Data Processing Addendum

Firmex Inc.

REVISION DATE JANUARY 2024

This Addendum on Data Processing (hereinafter: "Addendum") is by and between:

Subscriber and its Affiliates as defined by the ORDER:

hereinafter referred to as "**Subscriber**"–

AND

Firmex entity as defined by the Order:

hereinafter referred to as "**Firmex**"–

Hereinafter each individually referred to also as the "**Party**" and collectively as the "**Parties.**"

PREAMBLE

(A) The Parties have entered into an Agreement which outlines the Services to be provided (definitions provided in Section 1 below). As part of the provision of Services by Firmex, Personal Data may be transferred by the Subscriber to Firmex.

(B) Capitalized terms not defined in this Addendum are defined in the Agreement. In the event of any conflict between the provisions in this Addendum and the provisions set forth in the Agreement, the provision or provisions of this Addendum will prevail.

(C) To ensure compliance by the Parties with Processing obligations pursuant to the Data Protection Rules, as amended from time to time, the Parties hereby agree as follows:

1. DEFINITIONS

1.1 "**Agreement**" means the Order and the General Terms and Conditions between the Subscriber and Firmex.

1.2 "**Appendix**" means the appendices annexed to and forming an integral part of this Addendum.

1.3 "**Business Operations**" means: (1) billing, payments, and account management; (2) for the purposes of direct marketing; (3) internal reporting and business modeling (e.g. forecasting, revenue, capacity planning, product strategy); (4) improving and developing new products and services; (5) combatting fraud, cybercrime, or cyber-attacks that may affect Firmex or Firmex products; (6) improving the core functionality of accessibility, or privacy of the Website; and (7) financial reporting and compliance with legal obligations.

1.4 "**Controller**" means an entity that determines the purposes and means of the Processing of Personal Data.

1.5 "**Data Protection Rules**" means the relevant national laws that apply to the Processing of Personal Data, including but not limited to: European Data Protection Laws, US Data Protection Laws, Personal Information Protection and Electronic Documents Act 2000, and the Australian Privacy Principles, as applicable.

1.6 "**Data Subject**" means an identified or identifiable natural person whose Personal Data is subject to Processing; an identifiable person is one who can be identified, directly or indirectly, 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 physical, physiological, genetic, mental, economic, cultural, or social identity, or as otherwise defined in applicable Data Protection Rules.

1.7 "**European Data Protection Laws**" means the GDPR and the Swiss Data Protection Act collectively.

1.8 "**GDPR**" means UK GDPR and the EU General Data Protection Regulation 2016/679.

1.9 "**International Data Transfer Agreement**" or "**IDTA**" means the international data transfer agreement for the transfer of Personal Data to processors established in third countries pursuant to Article 46 and Chapter V of UK GDPR.

1.10 "**Personal Data**" means any information relating to a Data Subject contained within the Materials.

1.11 "**Personal Data Breach**" means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Personal Data transmitted, stored, or otherwise Processed, or as otherwise defined in applicable Data Protection Rules.

1.12 "**Process**", "**Processing**" or "**Processed**" means any operation or set of operations which is performed upon Personal Data, whether or not by automatic means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure, or destruction, or as otherwise defined in applicable Data Protection Rules.

1.13 "**Processor**" means an entity that Processes Personal Data on behalf of a Controller.

1.14 "**Services**" means the provision of services as described in the Agreement and this Addendum.

1.15 "**Special Categories of Data**" means the Personal Data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, genetic data, biometric data Processed for the purpose of uniquely identifying a natural person, as well as Personal Data concerning health, sex life or sexual orientation, or as otherwise defined in applicable Data Protection Rules.

1.16 "**Standard Contractual Clauses**" or "**SCCs**" means the Controller to Processor (Module 2) standard contractual clauses for the transfer of Personal Data to entities not subject to the GDPR/Swiss Data Protection Act, in line with the requirements of the GDPR and Swiss Data Protection Act, as applicable.

1.17 "**Subprocessor**" means an entity engaged by a Processor to Process Personal Data on behalf of a Controller.

1.18 "**Swiss Data Protection Act**" means the Swiss Federal Act on Data Protection of 19 June 1992 (SR 235.1) and Ordinances SR 235.11 and SR 235.13, as amended and following the coming into force of its revised version of 25 September 2020 on 1 January 2023 (or at the later date subject to the legislative procedure), subject to such revised version, as amended, replaced, or superseded from time to time, inso far as these apply to the Processing of Personal Data.

1.19 "**UK GDPR**" means s.3(10), 205(4) and the general processing provisions of the Data Protection Act of 2018, as updated, amended, replaced, or superseded from time to time.

1.20 "**US Data Protection Laws**" means the following laws to the extent applicable to Personal Data and the provision of the Services once they become effective: the California Consumer Privacy Act (and California Privacy Rights Act once effective), Cal. Civ. Code § 1798.100 et seq.; and other materially similar U.S. laws that may be enacted and that apply to Personal Data from time to time.

2. PROCESSING ACTIVITIES

2.1 Subscriber and Firmex agree that: (a) Subscriber is the Controller of Personal Data and Firmex is the Processor of such data, except when Subscriber acts as a Processor of Personal Data on behalf a third-party Controller ("Third-Party Controller"), in which case Firmex is a Subprocessor; and (b) this Addendum applies where and only to the extent that Firmex Processes Personal Data on behalf of Subscriber as Processor or Subprocessor in the course of providing the Services.

2.2 The Subscriber agrees that: (a) it has obtained all relevant consents or ensured it has other lawful legal basis (as applicable), permissions and rights and provided all relevant notices necessary under Data Protection Rules for Firmex to lawfully Process Personal Data in accordance with this Agreement including, without limitation, Subscriber's sharing and/or receiving of Personal Data with third-parties via the Services; (b) it shall comply with, and is responsible for its Affiliates and invited Users' compliance with applicable Data Protection Rules; and (c) its Processing instructions to Firmex are consistent with Data Protection Rules and all instructions from Third-Party Controllers, if applicable.

2.3 Firmex agrees to Process the Personal Data in accordance with: (a) this Addendum and the Agreement; (b) Subscriber's written instructions as set forth in Appendix 1 of this Addendum; and (c) as may be communicated by the Subscriber from time to time, if required under Data Protection Rules. Any additional requested instructions require the prior written agreement of Firmex.

2.4 To the extent Feedback, Usage Data, or User Data (collectively for purposes of this paragraph only, "Data") relate to an identified or identifiable person, the Parties agree that Firmex: (a) will act as an independent "controller" and/or "business" (as such terms are defined under Data Protection Rules) with respect to such Data; and (b) shall process such Data only for its Business Operations and in compliance with all applicable Data Protection Rules. Subscriber agrees that it has obtained all relevant consents, permissions and rights and provided all relevant notices necessary under Data Protection Rules for Firmex to lawfully process Data as an independent "controller" and/or "business" (as such terms are defined under Data Protection Rules) for Firmex's Business Operations.

2.5 If Firmex believes that an instruction infringes upon Data Protection Rules, it will notify the Subscriber without undue delay. Where the Subscriber is acting as Processor, it shall be responsible for any notification, assistance or authorization that may be required to be given to or received by its Third-Party Controller. Firmex acknowledges, when acting as a Service Provider, it does not receive any Personal Data as consideration for the Services (as such terms are defined under US Data Protection Laws).

3. DURATION AND TERMINATION OF THIS ADDENDUM

3.1 This Addendum is effective as of the Effective Date and shall remain in force during the term of the Agreement. This Addendum will terminate automatically with the termination or expiry of any ORDER.

3.2 Notwithstanding the termination of this Addendum, Firmex shall continue to be bound by its obligation of confidentiality.

4. INTERNATIONAL TRANSFERS

All Personal Data is stored at third-party hosting facilities within the United States, European Economic Area ("EEA") or Canada. Subscriber acknowledges that Firmex may transfer Personal Data to countries in which it and or its Subprocessors operate; however, Personal Data will continue to be stored in the United States, EEA, or Canada. Unless transferred on the basis of an adequacy decision issued by the applicable national authority, all transfers of Personal Data out of the United Kingdom, EEA and Switzerland shall be governed by the SCCs (as Appendix 3) and IDTA (as Appendix 4) incorporated into this Addendum. Firmex will abide by European Data Protection Laws regarding the collection, use, transfer, retention, and other processing of Personal Data from the EEA, UK and Switzerland.

5. CONFIDENTIALITY AND SECURITY

5.1 Firmex shall: (a) keep Personal Data confidential; and (b) ensure that its employees who Process Personal Data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

5.2 Subject to the Data Protection Rules, Firmex will implement appropriate operational, technical, and organizational measures to protect Personal Data against accidental or unlawful destruction, loss, alteration, unauthorized disclosure, or access as described in Appendix 2.

5.3 Subscriber is solely responsible for making an independent determination as to whether the technical and organizational measures put in place by Firmex meet Subscriber's requirements, including any of its security obligations under applicable Data Protection Rules. Subscriber acknowledges and agrees that (taking into account the state of the art, the costs of implementation, and the nature, scope, context and purposes of the Processing of its Personal Data as well as the risks to Data Subjects) the security practices and policies implemented and maintained by Firmex provide a level of security appropriate to the risk with respect to the Personal Data.

5.4 Firmex will update the technical and organizational security measures in line with reasonable technological developments as determined by Firmex.

6. COOPERATION AND NOTIFICATION OBLIGATIONS

6.1 The Parties will co-operate with each other to promptly and effectively handle enquiries, complaints, and claims relating to the Processing of Personal Data from any government authority or Data Subject.

6.2 If a Data Subject should apply directly to Firmex to exercise his/her Personal Data rights, Firmex will assist Subscriber with such request by forwarding this request to the Subscriber without undue delay if permitted by Data Protection Rules.

6.3 Unless prohibited by law, if the Personal Data is subject to a control, order, or investigation by public authorities, Firmex will: (a) promptly notify the Subscriber; and (b) disclose Personal Data only to the extent that is strictly necessary and proportionate to satisfy the request and in compliance with Data Protection Rules. Upon Subscriber's request, Firmex will provide the public authorities with information regarding Processing under this Addendum as well as allow inspections within the scope stated in Section 7, as required by Data Protection Rules.

6.4 Firmex will notify the Subscriber of a Personal Data Breach that is determined to affect Subscriber's Personal Data without undue delay. Firmex shall provide Subscriber with the information to reasonably assist Subscriber as required by Data Protection Rules.

6.5 Considering the nature of Processing and Personal Data, Firmex will provide reasonable assistance to Subscriber with carrying out a data protection impact assessment and prior consultation under Data Protection Rules to the extent Subscriber is not able to carry these out independently.

7. SUBSCRIBER'S AUDIT AND INSPECTION RIGHTS

Upon Subscriber's request, and subject to confidentiality requirements, Firmex shall make available to Subscriber information necessary to demonstrate compliance with Firmex's obligations under the Addendum and applicable Data Protection Rules in the form of its SOC 2 Type II audit reports, documentation, or compliance information Firmex makes generally available to its Subscribers.

8. USE OF SUBPROCESSORS

8.1 Subscriber hereby acknowledges and provides general authorization for Firmex to use Subprocessors to Process Personal Data. Firmex's current list of Subprocessors is available at https://www.firmex.com/sub-processors/. Firmex shall: (a) ensure that any Subprocessors

Process Personal Data only to deliver the Services Firmex has retained them to provide; (b) impose on any Subprocessor contractual obligations relating to Personal Data no less protective than this Addendum; and (c) be liable for each Subprocessor's compliance with such obligations.

8.2 If Firmex intends to appoint or replace a Subprocessor covered by this Addendum, at least sixty (60) days prior to allowing the new Subprocessor to Process Personal Data, Firmex shall notify by updating its Subprocessor site giving Subscriber the opportunity to object to such changes on reasonable grounds related to data protection. If the parties are unable to achieve a resolution, Subscriber, as its sole and exclusive remedy, may provide written notice to Firmex terminating the Order(s).

9. RETURN AND DELETION OF PERSONAL DATA

Upon the request of the Subscriber or upon termination of this Addendum, Firmex will, return (in accordance with the Order) or destroy all Personal Data and copies thereof, unless applicable Data Protection Rules or another legal obligation require Firmex to retain Personal Data for longer. Upon the request of the Subscriber, Firmex will certify that this has been done.

10. LIABILITY

Without prejudice to the rights or remedies available to Data Subjects under Data Protection Rules, the liability of the Parties and the limitation thereof, including any claim brought by an Affiliate, shall be in accordance with the Agreement.

Subscriber:		**Firmex:**	
By:	_____	By:	_____
Name:	_____	Name:	_____
Title:	_____	Title:	_____
Date:	_____	Date:	_____

Appendix 1: Processed Personal Data and Purposes

Personal Data are transferred and Processed for the following purposes:

- Secure online repository and data sharing for corporate transactions or internal business purposes.

SUBJECT MATTER AND NATURE OF PROCESSING

- As described in the Agreement, Firmex provides secure online repository tools for storing, managing, collaborating on, and distributing data and documents.

CATEGORIES OF PERSONAL DATA

The types of Personal Data are determined and controlled by Subscriber in its sole discretion, and may include, but are not limited to:

- Names, address, company email address, company phone number, compensation and benefits, holiday and pension information, job titles and functions and potentially other types of Personal Data uploaded by Subscriber Host Users (with upload rights) onto the Website.

SPECIAL CATEGORIES OF DATA ***(if applicable)***

Subject to any applicable condition in the Agreement, the types of Special Categories of Data are determined and controlled by Subscriber in its sole discretion, and may include, but are not limited to:

- None, unless otherwise identified by Subscriber.

DATA SUBJECTS

The categories of Data Subjects to which Personal Data relate are determined and controlled by Subscriber in its sole discretion, and may include, but are not limited to:

- Business information regarding current, past, and prospective owners, employees, agents, Subscribers, advisors, business partner, contractors, and vendor data subjects.

RETENTION

- All Personal Data is permanently deleted after termination of the Agreement between Subscriber and Firmex.

Appendix 2

TECHNICAL AND ORGANISATIONAL MEASURES INCLUDING TECHNICAL AND ORGANISATIONAL MEASURES TO ENSURE THE SECURITY OF THE DATA

	Security Requirement	How Firmex Implements the specific information security measure
1.	*Measures for encryption of personal data*	Personal Data is encrypted at rest and in-transit using industry standard encryption technologies, currently at rest using AES 256-bit encryption and In-transit via Transport Layer Security (TLS) 1.3 protocol, which shall be updated from time to time in line with reasonable technological developments as determined by Firmex.
2.	*Measures for ensuring ongoing confidentiality, integrity, availability, and resilience of processing systems and services*	Firmex is SOC 2 Type II compliant ensuring that it maintains and enforces appropriate administrative, physical and technical safeguards to protect the security, availability and confidentially of Subscriber's Personal Data.

	Security Requirement	How Firmex Implements the specific information security measure
3.	*Measures for ensuring the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident*	Firmex has redundancy with each platform and maintains logs of system availability. In addition, redundancy allows for continuous system backups. Firmex has Disaster Recovery and Business Continuity Plans that are reviewed, updated, and tested periodically.
4.	*Processes for regularly testing, assessing, and evaluating the effectiveness of technical and organizational measures in order to ensure the security of the processing*	Firmex completes regular code reviews, vulnerability testing and annual penetration testing on the Website.
5.	*Measures for user identification and authorization*	Access is governed by Firmex's access management standard that follows roles-based access controls. Access to Personal Data is provided only to personnel as strictly necessary for the sole purpose of satisfying Subscriber's instructions. The Access Management Standard requires that (a) access rights be reviewed, updated, and approved by management on a regular basis, and (2) access rights be withdrawn within 24 hours of employee's termination. Other types of relevant controls are password requirements, multi- factor authentication and restriction on removable media which are implemented at the corporate level.
6.	*Measures for the protection of data during transmission*	Personal Data is encrypted in transit using industry standard encryption technologies, currently via Transport Layer Security (TLS) 1.3 protocol, which shall be updated from time to time in line with reasonable technological developments as determined by Firmex.
7.	*Measures for the protection of data during storage*	Personal Data is encrypted at rest using industry standard encryption technologies, currently AES 256-bit encryption, which shall be updated from time to time in line with reasonable technological developments as determined by Firmex.
8.	*Measures for ensuring physical security of locations at which personal data are processed*	Firmex relies on cloud service providers for its data storage requirements. Information regarding AWS physical security protocols for its server locations is available at: https://aws.amazon.com/compliance/data-center/controls/. All data centers hold ISO 27001:2013 and SOC 2 Type II certifications. With respect to Firmex's facilities, all offices require badge access and utilize video surveillance using cameras with recordings stored in the cloud.
9.	*Measures for ensuring events logging*	Firmex performs logging and monitoring. Logs are retained for 365 days, and access is roles and responsibility based.
10.	*Measures for ensuring system configuration, including default configuration*	Firmex has standard build processes and applies CIS hardening standards.
11.	*Measures for internal IT and IT security governance and management*	Firmex maintains a robust information security management system governed by Firmex's Security and Compliance team that is responsible for implementing and maintaining a stable and secure environment.
12.	*Measures for certification/ assurance of processes and products*	Firmex has maintained a SOC 2 Type II attestation.

	Security Requirement	How Firmex Implements the specific information security measure
13.	*Measures for ensuring data minimization*	Personal Data collected and processed will not be held or used unless necessary to provide the Services in compliance with the Agreement and Firmex's policies and Privacy Notice.
14.	*Measures for ensuring data quality*	Firmex utilizes an anti-malware client on the Website. Personal Data uploaded to the Website is scanned by Firmex's anti- malware software as part of the document processing activities that occur within the platform.
15.	*Measures for ensuring limited data retention*	Personal Data is purged upon termination of Agreement.
16.	*Measures for ensuring accountability*	All activity logged is tracked and reportable. Personnel complete training and acknowledge compliance with Firmex's code of conduct and policies annually. All personnel are required to sign an NDA.
17.	*Measures for allowing data portability and ensuring erasure*	Subscriber host Personal Data on servers as defined in the Agreement which may be designated by Subscriber on prior to creation of the Website. Personal Data can be returned to clients via encrypted USB device, if requested. Deletion of Personal Data upon request or termination of the Agreement.
18.	*For transfers to (sub-) processors, also describe the specific technical and organizational measures to be taken by the (sub-) processor to be able to provide assistance to the controller and, for transfers from a processor to a sub-processor, to the data exporter*	Firmex maintains a Vendor Security Standard that details minimum vendor security standards necessary to store, process or transmit Personal Data that provides a baseline of control expectations for the evaluation of each vendor, conformance and risk acceptance based on the nature of the vendor relationship. Each in scope vendor is required to sign contracts (DPA SCCs) that ensure the same level or protection to Firmex as Firmex obligations to Subscriber.

Appendix 3: Standard Contractual Clauses

For the purposes of applicable Data Protection Laws for the transfer of personal data to processors established in third countries which do not ensure an adequate level of data protection

Name of the data exporting organisation: Subscriber as defined by the ORDER, unless otherwise identified in Annex 1.A:

(“**the data exporter**”)

AND

Name of the data importing organisation: Firmex Corp

(collectively “**the data importer**”) each a “party”; together “the parties”,

SECTION I

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)[1] for the transfer of personal data to a third country.

(b) The Data Exporter and Data Importer have agreed to these standard contractual clauses ("Clauses")

(c) These Clauses apply with respect to the transfer of personal data as specified in Annex 1.B.

(d) The Appendix to these Clauses containing the Annexes 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) [1]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(b), 8.9(a), (c), (d) and (e);

(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);

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

[1] Where the data exporter is a processor subject to Regulation (EU) 2016/679 acting on behalf of a Union institution or body as controller, reliance on these Clauses when engaging another processor (sub-processing) not subject to Regulation (EU) 2016/679 also ensures compliance with Article 29(4) of Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC (OJ L 295, 21.11.2018, p. 39), to the extent these Clauses and the data protection obligations as set out in the contract or other legal act between the controller and the processor pursuant to Article 29(3) of Regulation (EU) 2018/1725 are aligned. This will in particular be the case where the controller and processor rely on the standard contractual clauses included in Decision 2021/915.

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.B.

Clause 7 - Docking clause

(a) An entity that is not a Party to these Clauses may, with the agreement of the Parties, accede to these Clauses at any time, either as a data exporter or as a data importer, by completing and signing Appendix 1.A.

(b) Once it has completed and signed Appendix 1.A, the acceding entity shall become a Party to these Clauses and have the rights and obligations of a data exporter or data importer in accordance with its designation in Appendix 1.A.

(c) The acceding entity shall have no rights or obligations arising under these Clauses from the period prior to becoming a Party.

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 importer shall process the personal data only on documented instructions from the data exporter. The data exporter may give such instructions throughout the duration of the contract.

(b) The data importer shall immediately inform the data exporter if it is unable to follow those instructions.

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.B, unless on further instructions 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 the measures described in Annex II and personal data, the data exporter may redact part of the text of the Appendix to these Clauses 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. This

Clause is without prejudice to the obligations of the data exporter under Articles 13 and 14 of Regulation (EU) 2016/679.

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 erase or rectify 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 Annex I.B. 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 data exporter 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, the Parties 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 subjects. 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. In complying with its obligations under this paragraph, the data importer shall at least implement the technical and organisational measures specified in Annex II. 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 personal 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 the data exporter without undue delay 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 breach including, where appropriate, 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 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 described in Annex I.B.

8.8 Onward transfers

(a) The data importer shall only disclose the personal data to a third party on documented instructions from the data exporter. In addition, the data may only be disclosed to a third party located outside the European Union[2] (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:

[2] The Agreement on the European Economic Area (EEA Agreement) provides for the extension of the European Union's internal market to the three EEA States Iceland, Liechtenstein and Norway. The Union data protection legislation, including Regulation (EU) 2016/679, is covered by the EEA Agreement and has been incorporated into Annex XI thereto. Therefore, any disclosure by the data importer to a third party located in the EEA does not qualify as an onward transfer for the purpose of these Clauses.

(i) the onward transfer is to a country benefitting 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 Regulation of (EU) 2016/679 with respect to the processing in question;

(iii) the onward transfer is necessary for the establishment, exercise or defence 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 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 data exporter.

(c) The data importer shall make available to the data exporter all information necessary to demonstrate compliance with the obligations set out in these Clauses and at the data exporter's request, allow for and contribute to audits of the processing activities covered by these Clauses, at reasonable intervals or if there are indications of non-compliance. In deciding on a review or audit, the data exporter may take into account relevant certifications held by the data importer.

(d) 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.

(e) 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.[3]

Clause 9 - Use of sub-processors

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

(b) Where the data importer engages a sub-processor to carry out specific processing activities (on behalf of the data exporter), 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. [3] 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 request, a copy of such a sub-processor agreement and any subsequent amendments to the data exporter. 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.

[3] This requirement may be satisfied by the sub-processor acceding to these Clauses under the appropriate Module, in accordance with Clause 7.

Clause 10 - Data subject rights

(a) The data importer shall promptly notify the data exporter of any request it has received from a data subject. It shall not respond to that request itself unless it has been authorised to do so by the data exporter.

(b) The data importer shall assist the data exporter in fulfilling its obligations to respond to data subjects' requests for the exercise of their rights under Regulation (EU) 2016/679. In this regard, the Parties shall set out in Annex II 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 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 r esidence 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.

110 Spadina Avenue, Suite 700
Toronto, Ontario M5V 2K4

North America
+1.888.688.4042

Europe
+44 (0)20.3371.8476

International
+1.416.840.4241

firmex.com

Clause 13 - Supervision

(a) 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 Annex 1.C, 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[4];

(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).

(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 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.

---

[4] As regards the impact of such laws and practices on compliance with these Clauses, different elements may be considered as part of an overall assessment. Such elements may include relevant and documented practical experience with prior instances of requests for disclosure from public authorities, or the absence of such requests, covering a sufficiently representative time-frame. This refers in particular to internal records or other documentation, drawn up on a continuous basis in accordance with due diligence and certified at senior management level, provided that this information can be lawfully shared with third parties. Where this practical experience is relied upon to conclude that the data importer will not be prevented from complying with these Clauses, it needs to be supported by other relevant, objective elements, and it is for the Parties to consider carefully whether these elements together carry sufficient weight, in terms of their reliability and representativeness, to support this conclusion. In particular, the Parties have to take into account whether their practical experience is corroborated and not contradicted by publicly available or otherwise accessible, reliable information on the existence or absence of requests within the same sector and/or the application of the law in practice, such as case law and reports by independent oversight bodies.

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.

(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.).

(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.

(e) 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 minimisation

(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.

(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 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 Partiess agree that this shall be the law of Germany.

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 Germany.

(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.

110 Spadina Avenue, Suite 700
Toronto, Ontario M5V 2K4

North America
+1.888.688.4042

Europe
+44 (0)20.3371.8476

International
+1.416.840.4241

firmex.com

Annex 1

A. LIST OF PARTIES

Data exporter:

Name: Subscriber as defined by the ORDER, unless otherwise identified herein:

Address:

Contact person's name, position and contact details:

Activities relevant to the data transferred under these Clauses:
Data Exporter uses SaaS-based electronic secure online repository tools ("Website") for storing, managing, collaborating on and distributing data and documents ("Materials") pursuant to a service agreement between Data Exporter and Data Importer ("Agreement") (the "Services"). The Data Importer stores Materials on third party servers within the EU, US, and Canada to provide the Website to Data Exporter and host their Materials, which while not assessed for its substance, may contain Personal Data. Website's Materials remains stored on those servers, but may be accessed from Data Importers' personnel for the purpose of providing the Services as further described in
Appendix 1.
Role: Controller

Data importer:

Name: Firmex Corp, a limited liability company registered in Delaware, USA
Address: 251 Little Falls Drive, Wilmington, DE 19808

Contact person's name, position and contact details:
Patricia Elias, Director, Secretary and Data Protection Officer, patricia.elias@datasite.com, 651 632 4042

Activities relevant to the data transferred under these Clauses:
Data Importer provides the Website to Data Exporter to host Data Exporters's Materials on third party servers within the EU, US or Australia. The Materials, while not assessed for its substance, may contain Personal Data. Materials remains stored on those servers, but may be accessed from Data Importers' personnel for the purpose of providing the Services as further described in Appendix 1.
Role: Processor

B. DESCRIPTION OF TRANSFER

See Appendix 1 of the DPA

C. COMPETENT SUPERVISORY AUTHORITY

- *Germany Federal Commissioner for Data Protection and Freedom of Information*

110 Spadina Avenue, Suite 700
Toronto, Ontario M5V 2K4

North America
+1.888.688.4042

Europe
+44 (0)20.3371.8476

International
+1.416.840.4241

firmex.com

Annex 2

TECHNICAL AND ORGANISATIONAL MEASURES INCLUDING TECHNICAL AND ORGANISATIONAL MEASURES TO ENSURE THE SECURITY OF THE DATA

See Appendix 2 of the DPA

Appendix 4

INTERNATIONAL DATA TRANSFER ADDENDUM TO THE EU COMMISSION STANDARD CONTRACTUAL CLAUSES

This Addendum has been issued by the Information Commissioner for Parties making Restricted Transfers. The Information Commissioner considers that it provides Appropriate Safeguards for Restricted Transfers when it is entered into as a legally binding contract.

Part 1: Tables

Table 1: PARTIES AND SIGNATURE
Subscriber as defined by the ORDER, unless otherwise identified herein:

Execution of the Data Processing Agreement ("DPA") which this Addendum is appended to is deemed execution of this UK Addendum

hereinafter the '**Exporter;**' AND

Firmex Corp, a limited liability company registered in Delaware, USA

Key Contact: Patricia Elias, Director, Secretary and Data Protection Officer, patricia.elias@datasite.com, 651 632 4042
Execution of the DPA which this Addendum is appended to is deemed execution of this UK Addendum

hereinafter the '**Importer.**'

Table 2: SELECTED SCCS, MODULES AND SELECTED CLAUSES

Addendum EU SCCs:

Controller to Processor (Module 2) standard contractual clauses for the transfer of Personal Data to Processors established in third countries under Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016, adopted by Commission Implementing Decision (EU) 2021/914 of the European Commission dated 4 June 2021, as updated, amended, replaced or superseded from time to time ("EU SCCs")

Date: Effective Date of the Agreement

Reference: None

Table 3: APPENDIX INFORMATION

"Appendix Information" means the information which must be provided for the selected modules as set out in the Appendix of the Approved EU SCCs (other than the Parties), and which for this Addendum is set out in:

Annex 1A: List of Parties: See Part A of Annex 1 of Approved EU SCC's

Annex 1B: Description of Transfer: See Part B of Annex 1 of Approved EU SCC's

Annex II: See Appendix 2 of the DPA

Annex III: https://www.firmex.com/sub-processors/

Table 4: ENDING THIS ADDENDUM WHEN THE APPROVED ADDENDUM CHANGES
Ending this Addendum when the Approved Addendum changes:

Which Parties may end this Addendum as set out in Section 19: Importer and Exporter

Part 2: MANDATORY CLAUSES

Mandatory Clauses:

Part 2: Mandatory Clauses of the Approved Addendum, being the template Addendum B.1.0 issued by the ICO and laid before Parliament in accordance with s119A of the Data Protection Act 2018 on 2 February 2022, as it is revised under Section 18 of those Mandatory Clauses.

110 Spadina Avenue, Suite 700
Toronto, Ontario M5V 2K4

North America
+1.888.688.4042

Europe
+44 (0)20.3371.8476

International
+1.416.840.4241

firmex.com