DATA PROCESSING ADDENDUM

This Data Processing Addendum ("DPA") supplements and forms part of each agreement between NSF (hereinafter "the Provider") and Client for Services ("Agreement"). This DPA governs the processing of Personal Data by Provider, in the course of providing certain services in accordance with the Agreement. Client enters into this DPA on behalf of itself and, to the extent required under applicable data protection laws and relevant to the Services, in the name and on behalf of its affiliates. All capitalized terms not defined herein shall have the meaning given to them in the Agreement.

1. **Definitions**. All capitalized terms used in this DPA shall have the meanings given to them below:
   a. "Personal Data" means the personal data (as defined in Applicable Data Protection Laws) which is processed by Provider on behalf of Client under the Agreement.
   b. "Applicable Data Protection Laws" means all international, national, federal, and state laws and regulations, including laws and regulations of the European Union, the United Kingdom and the United States, in each case, to the extent applicable to the Processing of Personal Data under the Agreement.
   c. "processing" 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, restriction, erasure or destruction.

2. **Compliance with Laws.** Provider shall comply with Applicable Data Protection Laws applicable to the role and scope of responsibility with respect to the processing of Personal Data. Client shall comply with Applicable Data Protection laws, including maintaining lawful basis (e.g., consent) and rights to use and provide Personal Data to Provider. Client's instructions for the processing of Personal Data shall comply with Applicable Data Protection Laws.

3. **Instructions.** The nature and purpose of the processing, the type of Personal Data and categories of data subjects processed under this DPA are specified in Schedule 1 (Details of the Processing) to this DPA. Provider shall process Personal Data only on behalf of Client and in compliance with its instructions (which shall include this DPA and any further written agreement or documentation through which Client instructs Provider to perform specific processing of Personal Data) provided that such instructions comply with all applicable laws. In the event of a change in Applicable Data Protection Laws which is likely to have an adverse effect on the obligations provided under this DPA or Client's instructions, Provider will notify Client and Provider shall be entitled to suspend the processing of Personal Data and/or terminate all or part of the Agreement immediately, at no cost and as of right, without prejudice to its other rights and remedies.

4. **Use and Disclosure.** Provider shall treat Personal Data as confidential information and process Personal Data only as necessary to provide the Services to Client. Without limiting the generality of the foregoing, Provider shall not sell any Personal Data and the parties acknowledge and agree that Client does not sell (as such term is defined under Applicable Data Protection Laws) Personal Data to Provider in connection with the Services rendered by Provider to Client pursuant to the Agreement. Provider shall not transfer or disclose (and not allow its employees, contractors, agents or representatives to disclose) Personal Data to any third party (including affiliate) except as necessary to provide the Services to Client or with Client's prior written consent. Provider shall further ensure that access to Personal Data by Provider's employees, contractors, agents or representatives will be granted only on a strict need-to-know basis to provide the Services to Client. Provider warrants that any such employees, contractors, agents and representatives who participate to the processing of Personal Data are informed of the obligations of Provider under this DPA and applicable law and have committed themselves to confidentiality through appropriate contractual arrangements.

5. **Notification of Requests.** To the extent legally permitted, if Provider receives a request to exercise a data subject's right of access, right to rectification, restriction of processing, erasure (e.g., a "right to be forgotten"), data portability, object to the processing, or its right not to be subject to an automated individual decision making (each a "Data Subject Request") regarding Personal Data, Provider shall promptly notify Client or shall otherwise direct such data subject to Client. Taking into account the nature of the processing, Provider shall assist Client by appropriate technical and organizational measures, as is

technically feasible and commercially reasonable, for the fulfilment of Client's obligation to respond to a Data Subject Request under Applicable Data Protection Laws.

6. **Assistance to Client.** Taking into account the nature of the processing and the information available and not otherwise available to Client, Provider shall provide Client with such information and assistance as is reasonably necessary to assist Client in the fulfillment of its obligations under applicable data protection laws, including (i) in responding and acting upon requests from individuals to exercise their privacy rights under applicable law, (ii) Client's legal security obligations, (iii) the realization of a data protection impact assessment, and (iv) the consultation of a supervisory authority, where relevant.

7. **Notification of Security Incident**. Provider shall notify Client without delay upon – and in any event no later than 48 hours after – becoming aware of any security incident leading to the accidental, unauthorized or unlawful destruction, loss, damage, alteration, disclosure of, or access to, Personal Data. Notification provided under this Section shall not be interpreted or construed as an admission of fault or liability by Provider. Provider shall make reasonable efforts to identify the cause of such security incident and take those steps as Provider deems necessary and reasonable in order to remediate the cause of such a security incident to the extent the remediation is within Provider's reasonable control. Additionally, upon request, Provider shall provide Client with relevant information about the security incident, as reasonably required to assist the Client in compliance with its own obligations under Applicable Data Protection Laws to notify any supervisory authority or data subject in the event of a security incident.

8. **Deletion**. Upon written request, Provider shall delete all Personal Data and copies thereof (or, at the choice of Client, return all such Personal Data to Client). Where legislation imposed upon Provider prevents it from returning or deleting all or part of the Personal Data, Provider shall keep the Personal Data confidential cease actively processing it, and delete it as soon as legally allowed.

9. **Inspections.** Client may request, (i) at any time no more than once annually or (ii) where required by any relevant (supervisory) authority: (a) any written technical documentation that Provider makes available or generally provide to its client base; and (b) information regarding Provider's compliance with the obligations in this DPA, which may be provided in the form of the relevant third-party certifications and audits. Client shall promptly provide Provider with information regarding any non-compliance discovered during the course of its review.

10. **Subcontracting.** Provider shall be allowed to engage subcontractors for carrying out specific Personal Data processing activities, subject to the following: (i) Provider shall only retain subcontractors that Provider reasonably expects to appropriately protect the privacy, confidentiality and security of Personal Data; (ii) Provider shall notify Client of any intended changes concerning the addition or replacement of subcontractors, thereby giving Client the opportunity to object to such changes; (iii) Provider shall impose on its subcontractor(s), by way of a written agreement, the same obligations as are imposed on Provider under this DPA; and (iv) Provider remains fully liable to Client for the performance of its subcontractor's obligations.

11. **Cross-Border Data Transfers.** Provider acknowledges that some Applicable Data Protection Laws may require that additional measures be taken to secure transfers of Personal Data outside the country or region the Personal Data originates from. In such a case, Provider and Client shall implement these additional measures and, for instance, enter into separate agreements as directed by Provider, where and as mandated under Applicable Data Protection Law. In regard to transfers outside of the European Union, European Economic Area, Switzerland, and/or the United Kingdom ("Non-European Data Transfers"), the Standard Contractual Clauses and the International Data Transfer Addendum to the EU Standard Contractual Clauses set forth in Schedule 3 to this DPA shall apply subject to the additional terms of Schedule 2. In the event that the foregoing transfer mechanism is determined by any appropriate court or authority with jurisdiction not to be adequate, Provider shall, as soon as possible, adopt an appropriate alternative transfer mechanism and Client shall agree to any changes required by Provider. In any case, Client and Provider agree that, in relation to the transfer and processing of any Personal Data, the terms of the transfer mechanisms used (e.g., separate agreement(s)) will prevail over those of the Agreement and this DPA in case of inconsistency.

12. **Security.** Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of Processing as well as the risks to the rights and freedoms of natural persons, Provider shall implement appropriate physical,

technical and organizational measures to protect Personal Data against accidental or unauthorized loss, theft, alteration, damage, disclosure, access and against all forms of unlawful processing. Such measures shall ensure a level of security appropriate to the risk, including inter alia as appropriate: (i) the pseudonymization and/or encryption of Personal Data; (ii) the protection against viruses, worms, time bombs, Trojan horses and other harmful or malicious code, files, scripts, agents, or programs, including code that is intended to or has the effect of misappropriating, commandeering, or disrupting access to or use or operation of any information, device, or system; and (iii) a process for regularly testing, assessing and evaluating the effectiveness of technical, physical and organizational measures for ensuring the security of the processing.

13. **Term.** This DPA enters into force at the earliest of the execution of the Agreement or this DPA. It will be in force and effect until the Agreement has been terminated or expires.

14. **Entire Agreement.** This DPA sets out the entire agreement and understanding between Client and Provider with respect to the processing of Personal Data by Provider for the purpose of providing the Services and supersedes all other agreements made between Client and Provider on the same subject matter. In case of conflict between the Agreement and this DPA, the terms of this DPA shall prevail.

15. **Severance.** If any provision of this DPA is or becomes illegal, invalid or unenforceable, in any respect, whether by law, a decision of any court or administrative body of competent jurisdiction or otherwise, it shall not affect or impair the legality, validity or enforceability of any other provision of this DPA or the Agreement. In such case, Provider and Client will use reasonable endeavors to negotiate in good faith with a view to replacing it with a valid and enforceable provision which achieves to the greatest extent possible the same effect as would have been achieved by the illegal, invalid or unenforceable provision but differing from the replaced provision as little as possible.

16. **Governing Law.** Except as mandated under Applicable Data Protection Laws, any dispute relating to this DPA shall be governed by and interpreted in accordance with the law of the country and subject to the jurisdiction referred to in the Agreement.

17. **Contact.** Provider has appointed a specified contact to oversee its compliance with this DPA and act as the point of contact in the event of a breach, data subject request, audit or other issue which arises in relation to the processing. Such contact can be reached at data.protection@nsf.org.

Schedule 1 - DETAILS OF THE PROCESSING

Nature and Purpose of Processing

The objective and subject of the processing of Personal Data by Provider, as a processor, is providing, supporting, and operating the provision of the Services. Provider will process Personal Data, in its capacity as a processor, as necessary to perform and operate the Services pursuant to the Agreement and further instructed by Client through its use of the Services.

Type of Personal Data

Client may submit or direct third parties to submit Personal Data to Provider under the Services, which may include, but is not limited to the following categories of Personal Data:

- First and last name
- Title
- Position
- Employer
- Contact information (company, email, phone, physical business address)
- Device identification data and traffic data (e.g. MAC addresses, web logs, etc.)
- Professional life data
- Personal life data
- Localization data

Categories of Data Subjects

Client may submit or direct third parties to submit Personal Data to Provider under the Services, and which may include, but is not limited to Personal Data relating to the following categories of data subjects:

- Prospects, customers, business partners, suppliers, franchisees and vendors of Client (who are natural persons)
- Employees or contact persons of Client's prospects, customers, business partners suppliers, franchisees and vendors
- Employees, agents, advisors, freelancers of Client (who are natural persons)

Schedule 2 - TRANSFER MECHANISMS FOR EUROPEAN DATA TRANSFERS

1. The Standard Contractual Clauses and the International Data Transfer Addendum to the EU Standard Contractual Clauses and the additional terms specified in this Section of this Schedule 2 apply to: (i) Client's legal entity as a data exporter and its authorized affiliates; and (ii) all affiliates of Client established within the European Economic Area, United Kingdom and/or Switzerland. For the purpose of the Standard Contractual Clauses and this Section, the entities referenced in this Section shall be deemed "data exporters." The parties agree that Module 2: controller-to-processor transfers shall apply under the Standard Contractual Clauses, as included in Schedule 3.
2. Appointment of New Sub-processors and List of Current Sub-processors. Pursuant to Clause 9 of the Standard Contractual Clauses, Client acknowledges and expressly agrees that Option 2 shall apply (as reflected in Schedule 3) and that: (a) Provider's affiliates may be retained as sub-processors; and (b) Provider and Provider's affiliates, respectively, may engage third-party sub-processors in connection with the provision of the Services. Provider shall make available to Client the current list of sub-processors in accordance with this DPA.
3. Notice and Objection Rights for New Sub-processors. Pursuant to Clause 9 Option 2 of the Standard Contractual Clauses (as reflected in Schedule 3), Client acknowledges and expressly agrees that Provider may engage new sub-processors as described in the DPA.
4. Copies of Sub-processor Agreements. The parties agree that if copies of sub-processor agreements must be provided pursuant to Clause 9(c) Option 2 of the Standard Contractual Clauses, they may have all commercial information, or clauses unrelated to the applicable data protection legislation, removed beforehand; and, that such copies will be provided in a manner determined by Provider, in its sole discretion and only upon request by Client. If permitted by applicable law, Provider reserves the right to satisfy the obligations referenced in this Section by providing proof of the sub-processor agreements as opposed to copies thereof.
5. Governing law. The parties agree that Option 2 shall apply for Clause 17 (as reflected in Schedule 3). 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 Belgium. For Clause 18(b), the Parties agree that any dispute shall be resolved by the courts of Belgium.

Schedule 3

STANDARD CONTRACTUAL CLAUSES

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

(b) The Parties:

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

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 (in the same country as the data importer or in another third country, hereinafter 'onward transfer') if the third party is or agrees to be bound by these Clauses, under the appropriate Module, or if:

(i) the onward transfer is to a country 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.

(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. 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.

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.

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 _____ (*specify Member State*).

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 _____ (*specify Member State*).

(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

A. LIST OF PARTIES

Data exporter(s):

1.Name: The Client, as defined in the Agreement.

Address: The Client's address, as defined in the Agreement.

Contact person's name, position and contact details: The Client's contact details are specified in the Agreement.

Activities relevant to the data transferred under these Clauses: The Data exporter is the recipient of Services in accordance with the Agreement.

Signature and date: The Parties agree that these Clauses are incorporated by reference into the Agreement and the Data Processing Addendum and the execution of the Agreement by the Data exporter and Data importer shall constitute execution of these Clauses by both parties as of the Effective Date.

Role (controller/processor): Controller

…

Data importer(s):

1.Name: NSF International or its affiliate as defined in the Agreement

Address: 789 N. Dixboro Road, Ann Arbor, Michigan 48105, United States of America

Contact person's name, position and contact details: dataprotection@nsf.org. Further details are available upon request.

Activities relevant to the data transferred under these Clauses: NSF processes personal data for the purpose of providing Service to the Data exporter under the Agreement, including the Data Processing Addendum.

Signature and date: The Parties agree that these Clauses are incorporated by reference into the Agreement and the Data Processing Addendum and the execution of the Agreement by the Data exporter and Data importer shall constitute execution of these Clauses by both parties as of the Effective Date.

Role (controller/processor): Processor

2. …

B. DESCRIPTION OF TRANSFER

The Parties agree that description of transfer shall be as in Schedule 1 of the DPA to which these SCCs are attached.

C. COMPETENT SUPERVISORY AUTHORITY

The Parties agree that the Competent Supervisory Authority shall be the applicable supervisory authority of the jurisdiction in which the Data exporter is located.

ANNEX II

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

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

1. SECURITY POLICY. NSF maintains a company-wide information security program that includes written security policies, standards and procedures based upon ISO 27001 (collectively, the "NSF Information Security Program").
    a. NSF Information Security Program is reviewed and approved at planned intervals or when significant changes occur.
    b. Employees complete annual information security policy and security awareness training.
    c. Contractors are provided access to infosec policy and security awareness materials commensurate to their role.
2. ORGANIZATION OF INFORMATION SECURITY.
    a. Management framework is in place to initiate and control implementation and operation of information security.
    b. All information security responsibilities are defined and allocated with conflicting duties and areas segregated.
3. HUMAN RESOURCES SECURITY
    a. Background checks on candidates for employment are performed in accordance with applicable law.
    b. Agreements in place with employees and contractors address compliance with information security policies and procedures.
    c. System access is promptly removed or modified for those leaving NSF or changing roles.
4. ASSET MANAGEMENT
    a. Asset inventory list is maintained, asset tags are issued through helpdesk and are tied to asset owners on asset inventory list.
    b. NSF maintains an Acceptable Use Policy for assets.
    c. Data Classification Procedure
        i. There is a four-tiered data classification scheme, based on importance, sensitivity and potential for misuse.
        ii. Data assets are assigned a sensitivity level and labeled based on audience and use of data.
    d. Media Handling Policy
        i. This policy is in place for media management, and aligns with the data classification scheme.
        ii. Security measures are in place if removeable media is required for business purposes.
5. ACCESS CONTROL
    a. NSF User Access Control Policy
        i. Access is granteed on need-to-know basis to perform required tasks and least privilege basis with minimum privilege necessary to fulfill the role.
    b. Accounts
        i. All user accounts are unique.
        ii. Privileged user accounts are separate from standard user accounts.
        iii. User access is reviewed annually or when a change in employment occurs.
        iv. Accounts are subject to the NSF Password Policy, and passwords must not be shared or revealed to others.
        v. Multi-factor authentication is required for access to NSF's network, including email and file share applications.
6. CRYPTOGRAPHY
    a. NSF uses cryptography (encryption) solutions to protect information and comply with applicable laws and other requirements.
    b. Encryption solutions in use:
        i. Encryption of data-at-rest where appropriate, including backups.
        ii. Data-In-Use (DIU) to encrypt data on portable/mobile devices.

iii. Data-In-Transit (DIT) encryption in place for restricted data sent outside of NSF.

c. Keys are securely generated and distributed. Keys that have reached the end of their crypto-period are stored. Keys are retired or replaced if their integrity has been weakened or suspected of being compromised.

7. PHYSICAL AND ENVIRONMENTAL SECURITY.
   a. NSF has established secure areas requiring badge or key access for authorized personnel only.
   b. Cameras are in key areas to monitor and log activity.
   c. A risk-based process is in place to identify potential threats and vulnerabilities to offices, rooms storing restricted or confidential data, server rooms, IT storage areas, wiring closets, delivery areas, and laboratories.
   d. Procedural controls are in place to secure laboratory areas, and such controls include restrictions on use of recording equipment and restriction on unsupervised working within secure areas wherever possible.
   e. Assets including storage media are verified to ensure sensitive data and licensed software have been removed or securely overwritten prior to disposal or re-use.
   f. Security controls are applied to offsite assets.
   g. Assessments are performed to review operation of controls on a periodic basis.
8. OPERATIONS SECURITY
   a. Operating procedures are documented, and are made available as needed to perform job duties.
   b. Change management processes are documented for networks, systems and applications changes.
   c. Separation of development, testing and production environments is in place.
      i. Changes are tested in a separate environment.
      ii. Administrators do not have access to the live environment.
         1. Admin accounts, log monitoring and review are in place; appropriate levels of authorization are required for moving changes from one environment to another.
   d. Malware protection
      i. Such protection includes but is not limited to anti-virus software on endpoints and servers.
      ii. Patching of known system and software vulnerabilities is performed in a timely manner on critical systems.
   e. Vulnerability management scans
      i. Such scans are performed on servers and laptops, using CVSS based (Common Vulnerability Scoring System) risk scores; these scores are communicated the NSF Infrastructure team for analysis and remediation.
      ii. Managed Detection and Response service is used to perorm 24/7/365 montioring and proactive threat hunting.
      iii. Independent third parties perform annual network penetration tests.
   f. Monthly phishing campaigns are in place. Results are tracked and reported to senior leadership, and action is taken for anyone who falls victim
   g. Backups
      i. NSF performs regular testing of backup copies of information, software and system images to ensure restorations will be successful and timely.
      ii. Backups are protected and stored separately from production environment.
      iii. Backups, including review of failed backups, are monitored.
   h. Logs
      i. Logs of all types (e.g., system and event logs recording user activities, exceptions, faults and information security events) are stored in NSF's log aggregator.
      ii. NSF uses SIEM (Security Incident and Event Management) to identify and respond to incident and for investigation capabilities
      iii. Log information is secure, and is protected against tampering and unauthorized access.
      iv. Log procedures are regularly reviewed.
9. COMMUNICATIONS SECURITY
   a. The network perimeter is protected by next generation firewalls with intrusion detection/prevention, and are configured for monitoring, access control lists, and logical and virtual segregation.
   b. Duties of network operations and computer/system operations are segregated.
   c. Information transfer policies, procedures, controls are in place to protect against interception, copying, modification, mis-routing and destruction.

d. Data protection agreements and non-disclosure agreements are in place when sharing sensitive information with third parties.

10. SYSTEM ACQUISITION, DEVELOPMENT AND MAINTENANCE
    a. NSF maintains a secure development lifecycle policy.
    b. NSF performs a security assessment and determines requirements during new system development or changes to existing systems.
    c. Changes are controlled through formal change control procedures.
        i. If any personally identifiable information is used in development environments it is protected by hashing the data and controlling access to the algorithm.
    d. Development and non-production environments are secured.
        i. All NSF developers are required to complete secure code training.
    e. NSF performs of static code analysis (SAST), dynamic code analysis (DAST) and scan of libraries for vulnerabilities on critical systems developed by NSF.
    f. Scans of NSF applications are run within development pipeline and in non-runtime environment (staging) to identify and evaluate both web and non-web applications.
11. SUPPLIER RELATIONSHIPS.
    a. The NSF Supplier Security Policy describes information security risk assessment in the supplier selection process and includes supplier selection, management and control of information assets.
    b. The Information Security team performs risk assessment of potential high-risk and high-value suppliers. Risks are reviewed and approved by authorized NSF Senior Leadership prior to contract signing.
    c. Information security requirements are added to contracts for applicable suppliers.
    d. The Information Security team regularly monitors, review, audits service delivery and security and controls posture of selected suppliers.
    e. NSF request suppliers to provide ISO 27001 certification or SOC 2 Type 2 if available.
12. INFORMATION SECURITY INCIDENT MANAGEMENT.
    a. The NSF Incident Response Policy and Plan defines responsibilities and procedures to address weaknesses, events and security incidents.
    b. NSF employees must complete required security training modules, and are obligated along with interested parties to report security incidents.
    c. The Information Security Senior Director is responsible for security events and incidents and responsible for coordinating restoration of processes and systems to a normal level of security; collecting evidence as soon as possible after the occurrence; conducting an information security forensics analysis; escalation to NSF Legal Department and senior leadership and any relevant regulators; ensuring that all response activities are properly logged for later analysis; communicating existence of the information security incident or any relevant details to leadership and to NSF customers.
13. INFORMATION SECURITY ASPECTS OF BUSINESS CONTINUITY MANAGEMENT.
    a. NSF maintains processes, procedures and controls to ensure the required level of continuity for information security during a disruptive situation.
    b. Requirements are reviewed annually.
    c. Implemented information security continuity controls are tested at regular intervals.
    d. NSF information processing facilities are implemented with redundancy sufficient to meet availability requirements. Redundant components are secured at the same or greater level than the primary components.
14. COMPLIANCE.
    a. NSF complies with all applicable statutory, regulatory and contractual requirements.
    b. Independent reviews of information security and its implementation occur at planned intervals (annually) or when significant changes occur, including reviews to determine compliance with security policies and controls.
    c. Non-compliance is logged, managed, and addressed.

International Data Transfer Addendum to the EU Commission Standard Contractual Clauses

1.1 Part 1: Tables

Table 1: Parties

Start date		
The Parties	**Exporter (who sends the Restricted Transfer)**	**Importer (who receives the Restricted Transfer)**
Parties' details	The Client, as defined in the Agreement	NSF International and its affiliates as defined in the Agreement
Key Contact	*The Parties agree that the Key Contact shall be as set out in the Agreement between the Parties to which the Data Protection Addendum and the Approved EU SCCs and this Addendum are attached*	*The Parties agree that the Key Contact shall be as set out in the Agreement between the Parties to which the Data Protection Addendum and the Approved EU SCCs and this Addendum are attached*
Signature (if required for the purposes of Section 2)	N/A	N/A

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: Reference (if any): Other identifier (if any):

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: *The Parties agree that the List of Parties shall be as set out in the Approved EU SCCs to which this Addendum is attached.*

Annex 1B: Description of Transfer: *The Parties agree that the Description of Transfer shall be as set out in Schedule 1 of the Data Protection Addendum to which the Approved EU SCCs and this Addendum are attached.*

Annex II: Technical and organisational measures including technical and organisational measures to ensure the security of the data: *The Parties agree that the technical and organisational measures shall be as set out in Annex 2 of the Approved EU SCCs to which this Addendum are attached.*

Annex III: List of Sub processors (Modules 2 and 3 only): *The Parties agree that the List of Sub processors shall be as set out in Approved EU SCCs to which this Addendum is attached. In any event, in the case of the Importer, Sub processors shall include (i) NSF International and its affiliates, (ii) subcontractors, if any, who are involved in the provision of services under the applicable Agreement, and (iii) contractors necessary to provide administrative, infrastructure and other support services to Importer.*

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

1. 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.

2. 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

3. 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.

4. 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.

5. 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.

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

7. 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.

8. 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

9. 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.

10. 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.

11. 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

12. 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.

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

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

15. 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

16. 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.

17. 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.

18. 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.

19. 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.

20. 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.