II: Technical and organisational measures including technical and organisational measures to ensure the security of the data:	As described in the Agremenet, Appendix B.
Annex III: List of Sub-Processors (Modules 2 and 3 only):	https://community.hyland.com/en/connect/hyland-sub-processor-list

TABLE 4: Ending this Addendum when the Approved Addendum Changes	
Ending this Addendum when the Approved Addendum Changes	Which Parties may end this Addendum as set out in Section 19: Importer Exporter

Part 2: Mandatory Clauses

Mandatory Clauses	Part 2: Mandatory Clauses of the Approved Addendum, being the template Addendum B.1.0 issued by the ICO and laid before Parliament in accordance with s119A of the Data Protection Act 2018 on 2 February 2022, as it is revised under Section 18 of those Mandatory Clauses.

Addendum III

California, USA

The following additional provisions apply to Hyland's Processing of the Personal Information that is subject to the CPRA.

a. Definitions: Unless otherwise indicated in this DPA, the capitalized terms used in this section shall have the meaning assigned to them in the California Privacy Rights Act ("CPRA" or the "Act"), codified at Cal. Civ. Code §1798.100 *et seq*.

i. "Business Purpose(s)" means: (i) to provide technical support services, professional services, services relating to Hyland's hosted offering, or other services as specifically defined in the Hyland Master Agreement; (ii) to detect security incidents or protect the Personal Information against malicious, deceptive, fraudulent or illegal activity; (iii) to develop and improve the Services as permitted by the CPRA or the CPRA Regulations; or (iv) as otherwise expressly permitted by the CPRA or the CPRA Regulations.

ii. "Consumer" means a California resident (a) who is a natural person, and (b) whose Personal Information is Processed by Hyland on Customer's behalf for the Business Purposes.

iii. "CPRA Regulations" means final regulations implementing the CPRA after those regulations go into effect.

iv. "Personal Information" shall have the meaning set forth in the CPRA but shall be limited to Personal Information of Consumers which Hyland Processes on Customer's behalf pursuant to the Agreement.

b. Processing Of Personal Information: Customer is a Business and appoints Hyland as its Service Provider to Process

Personal Information only for the Business Purposes. Hyland shall comply with all applicable sections of the CPRA and/or the CPRA Regulations, including providing the same level of protection for Personal Information as the CPRA requires Customer, as a Business, to provide. Hyland grants Customer the right to take reasonable and appropriate steps to help ensure that Hyland uses Personal Information consistent with the CPRA and to stop and remediate unauthorized use of Personal Information.

c. Restrictions On Processing Personal Information: Hyland is prohibited from: (i) Processing Personal Information for any purposes but for the Business Purposes unless otherwise required by law to do so; (ii) Processing Personal information for any additional commercial purpose (other than the Business Purposes) including in the servicing of a different business, unless otherwise expressly permitted by the CPRA or the CPRA Regulations; (iii) Processing Personal Information outside the direct business relationship between Hyland and Customer unless otherwise expressly permitted by the CPRA or the CPRA Regulations; (iv) Selling or Sharing Personal Information; (v) combining Personal Information with personal information that it receives from, or on behalf of, a third party, or Collects from its own interaction with a Consumer (except as permitted by the CPRA Regulations); or (vi) Processing the Personal Information for any other purpose except as permitted by this DPA.

d. Inability To Comply With CPRA: Hyland shall notify Customer after Hyland determines that it no longer can meet its obligations under this Addendum, the CPRA or the CPRA Regulations. In the event Hyland is unable to meet its obligations, Customer may, in its discretion: (i) take reasonable and appropriate steps to stop and remediate any unauthorized use of Personal Information, or (ii) terminate the Hyland Master Agreement.

Appendix A

Subject Matter and Duration of the Processing	The subject matter of the Processing is Hyland's fulfilment of its obligations under the Hyland Master Agreement. The duration of the Processing is the term of the Hyland Master Agreement, and any exit period, if applicable.
Categories of Data Subjects whose Personal Data is Processed	Any Data Subject whose Personal Data is transferred to Hyland under the Hyland Master Agreement, which could include the following categories: ● Customer Employees (Past, potential, present and future staff of Customer) ● Customer Vendors (Past, present and potential advisors, consultants, vendors, contractors, subcontractors and other professionals engaged by Customer and related staff.) ● Customers End Users (Past, present and potential users of Customer services or products)
Nature and Purpose of the Processing	The purpose of the Processing is to provide the Services and otherwise for Hyland's fulfillment of its obligations under the Hyland Master Agreement. 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.
Categories of Personal Data Processed	Any Personal Data submitted by Customer to Hyland under the Hyland Master Agreement.

Categories of Sensitive Personal Data Processed	☒No collection of any Sensitive Personal Data by Hyland is anticipated. ☐ Customer will provide the following categories of Sensitive Personal Data to Hyland under the Hyland Master Agreement:
FOR USE ONLY WITH THE EU SCCS	
Data Exporter (including country of establishment)	Customer, as defined in this DPA.
Data Importer (including country of establishment)	Hyland, as defined in this DPA.
Frequency of the Transfer	Continuous basis (services related to Hyland's hosted offerings or cloud services); One-off basis (technical support, professional services or other applicable services)
Retention Period	For hosting or cloud customers, data is retained for the duration of the Hyland Master Agreement, including any applicable transition period subject to any shorter period which Customer may choose by permanently deleted the personal data from the Services. Personal data provided to Hyland during the performance of technical support or professional services is retained for no longer than necessary for the purposes for which the Personal Data was transferred and, in no event, longer than permitted under the laws of the country of the data exporter.
Sub-processors	Data importer may use the Sub-processors listed at https://community.hyland.com/en/connect/hyland-sub-processor-list.
Competent Supervisory Authority	The competent supervisory authority is the supervisory authority of the EU/EEA Member State where the Data Exporter is established.

Appendix B

Technical and organizational measures

Taking into account:

- the state of the art,
- the costs of implementation and
- the nature, scope, context and
- the purpose of processing as well as
- the risk of varying likelihood and severity for the rights and freedoms of natural persons

Hyland shall implement the technical and organisational measures set forth in the Hyland Master Agreement. To the extent the Hyland Master Agreement does not specify the applicable technical and organizational security measures, then Hyland shall implement the technical and organizational security measures set forth in this Appendix B as follows:

1. Measures for encryption

- encryption of mobile devices such as laptops, tablets, smartphones
- encryption of mobile storage media (CD/DVD- ROM, USB sticks, external hard drives)
- encrypted storage of passwords
- encryption option for sensitive e-mails and e-mail attachments
- secured data sharing (e.g. SSL, FTPS, TLS)
- secured WLAN

2. Measures to ensure confidentiality

a. Measures which ensure that unauthorized persons do not have access to Customer Personal Data:

- access control system, document reader (magnetic / chip card)
- door protections (electric door opener, number lock, etc.)
- protection of facilities, including security guards at Hyland headquarters.
- alarm system
- video surveillance
- special protective measures for the server room
- prohibited areas
- visitor rules (e.g. pick-up at reception, documentation of visiting hours, visitor pass, accompanying visitors to exit after visit)

b. Measures which prevent that unauthorized persons can use the systems that process Customer Personal Data:

- personal and individual user log-in for registration in the systems or company network
- authorization process for access authorizations
- limitation of authorized users
- single sign-on
- two-factor authentication
- BIOS passwords for corporate laptops
- password procedures (indication of password parameters with regard to complexity and update interval)
- logging of access
- additional system log-in for certain applications
- automatic locking of the clients after expiry of a certain period without user activity (also password-protected screensaver or automatic stand-by)
- firewall

c. Measures which ensure that only authorized persons have access to the systems that Process Customer Personal Data and that Customer Personal Data cannot be read, copied, modified or removed without authorization:

- evaluations/logging of data processing
- authorization process for authorizations
- approval routines
- profiles / roles
- encryption at rest and in transit for Customer Personal Data transferred to Hyland via its secure file transfer tool.
- Mobile Device Management system for corporate owned mobile devices and approved personal mobile devices (mobile devices are not part of the hosted solution)
- segregation of functions "segregation of duties"
- destruction of records and storage devices in accordance with NIST 800-88, as applicable
- cyber-related logs retained for no less than six months

3. Measures to ensure integrity

- access rights
- system-side logging
- document management system (DMS) with change history
- security / logging software
- functional responsibilities, organisationally specified responsibilities
- tunnelled remote data connections (VPN = virtual private network)
- electronic signature
- logging of data transfer or data transport
- logging of read accesses

4. Measures to ensure and restore availability

- security concept for software and IT applications
- back-up procedures, as applicable
- ensuring data storage in secured network
- need-based installation of security updates
- set-up of an uninterrupted power supply
- suitable archiving facilities for paper documents
- fire and/or extinguishing water protection for the server room
- air-conditioned server room
- virus protection
- firewall
- business continuity plan
- successful disaster recovery exercises
- redundant, locally separated data storage (off-site storage), as applicable

5. Measures to ensure resilience

- emergency plan in case of machine breakdown / business recovery plan
- redundant power supply
- sufficient capacity of IT systems and plants
- logistically controlled process to avoid power peaks
- redundant systems / plants
- resilience and error management

6. Procedure for regular review, assessment and evaluation of the effectiveness of the technical and organizational measures

- procedures for regular controls/audits
- concept for regular review, assessment and evaluation
- reporting system
- penetration tests
- emergency tests
- applicable certifications

7. "Control of instructions / assignment control"

- process of issuing and/or following instructions
- specification of contact persons and/or responsible employees
- control / examination that the assignment is executed in accordance with instructions
- training / instruction of all access-authorized employees
- independent auditing of adherence to instructions
- commitment of employees to maintain confidentiality
- agreement on penalties for infringements of instructions
- data protection manager / coordinator
- maintain records of processing activities in accordance with art. 30, para. 2 GDPR, as applicable
- documented Security Incident Response Policy, which includes escalation processes for Personal Data Breaches
- guidelines / instructions designed to ensure technical-organisational measures for the security of the processing
- process for forwarding requests of data subjects