Data Processing Addendum – Brazil

This Data Processing Addendum - Brazil together with all attachments and appendices ("Addendum") 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.

1. **DEFINITIONS**
    1. "Controller", "Processor", "Processing", and "National Authority" have the same meanings as in Article 5 of the LGPD.
    2. "Data Subject" means the subject of Personal Data.
    3. "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 Software, Inc.
    4. "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 Brazil. 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.
    5. "Personal Data Breach" means 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.
    6. "Required By Law" means that a statute, regulation, court order, or legal process, enforceable in a court of law, mandates the conduct.
    7. "Sensitive Personal Data" shall have the meaning given to it under Article 5 of the LGPD and also includes information about criminal history.
    8. "Sub-processor" means an entity that processes Personal Data at the request of Service Provider.
2. **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 Service 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 Addendum has violated, violates, or will violate Service Provider's or Hyland's obligations under applicable law.
    4. Disclosures of Personal Data. Service Provider may not disclose Personal Data to third parties unless the disclosure is (1) Required By Law, or (2) with the prior written consent of Hyland. Before disclosing Personal Data as Required By Law, Service Provider will immediately notify Hyland in writing of such required disclosure and will provide Hyland a reasonable opportunity to object to the request before Service Provider produces any Personal Data in response. Upon request, Service Provider will provide Hyland a copy of any Personal Data disclosed to a third party as Required by Law.
    5. Cross-Border Data Transfers. Service Provider will not transfer Personal Data outside of Brazil unless (1) Hyland has provided prior written permission for the transfer, and (2) in addition to the other requirements set forth in this Addendum, Service Provider ensures an adequate level

of protection in accordance with the LGPD or the transfer falls under a derogation in accordance with the LGPD.

3. **SERVICE PROVIDER'S SAFEGUARDS FOR PERSONAL DATA**
    1. Confidentiality Of Personal Data. Service Provider will maintain the confidentiality of all Personal Data. Service Provider has required employees responsible for Processing Personal Data to sign a confidentiality agreement prohibiting the disclosure of Personal Data Processed for Hyland to any third party except as permitted by this Addendum 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 the LGPD 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 within 24 hours of Service Provider's becoming aware of the incident and such 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 National 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: Person In Charge, 28500 Clemens Rd. Westlake, Ohio 44145, 440-788-5000, brazilprivacy@hyland.com, or such other person that Hyland may designate from time to time in writing to Service Provider without amending this Addendum. 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 National Authority and which National

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.

4. **SERVICE PROVIDER'S ASSISTANCE WITH AUDITS AND REQUESTS FROM DATA SUBJECTS**
    1. Information Technology Audits. Service Provider will permit Hyland, directly or through a contractor, to conduct audits of the information technology and information security controls to ensure that: (i) Service Provider is in compliance with this Addendum; and (ii) Service Provider provides the appropriate level of security for the Personal Data.

    2. 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 the LGPD.

    3. 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 LGPD. 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 five (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.

5. **SERVICE PROVIDER'S SUB-PROCESSORS**
    1. Consent To Processing By Sub-Processors. Service Provider will not disclose Personal Data to any sub-processor 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 Addendum 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 the LGPD; 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 Addendum 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 Addendum with respect to Personal Data shall survive the termination of the Service Agreement and of this Addendum 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 Data Processor, 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 including this Addendum, (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, unauthorised 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 7.1 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 Addendum 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. 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. 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: ***Employees*** - Past, potential, present and future staff of Hyland (including job candidates, volunteers, agents, independent contractors, interns, temporary and casual workers). ***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. ***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	The Personal Data transferred may concern the following categories: ***Employees*** Identification data: civil/marital status; first and last name; photograph; date and place of birth;

Processed	nationality; corporate identifier; gender. Contact details: address; telephone number (fixed and mobile); email address; fax number; emergency contact information. 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. National identifiers: national ID/passport number; tax ID; government identification number; driver's license, visa or immigration status. Academic and professional qualifications: degrees; titles; skills; language proficiency; training information; employment history; CV/résumé. 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. 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). Lifestyle: hobbies; social activities; holiday preferences. ***Vendors*** Identification data: first and last name; date of birth; place of birth; nationality; photograph; vendor ID. Contact details: address; professional email address; professional telephone number (including mobile telephone number). Professional details: job title; employer; academic and professional qualifications; data related to transactions involving goods and services. National identifiers: tax ID; government identification number. Financial data: bank account number; bank details. ***Website visitors*** 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. ***Customers, potential Customers and/or their staff, each as applicable*** 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.