STANDARD CONTRACTUAL CLAUSES

Controller to Processor

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 data to a third country.

(b) The Parties:

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

(ii) the entity/ies in a third country receiving the personal data from the data exporter, directly or indirectly via another entity also Party to these Clauses, as listed in Annex I.A (hereinafter each 'data importer')

have agreed to these standard contractual clauses (hereinafter: 'Clauses').

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

(d) The Appendix to these Clauses containing the Annexes referred to therein forms an integral part of these Clauses.

Clause 2

Effect and invariability of the Clauses

(a) These Clauses set out appropriate safeguards, including enforceable data subject rights and effective legal remedies, pursuant to Article 46(1) and Article 46(2)(c) of Regulation (EU) 2016/679 and, with respect to data transfers from controllers to processors and/or processors to processors, standard contractual clauses pursuant to Article 28(7) of Regulation (EU) 2016/679, provided they are not modified, except to select the appropriate Module(s) or to add or update information in the Appendix. This does not prevent the Parties from including the standard contractual clauses laid down in these Clauses in a wider contract and/or to add other clauses or additional safeguards, provided that they do not contradict, directly or indirectly, these Clauses or prejudice the fundamental rights or freedoms of data subjects.

(b) These Clauses are without prejudice to obligations to which the data exporter is subject by virtue of Regulation (EU) 2016/679.

Clause 3

Third-party beneficiaries

(a) Data subjects may invoke and enforce these Clauses, as third-party beneficiaries, against the data exporter and/or data importer, with the following exceptions:

(i) Clause 1, Clause 2, Clause 3, Clause 6, Clause 7;

(ii) Clause 8.1(b), 8.9(a), (c), (d) and (e);

(iii) Clause 9(a), (c), (d) and (e);

(iv) Clause 12(a), (d) and (f);

(v) Clause 13;

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

(vii) Clause 16(e);

(viii) Clause 18(a) and (b).

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

Clause 4

Interpretation

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

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

(c) These Clauses shall not be interpreted in a way that conflicts with rights and obligations provided for in Regulation (EU) 2016/679.

Clause 5

Hierarchy

In the event of a contradiction between these Clauses and the provisions of related agreements between the Parties, existing at the time these Clauses are agreed or entered into thereafter, these Clauses shall prevail.

Clause 6

Description of the transfer(s)

The details of the transfer(s), and in particular the categories of personal data that are transferred and the purpose(s) for which they are transferred, are specified in Annex I.B.

SECTION II – OBLIGATIONS OF THE PARTIES

Clause 8

Data protection safeguards

The data exporter warrants that it has used reasonable efforts to determine that the data importer is able, through the implementation of appropriate technical and organisational measures, to satisfy its obligations under these Clauses.

8.1 Instructions

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

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

8.2 Purpose limitation

The data importer shall process the personal data only for the specific purpose(s) of the transfer, as set out in Annex I.B, unless on further instructions from the data exporter.

8.3 Transparency

On request, the data exporter shall make a copy of these Clauses, including the Appendix as completed by the Parties, available to the data subject free of charge. To the extent necessary to protect business secrets or other confidential information, including the measures described in Annex II and personal data, the data exporter may redact part of the text of the Appendix to these Clauses prior to sharing a copy, but shall provide a meaningful summary where the data subject would otherwise not be able to understand the its content or exercise his/her rights. On request, the Parties shall provide the data subject with the reasons for the redactions, to the extent possible without revealing the redacted information. This Clause is without prejudice to the obligations of the data exporter under Articles 13 and 14 of Regulation (EU) 2016/679.

8.4 Accuracy

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

8.5 Duration of processing and erasure or return of data

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

8.6 Security of processing

(a) The data importer and, during transmission, also the data exporter shall implement appropriate technical and organisational measures to ensure the security of the data, including protection against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access to that data (hereinafter 'personal data breach'). In assessing the appropriate level of security, the Parties shall take due account of the state of the art, the costs of implementation, the nature, scope, context and purpose(s) of processing and the risks involved in the processing for the data subjects. The Parties shall in particular consider having recourse to encryption or pseudonymisation, including during transmission, where the purpose of processing can be fulfilled in that manner. In case of pseudonymisation, the additional information for attributing the personal data to a specific data subject shall, where possible, remain under the exclusive control of the data exporter. In complying with its obligations under this paragraph, the data importer shall at least implement the technical and organisational measures specified in Annex II. The data importer shall carry out regular checks to ensure that these measures continue to provide an appropriate level of security.

(b) The data importer shall grant access to the personal data to members of its personnel only to the extent strictly necessary for the implementation, management and monitoring of the contract. It shall ensure that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

(c) In the event of a personal data breach concerning personal data processed by the data importer under these Clauses, the data importer shall take appropriate measures to address the breach, including measures to mitigate its adverse effects. The data importer shall also notify the data exporter without undue delay after having become aware of the breach.

Such notification shall contain the details of a contact point where more information can be obtained, a description of the nature of the breach (including, where possible, categories and approximate number of data subjects and personal data records concerned), its likely consequences and the measures taken or proposed to address the breach including, where appropriate, measures to mitigate its possible adverse effects. Where, and in so far as, it is not possible to provide all information at the same time, the initial notification shall contain the information then available and further information shall, as it becomes available, subsequently be provided without undue delay.

(d) The data importer shall cooperate with and assist the data exporter to enable the data exporter to comply with its obligations under Regulation (EU) 2016/679, in particular to notify the competent supervisory authority and the affected data subjects, taking into account the nature of processing and the information available to the data importer.

8.7 Sensitive data

Where the transfer involves personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, or biometric data for the purpose of uniquely identifying a natural person, data concerning health or a person's sex life or sexual orientation, or data relating to criminal convictions and offences (hereinafter 'sensitive data'), the data importer shall apply the specific restrictions and/or additional safeguards described in Annex I.B.

8.8 Onward transfers

The data importer shall only disclose the personal data to a third party on documented instructions from the data exporter. In addition, the data may only be disclosed to a third party located outside the European Union ([2]) (in the same country as the data importer or in another third country, hereinafter 'onward transfer') if the third party is or agrees to be bound by these Clauses, under the appropriate Module, or if:

(i) the onward transfer is to a country benefitting from an adequacy decision pursuant to Article 45 of Regulation (EU) 2016/679 that covers the onward transfer;

(ii) the third party otherwise ensures appropriate safeguards pursuant to Articles 46 or 47 Regulation of (EU) 2016/679 with respect to the processing in question;

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

(iv) the onward transfer is necessary in order to protect the vital interests of the data subject or of another natural person.

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

8.9 Documentation and compliance

(a) The data importer shall promptly and adequately deal with enquiries from the data exporter that relate to the processing under these Clauses.

(b) The Parties shall be able to demonstrate compliance with these Clauses. In particular, the data importer shall keep appropriate documentation on the processing activities carried out on behalf of the data exporter.

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

(d) The data exporter may choose to conduct the audit by itself or mandate an independent auditor. Audits may include inspections at the premises or physical facilities of the data importer and shall, where appropriate, be carried out with reasonable notice.

(e) The Parties shall make the information referred to in paragraphs (b) and (c), including the results of any audits, available to the competent supervisory authority on request.

Clause 9

Use of sub-processors

(a) GENERAL WRITTEN AUTHORISATION 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 30 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. ([3]) The Parties agree that, by complying with this Clause, the data importer fulfils its obligations under Clause 8.8. The data importer shall ensure that the sub-processor

complies with the obligations to which the data importer is subject pursuant to these Clauses.

(c) The data importer shall provide, at the data exporter's request, a copy of such a sub-processor agreement and any subsequent amendments to the data exporter. To the extent necessary to protect business secrets or other confidential information, including personal data, the data importer may redact the text of the agreement prior to sharing a copy.

(d) The data importer shall remain fully responsible to the data exporter for the performance of the sub-processor's obligations under its contract with the data importer. The data importer shall notify the data exporter of any failure by the sub-processor to fulfil its obligations under that contract.

(e) The data importer shall agree a third-party beneficiary clause with the sub-processor whereby – in the event the data importer has factually disappeared, ceased to exist in law or has become insolvent – the data exporter shall have the right to terminate the sub-processor contract and to instruct the sub-processor to erase or return the personal data.

Clause 10

Data subject rights

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

(b) The data importer shall assist the data exporter in fulfilling its obligations to respond to data subjects' requests for the exercise of their rights under Regulation (EU) 2016/679. In this regard, the Parties shall set out in Annex II the appropriate technical and organisational measures, taking into account the nature of the processing, by which the assistance shall be provided, as well as the scope and the extent of the assistance required.

(c) In fulfilling its obligations under paragraphs (a) and (b), the data importer shall comply with the instructions from the data exporter.

Clause 11

Redress

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

(b) In case of a dispute between a data subject and one of the Parties as regards compliance with these Clauses, that Party shall use its best efforts to resolve the issue amicably in a

timely fashion. The Parties shall keep each other informed about such disputes and, where appropriate, cooperate in resolving them.

(c) Where the data subject invokes a third-party beneficiary right pursuant to Clause 3, the data importer shall accept the decision of the data subject to:

(i) lodge a complaint with the supervisory authority in the Member State of his/her habitual residence or place of work, or the competent supervisory authority pursuant to Clause 13;

(ii) refer the dispute to the competent courts within the meaning of Clause 18.

(d) The Parties accept that the data subject may be represented by a not-for-profit body, organisation or association under the conditions set out in Article 80(1) of Regulation (EU) 2016/679.

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

(f) The data importer agrees that the choice made by the data subject will not prejudice his/her substantive and procedural rights to seek remedies in accordance with applicable laws.

Clause 12

Liability

(a) Each Party shall be liable to the other Party/ies for any damages it causes the other Party/ies by any breach of these Clauses.

(b) The data importer shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages the data importer or its sub-processor causes the data subject by breaching the third-party beneficiary rights under these Clauses.

(c) Notwithstanding paragraph (b), the data exporter shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages the data exporter or the data importer (or its sub-processor) causes the data subject by breaching the third-party beneficiary rights under these Clauses. This is without prejudice to the liability of the data exporter and, where the data exporter is a processor acting on behalf of a controller, to the liability of the controller under Regulation (EU) 2016/679 or Regulation (EU) 2018/1725, as applicable.

(d) The Parties agree that if the data exporter is held liable under paragraph (c) for damages caused by the data importer (or its sub-processor), it shall be entitled to claim back from

the data importer that part of the compensation corresponding to the data importer's responsibility for the damage.

(e) Where more than one Party is responsible for any damage caused to the data subject as a result of a breach of these Clauses, all responsible Parties shall be jointly and severally liable and the data subject is entitled to bring an action in court against any of these Parties.

(f) The Parties agree that if one Party is held liable under paragraph (e), it shall be entitled to claim back from the other Party/ies that part of the compensation corresponding to its/their responsibility for the damage.

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

Clause 13

Supervision

(a) [Where the data exporter is established in an EU Member State:] The supervisory authority with responsibility for ensuring compliance by the data exporter with Regulation (EU) 2016/679 as regards the data transfer, as indicated in Annex I.C, shall act as competent supervisory authority.

[Where the data exporter is not established in an EU Member State, but falls within the territorial scope of application of Regulation (EU) 2016/679 in accordance with its Article 3(2) and has appointed a representative pursuant to Article 27(1) of Regulation (EU) 2016/679:] The supervisory authority of the Member State in which the representative within the meaning of Article 27(1) of Regulation (EU) 2016/679 is established, as indicated in Annex I.C, shall act as competent supervisory authority.

[Where the data exporter is not established in an EU Member State, but falls within the territorial scope of application of Regulation (EU) 2016/679 in accordance with its Article 3(2) without however having to appoint a representative pursuant to Article 27(2) of Regulation (EU) 2016/679:] The supervisory authority of one of the Member States in which the data subjects whose personal data is transferred under these Clauses in relation to the offering of goods or services to them, or whose behaviour is monitored, are located, as indicated in Annex I.C, shall act as competent supervisory authority.

(b) The data importer agrees to submit itself to the jurisdiction of and cooperate with the competent supervisory authority in any procedures aimed at ensuring compliance with these Clauses. In particular, the data importer agrees to respond to enquiries, submit to audits and comply with the measures adopted by the supervisory authority, including remedial and compensatory measures. It shall provide the supervisory authority with written confirmation that the necessary actions have been taken.

SECTION III – LOCAL LAWS AND OBLIGATIONS IN CASE OF ACCESS BY PUBLIC AUTHORITIES

Clause 14

Local laws and practices affecting compliance with the Clauses

(a) The Parties warrant that they have no reason to believe that the laws and practices in the third country of destination applicable to the processing of the personal data by the data importer, including any requirements to disclose personal data or measures authorising access by public authorities, prevent the data importer from fulfilling its obligations under these Clauses. This is based on the understanding that laws and practices that respect the essence of the fundamental rights and freedoms and do not exceed what is necessary and proportionate in a democratic society to safeguard one of the objectives listed in Article 23(1) of Regulation (EU) 2016/679, are not in contradiction with these Clauses.

(b) The Parties declare that in providing the warranty in paragraph (a), they have taken due account in particular of the following elements:

(i) the specific circumstances of the transfer, including the length of the processing chain, the number of actors involved and the transmission channels used; intended onward transfers; the type of recipient; the purpose of processing; the categories and format of the transferred personal data; the economic sector in which the transfer occurs; the storage location of the data transferred;

(ii) the laws and practices of the third country of destination– including those requiring the disclosure of data to public authorities or authorising access by such authorities – relevant in light of the specific circumstances of the transfer, and the applicable limitations and safeguards ([4]);

(iii) any relevant contractual, technical or organisational safeguards put in place to supplement the safeguards under these Clauses, including measures applied during transmission and to the processing of the personal data in the country of destination.

(c) The data importer warrants that, in carrying out the assessment under paragraph (b), it has made its best efforts to provide the data exporter with relevant information and agrees that it will continue to cooperate with the data exporter in ensuring compliance with these Clauses.

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

(e) The data importer agrees to notify the data exporter promptly if, after having agreed to these Clauses and for the duration of the contract, it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under paragraph (a), including following a change in the laws of the third country or a measure (such as a

disclosure request) indicating an application of such laws in practice that is not in line with the requirements in paragraph (a).

(f) Following a notification pursuant to paragraph (e), or if the data exporter otherwise has reason to believe that the data importer can no longer fulfil its obligations under these Clauses, the data exporter shall promptly identify appropriate measures (e.g. technical or organisational measures to ensure security and confidentiality) to be adopted by the data exporter and/or data importer to address the situation. The data exporter shall suspend the data transfer if it considers that no appropriate safeguards for such transfer can be ensured, or if instructed by the competent supervisory authority to do so. In this case, the data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses. If the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise. Where the contract is terminated pursuant to this Clause, Clause 16(d) and (e) shall apply.

Clause 15

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

15.1 Notification

(a) The data importer agrees to notify the data exporter and, where possible, the data subject promptly (if necessary with the help of the data exporter) if it:

(i) receives a legally binding request from a public authority, including judicial authorities, under the laws of the country of destination for the disclosure of personal data transferred pursuant to these Clauses; such notification shall include information about the personal data requested, the requesting authority, the legal basis for the request and the response provided; or

(ii) becomes aware of any direct access by public authorities to personal data transferred pursuant to these Clauses in accordance with the laws of the country of destination; such notification shall include all information available to the importer.

(b) If the data importer is prohibited from notifying the data exporter and/or the data subject under the laws of the country of destination, the data importer agrees to use its best efforts to obtain a waiver of the prohibition, with a view to communicating as much information as possible, as soon as possible. The data importer agrees to document its best efforts in order to be able to demonstrate them on request of the data exporter.

(c) Where permissible under the laws of the country of destination, the data importer agrees to provide the data exporter, at regular intervals for the duration of the contract, with as much relevant information as possible on the requests received

(in particular, number of requests, type of data requested, requesting authority/ies, whether requests have been challenged and the outcome of such challenges, etc.).

(d) The data importer agrees to preserve the information pursuant to paragraphs (a) to (c) for the duration of the contract and make it available to the competent supervisory authority on request.

(e) Paragraphs (a) to (c) are without prejudice to the obligation of the data importer pursuant to Clause 14(e) and Clause 16 to inform the data exporter promptly where it is unable to comply with these Clauses.

15.2 Review of legality and data minimisation

(a) The data importer agrees to review the legality of the request for disclosure, in particular whether it remains within the powers granted to the requesting public authority, and to challenge the request if, after careful assessment, it concludes that there are reasonable grounds to consider that the request is unlawful under the laws of the country of destination, applicable obligations under international law and principles of international comity. The data importer shall, under the same conditions, pursue possibilities of appeal. When challenging a request, the data importer shall seek interim measures with a view to suspending the effects of the request until the competent judicial authority has decided on its merits. It shall not disclose the personal data requested until required to do so under the applicable procedural rules. These requirements are without prejudice to the obligations of the data importer under Clause 14(e).

(b) The data importer agrees to document its legal assessment and any challenge to the request for disclosure and, to the extent permissible under the laws of the country of destination, make the documentation available to the data exporter. It shall also make it available to the competent supervisory authority on request.

(c) The data importer agrees to provide the minimum amount of information permissible when responding to a request for disclosure, based on a reasonable interpretation of the request.

SECTION IV – FINAL PROVISIONS

Clause 16

Non-compliance with the Clauses and termination

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

(b) In the event that the data importer is in breach of these Clauses or unable to comply with these Clauses, the data exporter shall suspend the transfer of personal data to the data

importer until compliance is again ensured or the contract is terminated. This is without prejudice to Clause 14(f).

(c) The data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses, where:

(i) the data exporter has suspended the transfer of personal data to the data importer pursuant to paragraph (b) and compliance with these Clauses is not restored within a reasonable time and in any event within one month of suspension;

(ii) the data importer is in substantial or persistent breach of these Clauses; or

(iii) the data importer fails to comply with a binding decision of a competent court or supervisory authority regarding its obligations under these Clauses.

In these cases, it shall inform the competent supervisory authority of such non-compliance. Where the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise.

(d) Personal data that has been transferred prior to the termination of the contract pursuant to paragraph (c) shall at the choice of the data exporter immediately be returned to the data exporter or deleted in its entirety. The same shall apply to any copies of the data. The data importer shall certify the deletion of the data to the data exporter. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit the return or deletion of the transferred personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process the data to the extent and for as long as required under that local law.

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

Clause 17

Governing law

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

Clause 18

Choice of forum and jurisdiction

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

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

(c) A data subject may also bring legal proceedings against the data exporter and/or data importer before the courts of the Member State in which he/she has his/her habitual residence.

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

---

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

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

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

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

ANNEX I

A. LIST OF PARTIES

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

Name: The entity identified as 'Company' in the MSA.

Address: As provided in the MSA.

Contact person's name, position and contact details: As provided in the MSA.

Activities relevant to the data transferred under these Clauses:

The activities as specified in Exhibit A of the TD Data Processing Agreement.

Signature and date: As per the Attachment to the Master Service Agreement. By signing this Attachment, the Company will be deemed to have signed this Annex I.

Role (controller/processor): Controller

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

Name: The Trade Desk as further specified in the MSA.

Address: As specified in the MSA.

Contact person's name, position and contact details: As specified in the MSA.

Activities relevant to the data transferred under these Clauses:

The activities as specified in Exhibit A of the TD Data Processing Agreement.

Signature and date: As per the Attachment to the Master Service Agreement. By signing this Attachment, TD will be deemed to have signed this Annex I.

Role (controller/processor): Processor

B. DESCRIPTION OF TRANSFER

Categories of data subjects whose personal data is transferred

As described in Exhibit A of the TD Data Processing Agreement.

Categories of personal data transferred

As described in Exhibit A of the TD 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.

Not applicable.

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

The frequency of the transfer is determined by the Data Exporter's use of the Services.

Nature of the processing

As described in Exhibit A of the TD Data Processing Agreement.

Purpose(s) of the data transfer and further processing

To provide the Services.

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

The criteria used to determine the retention period for the data collected are as follows:

- the amount, nature, and sensitivity of the personal data
- the risk of harm from unauthorized use or disclosure
- the purposes for which we process the data and how long we need the particular data to achieve these purposes
- how long the data is likely to remain accurate and up to date

- for how long the data might be relevant to possible future legal claims (for more details, see below)
- any applicable legal, contractual, accounting, reporting or regulatory requirements that specify how long certain records must be kept

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 as described in Exhibit A of the TD 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 to 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

The Trade Desk – Technical and Organisational Measures

Importer will always procure that it can provide adequate protection for data transferred from the European Economic Area (EEA) to the US or other third country through a combination of contractual, technical and administrative measures.

Importer undertakes to adopt supplementary measures to protect all personal data in accordance with the requirements of the GDPR, including but not limited to the implementation of appropriate technical and organizational safeguards, such as encryption or similar technologies, access controls or other compensating controls, to protect the personal data against any interference that goes beyond what is necessary in a democratic society to safeguard national security, defense and public security. In addition to the minimum technical and organizational measures in accordance with Article 32 of the General Data Protection Regulation, see Appendix 1 to Annex II, the importer guarantees to complete the following technical and organizational supplementary measures:

Technical and organisational safeguards/measures implemented by the data importer to ensure an appropriate level of security.

Importer hereby confirms to have implemented a number of privacy-by-design measures minimizing the types of data that is provided onto the Importer's platform and preventing unauthorized access to the data. The following measures apply to all data transfers

a. *Measures of pseudonymisation and encryption of personal data*

Encryption in transit: Importer undertakes to encrypt personal data that is transferred between the EEA and the US or other third country to prevent it from being read while in transit unless these data are truncated before transferred to the US or third countries. Importer further covenants that it already employs additional technical measures to protect EU data subjects' privacy. These measures include but are not limited to implementing robust network security controls including firewalls, Access Control List (ACL) methods and personnel access via VPN, use encrypted connection such as https, ssl and tls protocols, encryption of data before transit when possible, the use of appropriate cipher suites for bulk encryption rendering data non-personal and/or unusable for many purposes.

b. *Measures for ensuring data minimization (IP addresses)*

Importer guarantees to truncate IP addresses before they leave the EEA. IP-addresses from EEA users will be stored truncated, as they are truncated before the transfer to the US. This is inclusive of transfers to any AWS servers in any US region

c. *Measures for threat assessment and risk management*

The Trade Desk business-continuity planning includes practices to identify and manage risks that could affect either the organization's ability to provide reliable services to its clients (as further described below) or the privacy of data subjects. These practices are used to identify significant risks and potential threat vectors for the organization, initiate the identification and/or implementation of appropriate risk-mitigation measures, and assist management in monitoring risk and remediation activities.

The Trade Desk evaluates and manages risks related to its SaaS solutions throughout their life cycles, taking into consideration the consequences for our clients and data subjects of the loss of confidentiality, integrity, or availability of the information we collect, process, and store.

d. *Measures for ensuring accountability*

Importer will monitor updated guidance from data protection authorities and incorporate such guidance as appropriate into a robust privacy and security program that evolves with the changing legal and regulatory landscape.
Any legally binding request for disclosure of personal data by a law enforcement authority or state security body shall be communicated to the Importer unless otherwise legally prohibited (such as a prohibition under criminal law to preserve the confidentiality of a law enforcement investigation). In any case, the request for disclosure should be put on hold and the Supervisory Authority competent for the Importer and the competent Supervisory Authority for the Exporter should be clearly informed about the request, including information about the data requested, the requesting body and the legal basis for disclosure (unless otherwise prohibited). If the suspension and/or notification are prohibited, the Exporter will use its best endeavours to obtain the right to waive this prohibition in order to communicate as much information as it can and as soon as possible and be able to demonstrate that it did so.

e. *Measures for access controls, user identification and authorization*

The Trade Desk SaaS Solutions are multi-tenant environments that use logical access controls, such as authentication and roles, to ensure the necessary separation between data from different clients. The Trade Desk follows guidance from the ISO/IEC 27002:2015, NIST 800-53, Sarbanes-Oxley ITGC, and SSAE18 SOC1 and SOC2 standards. The Trade Desk also employs industry-standard practices and relies on its experience operating highly secure SaaS Solutions for security controls, such as firewall rule sets, change management, and written security policies.

The Trade Desk's Infrastructure team, in tandem with the Engineering team ("SaaS Operations"), is responsible for all aspects of the SaaS Solutions production environment. These groups are set up separately and independently from the Corporate-network IT organization to ensure the necessary separation of duties.

The Trade Desk SaaS Solutions infrastructure is physically separated from The Trade Desk Corporate facilities and managed by an independent SaaS Operations team.

Access to all facilities is controlled by electronic key systems. The Trade Desk's Corporate offices have security-badge access controls as well as CCTV monitoring, and all visitors must be registered and accompanied during visits. Additional electronic access controls restrict access to critical areas to authorized personnel only.

f. *Measures for ensuring Information Security*

The Trade Desk has adopted a decentralized approach to information security. The Trade Desk Information Security Officer, with support and oversight from the Global Operations team, Internal Privacy Counsel, and the Data Protection Officer (DPO), coordinates all security and privacy activities within The Trade Desk. Responsibilities of this position include:

- Driving security initiatives
- Reviewing policy
- Overseeing security planning and program management

The Trade Desk's information-security management system is based on ISO/IEC 27001 and includes multiple information-security policies, updated annually, that explicitly address the confidentiality, integrity, and availability of platform data and information-technology resources. These policies detail employees' responsibilities and managements' role in protecting employees.
Comprehensive technical policies govern various aspects of The Trade Desk SaaS Operations and Corporate-network operations and define security measures appropriate to the sensitivity of the data processed.

Policies are approved by senior management and communicated to all personnel to whom the policies apply. They clearly state the consequences of non-compliance. All employees must review The Trade Desk's Information Security Policy and agree to the Acceptable Use Policy during onboarding.

g. *Measures for ensuring correct handling of data /asset management*

All data collected by The Trade Desk on behalf of its clients is the property of the respective clients and classified as highly confidential under The Trade Desk Information Classification Policy, which provides employees with the necessary guidance for the handling of all information according to its classification. Access to Platform Data is restricted to legitimate business use only.

The Trade Desk SaaS Solutions process pseudonymous data. The Trade Desk Terms of Subscription Service prohibit the use of the SaaS Solutions to collect, process, and store certain types of data, such as sensitive data or data that directly identifies individuals.

Other than as specified in this Annex, The Trade Desk generally performs no additional encryption on data collected and stored within The Trade Desk SaaS production environment, due to the data's pseudonymous nature.

h. *Measures for ensuring accountability*

The Trade Desk Backup and Storage Media Policy prohibits copying Platform Data on removable media devices, including flash drives, hard drives, tapes, or other media, other than for legitimate business purposes. All personnel who handle storage media used in The Trade Desk SaaS solutions must comply with The Trade Desk Backup and Storage Media Policy.

The Trade Desk's decommissioning procedures are designed to prevent access to Platform Data by unauthorized persons and follow NIST guidelines for Media Sanitization (Special Pub 800-88) to destroy data. All printed Confidential Information, including Platform Data, is disposed of in secured containers for shredding.

i. *Measures for ensuring limited data retention*

The Trade Desk deletes all Platform Data, other than backup copies held for disaster recovery purposes, on a scheduled basis following termination of contract.

j. *Measures for ensuring access control and physical security*

The Trade Desk's Information Technology team manages access control policies and procedures for the Corporate network, and The Trade Desk's SaaS Operations team manages access-control policies and procedures for the SaaS production network as well as a list of all staff authorized to access SaaS Operations data centers.

Protection against Malware
The Trade Desk deploys anti-malware software with real-time scanning, automatic updates, and tamper protection on all user workstations. The Trade Desk uses a leading commercial solution for email security, including incoming and outgoing filtering for spam, phishing attacks, and malware.

k. *Measures for ensuring user access management*

Accounts on The Trade Desk SaaS production network, including for network administrators and database administrators, are mapped directly to employees, using unique identifiers based on employee names. Microsoft's Active Directory enforces uniqueness. Generic administrative accounts are not used. Upon notification by HR, as part of the formal termination notification process, all physical and system access is immediately adjusted to the new role or revoked both on The Trade Desk Corporate network and in The Trade Desk SaaS Solutions production network.

All requests for access to The Trade Desk SaaS Operations network must be submitted by the requestor's manager through the access-request system. After review and approval, the request is logged for implementation. Password complexity rules and account lockouts are enforced in all environments to protect against brute-force dictionary attacks or other password threats.

The Trade Desk periodically reviews employee access to internal systems. Reviews ensure that employees' access rights and access patterns are commensurate with their current positions.

l. *Measures for Logging and Monitoring*

The Trade Desk maintains audit information and logs for all information-technology resources, applications, and network accesses, monitors these logs for abnormal-pattern and unauthorized access attempts, and maintains defined processes for security alerting, escalation, and remediation. Logs are centralized in a limited-access system that prevents deletion and changes.

24/7 monitoring of critical network events and log aggregation with industry-standard enterprise application management solutions give The Trade Desk SaaS Operations the ability to identify and address any unauthorized access to assets (including access to client data) within the SaaS production network and to perform trend analysis and risk assessment. An alert system is in place to notify The Trade Desk SaaS Operations team of any issue.

Escalation procedures exist to ensure the timely communication of significant security incidents up through the management chain and, ultimately, to any affected client.

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

The Trade Desk runs regular security scans of the SaaS production environment and engages annually a reputable third-party security firm to conduct a comprehensive application penetration test and network vulnerability scan of The Trade Desk SaaS Solutions.

The primary objective of these scans and tests is to gain independent, third-party validation of The Trade Desk security stance and provide actionable recommendations for the mitigation of any identified risks.

Both white-box and black-box testing are used to assess both the strength of the environment and the defenses against known application vulnerabilities, through a penetration test using guidelines from OWASP.

communication of security incidents up through the management chain and, ultimately, to any affected client.

Information Transfer
The Trade Desk clients access our SaaS Solutions via the public internet. All data transfers from The Trade Desk SaaS Solutions must use secure protocols. All data transfers to The Trade Desk SaaS Solutions default to secure protocols.

Confidentiality and Non-Disclosure Agreements
The Trade Desk requires a non-disclosure agreement or confidentiality clauses in all contracts of third parties that access computing facilities or information assets, as well as prior to sharing or providing access to any confidential information outside of The Trade Desk.

n. *Measures for ensuring security 24*

The Trade Desk has developed a robust Security Incident Response Process (SIRP) to address security- and privacy-related events in an efficient and timely manner. The SIRP framework describes how the team is deployed, documents the criteria for incident severity, defines the investigation and diagnosis workflow, details documentation and reporting requirements, and establishes contact information.
All critical issues that are confirmed are remediated immediately. Issues of lesser severity are evaluated for resolution as part of the standard development process.

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

The Trade Desk maintains Platform Data within the SaaS Solutions production environment on fully redundant or replicated storage systems and uses a multi-tiered backup approach. The Trade Desk SaaS Solutions extend redundancy beyond storage to the entire infrastructure, from load balancers and processing engines to power and telecommunication providers.

The Trade Desk stores all Platform Data in the SaaS production environment on fully redundant storage systems and uses either a multi-tiered backup approach or replication to a separate data center. Only The Trade Desk SaaS Operations employees have access to backup media.

p. *Measures for assessing supplier relationships*

The Trade Desk may use contractors for development or security validation tasks. These organizations and individuals work under the direct supervision of The Trade Desk employees and may have access to client data where contractually permitted by master-service or non-disclosure agreements.

Colocation providers have access to the facility hosting the infrastructure and may provide remote-hand service for hardware maintenance under The Trade Desk supervision, but they do not have direct access to Platform Data.

The Trade Desk exclusively uses world-class, third-party suppliers with stellar backgrounds, such as Amazon Web Services (for cloud infrastructure), Unitas Global, and Cogeco Peer1 (managed hosting and co-location data centers).

The Trade Desk reviews AICPA SSAE16/18 SOC1 and SOC2 reports and/or ISO certification of its infrastructure providers to confirm their adherence to industry-standard security and operational requirements.

All suppliers or contractors that process or have access to Platform Data are under contractual obligations of security and confidentiality at least as stringent as our obligations to clients.

q. *Measures for communications security*

SaaS Network Security Management
Comprehensive and centralized system and application logging and monitoring facilitate alerting, trend analysis, and risk assessment. A network-configuration management tool tracks and catalog changes, which are reviewed. Escalation procedures exist to ensure the timely

The SIRP core team is composed of senior employees with an executive sponsor reporting directly to The Trade Desk CEO. This team is deployed and disbanded for each event and meets periodically in the absence of events for training and process maintenance. The SIRP process identifies key roles to facilitate the effective coordination of The Trade Desk response to a security incident and defines a secure methodology for the confidentiality of all information and communication.

Importer hereby confirms vis-à-vis Exporter that due to the nature and architecture of its platform, it is not feasible to limit processing services to a data centre located in the EEA.