Privileged & Confidential
Discussion Draft: September 4, 2021

GDPR DATA PROCESSING SCHEDULE

This GDPR Data Processing Schedule ("DPA") forms a part of the Solution Provider Agreement or any other agreement with Hyland which incorporates this GDPR Data Processing Schedule by reference (the "Solution Provider Agreement"). All capitalized terms not defined here shall have the meaning given to them under the General Terms and Conditions.

AGREEMENT

1. DEFINED TERMS

The following terms shall have the meanings given to them in them in the Article 28 Model Clauses or the EU Model Clauses, as applicable: "Controller", "Data Subject", "Personal Data Breach", "Process", "Processed", "Processing", and "Processor." Sensitive Personal Data shall mean the special categories of Personal Data set out in Article 9(1) of the GDPR.

"Article 28 Model Clauses" means the Commission Implementing Decision (EU) 2021/915 on Standard Contractual Clauses Between Controllers and Processors.

"Customer Personal Data" means any Personal Data and Sensitive Personal Data of a Data Subject Processed by (or on behalf of) Hyland during the performance of the Services as set out in the Solution Provider Agreement.

"Data Protection Law" means: (i) Regulation (EU) 2016/679 if the European Parliament and of the Counsel of 27 April 2016 ("GDPR"); (ii) the Swiss Federal Data Protection Act; and (iii) 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national data protection laws made under or pursuant to (i), (ii), or (iii) in each case as may be amended or superseded from time to time.

"EU Model Clauses" means the Commission Implementing Decision (EU) 2021/914 establishing Standard Contractual Clauses for data transfers to Third Countries. For purposes of this DPA, the applicable module within the EU Model Clauses is MODULE THREE (Transfer Processor to Processor). For the avoidance of doubt, neither MODULE ONE (Transfer Controller to Controller), MODULE TWO (Transfer Controller to Processor), nor MODULE FOUR (Transfer Processor to Controller) shall apply to this DPA.

"Services" means Secondary Support or other applicable services provided by Hyland to Solution Provider as defined in the Solution Provider Agreement.

"Sub-Processor," means an entity engaged by Hyland to perform certain services as described in Section 3(d).

2. OBLIGATIONS OF THE PARTIES

a. Where Hyland Processes Customer Personal Data as a sub-processor on behalf of Solution Provider and the transfer is not covered by Section 2(b) below, the Article 28 Model Clauses (as supplemented by Section 3 below) shall apply, which are incorporated by reference into this DPA. For purposes of the Article 28 Model Clauses the Parties agree that the purpose of such clauses are to comply with the GDPR and that:

i. Appendix A of this DPA shall serve as Annexes I and II.

ii. Appendix B of this DPA shall serve as Annexes III and IV.

and the remaining details required under the Article 28 Model Clauses being deemed completed as appropriate with the information set out in this DPA (including without limitation the Appendix) and the Solution Provider Agreement.

To the extent that Hyland transfers Customer Personal Data outside the European Union ("EU") in connection with the Services provided under a Solution Provider Agreement, the relevant transfer shall be governed MODULE THREE of the EU Standard Clauses 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 Appendices) and the Solution Provider Agreement. For the avoidance of doubt, for purposes of the EU Model Clauses, Appendix A of this DPA shall serve as Annex I and Appendix B shall serve as Annex II.

3. SUPPLEMENTAL OBLIGATIONS FOR ARTICLE 28 CLAUSES AND EU MODEL CLAUSES

a. For purposes of the EU Model Clauses, Clause 7 shall not apply and the optional language under Clause 11(a) shall not apply. For purposes of the Article 28 Clauses, Clause 5 shall not apply.

b. When, and if, required to provide a copy of the Solution Provider Agreement (including this DPA) to a third party or a Data Subject, Solution Provider agrees that prior to sharing such copies, Solution Provider will provide Hyland with a reasonable opportunity to redact any portion of the text, as reasonably necessary to protect Hyland's business secrets or other confidential information.

c. At the Solution Provider's reasonable request and to the extent Solution Provider does not otherwise have access to the relevant information, Hyland agrees to provide Solution Provider with reasonable cooperation necessary to assist Solution Provider with fulfilling its obligations under Data Protection Laws regarding the Processing of Customer Personal Data by Hyland. The Parties agree that Hyland does not have the ability and shall not: (i) directly respond to any actual or purported request from (or on behalf of) a Data Subject exercising his rights under applicable Data Protection Law; or (ii) provide notice to any Data Subject pursuant to the EU Model Clauses, Clause 15.1.

d. For Purposes of the EU Model Clauses, Clause 9(a) and the Article 28 Clauses, Clause 7.7(a), Option 2 ("General Written Authorization") shall apply. Solution Provider authorizes Hyland to engage, as Sub-Processors, the entities listed at https://community.hyland.com/en/connect/gdpr-sub-processors (as may be updated by Hyland from time to time). If Solution Provider subscribes to such webpage, Hyland shall inform Solution Provider of any sub-processor additions or replacements by updating such webpage at least ten (10) days prior to the addition or replacement. Solution Provider may object to a sub-processor addition or replacement solely on based on a Customer's reasonable objection to such sub-processor.

e. Solution Provider authorizes Hyland to transfer Customer Personal Data outside the EU, so long as it has taken such measures as required by the EU Model Clauses and Data Protection Law.

f. Except as otherwise set forth in the Solution Provider Agreement, at the Solution Provider's reasonable request but no more than once per annum (except in the event there are reasonable indications of non-compliance), Solution Provider may conduct an audit of Hyland's security and privacy policies and records in relation to Hyland's Processing of Customer Personal Data. To the extent that Solution Provider 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. Solution Provider 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, Solution Provider 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 Solution Provider mandate 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 Solution Provider internal use.

g. For purposes of the EU Model Clauses, Clause 17, Option 1 shall apply. The Parties agree that the EU Model Clauses shall be governed by the laws of the Netherlands. The Parties further agree that for purposes of the EU Model Clauses, Clause 18, any disputes arising from the EU Model Clauses shall be resolved by the courts of Netherlands.

4. ADDITIONAL TERMS

a. 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 laws.

b. CONFLICT. This DPA supersedes any inconsistent provision in the Solution Provider Agreement, and/or other existing agreements between the Hyland and Solution Provider with respect to the Parties' obligations to comply with Data Protection Laws with respect to Customer Personal Data. If there is any conflict between the EU Model Clauses, the Article 28 Model Clauses, this DPA and the Solution Provider Agreement(s), the terms of the EU Model Clauses or the Article 28 Model Clauses (as applicable) shall prevail.

c. THIRD PARTIES. Other than as set forth in the EU Model Clauses, the Parties to this DPA do not intend there to be any third-party beneficiary rights under this DPA or that any of its terms shall be enforceable by virtue of the Contracts (Rights of Third Parties) Act 1999 by any other person not a party to it.

d. SIGNATURES: The Parties agree that signature to the Solution Provider Agreement constitutes all necessary signatures to the EU Model Clauses, including the appendices attached thereto (where applicable).

Appendix A

Data exporter(s):
Name: Solution Provider, as defined in the Solution Provider Agreement
Address: As specified in the Solution Provider Agreement
Contact person's name, position, and contact details: As specified in the Solution Provider Agreement
Activities relevant to the data transferred under the SCCs: Sale of Hyland propriety software licenses, Professional Services, and Primary Support, as applicable.
Signature and date:
Role (controller / processor): Processor

Data importer(s):
Name: Hyland, as defined in the Solution Provider Agreement
Address: As specified in the Solution Provider Agreement
Contact person's name, position, and contact details: As specified in the Solution Provider Agreement
Activities relevant to the data transferred under the SCCs: Services, as defined in the Solution Provider Agreement.
Signature and date:
Role (controller / processor): Processor

Description of transfer:

Categories of data subjects whose personal data is transferred:

Any data subject whose personal data is transferred to Hyland in the course of Hyland's Services under the Related Agreements, which may include the following categories (if checked):

* 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)

Categories of personal data transferred:

Any Personal Data submitted or made available by the Solution Provider to Hyland in the course of Hyland's Services under the Solution Provider Agreement.

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 specialized training), keeping a record of access to the data, restrictions for onward transfers or additional security measures.

Solution Provider determines what Personal Data is provided to Hyland.

The frequency of the transfer (e.g. whether the data is transferred on a one-off or continuous basis).

· Continuous basis (services related to Hyland's hosted offerings or cloud services);

· One-off basis (technical support, professional services or other applicable services)

Nature of the processing

· The data is processes as part of the data exporter's and the data importer's regular business operations as well as on an *ad hoc* basis where a specific business need arises. 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.

Purpose(s) of the data transfer and further processing

· To provide the Services set forth in the Solution Provider Agreements.

The period for which the personal data will be retained, or, if that is not possible, the criteria used to determine that period:

· For hosting or cloud customers, data is retained for the duration of the applicable agreement, including any applicable transition period. Customer Personal data provided to Hyland during the performance of Secondary Support 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.

For transfers to (sub-) processors, also specify subject matter, nature and duration of the processing

· The data importer may use various processors to process the data for the purposes set out above. Such processors are typically engaged on the basis of a contract with an unlimited term. See also Section 3(d) of this DPA.

Competent supervisory authority

Unless otherwise stated in the DPA, 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 appropriate technical and organisational measures designed to ensure a level of security appropriate to the risk, including those security measures set forth in the Solution Provider Agreements and 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 organisational 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