DocuSign Envelope ID: 9252D79C-AE36-433F-8245-F45D2B700B91

DATA PROTECTION AGREEMENT

PARTIES

(1) iovation, Inc. (**"iovation" or "Company")**

(2) The organization identified in the signature block below ("**Client"**)

BACKGROUND

A. The Client is a user of one or more of iovation's products, pursuant to one or more Service Agreements. The Client's use of those products may from time to time involve the transfer of personal data to iovation in the United States.

B. The Client wishes to ensure that appropriate safeguards are in place in respect of any transfer of personal data to iovation in connection with the Service Agreements, and therefore wishes to ensure that the EU SCCs and/or UK SCCs apply to such transfers to the extent necessary to comply with the EU GDPR and UK GDPR (as applicable).

AGREEMENT

1 INTERPRETATION

1.1 The following definitions apply in this DPA.

DPA	this Data Protection Agreement
EU Adequacy Decision	a decision of the European Commission under Article 45(1) of the EU GDPR
EU GDPR	EU General Data Protection Regulation 2016/679, and any laws implementing or supplementing it
EU SCCs	the European Commission's standard contractual clauses for the transfer of personal data to a third country, in the form set out in Appendix 1
Party	a party to this DPA, being iovation or the Client
Service Agreements	any agreements for the supply of services by iovation to the Client
UK Addendum	the ICO's Addendum B.1.0, in the form set out in Appendix 2 (as may be revised under section 18 of the UK Addendum)
UK Adequacy Regulations	adequacy regulations made under section 17A of the UK's Data Protection Act 2018, including those deemed to have been made as a result of paragraphs 4 and 5 of Schedule 21 of that Act
UK GDPR	the EU GDPR as amended and incorporated into UK law under the UK's European Union (Withdrawal) Act 2018, read with the Data Protection Act 2018 and any applicable secondary legislation

DocuSign Envelope ID: 9252D79C-AE36-433F-8245-F45D2B700B91

1.2 Clause and Appendix headings shall not affect the interpretation of this DPA.

1.3 In this DPA, unless the context otherwise requires:

1.3.1 words in the singular shall include the plural and in the plural shall include the singular;

1.3.2 a reference to legislation or a legislative provision is a reference to it as amended, extended or re-enacted from time to time, and includes all subordinate legislation made under it;

1.3.3 any words following the terms **including**, **include**, **in particular**, **for example** or any similar expression shall be interpreted as illustrative and shall not limit the sense of any preceding words.

2 APPLICATION OF EU SCCS

2.1 The EU SCCs apply in relation to any transfer of personal data by the Client to iovation pursuant to the Service Agreements if, at the time of the transfer:

2.1.1 the EU GDPR applies to the transfer; and

2.1.2 there is no EU Adequacy Decision in effect which would permit such a transfer of personal data in the absence of the EU SCCs.

2.2 Accordingly:

2.2.1 if an EU Adequacy Decision is made which enables personal data to be lawfully transferred by the Client to iovation without the need for appropriate safeguards pursuant to Article 46 of the EU GDPR, the EU SCCs shall not apply to such transfers while that EU Adequacy Decision applies;

2.2.2 if such an EU Adequacy Decision is subsequently revoked or invalidated, the EU SCCs shall again apply to any further transfers of personal data while no applicable EU Adequacy Decision is in place.

3 APPLICATION OF UK ADDENDUM

3.1 The UK Addendum applies in relation to any transfer of personal data by the Client to iovation in connection with the Service Agreements if, at the time of the transfer:

3.1.1 the UK GDPR applies to the transfer; and

3.1.2 there is no UK Adequacy Decision in effect which would permit such a transfer of personal data in the absence of the UK Addendum.

3.2 Accordingly:

DocuSign Envelope ID: 9252D79C-AE36-433F-8245-F45D2B700B91

3.2.1 if a UK Adequacy Decision is made which enables personal data to be lawfully transferred by the Client to iovation without the need for appropriate safeguards pursuant to Article 46 of the UK GDPR, the UK Addendum shall not apply to such transfers while that UK Adequacy Decision applies;

3.2.2 if such a UK Adequacy Decision is subsequently revoked or invalidated, the UK Addendum shall again apply to any further transfers of personal data while no applicable UK Adequacy Decision is in place.

4 RELATIONSHIP WITH SERVICE AGREEMENTS

4.1 If there is an inconsistency between any of the provisions of the EU SCCs or UK Addendum and the provisions of the Service Agreements, the provisions of the EU SCCs or UK Addendum shall prevail. Otherwise, this DPA is without prejudice to the terms of the Service Agreements, which shall remain in full force and effect

4.2 As between the Parties, any limitations or exclusion of liability set out in the Service Agreements shall apply to the EU SCCs and UK Addendum as if the EU SCCs and UK Addendum were incorporated into and formed part of the Service Agreements.

4.3 Clause 4.2 does not affect any liability of either party to any third party who is entitled to enforce the EU SCCs or UK Addendum in accordance with their terms.

5 ENTIRE AGREEMENT

This DPA, together with the Service Agreements, constitutes the entire agreement between the parties. Each party acknowledges that in entering into this DPA it does not rely on any statement, representation, assurance or warranty (whether made innocently or negligently) that is not set out in this DPA.

6 VARIATION

No variation of this DPA shall be effective unless it is in writing and signed by the parties or their authorised representatives.

7 GOVERNING LAW AND JURISDICTION

7.1 This DPA and any dispute or claim (including non-contractual disputes or claims) arising out of or in connection with it or its subject matter or formation shall be governed by and construed in accordance with the law of Ireland.

7.2 Each party irrevocably agrees that the courts of Ireland shall have exclusive jurisdiction to settle any dispute or claim (including non-contractual disputes or claims) arising out of or in connection with this DPA or its subject matter or formation.

DocuSign Envelope ID: 9252D79C-AE36-433F-8245-F45D2B700B91

SIGNATURES

iovation, Inc.

Signed: DocuSigned by: Sean Donnelly 575CC913E31B41E...

Name: Sean Donnelly

Position: SVP

Date: 11/2/2022

Full name of Client company:	
Company number:	
Registered office address:	
Signed:	
Name:	
Position:	
Date:	

DocuSign Envelope ID: 9252D79C-AE36-433F-8245-F45D2B700B91

Appendix 1: EU SCCs

SECTION I

Clause 1

Purpose and scope

(a) The purpose of these standard contractual clauses is to ensure compliance with the requirements of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)[1] for the transfer of personal data to a third country.

(b) The 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

(e) 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 - Module One: Clause 8.5 (e) and Clause 8.9(b);

(iii) Clause 9 - N/A;

(iv) Clause 12 - Module One: Clause 12(a) and (d);

(v) Clause 13;

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

(vii) Clause 16(e);

(viii) Clause 18 - Modules One: Clause 18(a) and (b).

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

DocuSign Envelope ID: 9252D79C-AE36-433F-8245-F45D2B700B91

Clause 4

Interpretation

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

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

(i) 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 - Optional

Docking clause

Not applicable ("N/A").

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 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. It may only process the personal data for another purpose:

(i) where it has obtained the data subject's prior consent;

(ii) where necessary for the establishment, exercise or defence of legal claims in the context of specific administrative, regulatory or judicial proceedings; or

(iii) where necessary in order to protect the vital interests of the data subject or of another natural person.

8.2 Transparency

(j) In order to enable data subjects to effectively exercise their rights pursuant to Clause 10, the data importer shall inform them, either directly or through the data exporter:

(i) of its identity and contact details;

(ii) of the categories of personal data processed;

(iii) of the right to obtain a copy of these Clauses;

(iv) where it intends to onward transfer the personal data to any third party/ies, of the recipient or categories of recipients (as appropriate with a view to providing meaningful information), the purpose of such onward transfer and the ground therefore pursuant to Clause 8.7.

(k) Paragraph (a) shall not apply where the data subject already has the information, including when such information has already been provided by the data exporter, or providing the information proves impossible or would involve

DocuSign Envelope ID: 9252D79C-AE36-433F-8245-F45D2B700B91

a disproportionate effort for the data importer. In the latter case, the data importer shall, to the extent possible, make the information publicly available.

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

(m) Paragraphs (a) to (c) are without prejudice to the obligations of the data exporter under Articles 13 and 14 of Regulation (EU) 2016/679.

8.3 Accuracy and data minimisation

(n) Each Party shall ensure that the personal data is accurate and, where necessary, kept up to date. The data importer shall take every reasonable step to ensure that personal data that is inaccurate, having regard to the purpose(s) of processing, is erased or rectified without delay.

(o) If one of the Parties becomes aware that the personal data it has transferred or received is inaccurate, or has become outdated, it shall inform the other Party without undue delay.

(p) The data importer shall ensure that the personal data is adequate, relevant and limited to what is necessary in relation to the purpose(s) of processing.

8.4 Storage limitation

The data importer shall retain the personal data for no longer than necessary for the purpose(s) for which it is processed. It shall put in place appropriate technical or organisational measures to ensure compliance with this obligation, including erasure or anonymisation[2] of the data and all back-ups at the end of the retention period.

8.5 Security of processing

(q) The data importer and, during transmission, also the data exporter shall implement appropriate technical and organisational measures to ensure the security of the personal data, including protection against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access (hereinafter "personal data breach"). In assessing the appropriate level of security, they shall take due account of the state of the art, the costs of implementation, the nature, scope, context and purpose(s) of processing and the risks involved in the processing for the data subject. The Parties shall in particular consider having recourse to encryption or pseudonymisation, including during transmission, where the purpose of processing can be fulfilled in that manner.

(r) The Parties have agreed on the technical and organisational measures set out in Annex II. The data importer shall carry out regular checks to ensure that these measures continue to provide an appropriate level of security.

(s) The data importer shall ensure that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

(t) 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 personal data breach, including measures to mitigate its possible adverse effects.

(u) In case of a personal data breach that is likely to result in a risk to the rights and freedoms of natural persons, the data importer shall without undue delay notify both the data exporter and the competent supervisory authority pursuant to Clause 13. Such notification shall contain i) a description of the nature of the breach (including, where possible, categories and approximate number of data subjects and personal data records concerned), ii) its likely consequences, iii) the measures taken or proposed to address the breach, and iv) the details of a contact point from whom more information can be obtained. To the extent it is not possible for the data importer to provide all the information at the same time, it may do so in phases without undue further delay.

(v) In case of a personal data breach that is likely to result in a high risk to the rights and freedoms of natural persons, the data importer shall also notify without undue delay the data subjects concerned of the personal data breach and its nature, if necessary in cooperation with the data exporter, together with the information referred to in paragraph (e), points ii) to iv), unless the data importer has implemented measures to significantly reduce the risk

DocuSign Envelope ID: 9252D79C-AE36-433F-8245-F45D2B700B91

to the rights or freedoms of natural persons, or notification would involve disproportionate efforts. In the latter case, the data importer shall instead issue a public communication or take a similar measure to inform the public of the personal data breach.

(w) The data importer shall document all relevant facts relating to the personal data breach, including its effects and any remedial action taken, and keep a record thereof.

8.6 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 or offences (hereinafter "sensitive data"), the data importer shall apply specific restrictions and/or additional safeguards adapted to the specific nature of the data and the risks involved. This may include restricting the personnel permitted to access the personal data, additional security measures (such as pseudonymisation) and/or additional restrictions with respect to further disclosure.

8.7 Onward transfers

The data importer shall not disclose the personal data to a third party located outside the European Union[3] (in the same country as the data importer or in another third country, hereinafter "onward transfer") unless the third party is or agrees to be bound by these Clauses, under the appropriate Module. Otherwise, an onward transfer by the data importer may only take place if:

(i) it 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 of Regulation (EU) 2016/679 with respect to the processing in question;

(iii) the third party enters into a binding instrument with the data importer ensuring the same level of data protection as under these Clauses, and the data importer provides a copy of these safeguards to the data exporter;

(iv) it is necessary for the establishment, exercise or defence of legal claims in the context of specific administrative, regulatory or judicial proceedings;

(v) it is necessary in order to protect the vital interests of the data subject or of another natural person; or

(vi) where none of the other conditions apply, the data importer has obtained the explicit consent of the data subject for an onward transfer in a specific situation, after having informed him/her of its purpose(s), the identity of the recipient and the possible risks of such transfer to him/her due to the lack of appropriate data protection safeguards. In this case, the data importer shall inform the data exporter and, at the request of the latter, shall transmit to it a copy of the information provided to the data subject.

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

8.8 Processing under the authority of the data importer

The data importer shall ensure that any person acting under its authority, including a processor, processes the data only on its instructions.

8.9 Documentation and compliance

(x) Each Party shall be able to demonstrate compliance with its obligations under these Clauses. In particular, the data importer shall keep appropriate documentation of the processing activities carried out under its responsibility.

(y) The data importer shall make such documentation available to the competent supervisory authority on request.

DocuSign Envelope ID: 9252D79C-AE36-433F-8245-F45D2B700B91

Clause 9

Use of sub-processors

N/A

Clause 10

Data subject rights

(z) The data importer, where relevant with the assistance of the data exporter, shall deal with any enquiries and requests it receives from a data subject relating to the processing of his/her personal data and the exercise of his/her rights under these Clauses without undue delay and at the latest within one month of the receipt of the enquiry or request.[4] The data importer shall take appropriate measures to facilitate such enquiries, requests and the exercise of data subject rights. Any information provided to the data subject shall be in an intelligible and easily accessible form, using clear and plain language.

(aa) In particular, upon request by the data subject the data importer shall, free of charge :

(i) provide confirmation to the data subject as to whether personal data concerning him/her is being processed and, where this is the case, a copy of the data relating to him/her and the information in Annex I; if personal data has been or will be onward transferred, provide information on recipients or categories of recipients (as appropriate with a view to providing meaningful information) to which the personal data has been or will be onward transferred, the purpose of such onward transfers and their ground pursuant to Clause 8.7; and provide information on the right to lodge a complaint with a supervisory authority in accordance with Clause 12(c)(i);

(ii) rectify inaccurate or incomplete data concerning the data subject;

(iii) erase personal data concerning the data subject if such data is being or has been processed in violation of any of these Clauses ensuring third-party beneficiary rights, or if the data subject withdraws the consent on which the processing is based.

(bb) Where the data importer processes the personal data for direct marketing purposes, it shall cease processing for such purposes if the data subject objects to it.

(cc) The data importer shall not make a decision based solely on the automated processing of the personal data transferred (hereinafter “automated decision”), which would produce legal effects concerning the data subject or similarly significantly affect him / her, unless with the explicit consent of the data subject or if authorised to do so under the laws of the country of destination, provided that such laws lays down suitable measures to safeguard the data subject’s rights and legitimate interests. In this case, the data importer shall, where necessary in cooperation with the data exporter:

(i) inform the data subject about the envisaged automated decision, the envisaged consequences and the logic involved; and

(ii) implement suitable safeguards, at least by enabling the data subject to contest the decision, express his/her point of view and obtain review by a human being.

(dd) Where requests from a data subject are excessive, in particular because of their repetitive character, the data importer may either charge a reasonable fee taking into account the administrative costs of granting the request or refuse to act on the request.

(ee) The data importer may refuse a data subject’s request if such refusal is allowed under the laws of the country of destination and is necessary and proportionate in a democratic society to protect one of the objectives listed in Article 23(1) of Regulation (EU) 2016/679.

(ff) If the data importer intends to refuse a data subject’s request, it shall inform the data subject of the reasons for the refusal and the possibility of lodging a complaint with the competent supervisory authority and/or seeking judicial redress.

Clause 11

Redress

(gg) 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.

(hh) 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.

(ii) 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.

(jj) 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.

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

(ll) 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

(mm) 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.

(nn) Each Party shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages that the Party 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 under Regulation (EU) 2016/679.

(oo) 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.

(pp) The Parties agree that if one Party is held liable under paragraph (c), 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.

(qq) The data importer may not invoke the conduct of a processor or sub-processor to avoid its own liability.

Clause 13

Supervision

(rr) 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.

(ss) 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

(tt) 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

DocuSign Envelope ID: 9252D79C-AE36-433F-8245-F45D2B700B91

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.

(uu) 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[5];

(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.

(vv) 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.

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

(xx) 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). [For Module Three: The data exporter shall forward the notification to the controller.]

(yy) 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 [for Module Three: , if appropriate in consultation with the controller]. The data exporter shall suspend the data transfer if it considers that no appropriate safeguards for such transfer can be ensured, or if instructed by [for Module Three: the controller or] the competent supervisory authority to do so. In this case, the data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses. If the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise. Where the contract is terminated pursuant to this Clause, Clause 16(d) and (e) shall apply.

Clause 15

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

15.1 Notification

(zz) 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.

[For Module Three: The data exporter shall forward the notification to the controller.]

(aaa) 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

DocuSign Envelope ID: 9252D79C-AE36-433F-8245-F45D2B700B91

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.

(bbb) 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.). [For Module Three: The data exporter shall forward the information to the controller.]

(ccc) 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.

(ddd) 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

(eee) 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).

(fff) 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. [For Module Three: The data exporter shall make the assessment available to the controller.]

(ggg) 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

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

(iii) 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).

(jjj) 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 [for Module Three: and the controller] of such non-compliance. Where the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise.

(kkk) [For Modules One, Two and Three: 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.] [For Module Four: Personal data collected by the data exporter in the EU that has been transferred prior to the termination of the contract pursuant to paragraph (c) shall immediately be deleted in its entirety, including any copy thereof.] The data importer shall

DocuSign Envelope ID: 9252D79C-AE36-433F-8245-F45D2B700B91

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.

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

Clause 17

Governing law

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

Clause 18

Choice of forum and jurisdiction

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

(nnn) The Parties agree that those shall be the courts of Ireland.

(ooo) 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.

(ppp) The Parties agree to submit themselves to the jurisdiction of such courts.

APPENDIX TO THE CLAUSES

EXPLANATORY NOTE:

It must be possible to clearly distinguish the information applicable to each transfer or category of transfers and, in this regard, to determine the respective role(s) of the Parties as data exporter(s) and/or data importer(s). This does not necessarily require completing and signing separate appendices for each transfer/category of transfers and/or contractual relationship, where this transparency can achieved through one appendix. However, where necessary to ensure sufficient clarity, separate appendices should be used.

ANNEX I

A. LIST OF PARTIES

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]*

1. Name:

Address:

Contact person's name, position and contact details:

Activities relevant to the data transferred under these Clauses:

Data exporter is a business transferring personal data to iovation Inc. in order to receive iovation services.

Signature:_____

Date:_____

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]*

1. Name: iovation Inc.

Address: 1211 SW 5th Avenue 8th floor, Portland, OR 97204 United States

Contact person's name, position and contact details: Data Protection Officer, PDLGFSPrivacy@transunion.com

Activities relevant to the data transferred under these Clauses:

iovation, Inc. is a technology business, specializing in the delivery of fraud prevention, device reputation and multi-factor authentication technologies.

Signature: DocuSigned by: Sean Donnelly 575CC913E31B41E...

Date: 11/2/2022

Role (controller/processor): Controller

B. DESCRIPTION OF TRANSFER

Categories of data subjects whose personal data is transferred

- Individuals who access, register, sign in or carry out transactions through the Data Exporter products and services including via the delivery of the web, mobile or other online properties ("End-Users"),
- Individuals employed by the Data Exporter in order that the Data Importer might deliver their services and provide support to the Data Exporter

Categories of personal data transferred

The personal data transferred concern device information associated with the following categories of data:

• End-User's device attributes such as IP address, device identifiers, device type, screen resolution, operating system and browser type (to the extent such data constitutes Personal Data pursuant to Regulation (EU) 2016/679);

• End-User account information, which includes a unique account identifier and any other data that the Data Exporter chooses to transfer to the Data Importer for the provision of the fraud prevention services (such as billing/shipping city, country, currency etc.)

• Evidence labels which are placed by the Data Exporter to tag End-User devices that are associated with actual or suspected fraudulent activity.

• Data Exporter Staff identifiers including Name, Job Title, Employer, Telephone Number, Email Address and marketing preferences.

This information is provided by the Data Exporter who has implemented the solution in their websites, and is directly shared with the Data Importer , where the service is executed.

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

DocuSign Envelope ID: 9252D79C-AE36-433F-8245-F45D2B700B91

for staff having followed specialised training), keeping a record of access to the data, restrictions for onward transfers or additional security measures.

……...

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 specialized training), keeping a record of access to the data, restrictions for onward transfers or additional security measuresThe frequency of the transfer (e.g. whether the data is transferred on a one-off or continuous basis).

N/A

……

Nature of the processing

The Device Risk solution provided by iovation protects companies in their online channels and their end users against fraud and abuse, through a combination of advanced device identification functions, shared device reputation and evaluation of risks in real time. If a device has been associated with irregular behavior or fraud on any of the Device Risk protected sites, that information is immediately made available to all users of the service.

The information collected will include the IP address that the device used for the connection.

Data Exporter shall include when required, sufficient transparency to fulfil the duty of information to those affected (by making reference to www.transunion.com/privacy/iovation) .

With the data collected, the device originating the transaction will be uniquely identified and compared with the global Device Risk database, in order to determine if any fraudulent activity has been associated with that device in the past.

Finally, the preconfigured rules will be executed and stored for later analysis through the Device Risk Intelligence Center administration portal.

The Data will also incorporate unique account identifiers along with additional optional data of its choosing back to iovation such as billing/shipping city, country, currency etc. (called "Transaction Insights"). The unique account identifiers and Transaction Insights are only ever used within the confines of the Data Exporter's account and are not shared with other iovation Subscribers.

On receipt of the device data and the additional data elements, iovation processes the data through its database containing device attributes of all Devices that have been seen across iovation's Subscriber network. If there is no existing entry for a Device on the database, it is assigned a new device ID. If there is an existing match, then the Device is assigned the same iovation device ID as the matching device. Iovation then processes all the data it has about the device attributes, along with any other data that is held about the Device to assess the Device's risk reputation (i.e. whether that Device has previously been associated with any behaviours indicative of fraudulent activity). Iovation then returns a "Transaction Score" for the Device, which is a risk score based on customized business rules set by the Data Exporter.

The Data Exporter then decides what actions, if any, it will take based on the risk score it receives. Transactions with lower Transaction Scores may be denied, flagged for manual review or presented with further authentication challenges depending on the preferences of the Client. Higher Transaction Scores are generally just allowed to proceed by the iovation Subscriber. While iovation generates and returns the Transaction Score, it does not exercise any decision making about the subsequent actions to take (or not to take) with respect to a particular transaction.

iovation will also process the data for the purposes of ensuring the efficacy of its fraud prevention algorithms. Such processing activities will include the use of machine learning technologies.

……

Purpose(s) of the data transfer and further processing

The transfer is made for the following purposes:

- Fraud prevention

The period for which the personal data will be retained, or, if that is not possible, the criteria used to determine that period

For transfers to (sub-) processors, also specify subject matter, nature and duration of the processing

Please see the following password protected website for this information: https://transunion.com/GFSSPL

Please reach out to your iovation respresentative for the password.

Processors used by iovation may change from time to time and such changes will be available on the following website:

https://transunion.com/GFSSPL

DocuSign Envelope ID: 9252D79C-AE36-433F-8245-F45D2B700B91

C. COMPETENT SUPERVISORY AUTHORITY

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

Irish Data Protection Commission - www.dataprotection.ie

ANNEX II - TECHNICAL AND ORGANISATIONAL MEASURES INCLUDING TECHNICAL AND ORGANISATIONAL MEASURES TO ENSURE THE SECURITY OF THE DATA

EXPLANATORY NOTE:

The technical and organizational measures must be described in specific (and not generic) terms. See also the general comment on the first page of the Appendix, in particular on the need to clearly indicate which measures apply to each transfer/set of transfers.

Description of the technical and organizational 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.

iovation maintains an information security program, including the appropriate technical and organizational measures, for protection of the security of the data during processing.

Measures of pseudonymisation and encryption of personal data.

Transport encryption is used to ensure security over untrusted networks.

iovation employs Data Minimization techniques.

In all cases the encryption algorithm is implemented correctly and maintained without known vulnerabilities.

Measures for ensuring ongoing confidentiality, integrity, availability and resilience of processing systems and services.

Security Information and Event Monitoring software monitor for and alert on unauthorized access and/or malicious software installation.

File Integrity Monitoring tools (FIM) ensure that critical system files are not modified, and secure server configurations of servers are maintained every 30 minutes using configuration management software.

The active-active architecture allows the service to become automatically and fully available at the alternate hot site in the event of an outage at one datacenter.

Measures for ensuring the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident.

Core service components are deployed in an active-active configuration such that an outage of an entire datacenter would not result in a service outage. Rather, the service would become automatically and fully available at the alternate host site. This enables continuity of service and availability.

Processes for regularly testing, assessing and evaluating the effectiveness of technical and organizational measures in order to ensure the security of the processing.

iovation's external IP spaces and internal networks are scanned on a weekly basis, and a third party conducts external authenticated penetration testing annually.

All findings are investigated by Security and assigned a remediation due date, when appropriate.

The business is also subject to annual SSAE-16, SOC2-type II audits.

Measures for user identification and authorization.

All access to system components requires valid credentials.

iovation uses role-based access controls and grants access on the least-privilege principle; access requests must be approved by an appropriate manager.

Measures for the protection of data during transmission.

DocuSign Envelope ID: 9252D79C-AE36-433F-8245-F45D2B700B91

All data in transit across untrusted networks is encrypted.

TLS ensures that no third party can eavesdrop or tamper with any message.

Measures for the protection of data during storage.

Transport encryption is used to ensure that the personal data is securely transmitted across unsecure networks.

The dataset does not consist of data that enables an individual to be identified in the absence of information held by the Client. This data is pseudonymous.

The business employs Data Minimisation, in so far as we specifically collect a personal data set that does not enable an individual to be directly identified. The Dataset is pseudonymous and additional data required to render the Data Subject identifiable is retained in the EU/EEA by the Data Exporter.

The data is held within the Data Importer's production environment in a pseudonymous state.

The Data Importer also stores personal data in the cloudIn all cases the encryption algorithm is implemented correctly and maintained without known vulnerabilities.

Measures for ensuring physical security of locations at which personal data are processed.

All access to data centers is limited to appropriate, named personnel and requires evidence of identity in addition to other physical access controls. iovation requires that our data center facilities that host production systems are SOC-audited, and their SOC reports are reviewed annually. Each data center is equipped with armed guards.

Measures for ensuring events logging.

Systems log to a Security Information and Event Management (SIEM) to monitor for and alert on unauthorized access and/or malicious software installation. The SIEM is manually reviewed by Security personnel on a regular basis.

Measures for ensuring system configuration, including default configuration.

Secure configurations are maintained every 30 minutes using configuration management software.

Measures for internal IT and IT security governance and management.

TransUnion has a dedicated Information Security organization comprised of individuals with relevant experience which oversees the design, development, implementation, operation, maintenance and monitoring of the system to meet security and availability requirements and commitments.

The TransUnion Security Council and Board of Directors holds quarterly meetings to review the system of internal control, including the results of internal and external assessments, to communicate and assign responsibility for changes related to the internal control environment.

Measures for certification/assurance of processes and products

iovation undergoes a SOC2 Type 2 audit annually conducted by an independent third party.

Measures for ensuring data minimization

Whilst the Device Risk product collects personal data, the dataset does not consist of data that enables an individual to be identified in the absence of information held by the Client.

Additionally, the business employs Data Minimisation, in so far as we specifically collect a personal data set that does not enable an individual to be directly identified.

Measures for ensuring limited data retention.

iovation maintains a strict retention period, which is automated. When datasets reach their relevant retention periods, they are erased from our services.

Internal analysis has taken place that ensures that personal data is retained for no longer than is necessary.

DocuSign Envelope ID: 9252D79C-AE36-433F-8245-F45D2B700B91

Measures for ensuring accountability.

iovation maintains strict measures to maintain accountability.

iovation employs a Data Protection Officer who forms part of the TransUnion Data Privacy organisation.

Data processing activities are mapped to a Record of Processing Activities.

The processing activities that involve International Transfers are also logged, and Transfer Impact Assessments take place for transfers of personal data to Third Countries.

All decisions are documented and available for review by Regulatory Authorities.

Datasets are minimized, to ensure that only the data necessary to provide the service is collected for the delivery of the service.

Policies and processes are in place to ensure that requests for access to data by Public Authorities are responded to in a manner consistent with these Standard Contractual Clauses, including ensuring that the business understands the requirements of local laws that may permit access by Public Authorities, and how those requests for access should be reviewed and appealed against. Similarly, policies and procedures are in place to effect responses to requests for Standard Contractual Clauses from Data Subjects can be handled in accordance with these Standard Contractual Clauses.

iovation enables Data Subject Rights requests pursuant to Chapter III GDPR.

Measures for allowing data portability and ensuring erasure.

The business does not collect personal data under the lawful bases of consent or contract. As such the business is not obliged to offer a data portability facility.

The business has the ability to erase data upon request by contacting the privacy team, who will then facilitate such requests.

For transfers to (sub-) processors, also describe the specific technical and organizational measures to be taken by the (sub-) processor to be able to provide assistance to the controller and, for transfers from a processor to a sub-processor, to the data exporter
iovation (sub-) processors are contracted under legacy Standard Contractual Clauses (controller to processor) terms. The business will ensure that such terms are updated by December 2022.

DocuSign Envelope ID: 9252D79C-AE36-433F-8245-F45D2B700B91

Appendix 2: UK Addendum

International Data Transfer Addendum to the EU Commission Standard Contractual Clauses

VERSION B1.0, in force 21 March 2022

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 date of the last signature to the SCCs.	
The Parties	**Exporter (who sends the Restricted Transfer)**	**Importer (who receives the Restricted Transfer)**
Parties' details	**Full legal name:** **Trading name (if different):** **Main address (if a company registered address):** **Official registration number (if any) (company number or similar identifier):**	**Full legal name: iovation, Inc.** **Trading name (if different): N/A** **Main address (if a company registered address):** 1211 SW Fifth Avenue, Floor 8, Portland, OR 97204 United States of America **Official registration number (if any) (company number or similar identifier):**
Key Contact	**Full Name (optional):** **Job Title:** **Contact details including email:**	**Full Name (optional):** **Job Title:** **Contact details including email:**
Signature (if required for the purposes of Section 2)		

DocuSign Envelope ID: 9252D79C-AE36-433F-8245-F45D2B700B91

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: The date of the last signature to the EU SCCs. 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	C2C	No	Yes			
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: See Annex I to EU SCCs.
Annex 1B: Description of Transfer: See Annex I of EU SCCs.
Annex II: Technical and organisational measures including technical and organisational measures to ensure the security of the data: See Annex II to EU SCCs.
Annex III: List of Sub processors (Modules 2 and 3 only): N/A

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 17: ☒ Importer ☐ Exporter

DocuSign Envelope ID: 9252D79C-AE36-433F-8245-F45D2B700B91

	☐ 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

1. 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 16.
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.

2. 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.

3. 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.

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

5. 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.

6. 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

7. 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 8 will prevail.

8. 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.

9. 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

10. 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 7 to 9 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.

11. Unless the Parties have agreed alternative amendments which meet the requirements of Section 10, the provisions of Section 13 will apply.

12. No amendments to the Approved EU SCCs other than to meet the requirements of Section 10 may be made.

13. The following amendments to the Addendum EU SCCs (for the purpose of Section 10) are made:

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

    b. In Clause 2, delete the words:

DocuSign Envelope ID: 9252D79C-AE36-433F-8245-F45D2B700B91

"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

14. 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.

DocuSign Envelope ID: 9252D79C-AE36-433F-8245-F45D2B700B91

15. 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.

16. 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.

17. If the ICO issues a revised Approved Addendum under Section 16, 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.

18. 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.