DATA PROCESSING ADDENDUM

This Data Processing Addendum ("**DPA**") sets forth the Parties' obligations with respect to the processing and security of Personal Data in connection with the services listed in Schedule A to this DPA (the "**Services**"). The DPA is incorporated by reference into our Online Services Terms (the "**Terms of Services**"). You acknowledge that you, on your own behalf as an individual and on behalf of your employer or another legal entity (collectively, "**you**", "**your**" or the "**Organization**") have read and understood and agree to comply with this DPA, and are entering into a binding legal agreement with Devolutions inc. ("**Devolutions**") to reflect the Parties' agreement with regard to the Processing of Personal Data in the course of using or providing the Services. This DPA will not be valid and legally binding in respect of any individual or Organization that is not a Customer or an Authorized Affiliate. Both parties shall be referred to as the "**Parties**" and each, a "**Party**".

You represent and warrant that you have, or you were granted, full authority to bind the Organization and its Authorized Affiliates to this DPA. If you cannot, or do not agree to, comply with, and be bound by, this DPA or do not have authority to bind the Organization or any other entity, please do not supply or provide Personal Data to us.

In the course of providing the Services pursuant to the Terms of Services, we may process Personal Data on your behalf, in the capacity of a "Data Processor". The Parties agree to comply with the following provisions with respect to any Personal Data, each acting reasonably and in good faith.

If you need a signed copy of this DPA, you can send your request by email to privacy@devolutions.net.

1. Interpretation and definitions

1.1 The headings contained in this DPA are for convenience only and shall not be interpreted to limit or otherwise affect the provisions of this DPA.

1.2 References to clauses or sections are references to the clauses or sections of this DPA unless otherwise stated.

1.3 In addition to the terms defined elsewhere in this DPA, the terms below shall have the following meaning:

(a) "**Affiliate**" means an entity that a party controls or is controlled by, or with which a party is under common control. For purposes of this definition, "control" means direct or indirect ownership of more than fifty (50%) percent of the voting stock or equivalent ownership interest in an entity.

(b) "**Authorized Affiliate**" means any of Customer's Affiliate(s) which is permitted by Devolutions to use the Services pursuant to the Terms of Services entered into with or as agreed by Customer but has not entered into its own agreement with Devolutions.

(c) "**Customer**" means the Organization that has subscribed to a Service and is a party to the Terms of Services. For purpose of this DPA, unless otherwise specified, any reference to the Customer shall be deemed to include Authorized Affiliates.

(d) "**Data Controller**" means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the Processing of Personal Data.

(e) "**Data Processor**" means a natural or legal person, public authority, agency or other body which Processes Personal Data on behalf of the Data Controller.

(f) "**Data Protection Laws**" means, to the extent applicable to the Processing of Personal Data under the Terms of Service, the *General Data Processing Regulation* 2016/679 (the "**GDPR**"), other applicable EU and Member States' legislation relating to Personal Data protection; the United Kingdom *Data Protection Act* 2018 (the "**UK-GDPR**"), the Personal Information Protection and Electronic Documents Act (Canada) and substantially similar provincial laws; and the *California Consumer Privacy Act* of 2018 (the "**CCPA**").

(g) "**Data Subject**" means the individual to whom Personal Data relates.

(h) "**Member State**" means a country that is a member of the EU, of the European Economic Area and Switzerland.

(i) "**Personal Data**" means any information relating to an identified or identifiable individual; an identifiable individual is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that individual.

(j) "**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, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

(k) "**Restricted Transfer**" means a transfer of Personal Data by Devolutions to a Subprocessor; or an onward transfer of Personal Data from a Subprocessor to another Subprocessor, or between two establishments of a Subprocessor, in each case, where such transfer would be prohibited by Data Protection Laws in the absence of the Standard Contractual Clauses to be established. For the avoidance of doubt: (a) without limitation to the generality of the foregoing, the parties to this DPA intend that transfers of Personal Data from the EU or the UK to third countries shall be Restricted Transfers for such time and to such extent that such transfers would be prohibited by the GDPR or the UK-GDPR (as the case may be) in the absence of the Standard Contractual Clauses to be established; and (b) where a transfer of Personal Data is of a type authorized by Data Protection Laws in the exporting country, for example in the case of transfers from within the EU to a country which is approved by the European Commission as ensuring an adequate level of protection or any transfer which falls within a permitted derogation, such transfer shall not be a Restricted Transfer;

(l) "**Standard Contractual Clauses**" means (a) the Standard Contractual Clauses adopted by the European Commission in Decision 2021/914/EU of 4 June 2021 ("**New SCC**"), hereby incorporated by reference, or (b) if the transfer of Customer Personal Data is subject to Data Protection Laws of the UK, the Standard Contractual Clauses (controller to processor) adopted by the European Commission in Decision 2010/87/EC (the "**2010 SCC**"), which shall be deemed completed with the information set out in the Schedules to this DPA, in each case, as same may be amended, updated, completed or replaced from time to time to reflect changes in Data Protection Laws. Unless stated otherwise by Devolutions in

writing, the most current set of Standard Contractual Clauses adopted by the European Commission or UK's Information Commissioner's Office (as applicable) shall apply and deemed incorporated by reference. For the sake of clarity, Restricted Transfers between Devolutions and its Subprocessors shall be subject to Module Three (Processor to Processor) of the New SCC.

(m) "**Sub-processor**" means any person appointed by or on behalf of Devolutions to Process Personal Data on behalf of the Customer hereunder;

(n) "**Supervisory Authority**" means an independent public authority in charge of regulating privacy and data protection. This term shall include but not be limited to the Office of the Privacy Commissioner of Canada, and any supervisory public authority established pursuant to the GDPR or the UK-GDPR;

(o) "**UK**" means the United Kingdom.

(p) The terms "transfer" and "third country" shall have the same meaning as in the GDPR, and their cognate terms shall be construed accordingly.

2. Processing of Personal Data.

2.1 Roles of the Parties. Customer hereby appoints Devolutions as a Data Processor to Process the Personal Data on Customer's behalf through the Services. The Parties acknowledge and agree that with regard to the Processing of Personal Data pursuant to the Services, (i) Customer is the Data Controller, (ii) Devolutions is the Data Processor (unless Customer is a Processor, in which case Devolutions shall be Customer's Sub-processor), and (iii) Devolutions may engage Sub-processors pursuant to the requirements set forth in Section 4 below.

2.2 Customer's Processing of Personal Data. Customer shall, in its use of the Services, Process Personal Data in accordance with the requirements of Data Protection Laws. For the avoidance of doubt, Customer's instructions for the Processing of Personal Data shall comply with Data Protection Laws and Customer shall have sole responsibility for the lawful collection of Personal Data. Without limitation, Customer must collect, Process and transfer Personal Data to Devolutions in accordance with Data Protection Laws and ensure that Devolutions can lawfully Process such Personal Data in accordance with the Terms of Service and this DPA. Customer shall be fully responsible for the actions and omissions of its authorized users and their use of the Services. In any instance where Customer is a Data Processor, Customer warrants to Devolutions that Customer's instructions, including appointment of Devolutions as a Data Processor or Sub-processor, have been authorized by the relevant Data Controller.

2.3 Devolutions' Processing of Personal Data. Devolutions shall Process Personal Data in compliance with Data Protection Laws and only as described and subject to the limitations provided below to provide Customer the Services in accordance with Customer's documented instructions. Customer agrees that the foregoing purposes, along with the Terms of Services and related Service documentation as updated or amended from time to time, and Customer's use and configuration of features in the Services, are Customer's complete and final documented instructions to Devolutions for the Processing of Personal Data and that any additional or alternate instructions must be agreed in writing between Customer and Devolutions. Without limiting the foregoing, Devolutions may also Process Personal Data as required by applicable laws; in such a case, Devolutions shall inform the Customer of the legal requirement before Processing, unless that law prohibits such information. If Devolutions believes that any instruction from Customer is in violation of, or would result in Processing in violation

of applicable laws, it shall notify Customer immediately. Devolutions will maintain processing records required under the GDPR and the UK-GDPR, and, to the extent applicable to the processing of Personal Data on behalf of Customer, make them available to Customer upon request.

2.4 Details of the Processing. The subject-matter of Processing of Personal Data by Devolutions is the performance of the Services pursuant to the Terms of Service. The nature and purpose of the Processing, the duration of the Processing, the types of Personal Data and categories of Data Subjects Processed under this DPA are further specified in Schedule B (Details of the Processing) to this DPA. Customer may make reasonable amendments to Schedule B by written notice to Devolutions from time to time as Customer reasonably considers necessary to meet the requirements of applicable laws. Devolutions agrees to reasonably notify Customer in writing if it believes that Schedule B is not accurate or otherwise does not meet the requirements of applicable laws.

2.5 Devolutions' Personnel and Confidentiality. Devolutions shall ensure that its personnel engaged in the Processing of Personal Data are aware of, and subject to, enforceable obligations to maintain the confidentiality of the Personal Data and to comply with the other relevant obligations and restrictions of this DPA. Devolutions shall ensure in each case that access is strictly limited to those individuals who need to know or access the relevant Personal Data, as strictly necessary for the purposes of performing the Services.

2.6 Disclosure of Personal Data. Devolutions will not disclose the Personal Data to a third party unless (a) it obtains Customer's prior written consent; (b) as required by a court of competent jurisdiction; (c) as required by applicable law (in such a case, Devolutions shall inform the Customer of the legal requirement before the disclosure, unless that law prohibits such information), or (d) on a "need-to-know" basis under an obligation of confidentiality to its legal counsel(s), data protection advisor(s) and accountant(s).

2.7 Disclosure of Personal Data to governmental authorities. Devolutions shall not disclose Personal Data to law enforcement agencies and/or other government agencies unless such disclosure is mandatory under applicable law. Devolutions shall notify Customer of any such request for such disclosure, unless such notification is prohibited by applicable law, and to the extent possible, such notice shall be given at the earliest opportunity prior to the disclosure.

2.8 Retention and Deletion of Personal Data. Devolutions may retain Personal Data only for the period of time required for Devolutions to perform the Services, as otherwise mentioned in the Terms of Service or in accordance with applicable law. Devolutions will permanently delete all copies of Personal Data in its possession or control at the expiration of such applicable retention period.

3. Rights of Data Subjects

3.1 Data Subject Requests. If a Data Subject exercises his/her rights under Data Protection Laws in connection with Personal Data Processed by Devolutions on behalf of Customer (each a "**Data Subject Request**"), Devolutions will redirect the Data Subject Request to Customer or indicate to the Data Subject that (s)he must submit the Data Subject Request to Customer. Customer will be responsible for responding to any such Data Subject Request and Devolutions will comply with reasonable requests by Customer to assist with its response. Customer shall be responsible for any costs arising from Devolutions' provision of such assistance.

3.2 Assistance to Customer. To the extent Customer, in its use of the Services, does not have the ability to directly receive Data Subject Requests, Devolutions will, in a manner consistent with its role as a Data Processor and taking into account the nature of the Processing and the data available to Devolutions, (i) make available

Personal Data of Data Subjects to Customer, and (ii) make commercially reasonable efforts to assist Customer, insofar as this is possible and to the extent that Devolutions is legally permitted to do so, for the fulfilment of Customer's obligation to respond to Data Subject Requests. Customer shall be responsible for any costs arising from Devolutions' provision of such assistance.

4. Authorization Regarding Sub-processors

4.1 Appointment of Sub-processors. Customer grants Devolutions a general authorization to continue using and to engage third-party Sub-processors to Process Personal Data on Devolutions' behalf in connection with the provision of the Services.

4.2 List of Current Sub-processors. The Sub-processors currently engaged by Devolutions to Process Personal Data in the course of the Services are listed at https://devolutions.net/legal/ (the "**Sub-Processor List**"). The Sub-Processor List as of the date of publication of this DPA is hereby authorized by the Customer.

4.3 Changes to the Sub-Processors List and Customer's Objection Right. Devolutions may, by giving no less than thirty (30) days' notice to Customer, add or make changes to the Sub-Processors List. Customer must subscribe to receive notice of updates to the list of Sub-processors by sending its request at privacy@devolutions.net. Customer may object to Devolutions' appointment of a new Sub-processor by notifying Devolutions in writing within fourteen (14) calendar days of such notice on reasonable grounds relating to the protection of Personal Data. Failure to object to such new Sub-processor in writing within such period shall be deemed as acceptance of the new Sub-processor. In the event Customer reasonably objects to a new Sub-processor, Devolutions will use reasonable efforts to make available to Customer a change in the Services or recommend a commercially reasonable change to Customer's configuration or use of the Services to avoid Processing of Personal Data by the objected-to new Sub-processor without unreasonably burdening the Customer. If Devolutions is unable to make available such change to the mutual satisfaction of the Parties within a reasonable period of time, either Party may, as a sole remedy, terminate the applicable Terms of Services and this DPA with respect only to those Services which cannot be provided by Devolutions without the use of the objected-to new Sub-processor, and Customer will be entitled to a pro-rata refund of the fees prepaid for such Services. Until a decision is made regarding the new Sub-processor, Devolutions may temporarily suspend the Processing of the affected Personal Data and/or suspend access to the Services. Customer will have no further claims against Devolutions due to the termination of the Terms of Services in the situation described in this Section 4.3.

4.4 Agreements with Sub-processors. Devolutions has entered into a written and binding agreement with each Sub-processor, which contains appropriate safeguards for the protection of Personal Data in accordance with Data Protection Laws. Devolutions shall remain liable to the Customer for any breach of the DPA caused by its Sub-processors.

4.5 Emergency Replacement. Devolutions may replace a Sub-processor if the need for the change is urgent and necessary to provide the Services and the reason for the change is beyond Devolutions' reasonable control. In such instance, Devolutions shall notify Customer of the replacement as soon as reasonably practicable, and Customer shall retain the right to object to such new sub-processor pursuant to Section 4.3 above.

5. Security

5.1 Security Measures. Devolutions shall maintain industry-standard technical, physical and organizational measures for protection of the security, confidentiality and integrity of Personal Data (including protection against

unauthorized or unlawful Processing and against accidental or unlawful destruction, loss or alteration or damage, unauthorized disclosure of, or access to, Personal Data), in accordance with Data Protection Laws ("**Security Measures**"). The Security Measures shall include the measures detailed under Schedule C. The foregoing does not release Customer from its duty to implement and maintain its own privacy protections and security measures in respect of the Personal Data that it processes whether as a controller or as a processor.

5.2 Audits. Upon Customer's reasonable written request at reasonable intervals, and subject to the confidentiality obligations set forth in the Terms of Services and this DPA, Devolutions shall make available to Customer that is not a competitor of Devolutions (or to Customer's independent auditor reasonably accepted by Devolutions and bound by confidentiality obligations satisfactory to Devolutions, "**Auditor**") all information reasonably necessary to demonstrate compliance with this DPA and the obligations laid down in applicable Data Protection Laws. Devolutions will address a Customer's request for audit as follows: (1) Devolutions will answer questions asked by the Customer; and (2) in the event Customer reasonably considers that the answer provided by Devolutions justifies further analysis, Devolutions shall, in agreement with the Customer, allow for and contribute to audits, including inspections, conducted by Customer or its Auditor; provided, however, that (i) Customer shall provide Devolutions with an audit notice request that will include a detailed written audit plan reviewed and approved by Devolutions' Chief Information Security Officer and provide for compliance with Devolutions' on-site security policies and procedures; (ii) such audits must take place only in the presence of a representative of Devolutions' Chief Information Security Officer or such other person designated by the appropriate representative; (iii) the audits shall not be permitted to disrupt Devolutions' processing activities, cause damages to Devolutions' premises, equipment, personnel and business or compromise the security or confidentiality of personal data pertaining to Devolutions' other customers; (iv) any data, document, results and conclusions, including the documents reflecting the outcome of the audit and/or the inspections, shall only be used by Customer to assess compliance with this DPA, and shall not be used for any other purpose or disclosed to any third party without Devolutions' prior written approval; and (v) upon Devolutions' request, Customer shall return all records or documentation in Customer's possession or control provided by Devolutions in the context of the audit and/or the inspection.

5.3 Audit costs. Customer shall be fully responsible for bearing all the costs and expenses arising from or related to this Section and shall reimburse Devolutions for any time spent for in relation to any on-site audit at the Devolutions' then-current professional services rates, which shall be made available to Customer upon request. Before the commencement of any such on-site audit, Customer and Devolutions shall mutually agree upon the scope, timing, and duration of the audit in addition to the reimbursement rate for which Customer shall be responsible. All reimbursement rates shall be reasonable, taking into account the resources expended by Devolutions. Customer shall promptly notify Devolutions with information regarding any noncompliance discovered during the course of an audit.

5.4 Data Protection Impact Assessment and Prior Consultation. Upon Customer's request, Devolutions shall provide Customer, at Customer's cost, with reasonable cooperation and assistance needed to fulfil Customer's obligation under Data Protection Laws to carry out a data protection impact assessment related to Customer's use of the Services, to the extent Customer does not otherwise have access to the relevant information, and to the extent such information is available to Devolutions. Devolutions shall provide reasonable assistance to Customer with respect to its collaboration or prior consultation with a Supervisory Authority to the extent required under the Data Protection Laws and at Customer's cost.

6. Security Incident Management and Notification

6.1 Security Incident. If Devolutions becomes aware of a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Personal Data while processed by Devolutions or by its sub-processors (each a "**Security Incident**"), Devolutions will (i) notify Customer of the Security Incident without undue delay after becoming aware of such Security Incident by providing Customer with (a) a description of the circumstances surrounding the Security Incident; (b) what Personal Data is affected; (c) how many Data Subjects are affected; (d) what remedial action to limit damage has been and will be undertaken; and (e) a point of contact at Devolutions, and any other information that a processor must provide to a controller under Data Protection Laws to the extent such information is reasonably available to Devolutions or as such information becomes available to Devolutions; (ii) investigate the Security Incident and; and (iii) take reasonable steps to mitigate the effects and to minimize any damage resulting from the Security Incident, to the extent it is within Devolutions' reasonable control. The obligations herein shall not apply to Security Incidents that are caused by Customer or Customer's users and/or their instructions.

6.2 Notifications. Notification of Security Incidents will be delivered to one or more of Customer's representatives by any means Devolutions selects, including via email. It is Customer's sole responsibility to ensure that its contact information with Devolutions remains accurate. Customer is solely responsible for complying with its obligations under Data Protection Laws applicable to it and for fulfilling any reporting obligations to regulators (including Supervisory Authorities) and notification obligations related to any Security Incident. Customer must notify Devolutions promptly about any possible misuse of, or security incident related to, its accounts or authentication credentials with Devolutions.

6.3 General Assistance to Customer. Devolutions will make reasonable efforts to assist Customer in fulfilling its obligations under Data Protection Laws to notify the relevant Supervisory Authority and data subjects about such Security Incident. Devolutions' report or response to a Security Incident under this section shall not be construed as an acknowledgement by Devolutions of any fault or liability with respect to the Security Incident.

7. Authorized Affiliates

7.1 Contractual Relationship. The Parties acknowledge and agree that, by entering into the Terms of Service, Customer enters into the DPA on behalf of itself and, as applicable, in the name and on behalf of its Authorized Affiliates, thereby establishing a separate DPA between Devolutions and each such Authorized Affiliate subject to the provisions of the Agreement and of this Section 7 and Section 8. Each Authorized Affiliate agrees to be bound by the obligations under this DPA and, to the extent applicable, the Terms of Service. For the avoidance of doubt, an Authorized Affiliate is not and does not become a party to the Terms of Service and is only a party to the DPA. All access to and use of the Services by Authorized Affiliates must comply with the terms and conditions of the Terms of Service and any violation of the terms and conditions of the Terms of Service by an Authorized Affiliate shall be deemed a violation by Customer.

7.2 Communication. The Customer that is the contracting party to the Terms of Service shall remain responsible for coordinating all communication with Devolutions under this DPA and be entitled to make and receive any communication in relation to this DPA on behalf of its Authorized Affiliates.

7.3 Rights of Authorized Affiliates. Where an Authorized Affiliate becomes a party to the DPA with Devolutions, it shall to the extent required under Data Protection Laws be entitled to exercise the rights and seek remedies under this DPA, subject to the following:

7.3.1 Except where applicable Data Protection Laws require the Authorized Affiliate to exercise a right or seek any remedy under this DPA against Devolutions directly by itself, the parties agree that (i) solely the Customer that is the contracting party to the Terms of Service shall exercise any such right or seek any such remedy on behalf of the Authorized Affiliate, and (ii) the Customer that is the contracting party to the Terms of Service shall exercise any such rights under this DPA not separately for each Authorized Affiliate individually but in a combined manner for all of its Authorized Affiliates together (as set forth, for example, in Section 7.3.2, below).

7.3.2 The Parties agree that Customer shall, when carrying out an audit pursuant to section 5.2, take all reasonable measures to limit any impact on Devolutions and its Sub-processors by combining, to the extent reasonably possible, several audit requests carried out on behalf of different Authorized Affiliates in one single audit.

8. Limitation of Liability

To the maximum extent permitted by applicable law, and notwithstanding any limitation of liability that may be provided in the Terms of Services from time to time, in no event shall the aggregate liability of Devolutions arising out of or related to this DPA and all DPAs between Authorized Affiliates and Devolutions, or arising out of a breach by Devolutions of applicable Data Protection Laws, whether in contract, tort, negligence or under any other theory of liability, exceed the subscription fees paid by Customer during the 12-month period preceding the event leading to such liability. For the avoidance of doubt, (i) the present limitation of liability shall represent the maximum aggregate liability of Devolutions for all claims from Customer and its Authorized Affiliates arising out of or related to each and all DPAs established hereunder, and shall not be understood to apply individually and severally to Customer and/or to any Authorized Affiliate that is a contractual party to any such DPA, and (ii) should the aggregate damages and indemnities paid by Devolutions to Customer and/or its Authorized Affiliates hereunder exceed the limitation of liability provided in the Terms of Services, Customer and/or its Authorized Affiliates will be precluded from claiming any other damages under the Terms of Services (to the extent such damages are covered by such limitation of liability).

9. Restricted Transfers

9.1 Standard Contractual Clauses. To the extent Devolutions' Processing of Personal Data on behalf of Customer and/or its Authorized Affiliates under this DPA or pursuant to the Services involves a Restricted Transfer the Standard Contractual Clauses shall be entered into between the relevant parties to the Restricted Transfer.

9.2 Cross-Border Transfers by Devolutions. If Devolutions transfers Personal Data to a Sub-processor located in a third country or to an international organization, it will ensure that such transfer will be subject to appropriate safeguards and be documented in accordance with the requirements of Data Protection Laws. Without limiting the generality of the foregoing, with respect to the transfer of Personal Data from the EU or the UK, Devolutions will ensure that such transfer will be made: (i) to a country that offers adequate level of data protection under or pursuant to the adequacy decisions published by the relevant data protection authorities of the EU or the UK, as applicable, without any further safeguard being necessary; or (ii) to an entity or group of entities with whom Devolutions has entered into the then applicable Standard Contractual Clauses.

9.3 Restricted Transfers subject to the New SCC. The parties agree that, for the purposes of the New SCC :

9.3.1 Regarding Restricted Transfers between Devolutions and Sub-processors located in third countries, the parties shall be deemed to have selected module three (transfer processor to processor);

9.3.2 For the purpose of clause 9 (Use of Subprocessors), the parties shall be deemed to have selected *Option 2 General Written Authorisation* as per section 4 of this DPA;

9.3.3 For the purposes of clause 17 (Governing Law), the parties shall be deemed to have selected the laws of the Republic of Ireland; and

9.3.4 For the purposes of clause 18 (Choice of Forum and Jurisdiction), the parties shall be deemed to have selected the courts of Dublin, Ireland to resolve any dispute arising from the New SCC.

9.4 Variations to the Standard Contractual Clauses. Customer may: (a) by at least thirty (30) calendar days' written notice to Devolutions from time to time make any variations to the Standard Contractual Clauses, as they apply to Restricted Transfers which are subject to a particular Data Protection Law, which are required, as a result of any change in, or decision of a competent authority under, that Data Protection Law, to allow those Restricted Transfers to be made (or continue to be made) without breach of that Data Protection Law; and (b) propose any other variations to this DPA which Customer reasonably considers to be necessary to address the requirements of any Data Protection Law. If Customer gives such notice: (i) Customer shall not unreasonably withhold or delay agreement to any consequential variations to this DPA proposed by Devolutions; and (ii) the Parties shall promptly discuss the proposed variations and negotiate in good faith with a view to agreeing and implementing those or alternative variations designed to address the requirements identified in Customer's notice as soon as is reasonably practicable.

9.5 Instructions. This DPA and the Terms of Service are Customer's complete and final documented instructions to Devolutions for the Processing of Personal Data on behalf of Customer and/or its Authorized Affiliates. Any additional or alternate instructions must be agreed upon separately with Customer.

10. Miscellaneous

10.1 Conflicts. In the event of any conflict or inconsistency between:

10.1.1 the provisions of this DPA and the Terms of Service, the provisions of this DPA shall control with respect to the subject matter set forth herein; all the terms, provisions and requirements contained in the Terms of Service shall remain in full force and effect except to the extent they conflict with and are superseded by this DPA.

10.1.2 the body of this DPA and any of its Schedules (not including the Standard Contractual Clauses) and the Standard Contractual Clauses, the Standard Contractual Clauses shall prevail.

10.2 Term. This DPA shall remain in force for as long as Devolutions processes Personal Data on behalf of Customer in the course of the Services. Upon termination of the Terms of Services, this DPA will be terminated accordingly.

10.3 Binding Effect. The terms, provisions and conditions of this DPA shall be binding upon and inure to the benefit of each respective Party and their respective legal representatives, successors and assigns.

11. List of Schedules

Schedule A: Services
Schedule B: Details of Processing of Personal Data
Schedule C: Security Measures

12. How to Contact Devolutions

If Customer believes that Devolutions is not adhering to its privacy or security commitments, Customer may contact customer support (https://devolutions.net/support) or Devolutions' Director of Privacy (privacy@devolutions.net), or use Devolutions' mailing address below:

Devolutions inc.
1000, rue Notre-Dame
Lavaltrie (Québec) J5T 1M1
Canada

GDPREP.ORG has been appointed as Devolutions' representative in the European Union and United Kingdom for data protection matters pursuant to Article 27 of the EU GDPR and of the UK GDPR. GDPREP.ORG can be contacted in addition to Devolutions' points of contact above, at the following coordinates:

UK Address / Contact Information

a: Studio Office, 25A Archer Road, Penarth, CF64 3HJ
w: www.gdprep.org
e: info@gdprep.org
t: +44 (0) 7810 883333

EU Address / Contact Information

a: Suite 10357, 5 Fitzwilliam Square, Dublin 2, Ireland, D02 R744
w: www.gdprep.org
e: info@gdprep.org
t: +44 (0) 7810 883333

SCHEDULE A – SERVICES

For purposes of this DPA, a Service consists of delivering functional capabilities as licensed, configured and used by Customer and its users in respect of the following products and tools:

- Password Hub (Business & Personal)
- Lucid (authentication and identification service)
- Devolutions RDM Online Services, including:
    - Devolutions Online Database
    - Devolutions Online Drive
    - Devolutions Online Backup
    - Custom Installer Service

SCHEDULE B – DETAILS OF PROCESSING OF PERSONAL DATA
(Annex I of the New SCC; Appendix 1 of the 2010 SCC)

Nature and purpose of Processing

Devolutions will Process Personal Data as necessary to perform the Services to Customer pursuant to the Terms of Service and as further instructed by Customer in its use of the Services or otherwise in accordance with Section 2.3 of the DPA.

Duration of Processing

Subject to Section 2.8 of the DPA, the duration of the Processing shall be for the duration of Customer's right to use the Services, unless otherwise in accordance with Customer instructions and the terms of the DPA.

Categories of Data Subjects

Depending on Customer's use of the Services, categories of Data Subjects may include, without limitation:

- Customer's representatives and end users (current, former, prospective), such as employees, contractors and collaborators;
- Customer's customers and contact persons (natural persons) or employees, contractors or collaborators of legal entities doing business with Customer (current, former, prospective);
- Any other categories of Data Subjects as identified in records maintained by Customer acting as Data Controller pursuant to Article 30 of the GDPR.

Types of Personal Data

Depending on Customer's use of the Services, the types of Personal Data processed by Devolutions when providing the Services may include, without limitation:

- Personal Data that Customer elects to submit to the Services, which may include any categories of Personal Data identified in records maintained by Customer acting as controller pursuant to Article 30 of the GDPR;
- The types of Personal Data expressly identified in Article 4 of the GDPR.

Competent Supervisory Authority: Data Protection Commission of Ireland

SCHEDULE C – SECURITY MEASURES
(Annex II of the New SCC; Appendix 2 of the 2010 SCC)

Without limiting the generality of the foregoing, Devolutions' Security Measures must include the following elements and shall apply to all Personal Data Processed by Devolutions hereunder:

(a) Security Awareness and Training. A mandatory annual security awareness and training program for all members of Devolutions' workforce (including management), which includes: (i) training on how to implement and comply with its Security Program; and (ii) promoting a culture of security awareness through periodic communications from senior management with employees.

(b) Background Assessment and Monitoring. Policies and procedures to conduct background assessments for all current and prospective members of Devolutions' workforce who have access to Personal Data including criminal background verification procedures to the extent allowed under applicable law. Such assessments shall be performed on a regular basis to ensure members of Devolutions' workforce continue to comply with applicable standards and requirements related thereto.

(c) Access Controls. Policies, procedures, and logical controls: (i) to limit access to its information systems and the facility or facilities in which they are housed to properly authorized persons with a genuine need-to-know; (ii) to ensure that the least amount of Personal Data is made accessible to authorized persons as required to carry out their job-related functions; (iii) to prevent those workforce members and others who should not have access from obtaining access; and (iv) to remove access in a timely basis in the event of a change in job responsibilities or job status or as a result of a failed background assessment. These policies, procedures and logical controls include the use of multi-factor authentication and the implementation of a password policy guaranteeing that passwords are of a reasonable level of complexity.

(d) Physical and Environmental Security. Controls that provide reasonable assurance that physical access to Devolutions' facilities where Personal Data is stored, including physical servers, is limited to properly authorized individuals and that environmental controls are established to detect, prevent and control destruction due to environmental extremes. These controls include: (i) logging and monitoring of unauthorized access attempts to such facilities; (ii) camera surveillance systems at critical internal and external entry points of Devolutions' facilities; (iii) systems that monitor and control the air temperature and humidity at appropriate levels for the computing equipment; and (d) Uninterruptible Power Supply (UPS) modules and backup generators that provide back-up power in the event of an electrical failure.

(e) Data Incident Procedures. A data incident response plan that includes procedures to be followed in the event of a Security Incident. Such procedures include: (i) formation of an internal incident response team with a response leader; (ii) assessing the risk the incident poses and determining who may be affected; (iii) internal reporting as well as a notification process in the event of unauthorized disclosure of Personal Data; (iv) keeping a record of what was done and by whom to help in later analysis and possible legal action; and (v) conducting and documenting root cause analysis and remediation plan.

(f) Contingence Planning. Policies and procedures for responding to an emergency or other occurrence (for example, fire, vandalism, system failure, pandemic flu, and natural disaster) that could damage Personal Data or production systems that contain Personal Data. Such procedures include: (i) a policy for performing periodic backups of production file systems and databases containing Customer Personal Data, according to a defined schedule; (ii)

a formal disaster recovery plan for Devolutions' facilities, including requirements for the disaster plan to be tested on a regular basis; (iii) a formal process to address the framework by which an unplanned event might be managed in order to minimize the loss of vital resources.

(g) Audit Controls. Hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use electronic information. Such mechanisms must ensure that actions are attributable to an identifiable individual.

(h) Data Integrity. Policies and procedures to ensure the confidentiality, integrity, and availability of Customer Personal Data and protect it from disclosure, improper alteration, or destruction.

(i) Storage and Transmission Security. Security measures to guard against unauthorized access to Customer Personal Data that is being transmitted over a public electronic communications network or stored electronically. Such measures include (i) limiting the use of portable storage devices, such as USB (Universal Serial Bus) drives, to store or transfer Customer Personal Data to the extent demonstrably necessary to fulfill a specific and documented purpose; and (ii) requiring strong encryption of any Customer Personal Data stored at rest on our systems and in transit over the network.

(j) Assigned Security Responsibility. Assigning responsibility for the development, implementation, and maintenance of its Information Security Program, including: (i) designating a security official with overall responsibility; and (ii) defining security roles and responsibilities for individuals with security responsibilities.

(k) Testing. Regularly testing the key controls, systems and procedures of its Security Program to validate that they are properly implemented and effective in addressing the threats and risks identified. Such testing must be performed annually by an independent external firm. Where applicable, such testing includes: (i) internal risk assessments; and (ii) ISO 27001 certification and Service Organization Control 2 (SOC2) audit reports (or industry-standard successor reports).

(l) Logging and Monitoring. Active network and systems logging and monitoring, including error logs on servers, disks and security events for any potential problems. Such logging and monitoring includes: (i) reviewing changes affecting systems handling authentication, authorization, and auditing; (ii) reviewing privileged access to Devolutions' production systems at regular intervals; and (iii) engaging third Parties to perform network vulnerability assessments and penetration testing on a regular basis.

(m) Change and Configuration Management. Maintaining policies and procedures for managing changes Devolutions makes to production systems, applications, and databases. Such policies and procedures must include: (i) a process for documenting, testing and approving the patching and maintenance of the Service; (ii) a security patching process that requires patching systems in a timely manner based on a risk analysis; and (iii) a process for Devolutions to utilize a Third Party to conduct web application level security assessments.

(n) Program Adjustments. Devolutions must monitor, evaluate, and adjust, as appropriate, the Security Program in light of: (i) any relevant changes in technology and any internal or external threats to Devolutions, Customer Personal Data; (ii) security and data privacy regulations applicable to Customer and/or Devolutions; and (iii) Devolutions' own changing business arrangements, such as mergers and acquisitions, alliances and joint ventures, outsourcing arrangements, and changes to information systems.

(o) Devices. All laptop and desktop computing devices utilized by Devolutions when accessing Customer Personal Data must: (i) be equipped with strong full disk encryption; (ii) have up to date virus and malware detection and prevention software installed with virus definitions updated on a regular basis; and (iii) maintain virus and malware detection and response software. This shall include, but not be limited to, promptly implementing any applicable security-related enhancement or fix made available by supplier of such software.