DATA SUB-PROCESSING ADDENDUM

This Data Sub-Processing Addendum ("**Addendum**") amends and forms part of the Terms of Service agreement governing the use of the Services and Products, and the Order form, if any ("**Principal Agreement**"), entered by and between you, a customer of the Services and Products ("you" or "your" or "Customer") and Pathfix Inc. ("we" or "us" or "our" or "Pathfix") to reflect the parties agreement with regard to the Processing of Personal Data by Pathfix solely on behalf of the Customer. The Customer and Pathfix may hereinafter be referred to individually as a "**Party**" and collectively as the "**Parties**".

The scope and duration, as well as the extent and nature of the collection, processing and use of Customer Personal Data under this Addendum has been defined in the Principal Agreement. The term of this Addendum corresponds to the duration of the Principal Agreement.

Capitalized terms not defined herein shall have the meanings assigned to such terms in the Principal Agreement.

By using the Services, you accept the terms and conditions of this Addendum and you represent and warrant that you have full authority to bind the Customer to this Addendum. If you cannot, or do not agree to, comply with and be bound by this Addendum, or do not have authority to bind the Customer or any other entity, please do not provide Personal Data to us.

If you need a signed copy of this Addendum, you can download this Addendum and send a signed copy to info@pathfix.com and we'll provide you a countersigned copy.

NOW THEREFORE, THE PARTIES AGREE AS FOLLOWS:

1. DEFINITIONS AND INTERPRETATION

Unless otherwise defined herein, capitalized terms and expressions used in this Addendum shall have the following meaning;

a. **"Addendum"** means this Data Processing Addendum and all annexures attached hereto;

b. "**Pathfix**" means Pathfix Inc., a Delaware Corporation and its affiliates and subsidiaries.

c. **"Business',' "Business Purpose", Consumer", "Person", "Personal Information", "Sell", "Service Provider" and "Third Party"** shall have the meanings set forth in CCPA.

d. **“California Personal Information”** means Personal Data that is protected under the CCPA.

e. **"CCPA"** means California Civil Code Sec. 1798.100 et seq. (also known as the California Consumer Privacy Act of 2018) as may be amended from time to time, and any rules or regulations implementing the foregoing.

f. **“Customer Personal Data”** means any Personal Data Processed by Pathfix on behalf of the Customer pursuant to or in connection with the Principal Agreement.

g. **“Data Protection Laws”** means the data protection or privacy laws, rules, and regulations of the European Union, the European Economic Area and their member states, and the State of California, United States applicable to the Processing of Customer Personal Data under this Addendum.

h. **“Data Transfer”** means:

   i. A transfer of Customer Personal Data from the Customer to Pathfix; or

   ii. an onward transfer of Customer Personal Data from Pathfix to a Sub-processors, or between two establishments of Pathfix, in each case, where such transfer would be prohibited by Data Protection Laws

i. **“EEA”** means the European Economic Area;

j. **“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;

k. **“GDPR”** means EU General Data Protection Regulation 2016/679;

l. **“Services”** means the services provided by Pathfix to the Customer pursuant to the Principal Agreement.

m. **"Standard Contractual Clauses"** means the standard contractual clauses for Processors approved pursuant to the European Commission’s decision (EU) 2021/914 of 4 June 2021, for the transfer of personal data to third countries in the form set out in Annexure 3; as amended, superseded or replaced from time to time in accordance with this Addendum.

n. **“Sub-processors”** means any person or entity appointed by or on behalf of Pathfix to process Customer Personal Data on behalf of the Customer in connection with the Principal Agreement.

o. 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.

2. RELATIONSHIP AND ROLES OF THE PARTIES

The Parties acknowledge and agree that with regard to the Processing of Customer Personal Data performed solely on behalf of Customer, (i) Customer is (or represents that it is acting with full authority on behalf of) the Processor of the Customer Personal Data, (ii) Pathfix is the Sub-processor of such Customer Personal Data; (iii) for the purposes of the CCPA (and to the extent applicable), Customer is the “Business” and Pathfix is the “Service Provider” (as such terms are defined in the CCPA), with respect to Processing of Customer Personal Data. In some circumstances, Customer may be a Controller, in which case Customer appoints Pathfix as Customer’s Processor, which shall not change the obligations of either Customer or Pathfix under this Addendum.

3. PROCESSING OF CUSTOMER PERSONAL DATA

a. The Parties agree that this Addendum and the Principal Agreement constitute Customers documented instructions regarding Pathfix’s Processing of Customer Personal Data.

b. The scope of the processing of the Customer Personal Data provided by Customer to Pathfix for e.g. the subject-matter of the processing, the nature and purpose of the processing, the type of Personal Data and categories of data subjects are specified in Annexure 1 of this Addendum.

c. The Customer shall in its use of the Services, and Customer’s instructions to Pathfix, comply with Data Protection Laws. The Customer shall ensure that its instructions will not cause Pathfix to be in breach of the Data Protection Laws. The Customer shall establish and have any and all required legal basis in order to collect, Process and transfer to Pathfix the Customer Personal Data, and to authorize the Processing by Pathfix, and for Pathfix’s Processing activities on Customer’s behalf, including the pursuit of ‘business purposes’ as defined under the CCPA.

d. In processing your Customer Personal Data, we will comply with Data Protection Laws. We shall as per our obligations under Article 28 of GDPR;

    i. process the Customer Personal Data only in accordance with documented instructions from you (as set forth in this Addendum or the Principal Agreement or as directed by you through the Services). If Data Protection Laws require us to process the Customer Personal Data for any other purpose, we will inform you of this requirement first, unless such law(s) prohibit this on important grounds of public interest;

    ii. notify you promptly if, in our opinion, an instruction for the processing of Customer Personal Data given by you infringes upon the Data Protection Laws;

iii. make available to you all information reasonably requested by you for the purpose of demonstrating that your obligations relating to the appointment of Sub-Processors have been met;

iv. not generate copies, duplicates and/or backups of the Customer Personal Data without the prior written consent and knowledge of the Customer.

e. We will assist you in your obligations under Articles 35 and 36 of GDPR by performing any required data protection impact assessments, and informing any supervisory authority if such assessment indicates that such processing would result in high risk in the absence of measures taken by you to mitigate the risk.

f. We will assist you in your obligations under Articles 15 through 18 of GDPR by providing you documentation, product functionality, or processes to assist you in retrieving, correcting, deleting or restricting Customer Personal Data.

g. We shall ensure that our personnel required to access the Customer Personal Data are subject to a binding duty of confidentiality with regard to such Customer Personal Data; and ensure that none of our personnel publish, disclose or divulge any Customer Personal Data to any third party.

h. We will upon your written request following the expiration or earlier termination of the Principal Agreement securely delete such Customer Personal Data in our possession in compliance with procedures and retention periods outlined in our Principal Agreement.

i. Pathfix acknowledges and confirms that it does not receive or process any Customer Personal Data as consideration for any services or other items that Pathfix provides to the Customer under the Principal Agreement. Pathfix shall not have, derive, or exercise any rights or benefits regarding Customer Personal Data Processed on Customer's behalf, and may use and disclose Customer Personal Data solely for the purposes for which such Customer Personal Data was provided to it, as stipulated in the Principal Agreement and this Addendum. Pathfix certifies that it understands the rules, requirements and definitions of the CCPA and agrees to refrain from selling (as such term is defined in the CCPA) any Customer Personal Data Processed hereunder, without the Customer's prior written consent, nor taking any action that would cause any transfer of the Customer Personal Data to or from Pathfix under the Principal Agreement or this Addendum to qualify as "selling" such Customer Personal Data under the CCPA.

5. SECURITY

a. We implement and maintain appropriate technical and organizational measures (which may include, with respect to personnel, facilities, hardware and software, storage and networks, access controls, monitoring and logging, vulnerability and breach detection,

incident response, encryption of Customer Personal Data while in transit and at rest) to protect the Customer Personal Data against unauthorized or unlawful processing and against accidental loss, destruction, damage, theft, alteration or disclosure in accordance with Annexure 2. These measures shall be appropriate to the harm which might result from any unauthorized or unlawful processing, accidental loss, destruction, damage or theft of Customer Personal Data and appropriate to the nature of the Customer Personal Data which is to be protected. We may update the technical and organizational measures, provided, however, that such modifications shall not diminish the overall level of security.

b. Pathfix takes reasonable steps to confirm and ensure that all Pathfix representatives that may have access to the Customer Personal Data are protecting the security, privacy and confidentiality of the Customer Personal Data consistent with the requirements of this Addendum.

c. If Pathfix becomes aware of and confirm any accidental, unauthorized or unlawful destruction, loss, alteration, or disclosure of, or access to your Customer Personal Data that Pathfix Processes in the course of providing the Services, Pathfix will notify you without undue delay in a manner as provided for under Section 8 of this Addendum.

6. SUB-PROCESSORS

a. Pathfix shall not engage any Sub-processor to process any Customer Personal Data under this Addendum without the Customer's prior written consent. You provide general consent under Clause 11 of the Standard Contractual Clauses to our appointment of the applicable third party Sub-processors listed at our website for the Processing Customer Personal Data and for purposes described in this Addendum. Pathfix may update the list of approved Sub-processors at any time.

b. The Sub-processor list as of the date of first use of the Services by the Customer is hereby deemed authorized, upon first use of the Services. The Customer may reasonably object to Pathfix's use of an existing Sub-processor by providing a written objection to info@pathfix.com within thirty (30) days from the date on which the list of Sub-processors is updated by Pathfix. The Customer's failure to object to such a new Sub-processor in writing within thirty (30) days from the date on which the list of Sub-processors is updated by Pathfix shall be deemed as acceptance of the new Sub-processor by the Customer.

c. In the event Customer reasonably objects to an existing Sub-processor, as permitted in the preceding sentences, Customer may, as a sole remedy, terminate the applicable Principal Agreement and this Addendum with respect only to those Services which cannot be provided by Pathfix without the use of the objected to Sub-processor by providing written notice to Pathfix provided that all amounts due under the Principal

Agreement before the termination date with respect to the Processing at issue shall be duly paid to Pathfix. The Customer will have no further claims against Pathfix due to (i) past use of approved Sub-processors prior to the date of objection or (ii) the termination of the Principal Agreement (including, without limitation, requesting refunds) and the Addendum in the situation described in this paragraph.

d. Pathfix has entered into a written agreement with each Sub-processor containing appropriate safeguards to the protection of Customer Personal Data. Where Pathfix engages a new Sub-processor for carrying out specific Processing activities on behalf of the Customer, the same or materially similar data protection obligations as set out in this Addendum shall be imposed on such new Sub-processor by way of a contract, in particular providing sufficient guarantees to implement appropriate technical and organizational measures in such a manner that the processing will meet the requirements of the GDPR.

7. DATA SUBJECT RIGHTS

a. Pathfix shall, to the extent legally permitted, promptly notify the Customer or refer Data Subject or Consumer, as the case may be, to Customer, if Pathfix receives a request from a Data Subject or Consumer to exercise their rights (to the extent available to them under Data Protection Law) of access, right to rectification, restriction of Processing, erasure ("right to be forgotten"), data portability, object to the Processing, its right not to be subject to an automated individual decision making, to opt-out of the sale of Personal Information, or the right not to be discriminated against for exercising any CCPA Consumer rights ("Data Subject Request").

b. Taking into account the nature of the Processing, Pathfix shall assist Customer by appropriate technical and organizational measures, insofar as this is possible and reasonable, for the fulfillment of Customer's obligation to respond to a Data Subject Request under Data Protection Laws. Pathfix may refer Data Subject Requests received, and the Data Subjects making them, directly to the Customer for its treatment of such Data Subject Requests.

c. Pathfix shall not respond to Data Subject Requests except on the documented instructions of the Customer or as required by Data Protection Laws to which the Pathfix is subject, in which case Pathfix shall to the extent permitted by Data Protection Laws inform the Customer of that legal requirement before Pathfix responds to the Data Subject Request.

8. PERSONAL DATA BREACH

a. Pathfix shall to the extent required under applicable Data Protection Laws, notify the Customer without undue delay and in any event within forty eight (48) hours of

becoming aware of the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Customer Personal Data Processed on behalf of the Customer, including Customer Personal Data transmitted, stored or otherwise Processed by Pathfix or its Sub-processors of which Pathfix becomes aware (a "Personal Data Breach").

b. Pathfix shall at the Customer's instructions make reasonable efforts to identify the cause of such Personal Data Breach and take those steps that Pathfix deems necessary and reasonable in order to investigate, mitigate or remediate the cause of such a Personal Data Breach to the extent the investigation, mitigation and remediation is within Pathfix's reasonable control. The obligations herein shall not apply to incidents that are caused by the Customer or the Customer's end users i.e. Controllers.

c. Customer will not make, disclose, release or publish any finding, admission of liability, communication, notice, press release or report concerning any Personal Data Breach which directly or indirectly identifies Pathfix (including in any legal proceeding or in any notification to regulatory or supervisory authorities or affected individuals) without Pathfix's prior written approval, unless, and solely to the extent that, Customer is compelled to do so pursuant to applicable Data Protection Laws. In the latter case, unless prohibited by law, Customer shall provide Pathfix with reasonable prior written notice to provide Pathfix with the opportunity to object to such disclosure and in any case Customer will limit the disclosure to the minimum scope required.

9. DELETION OR RETURN OF CUSTOMER PERSONAL DATA

a. The Parties agree that on the termination of the Services or upon Customer's reasonable request, Pathfix shall, and shall cause any Sub-processors to, at the choice of the Customer.

   i. Return all the Customer Personal Data and copies of such Customer Personal Data to the Customer or

   ii. securely destroy them and demonstrate to the satisfaction of the Customer that it has taken such measures, unless Data Protection Laws prevent Pathfix from returning or destroying all or part of the Customer Personal Data disclosed.

b. In case Pathfix, under any Data Protection Laws is prevented from returning or destroying all or part of the Customer Personal Data disclosed, Pathfix agrees to preserve the confidentiality of the Customer Personal Data retained by it and shall ensure that it will only actively process such Customer Personal Data after such date in order to comply with Data Protection Laws.

c. To the extent authorized or required by Data Protection Laws, Pathfix may also retain one copy of the Customer Personal Data solely for evidence purposes and/or for the

establishment, exercise or defense of legal claims and/or for compliance with legal obligations.

10. AUDIT RIGHTS

a. Upon Customer's fourteen (14) days prior written request at reasonable intervals (no more than once every twelve (12) months), and subject to strict confidentiality undertakings by Customer, Pathfix shall make available to the Customer that is not a competitor of Pathfix (or Customer's independent, reputable, third-party auditor that is not a competitor of Pathfix and not in conflict with Pathfix, subject to their confidentiality and non-compete undertakings) all information necessary to demonstrate compliance with this Addendum and allow for and contribute to audits, including inspections, conducted by them (provided, however, that such information, audits, inspections and the results therefrom, including the documents reflecting the outcome of the audit and/or the inspections, shall only be used by Customer to assess compliance with this Addendum, and shall not be used for any other purpose or disclosed to any third party without Pathfix's prior written approval.

b. The scope of any audit shall not require us to disclose to you or your authorized representatives, or to allow you or your authorized representatives to access:

   i. any data or information of any other Pathfix customer;

   ii. any Pathfix internal accounting or financial information;

   iii. any Pathfix trade secret;

   iv. any information that, in our reasonable opinion could: 1) compromise the security of our systems or premises; or 2) cause us to breach our obligations under Data Protection Laws or our security, confidentiality and or privacy obligations to any other Pathfix customer or any third party; or

   v. any information that you or your authorized representatives seek to access for any reason other than the good faith fulfillment of your obligations under the Data Protection Laws and our compliance with the terms of this Addendum.

c. In addition, audits shall be limited to once per year, unless (i) we have experienced a Personal Data Breach within the prior twelve (12) months which has impacted your Customer Personal Data; or (ii) an audit reveals a material noncompliance. If we decline or are unable to follow your instructions regarding audits permitted under this Section (or the Standard Contractual Clauses, where applicable), you are entitled to terminate this Addendum and the Principal Agreement for convenience.

d. Upon Pathfix's first request, Customer shall return all records or documentation in Customer's possession or control provided by Pathfix in the context of the audit and/or

the inspection). The Customer shall be fully responsible for bearing all the costs and expenses arising from or related to this Section.

11. INTERNATIONAL DATA TRANSFER

a. Customer Personal Data that Pathfix processes on Customer's behalf will be transferred to, and stored and Processed in, North America. Customer hereby consents to the transfer of the Customer Personal Data to third countries and Customer consents to the storage and Processing of the Customer Personal Data in the North American region by Pathfix in order for Pathfix to provide the Services.

b. For transfers of European Personal Data to Pathfix for processing by the Pathfix in a jurisdiction other than a jurisdiction in the EU, The EEA, or the European Commission, Pathfix agrees that it will provide at least the same level of privacy protection for European Personal Data as required under the Applicable Data Protection Laws.

c. When Pathfix processes Customer Personal Data under European Data Protection Law in a country that does not ensure an adequate level of protection (within the meaning of applicable European Data Protection Law), then in such cases Pathfix shall process Customer Personal Data in accordance with the Standard Contractual Clauses in the form set out in Annexure 3, which are incorporated into and form a part of this Addendum. The Parties agree that for the purposes of the descriptions in the Standard Contractual Clauses, Pathfix is the "data importer" and Customer is the "data exporter" notwithstanding that Customer may itself be located outside Europe and/or is acting as a Processor on behalf of third party Controllers.

d. It is not the intention of either Party to contradict or restrict any of the provisions set forth in the Standard Contractual Clauses and, accordingly, in the event of any conflict or inconsistency between the provisions of the Addendum and the Standard Contractual Clauses, the provisions of the Standard Contractual Clauses shall prevail to the extent of such conflict.

12. INDEMNITY

Subject to the limitation of liability, either party agrees to indemnify and keep indemnified the other party against all costs, claims, damages (including all legal costs) or expenses incurred by such party, from and against any and all Losses resulting from or arising out of or in connection with any actual or threatened action by a third party against the indemnified party to the extent those losses relate to or are caused by the indemnifying party's breach of its obligations set forth in the Addendum.

13. LIMITATION OF LIABILITY

In no event, the aggregate liability of the Pathfix, its officers, directors, partners, employees and other representatives, arising out of this Addendum and the Principal Agreement or otherwise in connection with this Addendum and the Principal Agreement, shall exceed the total of the amount paid by Customer to Pathfix in twelve (12) months immediately preceding the date on which such liability arose. Pathfix shall not be liable for failure to carry out any of its obligations under this Addendum if such failures result from acts of any third-parties or of Customer.

14. TERM

The Term of this Addendum corresponds to the term of the Principal Agreement.

15. GENERAL TERMS

a. **Confidentiality -** Each Party must keep this Addendum and information it receives about the other Party and its business in connection with this Addendum ("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 the disclosure is required by law. Pathfix shall ensure that any representative of Pathfix shall be under an appropriate obligation of confidentiality.

b. **Entire Agreement -** In the event of inconsistencies between the provisions of this Addendum and any other agreements between the Parties, the provisions of this Addendum shall prevail with regard to the Parties' data protection obligations. In case of doubt as to whether clauses in such other agreements relate to the Parties' data protection obligations, this Addendum shall prevail.

c. **Severability -** Should any provision of this Addendum be invalid or unenforceable, then the remainder of this Addendum shall remain valid and in force. The invalid or unenforceable provision shall be either (i) amended as necessary to ensure its validity and enforceability, while preserving the Parties' intentions as closely as possible or (ii) construed in a manner as if the invalid or unenforceable part had never been contained therein.

d. **Notices -** All notices and communications given under this Addendum must be in writing and will be delivered personally, sent by post or sent by email to the address or email address set out herein and/or at such other address as notified from time to time by the Parties changing address.

If to the Customer:	**If to Pathfix:**
	Pathfix Inc.

Attn:	**Attn:**
Address:	**Address:**
Email:	**Email:**

14. GOVERNING LAW AND JURISDICTION

This Addendum is governed by the laws of the State of Delaware. Any dispute arising in connection with this Addendum, which the Parties fail to resolve amicably, will be submitted to the exclusive jurisdiction of the courts of the State of Delaware.

15. MODIFICATIONS

Pathfix may by at least thirty (30) days' prior written notice to the Customer, vary the terms of this Addendum and/or any Standard Contractual Clauses applicable, as necessary to allow the Processing of Customer Personal Data to be made (or continue to be made) without breach of applicable Data Protection Laws, or to otherwise protect the interests of Pathfix and/or the Customer, in each case as reasonably determined by Pathfix at its discretion. The Customer's continued use of the Services on expiry of the notice period shall be deemed as the Customer's acceptance of such revised terms. If Customer objects to said variations within the notice period, 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 Pathfix's notice as soon as is reasonably practicable. In the event that the Parties are unable to reach such an agreement within thirty (30) days of such notice, then Customer or Pathfix may, by written notice to the other Party, with immediate effect, terminate the Principal Agreement to the extent that it relates to the Services which is affected by the proposed variations (or lack thereof). The Customer will have no further claims against Pathfix (including, without limitation, requesting refunds for the Services) pursuant to the termination of the Principal Agreement and the Addendum as described in this Section.

IN WITNESS WHEREOF, the parties have caused this Addendum to be executed by their duly authorized representatives to be effective as of the Effective Date.

Customer	**Pathfix**
Customer Name: Signature: Name: Title: Date: Data Protection Officer: Contact Details:	Pathfix Inc. Signature: Name: Title: Date:

ANNEXURE 1 - PROCESSING ACTIVITIES

Categories of Data Subjects	The Customer Personal Data submitted to Pathfix shall include but shall not be limited to Personal Data concerning the following categories of Data Subjects, ● Employees, agents, advisors, freelancers of Customer (who are natural persons) ● Prospects, customers, business partners and vendors of Customer (who are natural persons) ● Any other third party individual with whom the Customer decides to communicate through the Services
Types of Personal Data	The Customer Personal Data collected, processed and used by Pathfix on behalf of the Customer shall include but shall not be limited to the following categories of Personal Data; ● Direct identifying information (e.g., name, email address, telephone, unique identification number). ● Indirect identifying information (e.g., job title, gender, date of birth). ● Device identification data and traffic data (e.g., IP addresses, web logs etc).
Special Categories of Data	Pathfix does not knowingly collect (and Customer shall not submit or upload) any special categories of data (as defined under the Data Protection Laws).

Subject Matter and nature of processing	The subject matter of Processing of Customer Personal Data by Pathfix is the provision of the Services to the Customer that involves the processing of Personal Data.
Purposes of Processing	Customer Personal Data will be Processed by Pathfix for purposes which shall include but shall not be limited to; ● Providing the Services to the Customer; ● Performing the Principal Agreement, this Addendum and/or other contracts executed by the Parties; ● Acting upon Customer's instructions, where such instructions are consistent with the terms of the Principal Agreement; ● Providing support and technical maintenance, if agreed in the Principal Agreement; ● Preventing, mitigating and investigating the risks of Personal Data Breach, fraud, error or any illegal or prohibited activity; ● Resolving disputes; ● Enforcing the Principal Agreement, this Addendum and/or defending Pathfix rights; ● Complying with applicable laws and regulations.

ANNEXURE 2 - SECURITY MEASURES

1. Wherever applicable, Pathfix employs the following measures to prevent unauthorized physical access to premises and facilities holding Customer Personal Data;

    i. Access control system
    ii. ID reader, magnetic card, chip card
    iii. Issue of keys
    iv. Door locking
    v. Surveillance facilities
    vi. Alarm system, video/CCTV monitor
    vii. Logging of facility exits/entries

2. The organizational and technical measures taken to prevent unauthorized access to the systems of Pathfix shall include but shall not be limited to;

    i. Password procedures (incl. special characters, minimum length, forced change of password)
    ii. No access for guest users or anonymous accounts
    iii. Central management of system access
    iv. Access to IT systems subject to approval from HR management and IT system administrators

3. Measures taken by Pathfix to prevent authorized users from accessing data beyond their authorized access rights and to prevent the unauthorized input, reading, copying, removal modification or disclosure of data shall include but shall not be limited to,

    i. Differentiated access rights
    ii. Access rights defined according to duties
    iii. Automated log of user access via IT systems
    iv. Measures to prevent the use of automated data-processing systems by unauthorized persons using data communication equipment

4. The following is a non-exhaustive list of all security measures adopted by Pathfix while transferring Customer Personal Data;

    i. Compulsory use of encrypted private networks for all data transfers
    ii. Encryption using a VPN for remote access, transport and communication of data.
    iii. Creating an audit trail of all data transfers

5. Pathfix employs the following measures to ensure that all data management and maintenance is logged, and an audit trail of whether data have been entered, changed or removed (deleted) and by whom is maintained;

    i. Logging user activities on IT systems
    ii. That it is possible to verify and establish to which bodies personal data have been or may be transmitted or made available using data communication equipment
    iii. That it is possible to verify and establish which personal data have been input into automated data-processing systems and when and by whom the data have been input;

6. The following is a non-exhaustive list of all the measures undertaken by Pathfix to protect data against any Personal Data Breach;

    i. Installed systems may, in the case of interruption, be restored
    ii. Systems are functioning, and that faults are reported
    iii. Stored personal data cannot be corrupted by means of a malfunctioning of the system
    iv. Uninterruptible power supply (UPS)
    v. Business Continuity procedures
    vi. Remote storage
    vii. Anti-virus / firewall systems

ANNEXURE 3 - STANDARD CONTRACTUAL CLAUSES

(Processor - to - Processor)

Clause 1

Purpose and scope

a. The purpose of these standard contractual clauses is to ensure compliance with the requirements of 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 (General Data Protection Regulation) for the transfer of personal data to a third country.

b. The Parties:

   i. The natural or legal person(s), public authority/ies, agency/ies or other body/ies (hereinafter 'entity/ies') transferring the personal data, as listed in Appendix 1 (hereinafter each 'data exporter'), and

   ii. the entity/ies in a third country receiving the personal data from the data exporter, directly or indirectly via another entity also Party to these Clauses, as listed in Appendix 1 (hereinafter each 'data importer') have agreed to these standard contractual clauses (hereinafter: 'Clauses').

c. These Clauses apply with respect to the transfer of personal data as specified in Appendix 1.

d. The Appendix to these Clauses containing the Appendices referred to therein forms an integral part of these Clauses.

Clause 2

Effect and invariability of the Clauses

a. These Clauses set out appropriate safeguards, including enforceable data subject rights and effective legal remedies, pursuant to Article 46(1) and Article 46(2)(c) of Regulation (EU) 2016/679 and, with respect to data transfers from controllers to processors and/or processors to processors, standard contractual clauses pursuant to Article 28(7) of Regulation (EU) 2016/679, provided they are not modified, except to select the appropriate Module(s) or to add or update information in the Appendix. This does not prevent the Parties from including the standard contractual clauses laid down in these Clauses in a wider contract and/or to add other clauses or additional safeguards, provided that they do not

contradict, directly or indirectly, these Clauses or prejudice the fundamental rights or freedoms of data subjects.

b. These Clauses are without prejudice to obligations to which the data exporter is subject by virtue of Regulation (EU) 2016/679.

Clause 3

Third-party beneficiaries

a. Data subjects may invoke and enforce these Clauses, as third-party beneficiaries, against the data exporter and/or data importer, with the following exceptions:

   i. Clause 1, Clause 2, Clause 3, Clause 6, Clause 7;

   ii. Clause 8.1(a), (c) and (d) and Clause 8.9(a), (c), (d), (e), (f) and (g);

   iii. Clause 9(a), (c), (d) and (e);

   iv. Clause 12(a), (d) and (f);

   v. Clause 13;

   vi. Clause 15.1(c), (d) and (e);

   vii. Clause 16(e);

   viii. Clause 18(a) and (b).

b. Paragraph (a) is without prejudice to rights of data subjects under Regulation (EU) 2016/679.

Clause 4

Interpretation

a. Where these Clauses use terms that are defined in Regulation (EU) 2016/679, those terms shall have the same meaning as in that Regulation.

b. These Clauses shall be read and interpreted in the light of the provisions of Regulation (EU) 2016/679.

c. These Clauses shall not be interpreted in a way that conflicts with rights and obligations provided for in Regulation (EU) 2016/679.

Clause 5

Hierarchy

In the event of a contradiction between these Clauses and the provisions of related agreements between the Parties, existing at the time these Clauses are agreed or entered into thereafter, these Clauses shall prevail.

Clause 6

Description of the transfer(s)

The details of the transfer(s), and in particular the categories of personal data that are transferred and the purpose(s) for which they are transferred, are specified in Appendix 1.

Clause 7 – Optional.

Not used.

SECTION II – OBLIGATIONS OF THE PARTIES

Clause 8

Data protection safeguards

The data exporter warrants that it has used reasonable efforts to determine that the data importer is able, through the implementation of appropriate technical and organisational measures, to satisfy its obligations under these Clauses.

8.1. Instructions

a. The data exporter has informed the data importer that it acts as processor under the instructions of its controller(s), which the data exporter shall make available to the data importer prior to processing.

b. The data importer shall process the personal data only on documented instructions from the controller, as communicated to the data importer by the data exporter, and any

additional documented instructions from the data exporter. Such additional instructions shall not conflict with the instructions from the controller. The controller or data exporter may give further documented instructions regarding the data processing throughout the duration of the contract.

c. The data importer shall immediately inform the data exporter if it is unable to follow those instructions. Where the data importer is unable to follow the instructions from the controller, the data exporter shall immediately notify the controller.

d. The data exporter warrants that it has imposed the same data protection obligations on the data importer as set out in the contract or other legal act under Union or Member State law between the controller and the data exporter.

8.2. **Purpose limitation.** The data importer shall process the personal data only for the specific purpose(s) of the transfer, as set out in Appendix 1, unless on further instructions from the controller, as communicated to the data importer by the data exporter, or from the data exporter.

8.3. **Transparency.** On request, the data exporter shall make a copy of these Clauses, including the Appendix as completed by the Parties, available to the data subject free of charge. To the extent necessary to protect business secrets or other confidential information, including personal data, the data exporter may redact part of the text of the Appendix prior to sharing a copy, but shall provide a meaningful summary where the data subject would otherwise not be able to understand its content or exercise his/her rights. On request, the Parties shall provide the data subject with the reasons for the redactions, to the extent possible without revealing the redacted information.

8.4. **Accuracy.** If the data importer becomes aware that the personal data it has received is inaccurate, or has become outdated, it shall inform the data exporter without undue delay. In this case, the data importer shall cooperate with the data exporter to rectify or erase the data.

8.5. **Duration of processing and erasure or return of data.** Processing by the data importer shall only take place for the duration specified in Appendix 1. After the end of the provision of the processing services, the data importer shall, at the choice of the data exporter, delete all personal data processed on behalf of the controller and certify to the data exporter that it has done so, or return to the data exporter all personal data processed on its behalf and delete existing copies. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit return or deletion of the personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process it to the extent and for as long as required under that local law. This is without prejudice to Clause 14, in particular the requirement for the data importer under Clause 14(e) to notify the data exporter throughout the duration of the contract if it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under Clause 14(a).

8.6. Security of processing

a. The data importer and, during transmission, also the data exporter shall implement appropriate technical and organisational measures to ensure the security of the data, including protection against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access to that data (hereinafter 'personal data breach'). In assessing the appropriate level of security, they shall take due account of the state of the art, the costs of implementation, the nature, scope, context and purpose(s) of processing and the risks involved in the processing for the data subject. The Parties shall in particular consider having recourse to encryption or pseudonymisation, including during transmission, where the purpose of processing can be fulfilled in that manner. In case of pseudonymisation, the additional information for attributing the personal data to a specific data subject shall, where possible, remain under the exclusive control of the data exporter or the controller. In complying with its obligations under this paragraph, the data importer shall at least implement the technical and organisational measures specified in Appendix 2. The data importer shall carry out regular checks to ensure that these measures continue to provide an appropriate level of security.

b. The data importer shall grant access to the data to members of its personnel only to the extent strictly necessary for the implementation, management and monitoring of the contract. It shall ensure that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

c. In the event of a personal data breach concerning personal data processed by the data importer under these Clauses, the data importer shall take appropriate measures to address the breach, including measures to mitigate its adverse effects. The data importer shall also notify, without undue delay, the data exporter and, where appropriate and feasible, the controller after having become aware of the breach. Such notification shall contain the details of a contact point where more information can be obtained, a description of the nature of the breach (including, where possible, categories and approximate number of data subjects and personal data records concerned), its likely consequences and the measures taken or proposed to address the data breach, including measures to mitigate its possible adverse effects. Where, and in so far as, it is not possible to provide all information at the same time, the initial notification shall contain the information then available and further information shall, as it becomes available, subsequently be provided without undue delay.

d. The data importer shall cooperate with and assist the data exporter to enable the data exporter to comply with its obligations under Regulation (EU) 2016/679, in particular to notify its controller so that the latter may in turn notify the competent supervisory authority and the affected data subjects, taking into account the nature of processing and the information available to the data importer.

8.7. **Sensitive data.** Where the transfer involves personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, or biometric data for the purpose of uniquely identifying a natural person, data concerning health or a person's sex life or sexual orientation, or data relating to criminal convictions and offences (hereinafter 'sensitive data'), the data importer shall apply the specific restrictions and/or additional safeguards set out in Appendix 1.

8.8. **Onward transfers.** The data importer shall only disclose the personal data to a third party on documented instructions from the controller, as communicated to the data importer by the data exporter. In addition, the data may only be disclosed to a third party located outside the European Union (in the same country as the data importer or in another third country, hereinafter 'onward transfer') if the third party is or agrees to be bound by these Clauses, under the appropriate Module, or if:

i. the onward transfer is to a country benefiting from an adequacy decision pursuant to Article 45 of Regulation (EU) 2016/679 that covers the onward transfer;

ii. the third party otherwise ensures appropriate safeguards pursuant to Articles 46 or 47 of Regulation (EU) 2016/679;

iii. the onward transfer is necessary for the establishment, exercise or defense of legal claims in the context of specific administrative, regulatory or judicial proceedings; or

iv. the onward transfer is necessary in order to protect the vital interests of the data subject or of another natural person.

Any onward transfer is subject to compliance by the data importer with all the other safeguards under these Clauses, in particular purpose limitation.

8.9. **Documentation and compliance**

a. The data importer shall promptly and adequately deal with enquiries from the data exporter or the controller that relate to the processing under these Clauses.

b. The Parties shall be able to demonstrate compliance with these Clauses. In particular, the data importer shall keep appropriate documentation on the processing activities carried out on behalf of the controller.

c. The data importer shall make all information necessary to demonstrate compliance with the obligations set out in these Clauses available to the data exporter, which shall provide it to the controller.

d. The data importer shall allow for and contribute to audits by the data exporter of the processing activities covered by these Clauses, at reasonable intervals or if there are indications of non-compliance. The same shall apply where the data exporter requests an audit on instructions of the controller. In deciding on an audit, the data exporter may take into account relevant certifications held by the data importer.

e. Where the audit is carried out on the instructions of the controller, the data exporter shall make the results available to the controller.

f. The data exporter may choose to conduct the audit by itself or mandate an independent auditor. Audits may include inspections at the premises or physical facilities of the data importer and shall, where appropriate, be carried out with reasonable notice.

g. The Parties shall make the information referred to in paragraphs (b) and (c), including the results of any audits, available to the competent supervisory authority on request.

Clause 9

Use of sub-processors

a. The data importer has the controller's general authorisation for the engagement of sub-processor(s) from an agreed list. The data importer shall specifically inform the controller in writing of any intended changes to that list through the addition or replacement of sub-processors at least at least 30 days in advance, thereby giving the controller sufficient time to be able to object to such changes prior to the engagement of the sub-processor(s). The data importer shall provide the controller with the information necessary to enable the controller to exercise its right to object. The data importer shall inform the data exporter of the engagement of the sub-processor(s).

b. Where the data importer engages a sub-processor to carry out specific processing activities (on behalf of the controller), it shall do so by way of a written contract that provides for, in substance, the same data protection obligations as those binding the data importer under these Clauses, including in terms of third-party beneficiary rights for data subjects. The Parties agree that, by complying with this Clause, the data importer fulfils its obligations under Clause 8.8. The data importer shall ensure that the sub-processor complies with the obligations to which the data importer is subject pursuant to these Clauses.

c. The data importer shall provide, at the data exporter's or controller's request, a copy of such a sub-processor agreement and any subsequent amendments. To the extent necessary to protect business secrets or other confidential information, including personal data, the data importer may redact the text of the agreement prior to sharing a copy.

d. The data importer shall remain fully responsible to the data exporter for the performance of the sub-processor's obligations under its contract with the data importer. The data importer shall notify the data exporter of any failure by the sub-processor to fulfil its obligations under that contract.

e. The data importer shall agree a third-party beneficiary clause with the sub-processor whereby – in the event the data importer has factually disappeared, ceased to exist in law or has become insolvent – the data exporter shall have the right to terminate the sub-processor contract and to instruct the sub-processor to erase or return the personal data.

Clause 10

Data subject rights

a. The data importer shall promptly notify the data exporter and, where appropriate, the controller of any request it has received from a data subject, without responding to that request unless it has been authorised to do so by the controller.

b. The data importer shall assist, where appropriate in cooperation with the data exporter, the controller in fulfilling its obligations to respond to data subjects' requests for the exercise of their rights under Regulation (EU) 2016/679 or Regulation (EU) 2018/1725, as applicable. In this regard, the Parties shall set out in Appendix 2 the appropriate technical and organisational measures, taking into account the nature of the processing, by which the assistance shall be provided, as well as the scope and the extent of the assistance required.

c. In fulfilling its obligations under paragraphs (a) and (b), the data importer shall comply with the instructions from the controller, as communicated by the data exporter.

Clause 11

Redress

a. The data importer shall inform data subjects in a transparent and easily accessible format, through individual notice or on its website, of a contact point authorised to handle complaints. It shall deal promptly with any complaints it receives from a data subject.

b. In case of a dispute between a data subject and one of the Parties as regards compliance with these Clauses, that Party shall use its best efforts to resolve the issue amicably in a timely fashion. The Parties shall keep each other informed about such disputes and, where appropriate, cooperate in resolving them.

c. Where the data subject invokes a third-party beneficiary right pursuant to Clause 3, the data importer shall accept the decision of the data subject to:

i. lodge a complaint with the supervisory authority in the Member State of his/her habitual residence or place of work, or the competent supervisory authority pursuant to Clause 13;

ii. refer the dispute to the competent courts within the meaning of Clause 18.

d. The Parties accept that the data subject may be represented by a not-for-profit body, organisation or association under the conditions set out in Article 80(1) of Regulation (EU) 2016/679.

e. The data importer shall abide by a decision that is binding under the applicable EU or Member State law.

f. The data importer agrees that the choice made by the data subject will not prejudice his/her substantive and procedural rights to seek remedies in accordance with applicable laws.

Clause 12

Liability

a. Each Party shall be liable to the other Party/ies for any damages it causes the other Party/ies by any breach of these Clauses.

b. The data importer shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages the data importer or its sub-processor causes the data subject by breaching the third-party beneficiary rights under these Clauses.

c. Notwithstanding paragraph (b), the data exporter shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages the data exporter or the data importer (or its sub-processor) causes the data subject by breaching the third-party beneficiary rights under these Clauses. This is without prejudice to the liability of the data exporter and, where the data exporter is a processor acting on behalf of a controller, to the liability of the controller under Regulation (EU) 2016/679 or Regulation (EU) 2018/1725, as applicable.

d. The Parties agree that if the data exporter is held liable under paragraph (c) for damages caused by the data importer (or its sub-processor), it shall be entitled to claim back from the data importer that part of the compensation corresponding to the data importer's responsibility for the damage.

e. Where more than one Party is responsible for any damage caused to the data subject as a result of a breach of these Clauses, all responsible Parties shall be jointly and

severally liable and the data subject is entitled to bring an action in court against any of these Parties.

f. The Parties agree that if one Party is held liable under paragraph (e), it shall be entitled to claim back from the other Party/ies that part of the compensation corresponding to its/their responsibility for the damage.

g. The data importer may not invoke the conduct of a sub-processor to avoid its own liability.

Clause 13

Supervision

a. Where the data exporter is established in an EU Member State: The supervisory authority with responsibility for ensuring compliance by the data exporter with Regulation (EU) 2016/679 as regards the data transfer, as indicated in Appendix 1, shall act as competent supervisory authority. Where the data exporter is not established in an EU Member State, but falls within the territorial scope of application of Regulation (EU) 2016/679 in accordance with its Article 3(2) and has appointed a representative pursuant to Article 27(1) of Regulation (EU) 2016/679: The supervisory authority of the Member State in which the representative within the meaning of Article 27(1) of Regulation (EU) 2016/679 is established, as indicated in Appendix 1, shall act as competent supervisory authority. Where the data exporter is not established in an EU Member State, but falls within the territorial scope of application of Regulation (EU) 2016/679 in accordance with its Article 3(2) without however having to appoint a representative pursuant to Article 27(2) of Regulation (EU) 2016/679: The supervisory authority of one of the Member States in which the data subjects whose personal data is transferred under these Clauses in relation to the offering of goods or services to them, or whose behaviour is monitored, are located, as indicated in Appendix 1, shall act as competent supervisory authority.

b. The data importer agrees to submit itself to the jurisdiction of and cooperate with the competent supervisory authority in any procedures aimed at ensuring compliance with these Clauses. In particular, the data importer agrees to respond to enquiries, submit to audits and comply with the measures adopted by the supervisory authority, including remedial and compensatory measures. It shall provide the supervisory authority with written confirmation that the necessary actions have been taken.

SECTION III – LOCAL LAWS AND OBLIGATIONS IN CASE OF ACCESS BY PUBLIC AUTHORITIES

Clause 14

Local laws and practices affecting compliance with the Clauses

a. The Parties warrant that they have no reason to believe that the laws and practices in the third country of destination applicable to the processing of the personal data by the data importer, including any requirements to disclose personal data or measures authorising access by public authorities, prevent the data importer from fulfilling its obligations under these Clauses. This is based on the understanding that laws and practices that respect the essence of the fundamental rights and freedoms and do not exceed what is necessary and proportionate in a democratic society to safeguard one of the objectives listed in Article 23(1) of Regulation (EU) 2016/679, are not in contradiction with these Clauses.

b. The Parties declare that in providing the warranty in paragraph (a), they have taken due account in particular of the following elements:

    i. the specific circumstances of the transfer, including the length of the processing chain, the number of actors involved and the transmission channels used; intended onward transfers; the type of recipient; the purpose of processing; the categories and format of the transferred personal data; the economic sector in which the transfer occurs; the storage location of the data transferred;

    ii. the laws and practices of the third country of destination– including those requiring the disclosure of data to public authorities or authorising access by such authorities – relevant in light of the specific circumstances of the transfer, and the applicable limitations and safeguards;

    iii. any relevant contractual, technical or organisational safeguards put in place to supplement the safeguards under these Clauses, including measures applied during transmission and to the processing of the personal data in the country of destination.

c. The data importer warrants that, in carrying out the assessment under paragraph (b), it has made its best efforts to provide the data exporter with relevant information and agrees that it will continue to cooperate with the data exporter in ensuring compliance with these Clauses.

d. The Parties agree to document the assessment under paragraph (b) and make it available to the competent supervisory authority on request.

e. The data importer agrees to notify the data exporter promptly if, after having agreed to these Clauses and for the duration of the contract, it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under

paragraph (a), including following a change in the laws of the third country or a measure (such as a disclosure request) indicating an application of such laws in practice that is not in line with the requirements in paragraph (a). The data exporter shall forward the notification to the controller.

f. Following a notification pursuant to paragraph (e), or if the data exporter otherwise has reason to believe that the data importer can no longer fulfil its obligations under these Clauses, the data exporter shall promptly identify appropriate measures (e.g. technical or organisational measures to ensure security and confidentiality) to be adopted by the data exporter and/or data importer to address the situation, if appropriate in consultation with the controller. The data exporter shall suspend the data transfer if it considers that no appropriate safeguards for such transfer can be ensured, or if instructed by the controller or the competent supervisory authority to do so. In this case, the data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses. If the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise. Where the contract is terminated pursuant to this Clause, Clause 16(d) and (e) shall apply.

Clause 15

Obligations of the data importer in case of access by public authorities

15.1. Notification

a. The data importer agrees to notify the data exporter and, where possible, the data subject promptly (if necessary with the help of the data exporter) if it:

   i. receives a legally binding request from a public authority, including judicial authorities, under the laws of the country of destination for the disclosure of personal data transferred pursuant to these Clauses; such notification shall include information about the personal data requested, the requesting authority, the legal basis for the request and the response provided; or

   ii. becomes aware of any direct access by public authorities to personal data transferred pursuant to these Clauses in accordance with the laws of the country of destination; such notification shall include all information available to the importer. The data exporter shall forward the notification to the controller.

b. If the data importer is prohibited from notifying the data exporter and/or the data subject under the laws of the country of destination, the data importer agrees to use its best efforts to obtain a waiver of the prohibition, with a view to communicating as much

information as possible, as soon as possible. The data importer agrees to document its best efforts in order to be able to demonstrate them on request of the data exporter.

c. Where permissible under the laws of the country of destination, the data importer agrees to provide the data exporter, at regular intervals for the duration of the contract, with as much relevant information as possible on the requests received (in particular, number of requests, type of data requested, requesting authority/ies, whether requests have been challenged and the outcome of such challenges, etc.). The data exporter shall forward the information to the controller.

d. The data importer agrees to preserve the information pursuant to paragraphs (a) to (c) for the duration of the contract and make it available to the competent supervisory authority on request. Eeeeee Paragraphs (a) to (c) are without prejudice to the obligation of the data importer pursuant to Clause 14(e) and Clause 16 to inform the data exporter promptly where it is unable to comply with these Clauses.

15.2. Review of legality and data minimization

a. The data importer agrees to review the legality of the request for disclosure, in particular whether it remains within the powers granted to the requesting public authority, and to challenge the request if, after careful assessment, it concludes that there are reasonable grounds to consider that the request is unlawful under the laws of the country of destination, applicable obligations under international law and principles of international comity. The data importer shall, under the same conditions, pursue possibilities of appeal. When challenging a request, the data importer shall seek interim measures with a view to suspending the effects of the request until the competent judicial authority has decided on its merits. It shall not disclose the personal data requested until required to do so under the applicable procedural rules. These requirements are without prejudice to the obligations of the data importer under Clause 14(e).

b. The data importer agrees to document its legal assessment and any challenge to the request for disclosure and, to the extent permissible under the laws of the country of destination, make the documentation available to the data exporter. It shall also make it available to the competent supervisory authority on request. The data exporter shall make the assessment available to the controller.

c. The data importer agrees to provide the minimum amount of information permissible when responding to a request for disclosure, based on a reasonable interpretation of the request.

SECTION IV – FINAL PROVISIONS

Clause 16

Non-compliance with the Clauses and termination

a. The data importer shall promptly inform the data exporter if it is unable to comply with these Clauses, for whatever reason.

b. In the event that the data importer is in breach of these Clauses or unable to comply with these Clauses, the data exporter shall suspend the transfer of personal data to the data importer until compliance is again ensured or the contract is terminated. This is without prejudice to Clause 14(f).

c. The data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses, where:

   i. the data exporter has suspended the transfer of personal data to the data importer pursuant to paragraph (b) and compliance with these Clauses is not restored within a reasonable time and in any event within one month of suspension;

   ii. the data importer is in substantial or persistent breach of these Clauses; or

   iii. the data importer fails to comply with a binding decision of a competent court or supervisory authority regarding its obligations under these Clauses.

   In these cases, it shall inform the competent supervisory authority and the controller of such non-compliance. Where the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise.

d. Personal data that has been transferred prior to the termination of the contract pursuant to paragraph (c) shall at the choice of the data exporter immediately be returned to the data exporter or deleted in its entirety. The same shall apply to any copies of the data. The data importer shall certify the deletion of the data to the data exporter. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit the return or deletion of the transferred personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process the data to the extent and for as long as required under that local law.

e. Either Party may revoke its agreement to be bound by these Clauses where (i) the European Commission adopts a decision pursuant to Article 45(3) of Regulation (EU) 2016/679 that covers the transfer of personal data to which these Clauses apply; or (ii) Regulation (EU) 2016/679 becomes part of the legal framework of the country to which the personal data is transferred. This is without prejudice to other obligations applying to the processing in question under Regulation (EU) 2016/679.

Clause 17

Governing law

These Clauses shall be governed by the law of one of the EU Member States, provided such law allows for third-party beneficiary rights. The Parties agree that this shall be the law of the Republic of Ireland.

Clause 18

Choice of forum and jurisdiction

a. Any dispute arising from these Clauses shall be resolved by the courts of an EU Member State.

b. The Parties agree that those shall be the courts of the state that the client is situated.

c. A data subject may also bring legal proceedings against the data exporter and/or data importer before the courts of the Member State in which he/she has his/her habitual residence.

d. The Parties agree to submit themselves to the jurisdiction of such courts.

IN WITNESS WHEREOF, the parties have caused these Standard Contractual Clauses to be executed by their authorized representative:

On behalf of the data exporter:

Sign: _____

Name: _____

Position: _____

Address: _____

On behalf of the data importer:

Sign: _____

Name: _____

Position: _____

Address: _____

APPENDIX 1 to the Standard Contractual Clauses

LIST OF PARTIES

Data exporter(s):

Name: The entity identified as “Customer” in the Principal Agreement.

Address: The address for Customer specified in the Principal Agreement.

Contact person’s name, position and contact details: The contact details for Customer as specified in the Addendum or the Principal Agreement.

Signature and date: _____

Role (controller / processor): Processor

Data importer(s):

Name: Pathfix Inc.

Address: _____

Contact person’s name, position and contact details: _____

Signature and date: _____

Role (controller / processor): Sub-Processor

DESCRIPTION OF TRANSFER

1. Data subjects

The personal data submitted to Pathfix shall include but shall not be limited to personal data concerning the following categories of data subjects,

a. Employees, agents, advisors, freelancers of Customer (who are natural persons)

b. Prospects, customers, business partners and vendors of Customer (who are natural persons)

c. Employees or contact persons of Customer’s prospects, customers, business partners and vendors

d. Any other third party individual with whom the Customer decides to communicate through the Services

e. _____

2. Categories of personal data transferred/ Processed

The personal data collected, processed and used by Pathfix on behalf of the Customer shall include but shall not be limited to the following categories of personal data;

a. Direct identifying information (e.g., name, email address, telephone)

b. Indirect identifying information (e.g., job title, gender, date of birth).

c. Device identification data and traffic data (e.g., IP addresses, web logs etc).

d. Any personal data supplied by Customer

e. _____

3. Special categories of data

Pathfix does not knowingly collect (and Customer shall not submit or upload) any special categories of data (as defined under the Data Protection Laws).

4. Purposes of processing

Personal data will be processed by Pathfix for purposes which shall include but shall not be limited to;

a. Providing the Services to the Customer;

b. Performing the Principal Agreement, this Addendum and/or other contracts executed by the Parties;

c. Acting upon Customer's instructions, where such instructions are consistent with the terms of the Principal Agreement;

d. Providing support and technical maintenance, if agreed in the Principal Agreement;

e. Preventing, mitigating and investigating the risks of Personal Data Breach, fraud, error or any illegal or prohibited activity;

f. Resolving disputes;

g. Enforcing the Principal Agreement, this Addendum and/or defending Pathfix rights;

h. Complying with applicable laws and regulations.

i. _____

5. Frequency of Transfer

Continuous basis as needed for performance of Services and throughout the Agreement term and until the Addendum Termination Date.

6. The period for which the Personal Data will be retained, or, if that is not possible, the criteria used to determine that period.

For the duration of the Principal Agreement term as defined in the Principal Agreement, pursuant to the terms stated in the Addendum, unless otherwise required by applicable law.

APPENDIX 2 to the Standard Contractual Clauses

Description of the technical and organizational measures implemented by the data importer (including any relevant certifications) to ensure an appropriate level of security, taking into account the nature, scope, context and purpose of the Processing, and the risks for the rights and freedoms of natural persons.

The technical and organizational security measures implemented by the data importer are as described in Annexure 2 of the Data Processing Addendum.