Statisfy Data Processing Addendum

This Data Processing Addendum (hereinafter **"DPA"**) is effective as of as of January 28, 2025 **("Effective Date"**) by and between [ ] (the **"Controller"**) having its registered office at [.], and Statisfy Inc. (the **"Processor"**) having its registered office at 101 Jefferson St, #227A, Menlo Park, CA 94025. The Controller and the Processor are individually referred to as **"Party"** and collectively as **"Parties"**. This DPA supplements the [.] agreement dated [.], executed between the Parties ("**Agreement**") under which the Processor provides the Controller [.] services (the "**Services**").

The Parties seek to implement this DPA in order to comply with the requirements of EU and UK Data Protection Law, the CCPA and the CPRA (as defined hereunder) in relation to Processor's Processing of Personal Data (each capitalised term as defined under the EU and UK Data Protection Law) as part of its obligations under the Agreement. The terms **"Process"**, **"Processing"** and **"Personal Data"** used in this DPA shall have the same meaning as defined in the EU and UK Data Protection Law. The terms "Business Purpose," "Consumer," "Contractor," "Personal Information," "Sell," "Service Provider," "Share," and "Third Party" shall have the meanings ascribed to them under the CPRA.

This DPA shall apply to Processor's Processing of Personal Data, whether provided by the Controller or its client (the **"Client"**) or/and its affiliates, or otherwise, as part of Processor's obligations under the Agreement.

Except as modified below, the terms of the Agreement shall remain in full force and effect.

1. Definitions.

Capitalized terms not otherwise defined herein shall have the meaning given to them in the EU and UK Data Protection Law, the CCPA, the CPRA or the Agreement. The following terms shall have the corresponding meanings assigned to them below:

1.1. "**Data Transfer**" means (1) a transfer of the Personal Data from the Client to Controller or the Processor on behalf of the Controller; or (2) an onward transfer of the Personal Data from the Controller to the Processor, or between two establishments of the Processor, or with a Sub processor by the Processor.

1.2. **"EU and UK Data Protection Law**" means the EU General Data Protection Regulation 2016/679 "GDPR", and any applicable national laws made under the GDPR, and any regulation superseding any of the foregoing and the UK Data Protection Law.

1.3. "**EU Standard Contractual Clauses**" means the contractual clauses attached hereto as Schedule 1 pursuant to the European Commission's IMPLEMENTING DECISION (EU) 2021/914 of 4 June 2021 on Standard Contractual Clauses for the transfer of Personal Data to processors established in third countries which do not ensure an adequate level of data protection or any updated version thereof.

1.4. **"IDTA"** means International Data Transfer Addendum to the EU Standard Contractual Clauses the contractual clauses attached hereto as Schedule 2 issued by the commissioner under S119A(1) Data Protection Act 2018.

1.5. "**Sub processor**" means a processor/ sub-contractor appointed by the Processor for the provision of all or parts of the Services and who Processes the Personal Data as provided by the Controller and/or the Processor.

1.6. **"UK Data Protection Law"** means the UK GDPR, the United Kingdom Data Protection Act 2018, the Privacy and Electronic Communications Regulations, and any regulation superseding any of the foregoing.

1.7. "**CCPA**" means the California Consumer Protection Act of 2018

1.8. "**CPRA**" means the California Privacy Rights Act of 2020.

2. Purpose of this Addendum:

This DPA sets out various obligations of the Processor in relation to the Processing of Personal Data and shall be limited to the Processor's obligations under the Agreement. If there is a conflict between the provisions of the Agreement and this DPA, the provisions of this DPA shall prevail.

3. Categories of Personal Data and Data Subjects. The Controller authorizes the Processor to Process such Personal Data the extent of which is determined and controlled by the Controller. The current nature of the Personal Data is specified in Annex 1 to Schedule 1 and Appendix 1 to Schedule 2 to this DPA.

4. Purpose of Processing. The objective of Processing of Personal Data by the Processor shall be limited to the Processor's provision of the Services to the Controller/ its Client, pursuant to the Agreement.

5. Controller's Processing of Personal Data. The Controller warrants that it has the right and authority to request the Processor to Process the Personal Data and that its instructions for the Processing of Personal Data shall comply with applicable data protection laws and regulations. The Controller shall have sole responsibility for the accuracy, quality, and legality of Personal Data, and the means by which the Controller acquired Personal Data.

6. Duration of Processing. The Processor will Process Personal Data for the duration of the Agreement, unless otherwise agreed upon in writing by the Controller.

7. The Processor's obligations.

a. The Processor will follow written and documented instructions received, including by email, from the Controller, its affiliate, agents or personnel, with respect to the Processing of Personal Data (each, an "**Instruction**").

b. The Processing described in the Agreement and the relating documentation shall be considered as Instruction from the Controller.

c. At the Controller's request, the Processor will provide reasonable assistance to the Controller in responding to/ complying with requests / directions by Data Subject in exercising their rights or of the applicable regulatory authorities regarding Processor's Processing of Personal Data.

d. Processor may notify Controller if an instruction, in Processor's opinion, infringes the EU and UK

Data Protection Law, the CCPA and the CPRA and further reserves its right not to provide any further assistance on such reported instruction.

8. **Processing purposes, scope, and Controller's processing instructions.**

Processor shall only process Personal Information in accordance with Controller's instructions and to the extent necessary for providing the services as described in the Agreement, which constitutes a business purpose under the CCPA and the CPRA. To the extent the CCPA and the CPRA applies, the parties acknowledge that Controller's transfer of any Personal Information to Processor is not a sale, and Processor provides no monetary or other valuable consideration to Controller in exchange for Personal Information. Except as otherwise instructed by Controller, Processor is prohibited from (a) selling the Personal Information or (b) collecting, retaining, using or disclosing the Personal Information for any purpose (including any commercial purpose) other than for the specific purpose of providing the services under the Agreement, or as otherwise permitted by the CCPA and the CPRA. Processor shall not further collect, sell, or use Personal Information except as necessary to perform services under the Agreement. For the avoidance of doubt, Processor shall not use the Personal Information for the purpose of providing services to another person or entity, except that Processor may combine Personal Information received from one or more entities to which it provides similar services to the extent necessary to detect data security incidents or protect against fraudulent or illegal activity. The Agreement, this DPA and any additional data processing instructions provided by Controller shall constitute "instructions", so long as any additional or alternate instructions are consistent with the purpose and scope of the Agreement and are provided and/or confirmed in writing by the Controller. Processor shall immediately notify Controller if an instruction, in Processor's opinion, infringes the GDPR, the CCPA, the CPRA or any other applicable law.

9. **Data subject requests.**

CCPA.

Processor shall provide reasonable assistance to Controller for the fulfilment of Controller's obligation to respond to and address requests of Data Subjects who are consumers under the CCPA and the CPRA relating to rights provided by the CCPA and the CPRA. Controller shall be responsible for any costs arising from Processor's provision of such assistance. Processor shall not be required to delete any of the Personal Information to comply with a request to exercise the CCPA and the CPRA rights directed by Controller if it is necessary to maintain such information in accordance with Cal. Civ. Code 1798.105(d), in which case Processor shall promptly inform Controller of the exceptions relied upon under 1798.105(d) and Processor shall not use the Personal Information retained for any other purpose than provided for by that exception.

10. **Data Secrecy.** To Process the Personal Data, the Processor will only use personnel who are (i) informed of the confidential nature of the Personal Data, (ii) actually performing the Services in accordance with the Agreement. The Processor will regularly train individuals having access to Personal Data in data security and data privacy in accordance with accepted industry practice and shall ensure that all the Personal Data is kept as strictly confidential. Further, the Processor will maintain appropriate technical and organizational measures for protection of the security,

confidentiality and integrity of the Personal Data as per the specifications as per the standards mutually agreed in writing by the Parties. For this clause, an email form of communication by the Parties in determining project specific security standards shall be accepted.

11. **Data Protection Impact Assessments.** Upon Controller's request, the Processor will provide the Controller with reasonable cooperation and assistance needed to fulfil the Controller's obligation under the EU and UK Data Protection Law to carry out a data protection impact assessment related to the Controller's use of the Services.

12. **Audit Rights.**

    a. Upon Controller's reasonable request, the Processor will make available to the Controller, information as is reasonably necessary to demonstrate Processor's compliance with its obligations under the GDPR or other applicable laws in respect of its Processing of the Personal Data. When the Controller wishes to conduct the audit (by itself or through a representative) at Processor's site, it shall provide at least thirty (30) days' prior written notice to the Processor; the Processor will provide reasonable cooperation and assistance in relation to audits, including inspections, conducted by the Controller or its representative.

    b. The Controller shall bear the expense of such an audit.

13. **Mechanism of Data Transfers.** Any Data Transfer for the purpose of Processing by the Processor in a country outside the European Economic Area (the "***EEA***") shall only take place in compliance with the EU Standard Contractual Clauses and UK Standard Contractual Clauses as detailed in Schedule 1 and Schedule 2 to the DPA as the case may be. Where such model clauses have not been executed at the same time as this DPA, the Processor shall not unduly withhold the execution of such template model clauses, where the transfer of Personal Data outside of the EEA is required for the performance of the Agreement.

14. **Sub processors.**

    a. The Controller acknowledges and agrees that the Processor may engage a third-party Sub processor(s) in connection with the performance of the Services. The current Sub processors engaged by the Processors and approved by the Controller are listed in Schedule 2 hereto. The Processor shall remain liable to Controller for any failure on behalf of a Sub processor to fulfil its data protection obligations under the DPA in connection with the performance of the Services.

    b. The Processor shall execute the appropriate written agreements with the Sub processors in accordance with, and not less protective than, the provisions of this DPA.

    c. If the Controller has a concern that the Sub processor(s) Processing of Personal Data is reasonably likely to cause the Controller to breach its data protection obligations under the GDPR, the Controller may object to Processor's use of such Sub processor and the Processor shall comply with the directions/ Instructions of the Controller.

15. **Personal Data Breach Notification.**

    a. The Processor shall maintain defined procedures in case of a Personal Data Breach (as defined

under the EU and UK Data Protection Law) and shall without undue delay notify Controller if it becomes aware of any Personal Data Breach, unless such Data Breach is unlikely to result in a risk to the rights and freedoms of natural persons.

b. The Processor shall provide the Controller with all reasonable assistance to comply with the notification of Personal Data Breach to Supervisory Authority and/or the Data Subject, to identify the cause of such Data Breach and take such commercially reasonable steps as reasonably required to mitigate and remedy such Data Breach.

c. No Acknowledgement of Fault by Processor. Processor's notification of or response to a Personal Data Breach under this DPA will not be construed as an acknowledgement by Processor of any fault or liability with respect to the data incident.

16. Return and Deletion of Personal Data.

a. The Processor shall at least thirty (30) days from the end of the Agreement or cessation of the Processor's Services under the Agreement, whichever occurs earlier, the Processor shall have the Personal Data deleted, or if the Controller so instructs, shall return to the Controller all the Personal Data. The Processor shall return such Personal Data in a commonly used format or in the then current format in which it was stored at discretion of the Controller, soon as reasonably practicable following receipt of Controller's notification.

b. In any case, the Processor shall delete Personal Data including all the copies of it as soon as reasonably practicable following the end of the Agreement.

17. Technical and Organizational Measures. Having regard to the state of technological development and the cost of implementing any measures, the Processor will take appropriate technical and organizational measures against the unauthorized or unlawful processing of Personal Data and against the accidental loss or destruction of, or damage to, Personal Data to ensure a level of security appropriate to: (a) the harm that might result from unauthorized or unlawful processing or accidental loss, destruction or damage; and (b) the nature of the data to be protected [including the measures stated in Annex 2 of Schedule 1 and Appendix 2 of Schedule 2].

18. Liability The Processor's maximum aggregate liability directly arising under this DPA (whether in contract, tort, including negligence) for all direct damages shall be limited to fees paid by the Controller in 3 months immediately preceding the date on which such claim has arisen. For the avoidance of doubt, this liability cap is an aggregate liability for this agreement and the incidence of more than one claim will not enlarge this limit.

IN WITNESS WHEREOF, this DPA is entered into and becomes a binding part of the Agreement with effect from the Effective Date set out above.

Processor.	**Controller.**
Signature _____	Signature _____
Name _____	Name _____
Title _____	Title _____
Date Signed _____	Date Signed _____

Schedule 1

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)

(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 Annex I.A (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 Annex I.A (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 Annex I.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)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);

(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 Annex I.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 the Appendix and signing Annex I.A.

(b) Once it has completed the Appendix and signed Annex I.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 Annex I.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 Annex I. 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 the 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**

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

(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.

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 10 days 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. 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 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.

(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.

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 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 Annex I.C, 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 Annex I.C, 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 Annex I.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;

(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. 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.

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 the EU Member State in which the data exporter is established. Where such law does not allow for third-party beneficiary rights, they shall be governed by the law of another EU Member State that does allow for third-party beneficiary rights. The Parties agree that this shall be the law 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 Ireland.

(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.

ANNEX I

Data exporter(s)*: [Identity and contact details of the data exporter(s) and, where applicable, of its/their data protection officer and/or representative in the European Union]*

Name:	
Address:	
Contact person's name, position and contact details:	
Activities relevant to the data transferred under these Clauses:	
Signature and date:	Refer date of DPA signing.
Role (controller/processor):	Controller

Data importer(s): [Identity and contact details of the data importer(s), including any contact person with responsibility for data protection]

Name:	Statisfy Inc.
Address:	101 Jefferson St, #227A, Menlo Park, CA 94025
Contact person's name, position and contact details:	*Data Protection Officer, privacy@statisfy.com*
Activities relevant to the data transferred under these Clauses:	Processing on behalf of the Controller for rendering Services.
Signature and date:	Refer date of Agreement.
Role (controller/processor):	Processor

B. ***DESCRIPTION OF TRANSFER***

Categories of data subjects whose personal data is transferred:	
Categories of personal data transferred:	Name, Email address
Sensitive data transferred (if applicable) and applied restrictions or safeguards that fully take into consideration the nature of the data and the risks involved, such as for instance strict purpose limitation, access restrictions (including access only for staff having followed	Not Applicable

specialised training), keeping a record of access to the data, restrictions for onward transfers or additional security measures.	
The frequency of the transfer (e.g. whether the data is transferred on a one-off or continuous basis).	Continuously
Nature of the processing:	Data is collected and stored to link customer accounts with employee account owners
Purpose(s) of the data transfer and further processing:	To improve and streamline customer engagement processes, and drive customer retention and growth
The period for which the personal data will be retained, or, if that is not possible, the criteria used to determine that period:	Data is retained for the duration of the customer relationship
For transfers to (sub-) processors, also specify subject matter, nature and duration of the processing	Data is transferred to sub-processor for delivery of Statisfy services. Other than two sub-processors (Google Cloud and Clerk), data is not persisted with any other sub-processors

C. COMPETENT SUPERVISORY AUTHORITY

Identify the competent supervisory authority/ies in accordance with Clause 13

ANNEX II

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

Statisfy maintains an annually audited SOC2 Type 2 report, which is available on request.

Further, Statisfy has a trust centre containing all policies and procedures depicting the technical and organisational measures to ensure the security of the data, link is available upon request.

ANNEX III

LIST OF SUB-PROCESSORS

The controller has authorised the use of the following sub-processors:

1. Name: Google Cloud Platform

Country: USA

Description: Cloud hosting provider providing compute, storage, AI services (Gemini, model hosting) etc.

2. Name: Paragon

Country: USA

Description: Integration provider to connect to various SaaS applications.

3. Name: Clerk

Country: USA

Description: Auth provider.

4. Name: Recall

Country: USA

Description: Meeting recorder for Notetaker.

5. Name: Deepgram

Country: USA

Description: Speech to text.

6. Name: OpenAI

Country: USA

Description: Various LLMs & embedding models.

7. Name: Pendo

Country: USA

Description: Analytics, Inapp Guides etc.

8. Name: Sentry

Country: USA

Description: Application monitoring, crash reporting

9. Name: Sendgrid

Country: USA

Description: Sending Email

10. Name: PostHog

Country: USA

Description: Analytics

11. Name: Microsoft Azure

Country: USA

Description: Various LLMs & embedding models.

12. Name: Anthropic

Country: USA

Description: LLMs

Schedule 2

IDTA

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

Start date		
The Parties	Exporter (who sends the Restricted Transfer)	Importer (who receives the Restricted Transfer)
Parties' details	Full legal name: *As per Schedule 1, Annex I of this DPA.* Trading name (if different): Main address (if a company registered address): *As per Schedule 1, Annex I of this DPA.* Official registration number (if any) (company number or similar identifier):	Full legal name: *As per Schedule 1, Annex I of this DPA*. Trading name (if different): Main address (if a company registered address): *As per Schedule 1, Annex I of this DPA.* Official registration number (if any) (company number or similar identifier):
Key Contact	Full Name (optional): *As per Schedule 1, Annex I of this DPA.* Job Title: *As per Schedule 1, Annex I of this DPA.* Contact details including email: *As per Schedule 1, Annex I of this DPA.*	Full Name (optional): *As per Schedule 1, Annex I of this DPA.* Job Title: *As per Schedule 1, Annex I of this DPA.* Contact details including email: *As per Schedule 1, Annex I of this DPA.*
Signature (if required for the purposes of Section 2)		

Table 2: Selected SCCs, Modules and Selected Clauses

Addendum EU SCCs	☒ **The version of the Approved EU SCCs which this Addendum is appended to, detailed below, including the Appendix Information**: Date: As per the DPA date. Reference (if any): Other identifier (if any): Or ☐ the Approved EU SCCs, including the Appendix Information and with only the following modules, clauses or optional provisions of the Approved EU SCCs brought into effect for the purposes of this Addendum:

Module	Module in operation	Clause 7 (Docking Clause)	Clause 11 (Option)	Clause 9a (Prior Authorisation or General Authorisation)	Clause 9a (Time period)	Is personal data received from the Importer combined with personal data collected by the Exporter?
1						
2						
3						
4						

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:
Annex 1B: Description of Transfer:
Annex II: Technical and organisational measures including technical and organisational measures to ensure the security of the data:
Annex III: List of Sub processors (Modules 2 and 3 only):

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 ☒ Exporter ☐ neither Party

Part 2: Mandatory Clauses

Entering into this Addendum

Each Party agrees to be bound by the terms and conditions set out in this Addendum, in exchange for the other Party also agreeing to be bound by this Addendum.

Although Annex 1A and Clause 7 of the Approved EU SCCs require signature by the Parties, for the purpose of making Restricted Transfers, the Parties may enter into this Addendum in any way that makes them legally binding on the Parties and allows data subjects to enforce their rights as set out in this Addendum. Entering into this Addendum will have the same effect as signing the Approved EU SCCs and any part of the Approved EU SCCs.

Interpretation of this Addendum

Where this Addendum uses terms that are defined in the Approved EU SCCs those terms shall have the same meaning as in the Approved EU SCCs. In addition, the following terms have the following meanings:

Addendum	This International Data Transfer Addendum which is made up of this Addendum incorporating the Addendum EU SCCs.
Addendum EU SCCs	The version(s) of the Approved EU SCCs which this Addendum is appended to, as set out in Table 2, including the Appendix Information.
Appendix Information	As set out in Table 3.
Appropriate Safeguards	The standard of protection over the personal data and of data subjects' rights, which is required by UK Data Protection Laws when you are making a Restricted Transfer relying on standard data protection clauses under Article 46(2)(d) UK GDPR.
Approved Addendum	The template Addendum 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.
Approved EU SCCs	The Standard Contractual Clauses set out in the Annex of Commission Implementing Decision (EU) 2021/914 of 4 June 2021.
ICO	The Information Commissioner.
Restricted Transfer	A transfer which is covered by Chapter V of the UK GDPR.
UK	The United Kingdom of Great Britain and Northern Ireland.
UK Data Protection Laws	All laws relating to data protection, the processing of personal data, privacy and/or electronic communications in force from time to time in the UK, including the UK GDPR and the Data Protection Act 2018.
UK GDPR	As defined in section 3 of the Data Protection Act 2018.

This Addendum must always be interpreted in a manner that is consistent with UK Data Protection Laws and so that it fulfils the Parties' obligation to provide the Appropriate Safeguards.

If the provisions included in the Addendum EU SCCs amend the Approved SCCs in any way which is not permitted under the Approved EU SCCs or the Approved Addendum, such amendment(s) will not be incorporated in this Addendum and the equivalent provision of the Approved EU SCCs will take their place.

If there is any inconsistency or conflict between UK Data Protection Laws and this Addendum, UK Data Protection Laws applies.

If the meaning of this Addendum is unclear or there is more than one meaning, the meaning which most closely aligns with UK Data Protection Laws applies.

Any references to legislation (or specific provisions of legislation) means that legislation (or specific provision) as it may change over time. This includes where that legislation (or specific provision) has been consolidated, re-enacted and/or replaced after this Addendum has been entered into.

Hierarchy

Although Clause 5 of the Approved EU SCCs sets out that the Approved EU SCCs prevail over all related agreements between the parties, the parties agree that, for Restricted Transfers, the hierarchy in Section 10 will prevail.

Where there is any inconsistency or conflict between the Approved Addendum and the Addendum EU SCCs (as applicable), the Approved Addendum overrides the Addendum EU SCCs, except where (and in so far as) the inconsistent or conflicting terms of the Addendum EU SCCs provides greater protection for data subjects, in which case those terms will override the Approved Addendum.

Where this Addendum incorporates Addendum EU SCCs which have been entered into to protect transfers subject to the General Data Protection Regulation (EU) 2016/679 then the Parties acknowledge that nothing in this Addendum impacts those Addendum EU SCCs.

Incorporation of and changes to the EU SCCs

This Addendum incorporates the Addendum EU SCCs which are amended to the extent necessary so that:

a. together they operate for data transfers made by the data exporter to the data importer, to the extent that UK Data Protection Laws apply to the data exporter's processing when making that data transfer, and they provide Appropriate Safeguards for those data transfers;

b. Sections 9 to 11 override Clause 5 (Hierarchy) of the Addendum EU SCCs; and

c. this Addendum (including the Addendum EU SCCs incorporated into it) is (1) governed by the laws of England and Wales and (2) any dispute arising from it is resolved by the courts of England and Wales, in each case unless the laws and/or courts of Scotland or Northern Ireland have been expressly selected by the Parties.

Unless the Parties have agreed alternative amendments which meet the requirements of Section 12, the provisions of Section 15 will apply.

No amendments to the Approved EU SCCs other than to meet the requirements of Section 12 may be made.

The following amendments to the Addendum EU SCCs (for the purpose of Section 12) are made:

a. References to the "Clauses" means this Addendum, incorporating the Addendum EU SCCs;

b. In Clause 2, delete the words:

"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";

c. Clause 6 (Description of the transfer(s)) is replaced with:

"The details of the transfers(s) and in particular the categories of personal data that are transferred and the purpose(s) for which they are transferred) are those specified in Annex I.B where UK Data Protection Laws apply to the data exporter's processing when making that transfer.";

d. Clause 8.7(i) of Module 1 is replaced with:

"it is to a country benefitting from adequacy regulations pursuant to Section 17A of the UK GDPR that covers the onward transfer";

e. Clause 8.8(i) of Modules 2 and 3 is replaced with:

"the onward transfer is to a country benefitting from adequacy regulations pursuant to Section 17A of the UK GDPR that covers the onward transfer;"

f. References to "Regulation (EU) 2016/679", "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)" and "that Regulation" are all replaced by "UK Data Protection Laws". References to specific Article(s) of "Regulation (EU) 2016/679" are replaced with the equivalent Article or Section of UK Data Protection Laws;

g. References to Regulation (EU) 2018/1725 are removed;

h. References to the "European Union", "Union", "EU", "EU Member State", "Member State" and "EU or Member State" are all replaced with the "UK";

i. The reference to "Clause 12(c)(i)" at Clause 10(b)(i) of Module one, is replaced with "Clause 11(c)(i)";

j. Clause 13(a) and Part C of Annex I are not used;

k. The "competent supervisory authority" and "supervisory authority" are both replaced with the "Information Commissioner";

l. In Clause 16(e), subsection (i) is replaced with:

"the Secretary of State makes regulations pursuant to Section 17A of the Data Protection Act 2018 that cover the transfer of personal data to which these clauses apply;";

m. Clause 17 is replaced with:

"These Clauses are governed by the laws of England and Wales.";

n. Clause 18 is replaced with:

"Any dispute arising from these Clauses shall be resolved by the courts of England and Wales. A data subject may also bring legal proceedings against the data exporter and/or data importer before the courts of any country in the UK. The Parties agree to submit themselves to the jurisdiction of such courts."; and

o. The footnotes to the Approved EU SCCs do not form part of the Addendum, except for footnotes 8, 9, 10 and 11.

Amendments to this Addendum

The Parties may agree to change Clauses 17 and/or 18 of the Addendum EU SCCs to refer to the laws and/or courts of Scotland or Northern Ireland.

If the Parties wish to change the format of the information included in Part 1: Tables of the Approved Addendum, they may do so by agreeing to the change in writing, provided that the change does not reduce the Appropriate Safeguards.

From time to time, the ICO may issue a revised Approved Addendum which:

a. makes reasonable and proportionate changes to the Approved Addendum, including correcting errors in the Approved Addendum; and/or

b. reflects changes to UK Data Protection Laws;

The revised Approved Addendum will specify the start date from which the changes to the Approved Addendum are effective and whether the Parties need to review this Addendum including the Appendix Information. This Addendum is automatically amended as set out in the revised Approved Addendum from the start date specified.

If the ICO issues a revised Approved Addendum under Section 18, if any Party selected in Table 4 "Ending the Addendum when the Approved Addendum changes", will as a direct result of the changes in the Approved Addendum have a substantial, disproportionate and demonstrable increase in:

a its direct costs of performing its obligations under the Addendum; and/or

b its risk under the Addendum,

and in either case it has first taken reasonable steps to reduce those costs or risks so that it is not substantial and disproportionate, then that Party may end this Addendum at the end of a reasonable notice period, by providing written notice for that period to the other Party before the start date of the revised Approved Addendum.

The Parties do not need the consent of any third party to make changes to this Addendum, but any changes must be made in accordance with its terms.

Alternative 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.