

## Data Processing Agreement — Sendlinx Inc.

This Data Processing Agreement ("**Agreement**") forms part of the Contract for Services ("**Principal Agreement**") between

\_\_\_\_\_  
\_\_\_\_\_

(the "**Company**") and

\_\_\_\_\_  
\_Sendlinx Inc\_\_\_\_\_

(the "Data Processor")  
(together as the "**Parties**")

WHEREAS

(A) The Company acts as a Data Controller.

(B) The Company wishes to subcontract certain Services, which imply the processing of personal data, to the Data Processor.

(C) The Parties seek to implement a data processing agreement that complies with the requirements of the current legal framework in relation to data processing and with the Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).

(D) The Parties wish to lay down their rights and obligations.

IT IS AGREED AS FOLLOWS:

### 1. Definitions and Interpretation

1.1 Unless otherwise defined herein, capitalized terms and expressions used in this Agreement shall have the following meaning:

1.1.1 "Agreement" means this Data Processing Agreement and all Schedules;

1.1.2 "Company Personal Data" means any Personal Data Processed by a Contracted Processor on behalf of Company pursuant to or in connection with the Principal Agreement;

1.1.3 "Contracted Processor" means a Subprocessor;

1.1.4 "Data Protection Laws" means EU Data Protection Laws and, to the extent applicable, the data protection or privacy laws of any other country;

1.1.5 "EEA" means the European Economic Area;

1.1.6 "EU Data Protection Laws" means EU Directive 95/46/EC, as transposed into domestic legislation of each Member State and as amended, replaced or superseded from time to time, including by the GDPR and laws implementing or supplementing the GDPR;

1.1.7 "GDPR" means EU General Data Protection Regulation 2016/679;

1.1.8 "Data Transfer" means:

1.1.8.1 a transfer of Company Personal Data from the Company to a Contracted Processor; or

1.1.8.2 an onward transfer of Company Personal Data from a Contracted Processor to a Subcontracted Processor, or between two establishments of a Contracted Processor, in each case, where such transfer would be prohibited by Data Protection Laws (or by the terms of data transfer agreements put in place to address the data transfer restrictions of Data Protection Laws);

1.1.9 "Services" means the File Transfer services the Company provides.

1.1.10 "Subprocessor" means any person appointed by or on behalf of Processor to process Personal Data on behalf of the Company in connection with the Agreement.

1.2 The terms, "Commission", "Controller", "Data Subject", "Member State", "Personal Data", "Personal Data Breach", "Processing" and "Supervisory Authority" shall have the same meaning as in the GDPR, and their cognate terms shall be construed accordingly.

## **2. Processing of Company Personal Data**

2.1 Processor shall:

2.1.1 comply with all applicable Data Protection Laws in the Processing of Company Personal Data; and

2.1.2 not Process Company Personal Data other than on the relevant Company's documented instructions.

2.2 The Company instructs Processor to process Company Personal Data.

## **3. Processor Personnel**

Processor shall take reasonable steps to ensure the reliability of any employee, agent or contractor of any Contracted Processor who may have access to the Company Personal Data, ensuring in each case that access is strictly limited to those individuals who need to know / access the relevant Company Personal Data, as strictly necessary for the purposes of the Principal Agreement, and to comply with Applicable Laws in the context of that individual's duties to the Contracted Processor, ensuring that all such individuals are subject to confidentiality undertakings or professional or statutory obligations of confidentiality.

## **4. Security**

4.1 Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of Processing as well as the risk of varying likelihood and severity for the rights and

freedoms of natural persons, Processor shall in relation to the Company Personal Data implement appropriate technical and organizational measures to ensure a level of security appropriate to that risk, including, as appropriate, the measures referred to in Article 32(1) of the GDPR.

4.2 In assessing the appropriate level of security, Processor shall take account in particular of the risks that are presented by Processing, in particular from a Personal Data Breach.

## **5. Subprocessing**

5.1 Controller gives general authorisation to Processor for the addition or replacement of data processors under the conditions set out in this Agreement. Controller will be offered the possibility to object to changes concerning the addition or replacement of data processors, but the objection may not be disproportionate.

5.2 Processor enters into a written data processing agreement with all permitted sub-processors. Processor shall ensure that sub-processors are contractually bound to the same or higher obligations with respect to the processing as those which Processor is bound to under this Agreement.

## **6. Data Subject Rights**

6.1 Taking into account the nature of the Processing, Processor shall assist the Company by implementing appropriate technical and organisational measures, insofar as this is possible, for the fulfilment of the Company obligations, as reasonably understood by Company, to respond to requests to exercise Data Subject rights under the Data Protection Laws.

6.2 Processor shall:

6.2.1 promptly notify Company if it receives a request from a Data Subject under any Data Protection Law in respect of Company Personal Data; and

6.2.2 ensure that it does not respond to that request except on the documented instructions of Company or as required by Applicable Laws to which the Processor is subject, in which case Processor shall to the extent permitted by Applicable Laws inform Company of that legal requirement before the Contracted Processor responds to the request.

## **7. Personal Data Breach**

7.1 Processor shall notify Company without undue delay upon Processor becoming aware of a Personal Data Breach affecting Company Personal Data, providing Company with sufficient information to allow the Company to meet any obligations to report or inform Data Subjects of the Personal Data Breach under the Data Protection Laws.

7.2 Processor shall co-operate with the Company and take reasonable commercial steps as are directed by Company to assist in the investigation, mitigation and remediation of each such Personal Data Breach.

## **8. Data Protection Impact Assessment and Prior Consultation**

8.1 Processor shall provide reasonable assistance to the Company with any data protection impact assessments, and prior consultations with Supervising Authorities or other competent data privacy authorities, which Company reasonably considers to be required by article 35 or 36 of the GDPR or equivalent provisions of any other Data Protection Law, in each case solely in relation to Processing of Company Personal Data by, and taking into account the nature of the Processing and information available to, the Contracted Processors.

8.2 Controller shall indemnify and hold harmless Processor, its officers, directors, employees, contractors, and agents from and against all claims, liabilities, administrative fines, suits, judgments, actions, investigations, settlements, penalties, fines, damages and losses, demands, costs, expenses, and fees including reasonable attorneys' fees and expenses, arising out of or in connection with any claims, demands, investigations, proceedings, or actions brought by Data Subjects, legal persons (e.g., corporations and organizations), or supervisory authorities under the Data Protection Laws that apply to the Processor or any Sub-processor engaged by Processor in respect of the Personal Data Processed under this DPA and under the General Data Protection Regulation.

## 9. Deletion or return of Company Personal Data

9.1 Subject to this section 9 Processor shall promptly and in any event within

10 business days of the date of cessation of any Services involving the Processing of Company Personal Data (the "Cessation Date"), delete and procure the deletion of all copies of those Company Personal Data.

## 10. Audit rights

10.1 Processors shall make the processing systems, facilities and supporting documentation relevant to the processing of Personal Data available for an audit by a qualified independent assessor selected by Processor. Processor will provide reasonable and necessary cooperation to such audits and will ensure that its subcontractors do likewise.

10.2 An audit may be performed during Processor's normal working days and normal working hours, no more than once per year or if requested by a relevant authority, subject to notice given in advance with a reasonable notice period. The audit may take place at Processor's place of business by inspecting the stored Controller Personal Data in a storage facility or data centre and the Processing activities taking place at the premises of Processor in accordance with Processor's security and access policies.

10.3 Controller shall bear the costs of any audit that is requested additionally to the yearly audit described in 6.1.

## 11. Data Transfer

11.1 The Processor may not transfer or authorize the transfer of Data to countries outside the EU and/or the European Economic Area (EEA) without the prior written consent of the Company. If personal data processed under this Agreement is transferred from a country within the European Economic Area to a country outside the European Economic Area, the Parties shall ensure that the personal data are adequately protected. To achieve this, the Parties shall, unless agreed otherwise, rely on EU approved standard contractual clauses for the transfer of personal data.

## **12. General Terms**

12.1 Confidentiality. Each Party must keep this Agreement and information it receives about the other Party and its business in connection with this Agreement ("Confidential Information") confidential and must not use or disclose that Confidential Information without the prior written consent of the other Party except to the extent that:

- (a) disclosure is required by law;
- (b) the relevant information is already in the public domain.

12.2 Notices. All notices and communications given under this Agreement must be in writing and will be delivered personally, sent by post or sent by email to the address or email address set out in the heading of this Agreement at such other address as notified from time to time by the Parties changing address.

## **13. Governing Law and Jurisdiction**

13.1 This Agreement is governed by the laws of Ontario.

13.2 Any dispute arising in connection with this Agreement, which the Parties will not be able to resolve amicably, will be submitted to the exclusive jurisdiction of the courts of Ontario, Canada.

13.3 Any standard terms of business and other standard or special terms and conditions of Controller do not apply to this Agreement and are explicitly dismissed by Processor.

13.4 Processor does not have the right to transfer its rights and obligations under this Agreement to third parties without Controller's prior written consent.

## **14. Changes and Renegotiations**

14.1 Deviations from and additions to this Agreement are only valid if agreed explicitly and in writing.

14.2 Processor hereby agrees in advance to changes in the Agreement as a result of changes to the legal framework for protection of personal data that are strictly necessary for compliance with the relevant laws and regulations or the interpretation thereof or the policies of the authorities.

14.3 The Agreement will only be valid while the Controller follows and adheres to the accompanying Assignment as mentioned in clause 2.1 and 2.2. If the Controller fails to comply with any version of the accompanying assignment, no claim as stated in clause 8.1 can be made.

## **15. Inspection or audits by public authorities**

15.1 Processor shall submit its relevant processing systems, facilities and supporting documentation to an inspection or audit relating to the Processing by a competent public authority if this is necessary to comply with a legal obligation. In the event of any inspection or audit, each Party shall provide all reasonable assistance to the other Party in responding to that inspection or audit. If a competent public authority deems the Processing in relation to the Agreement unlawful, the Parties shall take immediate action to ensure future compliance with the applicable data protection laws

IN WITNESS WHEREOF, this Agreement is entered into with effect from the date first set out below.

Your Company

Signature \_\_\_\_\_

Name: \_\_\_\_\_

Title: \_\_\_\_\_

Date Signed: \_\_\_\_\_

Processor Company

Signature \_\_\_\_\_

Name \_\_\_\_\_

Title \_\_\_\_\_

Date Signed \_\_\_\_\_