

METASWITCH DATA PROCESSING AGREEMENT FOR CUSTOMERS

1. General

- 1.1 This Data Processing Agreement is effective as of 22nd September 2022, replacing the prior Data Processing Agreement available at www.metaswitch.com/legal/standard-terms-and-conditions, and sets out the terms and conditions between Metaswitch Networks Ltd ("**Service Provider**") and Customer relating to the processing of personal data as part of the Services provided to Customer pursuant to the contract between the parties for such Services (the "**Agreement**").
- 1.2 In consideration of the mutual obligations set out herein, the parties hereby agree that the terms and conditions set out below shall be added as an addendum to the Agreement.
- 1.3 This Data Processing Agreement may be updated by Service Provider from time to time by providing at least 30 days' prior written notice to Customer (which may be by e-mail) or by publication of an updated Data Processing Agreement, and deemed accepted by the Customer, unless Customer states in writing that they will not accept such update within 20 days of such notice or publication being issue by Service Provider. Parties agree and acknowledge that Service Provider may update the Data Processing Agreement in its sole discretion to comply with Data Protection Legislation.

2. Definitions

- 2.1 In this Data Processing Agreement, the following terms shall have the meanings set out below:
- (a) "**CCPA**" or "**California Consumer Privacy Act**" means the California Consumer Privacy Act of 2018, Cal. Civ. Code § 1798.100 et seq., as amended;
 - (b) "**Data Protection Legislation**" means Data Protection Act 1998, the EU Data Protection Directive 95/46/EC, the GDPR, the Privacy and Electronic Communications (EC Directive) Regulations 2003, the CCPA, and all applicable laws and regulations relating to the processing of personal data and privacy, including where applicable, any guidance notes and codes of practice issued by the European Commission and applicable national Regulators including the UK Information Commissioner;
 - (c) "**EU SCCs**" means the standard data protection clauses for the transfer of personal data from controllers or processors in the EEA to processors established in third countries which do not ensure an adequate level of data protection, as described in Article 46 of the GDPR and approved by the European Commission in decision 2021/914/EC, dated 4 June 2021, and attached hereto as Schedule 2;
 - (d) "**GDPR**" means, where applicable, either: 1) the EC Regulation 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data; and 2) the United Kingdom General Data Protection Regulation;
 - (e) "**Regulator**" means any regulatory body with responsibility for ensuring compliance with Data Protection Legislation.
 - (f) "**Security Breach**" means accidental or deliberate, unauthorised or unlawful acquisition, destruction, loss, alteration, corruption, access, use or disclosure of personal data

processed under to this Data Processing Agreement or breach of Service Provider's security obligations under this Data Processing Agreement (including clause 3.3(c)).

- (g) **"Services"** means the services described in the Agreement.
- (h) **"UK SCCs"** means the International Data Transfer Addendum to the EU Commission Standard Contractual Clauses, version B1.0, in force 21 March 2022, or such similar provisions that the applicable Regulator promulgates, and attached hereto as Schedule 3.

2.2 References to "data controller", "data processor", "processing", "data protection officer" and "personal data" shall have the same meaning as defined in Data Protection Legislation.

3. Data Processing

3.1 The parties acknowledge and agree that in order to provide the Services, Service Provider may process personal data. Schedule 1 sets out the subject matter and duration of the processing; nature and purpose of the processing; the type of personal data being processed; and the categories of data subject.

3.2 The parties agree that in respect of any personal data processed in connection with this Data Processing Agreement that Customer shall be the **"data controller"** and Service Provider or Sub Processor shall be the **"data processor"**. In addition, where Services Provider receives any other personal data as a controller in order to provide business operations incident to providing the Services (for example, personal data relating to Customer personnel that Service Provider routinely receives in connection with the administration of its Services), Service Provider agrees to comply with obligations applicable to controllers in respect of that personal data.

3.3 Each party acknowledges and agrees that each party has respective rights and obligations under applicable Data Protection Legislation. Service Provider shall, without prejudice to its other rights or obligations, in respect of its processing of such personal data:

- (a) process the data only to the extent, and in such a manner, as is necessary for the purposes of this Data Processing Agreement and in accordance with Customer's lawful written instructions from time to time. If Service Provider is unsure as to the parameters of the instructions issued by Customer and/or believes that Customer's instructions may conflict with the requirements of Data Protection Legislation or other applicable laws, Service Provider may notify Customer for clarification and provide reasonable details in support of any assertion that Customer's instructions may not be lawful;
- (b) ensure the reliability of all its personnel who have access to the data and shall in particular ensure that any person authorised to process data in connection with this Data Processing Agreement is subject to a duty of confidentiality;
- (c) having regard to the state of technological development and the cost of implementing any measures, take such technical and organisational measures against the unauthorised or unlawful processing of data and against the accidental loss or destruction of, or damage to data, to ensure a level of security appropriate to: a) the harm that might result from such unauthorised or unlawful processing or accidental loss, destruction or damage of the data; and b) the nature of the data to be protected, provided that where such measures may require the use of resource and/or cost additional to that usually provided or incurred, or anticipated, by Service Provider, Customer agrees to pay for the same (in addition to any other charges or fees, provided that Service Provider has notified Customer of the fact that additional charges or cost may be payable;

- (d) subject to agreement on costs assist Customer by using appropriate technical and organisational measures in responding to, and complying with, data subject requests;
- (e) subject to agreement on costs provide Customer with reasonable co-operation and assistance in relation to Customer's obligations and rights under Data Protection Legislation, taking into account the nature of the processing and the information available to the processor, including providing Customer and relevant Regulators (as applicable) with all information and assistance reasonably necessary to investigate Security Breaches and where relevant notify the relevant Regulator and/or affected data subject of the relevant Security Breach, carry out privacy impact assessments or otherwise to demonstrate compliance by the parties with Data Protection Legislation;
- (f) subject to agreement on costs, without undue delay notify Customer, and provide such co-operation, assistance and information as Customer may reasonably require if Service Provider:
 - (i) receives any complaint, notice or communication which relates directly or indirectly to the processing of the personal data under this Data Processing Agreement or to either party's compliance with Data Protection Legislation; and/or
 - (ii) becomes aware of any Security Breach;
- (g) keep at its normal place of business a written record of any processing of the data carried out in the course of the Services ("**Records**");
- (h) permit no more than once per year Customer or a Regulator, on reasonable notice during normal business hours, but without notice in case of any reasonably suspected breach of this clause by Service Provider, access to inspect, and take copies of, the Records for the purpose of auditing Service Provider's compliance with its obligations under this clause. Service Provider shall at Customer's cost give all reasonably necessary assistance to the conduct of such audit;
- (i) may engage a sub processor to process data (or otherwise sub-contract or outsource the processing of any data to a third party) (a "**Sub processor**"), provided that it:
 - (i) notifies Customer of any new or replacement Sub processors. If Customer objects to the appointment of a new or replacement Sub processor, it shall notify Service Provider within five business days. Customer shall be deemed to have accepted the Sub processor if Service Provider does not receive an objection within five Business Days. If the objection cannot be resolved by the parties within five Business Days of receipt by the Companies of the written objection, Service Provider shall not be in breach of this Data Processing Agreement or the obligations of any other agreement to Customer to the extent it cannot provide its services or otherwise comply with its obligations as a result;
 - (ii) enters into a written contract with the Sub processor that:
 - (1) provides protections or guarantees that Sub processor considers necessary to implement appropriate technical and organisation measures in compliance with the Data Protection Legislation; and
 - (2) terminates automatically on termination or expiry of this Data Processing Agreement for any reason; and

- (iii) remains liable for all acts or omissions of the Sub processors as if they were acts or omissions of Service Provider (except to the extent caused or exacerbated by Customer).

As at the date of this Data Processing Agreement, Service Provider uses the Sub processors set out in Schedule 1 for the activities set out in Schedule 1 in connection with the provision of the Services;

- (j) at Customer's cost return or destroy (as directed in writing by Customer) all personal data it has in its possession and delete existing copies unless applicable law requires storage of the personal data.
- (k) Customer acknowledges and agrees that personal data may be transferred to those locations set out in Schedule 1 as well as any applicable order, quotation agreement or statement of work in accordance with any lawful transfer mechanisms. The EU SCCs implemented by Service Provider, Schedule 2, are agreed to by the parties and a lawful transfer mechanism for all transfers of personal data out of the European Union, European Economic Area, United Kingdom, and Switzerland to provide the Services. The UK SCCs implemented by Service Provider, Schedule 3, in addition to the EU SCCs are agreed to by the parties and a lawful transfer mechanism for transfer of personal data out of the United Kingdom to provide the Services. The parties agree that if the transfer mechanism used ceases to exist or is no longer considered to be a lawful method of transferring personal data outside of the European Economic Area ("**EEA**"), the parties shall have a good faith discussion and agree an alternative lawful transfer mechanism and Service Provider may cease, or procure that the relevant third party ceases, the processing of personal data until the parties have agreed on an alternative transfer mechanism to enable the personal data to be transferred outside of the EEA in a compliant manner. Service Provider shall not be in breach of this Data Processing Agreement or the Agreement to the extent that the parties do not promptly reach any such agreement.
- (l) If and to the extent Service Provider is processing personal data on behalf and in accordance with the documented instructions of Customer within the scope of the CCPA, Service Provider makes the following additional commitments to Customer. Service Provider will process the personal data on behalf of Customer and will not:
 - (i) sell the personal data, as the term "selling" is defined in the CCPA;
 - (ii) share, rent, release, disclose, disseminate, make available, transfer or otherwise communicate orally, in writing or by electronic or other means, the personal data to a third party for cross-context behavioural advertising, whether or not for monetary or other valuable consideration, including transactions for cross-context behavioural advertising in which no money is exchanged;
 - (iii) retain, use or disclose the personal data for any purpose other than for the business purposes specified in this Data Processing Addendum and the Agreement, including retaining, using or disclosing the personal data for a commercial purpose other than the business purposes specified in the Data Processing Addendum and the Agreement, or as otherwise permitted by the CCPA;
 - (iv) retain, use or disclose the personal data outside of the direct business relationship with Customer; and

- (v) combine the personal data with personal information that it receives from or on behalf of a third party or collects from California residents, except that Service Provider may combine personal data to perform any business purpose as permitted by the CCPA or any regulations adopted or issued under the CCPA.

3.4 Customer agrees to comply with its obligations under applicable Data Protection Legislation in respect of the processing of personal data under or in connection this Data Processing Agreement and shall in particular ensure that, as a condition of this Data Processing Agreement, Service Provider is lawfully permitted to process personal data on its behalf. Customer shall indemnify Service Provider on demand against all claims, liabilities, costs, expenses, damages and losses (including all interest, penalties and legal costs and all other professional costs and expenses) suffered or incurred by Service Provider arising out of Customer's breach of this clause 3.4 ("**Claims**"). Each party acknowledges that Claims include any claim or action brought by a data subject arising from the Service Provider's breach of its obligations in this clause.

Schedule 1

- (A) **Subject matter:** The subject matter of the data processing under this Data Processing Agreement is Customer subscriber data, including call record, IP addresses and network configuration, country of residence, product usage profiles.
- (B) **Duration:** The duration of data processing under this Data Processing Agreement is as described in the Agreement and as otherwise determined by Customer.
- (C) **Purpose:** The purpose of data processing under this Data Processing Agreement is the provision and performance of Services purchased by Customer under the Agreement.
- (D) **Nature of the processing:** The nature of data processing is providing Customer support, software development, and providing, maintaining, and securing Service Provider services.
- (E) **Categories of data subjects:** The categories of data subjects under this Data Processing Agreement could include Customer's customers (subscribers), third-party callers, employees, contractors, suppliers, and vendors.
- (F) **Permitted sub-processors and location of processing:**

Name	Sub processing services	Location
Metaswitch Networks Corporation with an address at 2711 Centerville Road, Suite 400 Wilmington, Delaware 19808	Support and maintenance services for Metaswitch products.	United States
Metaswitch Networks PTY (Australia) with an address at Level 4 - 147 Collins Street, Melbourne, Victoria 3000	Support and maintenance services for Metaswitch products.	Australia
Open Cloud NZ Limited with an address at SOINet Limited, Level 12, Sun Microsystems House, 70 The Terrace, Wellington	Support, maintenance and software development services for Metaswitch products.	New Zealand
Réseaux Metaswitch Inc./Metaswitch Networks Inc. with an address at 1000 rue de la Gauchetière Ouest Suite 2900, Montreal Canada H3B 4W5	Support and maintenance services for Metaswitch products.	Canada
Metaswitch Networks Ltd. Mexico S.A. de C.V. with an address at Edificio Terret, Blvd. Miguel de Cervantes Saavedra 301, Torre Sur. Piso 14, Col. Granada, Mexico City 11520	Support and maintenance services for Metaswitch products.	Mexico
Open Cloud Spain S.L. with an address at Madrid, calle Pinar, No. 5	Support and maintenance services for Metaswitch products.	Spain
PT Open Cloud Indonesia with an address at Talavera Office Tower	Support and maintenance services for Metaswitch products.	Indonesia

28th floor, Jl. TB. Simatupang Kav.22-26, Jakarta 12430, Indonesia.		
Metaswitch Networks Limited (Thailand), with an address of 90/40-41 Sathorn Thani Building 1, 15 th floor, North Sathom Road, Silom Sub-District, Bangrak District, Bangkok Metropolis	Support and maintenance services for Metaswitch products.	Thailand
Microsoft Corporation with an address at One Microsoft Way, Redmond, WA 98052	Cloud hosting, support and maintenance services for Metaswitch products.	United States
Amazon Web Services, Inc. with an address of 410 Terry Avenue N, Seattle WA 98109	Cloud hosting services for provision of support for Max UC product.	United Kingdom; United States
Telax Voice Solutions Inc. with an address at 365 Evans Ave. Suite #302, Toronto, ON M8Z1k2	Support, maintenance and development services for Telax products resold by Metaswitch.	Canada
Zoom Video Communications, Inc. with an address at 55 Almaden Blvd. 6 th Floor, San Jose CA 95113 USA	Support, maintenance and development services for Accession Meeting product.	United States
Netnumber, Inc. with an address at 650 Suffolk Street, Suite 307, Lowell, MA 01854	Support, maintenance and development services for NetNumber products resold by Metaswitch.	United States
JoHeR SARL with an address at 23 rue Balzac, 75008 Paris, France	Support, maintenance and development services for JoHeR products resold by Metaswitch.	France
Cordell Manufacturing, Inc. with an address at 918 Palomares Ave, La Verne, CA 91750	Support, maintenance and development services for Cordell products resold by Metaswitch.	United States
RadiSys Corporation with an address at 5435 NE Dawson Creek Drive, Hillsboro, Oregon 97124	Support, maintenance and development services for RadiSys products resold by Metaswitch.	United States
Nuance Communications International BVBA with an address at Guldensporenpark 32 B-9820 Merelbeke, Belgium	Support, maintenance and development services for Nuance products resold by Metaswitch.	Belgium

(G) **Service Provider Contact Details:** privacy@metaswitch.com

Schedule 2

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

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

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 - Module One: Clause 8.5(e) and Clause 8.9(b); Module Two: Clause 8.1(b), 8.9(a), (c), (d) and (e); Module Three: Clause 8.1(a), (c) and (d) and Clause 8.9(a), (c), (d), (e), (f) and (g);
 - (iii) Clause 9 - Module Two: Clause 9(a), (c), (d) and (e); Module Three: Clause 9(a), (c), (d) and (e);
 - (iv) Clause 12 – Module One: Clause 12(a) and (d); Modules Two and Three: Clause 12(a), (d) and (f);
 - (v) Clause 13;
 - (vi) Clause 15.1(c), (d) and (e);
 - (vii) Clause 16(e);
 - (viii) Clause 18 - Modules One, Two and Three: Clause 18(a) and (b).
- (b) Paragraph (a) is without prejudice to rights of data subjects under Regulation (EU) 2016/679.

Clause 4

Interpretation

- (c) Where these Clauses use terms that are defined in Regulation (EU) 2016/679, those terms shall have the same meaning as in that Regulation.
- (d) These Clauses shall be read and interpreted in the light of the provisions of Regulation (EU) 2016/679.
- (e) 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

(f) [RESERVED].

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.

MODULE ONE: Transfer controller to controller

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

(g) 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.

- (h) 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 a disproportionate effort for the data importer. In the latter case, the data importer shall, to the extent possible, make the information publicly available.
- (i) 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.
- (j) 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

- (k) 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.
- (l) 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.
- (m) 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 anonymisation² of the data and all back-ups at the end of the retention period.

8.5 Security of processing

- (n) 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.
- (o) 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.
- (p) 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.

- (q) 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.
- (r) 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.
- (s) 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 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.
- (t) 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 Union³ (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;

³ The Agreement on the European Economic Area (EEA Agreement) provides for the extension of the European Union's internal market to the three EEA States Iceland, Liechtenstein and Norway. The Union data protection legislation, including Regulation (EU) 2016/679, is covered by the EEA Agreement and has been incorporated into Annex XI thereto. Therefore, any disclosure by the data importer to a third party located in the EEA does not qualify as an onward transfer for the purpose of these Clauses.

- (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

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

MODULE TWO: Transfer controller to processor

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 Union⁴ (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.

⁴ The Agreement on the European Economic Area (EEA Agreement) provides for the extension of the European Union's internal market to the three EEA States Iceland, Liechtenstein and Norway. The Union data protection legislation, including Regulation (EU) 2016/679, is covered by the EEA Agreement and has been incorporated into Annex XI thereto. Therefore, any disclosure by the data importer to a third party located in the EEA does not qualify as an onward transfer for the purpose of these Clauses.

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.

MODULE THREE: Transfer processor to processor

8.1 Instructions

- (a) The data exporter has informed the data importer that it acts as processor under the instructions of its controller(s), which the data exporter shall make available to the data importer prior to processing.
- (b) The data importer shall process the personal data only on documented instructions from the controller, as communicated to the data importer by the data exporter, and any additional documented instructions from the data exporter. Such additional instructions shall not conflict with the instructions from the controller. The controller or data exporter may give further documented instructions regarding the data processing throughout the duration of the contract.
- (c) The data importer shall immediately inform the data exporter if it is unable to follow those instructions. Where the data importer is unable to follow the instructions from the controller, the data exporter shall immediately notify the controller.
- (d) The data exporter warrants that it has imposed the same data protection obligations on the data importer as set out in the contract or other legal act under Union or Member State law between the controller and the data exporter⁵.

8.2 Purpose limitation

⁵ See Article 28(4) of Regulation (EU) 2016/679 and, where the controller is an EU institution or body, Article 29(4) of Regulation (EU) 2018/1725.

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 controller, as communicated to the data importer by the data exporter, or from the data exporter.

8.3 Transparency

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

8.4 Accuracy

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

8.5 Duration of processing and erasure or return of data

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

8.6 Security of processing

- (a) The data importer and, during transmission, also the data exporter shall implement appropriate technical and organisational measures to ensure the security of the data, including protection against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access to that data (hereinafter “personal data breach”). In assessing the appropriate level of security, they shall take due account of the state of the art, the costs of implementation, the nature, scope, context and purpose(s) of processing and the risks involved in the processing for the data subject. The Parties shall in particular consider having recourse to encryption or pseudonymisation, including during transmission, where the purpose of processing can be fulfilled in that manner. In case of pseudonymisation, the additional information for attributing the personal data to a specific data subject shall, where possible, remain under the exclusive control of the data exporter or the controller. In complying with its obligations under this paragraph, the data importer shall at least implement the technical and organisational measures specified in 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 data to members of its personnel only to the extent strictly necessary for the implementation, management and monitoring of the contract. It shall ensure that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.
- (c) In the event of a personal data breach concerning personal data processed by the data importer under these Clauses, the data importer shall take appropriate measures to address the breach, including measures to mitigate its adverse effects. The data importer shall also notify, without undue delay, the data exporter and, where appropriate and feasible, the controller after having become aware of the breach. Such notification shall contain the details of a contact point where more information can be obtained, a description of the nature of the breach (including, where possible, categories and approximate number of data subjects and personal data records concerned), its likely consequences and the measures taken or proposed to address the data breach, including measures to mitigate its possible adverse effects. Where, and in so far as, it is not possible to provide all information at the same time, the initial notification shall contain the information then available and further information shall, as it becomes available, subsequently be provided without undue delay.
- (d) The data importer shall cooperate with and assist the data exporter to enable the data exporter to comply with its obligations under Regulation (EU) 2016/679, in particular to notify its controller so that the latter may in turn notify the competent supervisory authority and the affected data subjects, taking into account the nature of processing and the information available to the data importer.

8.7 Sensitive data

Where the transfer involves personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, or biometric data for the purpose of uniquely identifying a natural person, data concerning health or a person's sex life or sexual orientation, or data relating to criminal convictions and offences (hereinafter "sensitive data"), the data importer shall apply the specific restrictions and/or additional safeguards set out in 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 controller, as communicated to the data importer by the data exporter. In addition, the data may only be disclosed to a third party located outside the European Union⁶ (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 of Regulation (EU) 2016/679;

⁶ The Agreement on the European Economic Area (EEA Agreement) provides for the extension of the European Union's internal market to the three EEA States Iceland, Liechtenstein and Norway. The Union data protection legislation, including Regulation (EU) 2016/679, is covered by the EEA Agreement and has been incorporated into Annex XI thereto. Therefore, any disclosure by the data importer to a third party located in the EEA does not qualify as an onward transfer for the purposes of these Clauses.

- (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 or the controller that relate to the processing under these Clauses.
- (b) The Parties shall be able to demonstrate compliance with these Clauses. In particular, the data importer shall keep appropriate documentation on the processing activities carried out on behalf of the controller.
- (c) The data importer shall make all information necessary to demonstrate compliance with the obligations set out in these Clauses available to the data exporter, which shall provide it to the controller.
- (d) The data importer shall allow for and contribute to audits by the data exporter of the processing activities covered by these Clauses, at reasonable intervals or if there are indications of non-compliance. The same shall apply where the data exporter requests an audit on instructions of the controller. In deciding on an audit, the data exporter may take into account relevant certifications held by the data importer.
- (e) Where the audit is carried out on the instructions of the controller, the data exporter shall make the results available to the controller.
- (f) The data exporter may choose to conduct the audit by itself or mandate an independent auditor. Audits may include inspections at the premises or physical facilities of the data importer and shall, where appropriate, be carried out with reasonable notice.
- (g) The Parties shall make the information referred to in paragraphs (b) and (c), including the results of any audits, available to the competent supervisory authority on request.

Clause 9

Use of sub-processors

MODULE TWO: Transfer controller to processor

- (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 five business 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.⁷ 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.

MODULE THREE: Transfer processor to processor

- (a) The data importer has the controller's general authorisation for the engagement of sub-processor(s) from an agreed list. The data importer shall specifically inform the controller in writing of any intended changes to that list through the addition or replacement of sub-processors at least five business days in advance, thereby giving the controller sufficient time to be able to object to such changes prior to the engagement of the sub-processor(s). The data importer shall provide the controller with the information necessary to enable the controller to exercise its right to object. The data importer shall inform the data exporter of the engagement of the sub-processor(s).
- (b) Where the data importer engages a sub-processor to carry out specific processing activities (on behalf of the controller), it shall do so by way of a written contract that provides for, in substance, the same data protection obligations as those binding the data importer under these Clauses, including in terms of third-party beneficiary rights for data subjects.⁸ The Parties agree that, by complying with this Clause, the data importer fulfils its obligations under Clause 8.8. The data importer shall ensure that the sub-processor complies with the obligations to which the data importer is subject pursuant to these Clauses.
- (c) The data importer shall provide, at the data exporter's or controller's request, a copy of such a sub-processor agreement and any subsequent amendments. To the extent necessary to protect

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

⁸ This requirement may be satisfied by the sub-processor acceding to these Clauses under the appropriate Module, in accordance with Clause 7.

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

MODULE ONE: Transfer controller to controller

- (f) 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.⁹ 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.
- (g) 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.
- (h) 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.
- (i) 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

⁹ That period may be extended by a maximum of two more months, to the extent necessary taking into account the complexity and number of requests. The data importer shall duly and promptly inform the data subject of any such extension.

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.
- (j) 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.
- (k) 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.
- (l) 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.

MODULE TWO: Transfer controller to processor

- (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.

MODULE THREE: Transfer processor to processor

- (a) The data importer shall promptly notify the data exporter and, where appropriate, the controller of any request it has received from a data subject, without responding to that request unless it has been authorised to do so by the controller.
- (b) The data importer shall assist, where appropriate in cooperation with the data exporter, the controller in fulfilling its obligations to respond to data subjects' requests for the exercise of their rights under Regulation (EU) 2016/679 or Regulation (EU) 2018/1725, as applicable. In this regard, the Parties shall set out in 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 controller, as communicated by the data exporter.

Clause 11

Redress

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

MODULE ONE: Transfer controller to controller

MODULE TWO: Transfer controller to processor

MODULE THREE: Transfer processor to processor

- (b) In case of a dispute between a data subject and one of the Parties as regards compliance with these Clauses, that Party shall use its best efforts to resolve the issue amicably in a timely fashion. The Parties shall keep each other informed about such disputes and, where appropriate, cooperate in resolving them.
- (c) Where the data subject invokes a third-party beneficiary right pursuant to Clause 3, the data importer shall accept the decision of the data subject to:
 - (i) lodge a complaint with the supervisory authority in the Member State of his/her habitual residence or place of work, or the competent supervisory authority pursuant to Clause 13;
 - (ii) refer the dispute to the competent courts within the meaning of Clause 18.
- (d) The Parties accept that the data subject may be represented by a not-for-profit body, organisation or association under the conditions set out in Article 80(1) of Regulation (EU) 2016/679.
- (e) The data importer shall abide by a decision that is binding under the applicable EU or Member State law.
- (f) The data importer agrees that the choice made by the data subject will not prejudice his/her substantive and procedural rights to seek remedies in accordance with applicable laws.

Clause 12

Liability

MODULE ONE: Transfer controller to controller

- (g) 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.
- (h) 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.
- (i) 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.

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

MODULE TWO: Transfer controller to processor

MODULE THREE: Transfer processor to processor

- (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

MODULE ONE: Transfer controller to controller

MODULE TWO: Transfer controller to processor

MODULE THREE: Transfer processor to processor

- (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

MODULE ONE: Transfer controller to controller

MODULE TWO: Transfer controller to processor

MODULE THREE: Transfer processor to processor

- (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 safeguards¹⁰;
 - (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). [For Module Three: The data exporter shall forward the notification to the controller.]
- (f) Following a notification pursuant to paragraph (e), or if the data exporter otherwise has reason to believe that the data importer can no longer fulfil its obligations under these Clauses, the data exporter shall promptly identify appropriate measures (e.g. technical or organisational measures to ensure security and confidentiality) to be adopted by the data exporter and/or data importer to address the situation [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

¹⁰ As regards the impact of such laws and practices on compliance with these Clauses, different elements may be considered as part of an overall assessment. Such elements may include relevant and documented practical experience with prior instances of requests for disclosure from public authorities, or the absence of such requests, covering a sufficiently representative time-frame. This refers in particular to internal records or other documentation, drawn up on a continuous basis in accordance with due diligence and certified at senior management level, provided that this information can be lawfully shared with third parties. Where this practical experience is relied upon to conclude that the data importer will not be prevented from complying with these Clauses, it needs to be supported by other relevant, objective elements, and it is for the Parties to consider carefully whether these elements together carry sufficient weight, in terms of their reliability and representativeness, to support this conclusion. In particular, the Parties have to take into account whether their practical experience is corroborated and not contradicted by publicly available or otherwise accessible, reliable information on the existence or absence of requests within the same sector and/or the application of the law in practice, such as case law and reports by independent oversight bodies.

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

MODULE ONE: Transfer controller to controller

MODULE TWO: Transfer controller to processor

MODULE THREE: Transfer processor to processor

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.

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

- (b) If the data importer is prohibited from notifying the data exporter and/or the data subject under the laws of the country of destination, the data importer agrees to use its best efforts to obtain a waiver of the prohibition, with a view to communicating as much information as possible, as soon as possible. The data importer agrees to document its best efforts in order to be able to demonstrate them on request of the data exporter.
- (c) Where permissible under the laws of the country of destination, the data importer agrees to provide the data exporter, at regular intervals for the duration of the contract, with as much relevant information as possible on the requests received (in particular, number of requests, type of data requested, requesting authority/ies, whether requests have been challenged and the outcome of such challenges, etc.). For Module Three: The data exporter shall forward the information to the controller.
- (d) The data importer agrees to preserve the information pursuant to paragraphs (a) to (c) for the duration of the contract and make it available to the competent supervisory authority on request.
- (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. For Module Three: The data exporter shall make the assessment available to the controller.
- (c) The data importer agrees to provide the minimum amount of information permissible when responding to a request for disclosure, based on a reasonable interpretation of the request.

SECTION IV – FINAL PROVISIONS

Clause 16

Non-compliance with the Clauses and termination

- (a) The data importer shall promptly inform the data exporter if it is unable to comply with these Clauses, for whatever reason.
- (b) In the event that the data importer is in breach of these Clauses or unable to comply with these Clauses, the data exporter shall suspend the transfer of personal data to the data importer until compliance is again ensured or the contract is terminated. This is without prejudice to Clause 14(f).
- (c) The data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses, where:
 - (i) the data exporter has suspended the transfer of personal data to the data importer pursuant to paragraph (b) and compliance with these Clauses is not restored within a reasonable time and in any event within one month of suspension;
 - (ii) the data importer is in substantial or persistent breach of these Clauses; or
 - (iii) the data importer fails to comply with a binding decision of a competent court or supervisory authority regarding its obligations under these Clauses.

In these cases, it shall inform the competent supervisory authority, 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.

- (d) 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. 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

MODULE ONE: Transfer controller to controller

MODULE TWO: Transfer controller to processor

MODULE THREE: Transfer processor to processor

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

MODULE ONE: Transfer controller to controller

MODULE TWO: Transfer controller to processor

MODULE THREE: Transfer processor to processor

- (a) Any dispute arising from these Clauses shall be resolved by the courts of an EU Member State.
- (b) The Parties agree that those shall be the courts of Ireland.
- (c) A data subject may also bring legal proceedings against the data exporter and/or data importer before the courts of the Member State in which he/she has his/her habitual residence.
- (d) The Parties agree to submit themselves to the jurisdiction of such courts.

APPENDIX

ANNEX I

A. LIST OF PARTIES

Data exporter(s):

Name: The entity defined as “Customer” in Section 1.1 of this Data Processing Agreement.

Address: The address for Customer listed in the Agreement.

Contact person’s name, position and contact details: The contact details associated with the Customer as listed in the Agreement.

Activities relevant to the data transferred under these Clauses: The activities specified in Schedule 1 of this Data Processing Agreement.

Role (controller/processor): Controller for Module Two; or processor for Module Three

Data importer(s):

Name: The entity defined as “Service Provider” in Section 1.1 of this Data Processing Agreement.

Address: The address for Service Provider listed in the Agreement.

Contact person’s name, position and contact details: The contact details associated with the Service Provider as listed in the Agreement.

Activities relevant to the data transferred under these Clauses: The activities specified in Schedule 1 of this Data Processing Agreement.

Role (controller/processor): Processor for Module Two and Module Three

B. DESCRIPTION OF TRANSFER

Categories of data subjects whose personal data is transferred

Categories of data subjects are specified in Schedule 1 of this Data Processing Agreement.

Categories of personal data transferred

Categories of personal data are specified in Schedule 1 of this Data Processing Agreement.

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

N/A

The frequency of the transfer (e.g. whether the data is transferred on a one-off or continuous basis).

Personal data is transferred in accordance with Customer's instructions as described in Section 3.3 of this Data Processing Agreement.

Nature of the processing

The nature of processing is described in Schedule 1 of this Data Processing Agreement.

Purpose(s) of the data transfer and further processing

To fulfil the Agreement.

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

The data exporter determines the duration of processing in accordance with the terms of this Data Processing Agreement.

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

The subject matter, nature and duration of the processing are described in Schedule 1 of this Data Processing Agreement.

C. COMPETENT SUPERVISORY AUTHORITY

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

The data exporter's competent supervisory authority will be determined in accordance with the GDPR.

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

Metaswitch has implemented and will maintain for personal data processed by Metaswitch as described in the Metaswitch Data Processing Agreement the following security measures, which in conjunction with the security commitments in the body of the Data Processing Agreement are Metaswitch’s sole and exclusive responsibility with respect to the security of that personal data.

Domain	Practices
Organization of Information Security	<p>Security Ownership. Metaswitch has a cross-team group of experts responsible for coordinating and monitoring the security rules and procedures.</p> <p>Security Roles and Responsibilities. Metaswitch personnel with access to personal data are subject to confidentiality obligations.</p> <p>Risk Management Program. Metaswitch performed a risk assessment before processing the personal data or launching the applicable Service and before processing any personal data in a support or professional services context.</p> <p>Metaswitch retains its security documents pursuant to its retention requirements after they are no longer in effect.</p>
Asset Management	<p>Asset Control. Metaswitch maintains policies limiting the storage and processing of personal data to defined secure assets which have access controlled to trained personnel authorized in writing.</p> <p>Asset Handling</p> <ul style="list-style-type: none"> - Metaswitch classifies personal data to help identify it and to allow for access to it to be appropriately restricted. - Metaswitch imposes restrictions on printing personal data and has procedures for disposing of printed materials that contain such data. - Metaswitch has policies controlling the storage or processing personal data on portable devices, remotely accessing such data, and employee use of approved devices to store or process such data outside Metaswitch facilities.
Human Resources Security	<p>Security Training. Metaswitch, and affiliates, informs its personnel about relevant security procedures and their respective roles. Metaswitch also informs its personnel of possible consequences of breaching the security rules and procedures. Metaswitch will only use anonymous, lab-generated, or fictional data in training.</p>
Physical and Environmental Security	<p>Physical Access to Facilities. Metaswitch limits access to facilities where information systems that process personal data are located to identified authorized individuals.</p> <p>Physical Access to Components. Metaswitch maintains records of the incoming and outgoing media containing personal data, including the kind of media, the authorized sender/recipients, date and time, the number, and types of media.</p> <p>Protection from Disruptions. Metaswitch uses a variety of industry standard systems to protect against loss of data due to power supply failure or line interference.</p> <p>Component Disposal. Metaswitch uses industry standard processes to delete personal data when it is no longer needed.</p>

Communications and Operations Management	<p>Operational Policy. Metaswitch maintains security documents describing its security measures and the relevant procedures and responsibilities of its personnel who have access to personal data.</p> <p>Data Recovery Procedures</p> <ul style="list-style-type: none">- On an ongoing basis, but in no case less frequently than once a week (unless no updates have occurred during that period), Metaswitch maintains multiple copies of primary personal data stores, from which such data can be recovered.- Metaswitch stores copies of personal data and data recovery procedures in a different place from where the primary computer equipment processing the personal data are located.- Metaswitch has specific procedures in place governing access to copies of personal data.- Metaswitch reviews data recovery procedures regularly.- Metaswitch logs data restoration efforts, including the person responsible, the description of the restored data and where applicable, the person responsible and which data (if any) had to be input manually in the data recovery process. <p>Malicious Software. Metaswitch has anti-malware controls to help avoid malicious software gaining unauthorized access to personal data, including malicious software originating from public networks.</p> <p>Data Beyond Boundaries</p> <ul style="list-style-type: none">- In most instances, Metaswitch encrypts, or enables Customer to encrypt, personal data that is transmitted over public networks. Otherwise, Metaswitch advises Customer to use appropriate third-party tools to encrypt personal data that is transmitted over public networks.- Metaswitch restricts access to personal data in media leaving its facilities. <p>Event Logging. Where practicable, Metaswitch logs, or enables Customer to log, access and use of information systems storing personal data, registering the access ID, time, authorization granted or denied, and relevant activity.</p>
Access Control	<p>Access Policy. Metaswitch maintains a record of security privileges of individuals having access to personal data.</p> <p>Access Authorization</p> <ul style="list-style-type: none">- Metaswitch maintains and updates a record of personnel authorized to access Metaswitch systems that contain personal data.- Metaswitch deactivates user accounts, and therefore removes attendant access, on personnel departure and arranges the return of all Metaswitch-issued equipment.- Metaswitch identifies those personnel who may grant, alter, or cancel authorized access to data and resources.- Metaswitch ensures that where more than one individual has access to systems storing personal data, the individuals have separate identifiers/log-ins. <p>Least Privilege</p> <ul style="list-style-type: none">- Personnel are only permitted to have access to personal data when needed by the role they are in or the work they are doing. <p>Integrity and Confidentiality</p> <ul style="list-style-type: none">- Metaswitch instructs personnel to disable administrative sessions when leaving premises Metaswitch controls or when computers are otherwise left unattended.

	<p>- Metaswitch stores passwords in a way that makes them unintelligible while they are in force.</p> <p>Authentication</p> <ul style="list-style-type: none"> - Metaswitch uses industry standard practices to identify and authenticate users who attempt to access information systems. - Where authentication mechanisms are based on passwords, Metaswitch follows industry best practice with regards to password longevity. - Where authentication mechanisms are based on passwords, Metaswitch requires the password to be at least eight characters long. - Metaswitch ensures that de-activated or expired identifiers are not granted to other individuals. - Metaswitch monitors, or enables Customer to monitor, repeated attempts to gain access to the information system using an invalid password. - Metaswitch maintains industry standard procedures to deactivate passwords that have been corrupted or inadvertently disclosed. - Metaswitch uses industry standard password protection practices, including practices designed to maintain the confidentiality and integrity of passwords when they are assigned and distributed, and during storage. <p>Network Design. Metaswitch has controls to avoid individuals assuming access rights they have not been assigned to gain access to personal data they are not authorized to access</p>
Information Security Incident Management	<p>Incident Response Process</p> <ul style="list-style-type: none"> - Metaswitch maintains a record of security breaches with a description of the breach, the time period, the consequences of the breach, the name of the reporter, and to whom the breach was reported, and the procedure for recovering data. - For each Security Breach, notification by Metaswitch (as defined in the Data Protection Addendum section above) will be made without undue delay and, in any event, within 72 hours of Metaswitch becoming aware of such Security Breach. - Metaswitch tracks, or enables Customer to track, disclosures of personal data, including what data has been disclosed, to whom, and at what time. <p>Service Monitoring. Metaswitch security personnel verify logs at least every six months to propose remediation efforts if necessary.</p>
Business Continuity Management	<ul style="list-style-type: none"> - Metaswitch maintains emergency and contingency plans for the facilities in which Metaswitch information systems that process personal data are located. - Metaswitch's redundant storage and its procedures for recovering data are designed to attempt to reconstruct personal data in its original or last-replicated state from before the time it was lost or destroyed.

ANNEX III – LIST OF SUB-PROCESSORS

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

See Schedule 1 of this Data Processing Agreement.

Schedule 3

UK SCCs



Information Commissioner's Office

**STANDARD DATA PROTECTION CLAUSES TO BE ISSUED BY THE COMMISSIONER UNDER S119A(1)
DATA PROTECTION ACT 2018**

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 later of 22 September 2022 and the Agreement effective date.	
The Parties	Exporter (who sends the Restricted Transfer)	Importer (who receives the Restricted Transfer)
Parties' details	Full legal name: The entity defined as "Customer" in Section 1.1 of this Data Processing Agreement. Trading name (if different): N/A Main address (if a company registered address): The address for Customer listed in the Agreement Official registration number (if any) (company number or similar identifier): [REDACTED]	Full legal name: The entity defined as "Service Provider" in Section 1.1 of this Data Processing Agreement. Trading name (if different): N/A Main address (if a company registered address): The address for Service Provider listed in the Agreement Official registration number (if any) (company number or similar identifier): [REDACTED]

Key Contact	Full Name (optional): The name and contact information for Customer listed in the Agreement. Job Title: <input type="text"/> Contact details including email: <input type="text"/>	Full Name (optional): The name and contact information listed for Service Provider in the Agreement. Job Title: <input type="text"/> Contact details including email: <input type="text"/>
Signature (if required for the purposes of Section 2)	N/A	N/A

Table 2: Selected SCCs, Modules and Selected Clauses

Addendum EU SCCs		<input type="checkbox"/> The version of the Approved EU SCCs which this Addendum is appended to, detailed below, including the Appendix Information: Date: <input type="text"/> Reference (if any): <input type="text"/> Other identifier (if any): <input type="text"/> Or <input checked="" type="checkbox"/> the Approved EU SCCs, including the Appendix Information and with only the following modules, clauses or optional provisions of the Approved EU SCCs brought into effect for the purposes of this Addendum:				
Module	Module in operation	Clause 7 (Docking Clause)	Clause 11 (Option)	Clause 9a (Prior Authorisation or General Authorisation)	Clause 9a (Time period)	Is personal data received from the Importer combined with personal data collected by the Exporter?
1						
2	Yes	Removed	Removed	General	5 business days	No
3	Yes	Removed	Removed	General	5 business days	No

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: Exporter (meaning the entity defined as “Customer” in Section 1.1 of this Data Processing Agreement) and Importer (meaning the entity defined as “Service Provider” in Section 1.1 of this Data Processing Agreement).

Annex 1B: Description of Transfer: See Schedule 1 of the DPA.

Annex II: Technical and organisational measures including technical and organisational measures to ensure the security of the data: See Annex II of the EU SCCs.

Annex III: List of Sub processors (Modules 2 and 3 only): See Schedule 1 of the DPA.

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: <input checked="" type="checkbox"/> Importer <input type="checkbox"/> Exporter <input type="checkbox"/> neither Party
--	--

Part 2: Mandatory Clauses

Entering into this Addendum

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

Interpretation of this Addendum

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

Addendum	This International Data Transfer Addendum which is made up of this Addendum incorporating the Addendum EU SCCs.
-----------------	---

Addendum EU SCCs	The version(s) of the Approved EU SCCs which this Addendum is appended to, as set out in Table 2, including the Appendix Information.
Appendix Information	As set out in Table 3.
Appropriate Safeguards	The standard of protection over the personal data and of data subjects' rights, which is required by UK Data Protection Laws when you are making a Restricted Transfer relying on standard data protection clauses under Article 46(2)(d) UK GDPR.
Approved Addendum	The template Addendum issued by the ICO and laid before Parliament in accordance with s119A of the Data Protection Act 2018 on 2 February 2022, as it is revised under Section 18.
Approved EU SCCs	The Standard Contractual Clauses set out in the Annex of Commission Implementing Decision (EU) 2021/914 of 4 June 2021.
ICO	The Information Commissioner.
Restricted Transfer	A transfer which is covered by Chapter V of the UK GDPR.
UK	The United Kingdom of Great Britain and Northern Ireland.
UK Data Protection Laws	All laws relating to data protection, the processing of personal data, privacy and/or electronic communications in force from time to time in the UK, including the UK GDPR and the Data Protection Act 2018.
UK GDPR	As defined in section 3 of the Data Protection Act 2018.

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.