DATA PROCESSING ADDENDUM INSTRUCTIONS

FOR CDNETWORKS CUSTOMERS

Revised: December 1, 2022

Who?

This Data Processing Addendum ("DPA", "addendum") has been prepared for those Customers of CDNetworks that are data controllers and who have determined a need for a data processing agreement addendum to be in place with CDNetworks who processes personal data on their behalf.

What?

This Addendum has been prepared by CDNetworks in compliance with the data processor obligations laid out under the terms of the General Data Protection Regulation ("GDPR") and other relevant government privacy regulations. This document is ready for your signature in accordance with the instructions below and is designed to complement the existing contractual documentation between CDNetworks and its Customers.

How?

1. This DPA consists of two parts: the main body of the DPA and Annexes.
2. To complete this DPA, Customer must complete the information in the signature boxes and sign on Pages 7.
3. Customer should return the physical or electronic copy of the signed DPA to the Customer's dedicated account manager.
4. Upon CDNetworks account manager's receipt of the validly completed and signed DPA, this DPA shall become legally binding (provided that the terms of the DPA have not been supplemented, overwritten, or otherwise modified).

Data Processing Addendum (version 9 – December 2022)

This Data Processing Addendum ("DPA") forms part of the Master Services Agreement ("MSA"), Service Order Forms, CDNetworks "Acceptable User Policy" ("AUP") (https://www.cdnetworks.com/acceptable-use-policy), or other written or electronic agreement, by and between CDNetworks Europe, Co. Ltd. ("CDNetworks") and the undersigned customer of CDNetworks ("Customer"). This DPA, as well as the MSA, SOF, AUP and other written or electronic agreements, shall be collectively referred to as "the Agreement".

All capitalised terms not defined herein shall have the meanings set forth in the Agreement. Each of Customer and CDNetworks may be referred to herein as a "Party" and together as the "Parties."

In connection with the Service, the Parties anticipate that CDNetworks may process outside of the European Union ("EU") or European Economic Area ("EEA") certain Personal Data in respect of which the Customer or any member of the Customer Group may be a data controller or data processor, as applicable, under the applicable EU Data Protection Laws and other relevant government privacy laws.

The Parties have agreed to enter into this DPA in order to ensure that adequate safeguards are put in place with respect to the protection of such Personal Data as required by EU Data Protection Laws and other relevant government privacy laws.

How to Execute this DPA:

1. This DPA consists of two parts: the main body of the DPA and Annexes.
2. To complete this DPA, Customer must complete the information in the signature boxes and sign on Pages 7.
3. Customer should return the physical or electronic copy of the signed DPA to the Customer's dedicated account manager.
4. Upon CDNetworks account manager's receipt of the validly completed and signed DPA, this DPA shall become legally binding (provided that the terms of the DPA have not been supplemented, overwritten, or otherwise modified).

How this DPA Applies

This DPA is an addendum to and forms part of the Agreement. The Customer entity signing this DPA must be the same as the Customer entity party to the Agreement. If the Customer entity signing this DPA is not a party to the Agreement, this DPA is not valid and is not legally binding.

Any partner/reseller should contact its dedicated account manager to discuss whether any amendment to be made in the case its customer (end user) requests a DPA to be signed.

Data Processing Terms

In the course of providing the Service to Customer pursuant to the Agreement, CDNetworks may process personal data on behalf of Customer.

CDNetworks agrees to comply with the following provisions with respect to any Personal Data submitted by or for Customer to CDNetworks or collected and processed by or for Customer using CDNetworks' services. The Parties agree that the obligations under this DPA will be subject to laws and regulations applicable to the processing of Personal Data under the Agreement, including such laws and regulations of the European Union, the European Economic Area and their member states, Switzerland, the United Kingdom and the United States and its states.

1. Definitions

1.1. The following definitions are used in this DPA:

a) "Adequate Country" means a country or territory that is recognised under EU Data Protection Laws as providing adequate protection for Personal Data;

b) "Affiliate" means, with respect to a party, any corporate entity that, directly or indirectly, Controls, is Controlled by, or is under Common Control with such party (but only for so long as such Control exists);

c) "CDNetworks Group" herein means CDNetworks Inc., CDNetworks Europe, Co. LTD., CDNetworks Singapore Pte. Ltd., CDNetworks Co., Ltd., and/or any of its Affiliates;

d) "Customer Group" means Customer and any of its Affiliates established and/or doing business in the EU or EEA; "CCPA" means the California Consumer Privacy Act, Cal. Civ. Code § 1798.100 et seq., and its implementing regulations.

e) "EU Data Protection Laws" means all laws and regulations of the European Union, the European Economic Area, their member states, and the United Kingdom, applicable to the processing of Personal Data under the Agreement, including (where applicable) the General Data Protection Regulation ("GDPR");

f) "GDPR" means the General Data Protection Regulation (Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons regarding the processing of personal data and on the free movement of such data);

g) "Personal Data" means all data which is defined as 'personal data' under EU Data Protection Laws and to which EU Data Protection Laws apply and similarly defined by other relevant government data privacy laws and which is provided by the Customer to CDNetworks, and accessed, stored or otherwise processed by CDNetworks as a data processor as part of its provision of the Service to Customer;

h) "Processing", "data controller", "data subject", "supervisory authority" and "data processor" shall have the meanings ascribed to them in EU Data Protection Laws;

1.2. An entity "Controls" another entity if it: (a) holds a majority of the voting rights in it; (b) is a member or shareholder of it and has the right to remove a majority of its board of directors or equivalent managing body; (c) is a member or shareholder of it and controls alone or pursuant to an agreement with other shareholders or members, a majority of the voting rights in it; or (d) has the right to exercise a dominant influence over it pursuant to its constitutional documents or pursuant to a contract; and two entities are treated as being in "Common Control" if either controls the other (directly or indirectly) or both are controlled (directly or indirectly) by the same entity.

2. Status of the Parties

2.1. The type of Personal Data processed pursuant to this DPA and the subject matter, duration, nature and purpose of the processing, and the categories of data subjects, are as described in Section 3.

2.2. Each Party warrants in relation to Personal Data that it will comply (and will procure that any of its personnel comply and use commercially reasonable efforts to procure that its sub-processors comply), with EU Data Protection Laws and other relevant government data privacy laws. As between the Parties, the Customer shall have sole responsibility for the accuracy, quality, and lawfulness of processing the Personal Data and the means by which the Customer acquired Personal Data.

2.3. In respect of the Parties' rights and obligations under this DPA regarding the Personal Data, the Parties hereby acknowledge and agree that the Customer is the data controller or processor, and CDNetworks is the data processor or sub-processor, as applicable, and accordingly CDNetworks agrees that it shall process all Personal Data in accordance with its obligations pursuant to this DPA.

2.4. If Customer is a data processor, Customer warrants to CDNetworks that Customer's instructions and actions with respect to the Personal Data, including its appointment of CDNetworks as another processor and concluding the standard contractual clauses (Annex I), have been authorised by the relevant controller.

2.5. Where and to the extent that CDNetworks processes data which is defined as 'Personal Data' under EU Data Protection Laws and defined similarly by other relevant government data privacy laws as a data controller CDNetworks will comply with applicable EU and the relevant country data protection laws in respect of that processing.

3. Details of the Personal Data and Data Processing Activities

3.1. Personal Data we collect comprises:

a) in relation to visitors of the Customer's online properties:

i. identification data;

ii. professional life data;

iii. connection data; and/or

iv. localisation data (including IP addresses).

b) Customer, its online visitors and/or other partners may also upload content to Customer's online properties which may include personal data and special categories of data, the extent of which is determined and controlled by the Customer in its sole discretion.

c) Such special categories of data include, but may not be limited to, personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data, biometric data, data concerning health or data concerning an individual's sex life or sexual orientation.

d) in relation to users of the Customer for its account management, servicing, and support:

a. identification data;

b. professional life data;

c. connection data; and/or

d. localisation data (including IP addresses).

3.2. The duration of the processing will be: until the earliest of

a) expiry/termination of the Agreement, or

b) the date upon which processing is no longer necessary for the purposes of either Party performing its obligations under the Agreement (to the extent applicable);

3.3. The processing will comprise: Processing necessary to provide the Service to Customer, pursuant to the Agreement;

3.4. The purpose(s) of the processing is/ are: necessary for the provision of the Service under the Agreement;

3.5. Personal data may concern the following data subjects:

a) Prospective customers, Customers, resellers, referrers, business partners, and vendors of the Customer (who are natural persons);

b) Employees or contact persons of the Customer’s prospective customers, Customers, resellers, referrers, sub-processors, business partners, and vendors (who are natural persons);

c) Employees, agents, advisors, and freelancers of the Customer (who are natural persons); and/or

d) Natural persons authorised by the Customer to use the Service.

4. CDNetworks Obligations

4.1. With respect to all Personal Data, CDNetworks warrants that it shall:

a) only process Personal Data in order to provide the Service, and shall act only in accordance with:

i. this DPA;

ii. the Customer's written instructions as represented by the Agreement and this DPA; and

iii. obligations as required by applicable laws, including, but not limited to EU Data Protection Laws.

b) maintain a record of all categories of processing activities (as such term is defined in the GDPR) carried out on behalf of a controller;

c) upon becoming aware, inform the Customer if, in CDNetworks’ opinion, any instructions provided by the Customer under clause 4.1(a) infringe the GDPR or other relevant government privacy laws;

d) implement appropriate technical and organisational measures to ensure a level of security appropriate to the risks that are presented by the processing of Personal Data, in particular written authorisation

protection against accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to Personal Data. Such measures include, without limitation, the security measures set out in Annex II;

e) take reasonable steps to ensure that only authorised personnel have access to such Personal Data and that any persons whom it authorises to have access to the Personal Data are under obligations of confidentiality;

f) without undue delay after becoming aware, notify the Customer of any breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, Personal Data transmitted, stored or otherwise processed by CDNetworks, its sub-processors, or any other identified or unidentified third Party (a "Personal Data Breach");

g) promptly provide the Customer with reasonable cooperation and assistance in respect of a Personal Data Breach and all reasonable information in CDNetworks' possession concerning such Personal Data Breach insofar as it affects the Customer, including the following to the extent then known:

i. the possible cause and consequences for the Data Subjects of the Personal Data Breach;
ii. the categories of Personal Data involved;
iii. a summary of the possible consequences for the relevant data subjects;
iv. a summary of the unauthorised recipients of the Personal Data; and
v. the measures taken by CDNetworks to mitigate any damage;

h) not make any public announcement about a Personal Data Breach (a "Breach Notice") without the prior written consent of the Customer, unless required by applicable law;

i) promptly notify the Customer if it receives a request from a data subject to access, rectify or erase that individual's Personal Data, or if a data subject objects to the processing of, or makes a data portability request in respect of, such Personal Data (each a "Data Subject Request"). CDNetworks shall not respond to a Data Subject Request without the Customer's prior written consent except to confirm that such request relates to the Customer, to which the Customer hereby agrees. To the extent that the Customer does not have the ability to address a Data Subject Request, then upon Customer's request CDNetworks shall provide reasonable assistance to the Customer to facilitate such Data Subject Request to the extent able and in line with applicable law. Customer shall cover all costs incurred by CDNetworks in connection with its provision of such assistance;

j) other than to the extent required to comply with applicable law, following termination or expiry of the Agreement or completion of the Service, CDNetworks will delete all Personal Data (including copies thereof) processed pursuant to this DPA;

k) taking into account the nature of processing and the information available to CDNetworks, provide such assistance to the Customer as the Customer reasonably requests in relation to CDNetworks' obligations under EU Data Protection Laws and other relevant government privacy laws with respect to:

i. data protection impact assessments (as such term is defined in the GDPR);
ii. the cooperation or prior consultation with the Supervisory Authority in the performance of its tasks relating to Section 4 of this DPA, to the extent required under the GDPR and other relevant government privacy laws;
iii. notifications to the supervisory authority under EU Data Protection Laws and other relevant government privacy laws and/or communications to data subjects by the Customer in response to any Security Breach; and
iv. the Customer's compliance with its obligations under the GDPR and other relevant government privacy laws with respect to the security of processing;

provided that the Customer shall cover all costs incurred by CDNetworks in connection with its provision of such assistance.

5. Sub-processing

5.1. The Customer grants a general authorisation: (a) to CDNetworks to appoint other members of the CDNetworks Group as sub-processors, and (b) to CDNetworks and other members of the CDNetworks Group to appoint third Party suppliers, and outsourced marketing, business, engineering and customer support providers as sub-processors to support the performance of the Service.

5.2. CDNetworks will maintain a list of sub-processors on the CDNetworks.com website and will add the names of new and replacement sub-processors to the list prior to them starting sub-processing of Personal Data. If the Customer has a reasonable objection to any new or replacement sub-processor, it shall notify

CDNetworks of such objections in writing within ten (10) days of the notification and the Parties will seek to resolve the matter in good faith. If CDNetworks is reasonably able to provide the Service to the Customer in accordance with the Agreement without using the sub-processor and decides in its discretion to do so, then the Customer will have no further rights under this clause 5.2 in respect of the proposed use of the sub-processor. If CDNetworks requires use of the sub-processor in its discretion and is unable to satisfy the Customer as to the suitability of the sub-processor or the documentation and protections in place between CDNetworks and the sub-processor within ninety (90) days from the Customer's notification of objections, the Customer may within thirty (30) days following the end of the ninety (90) day period referred to above, terminate the applicable Service Order Form with at least thirty (30) days written notice, solely with respect to the service(s) to which the proposed new sub-processor's processing of Personal Data relates. If the Customer does not provide a timely objection to any new or replacement sub-processor in accordance with this clause 5.2, it shall be regarded as Customer has given its consent to the involvement of the sub-processor and waived its right to object. CDNetworks may use a new or replacement sub-processor whilst the objection procedure in this clause 5.2 is in process.

5.3. CDNetworks will ensure that any sub-processor it engages to provide an aspect of the Service on its behalf in connection with this DPA does so only on the basis of a written contract which imposes on such sub processor terms substantially no less protective of Personal Data than those imposed on CDNetworks in this DPA (the "**Relevant Terms**"). CDNetworks shall procure the performance by such sub-processor of the Relevant Terms and shall be liable to the Customer for any breach by such person of any of the Relevant Terms.

6. Audit and Records

6.1. CDNetworks shall, in accordance with EU Data Protection Laws and other relevant government privacy laws, make available to the Customer such information in CDNetworks' possession or control as the Customer may reasonably request with a view to demonstrating CDNetworks' compliance with the obligations of data processors under EU Data Protection Law and other relevant government privacy laws in relation to its processing of Personal Data.

6.2. The Customer may exercise its right of audit under EU Data Protection Laws and other relevant government privacy laws in relation to Personal Data, through CDNetworks providing:

a) Customer and its respective auditors or authorized agents access to conduct audits or inspections during the term of the Agreement, which shall include providing reasonable access to the premises, resources and personnel used by CDNetworks in connection with its processing of Customer data, and provide all reasonable assistance in order to assist Customer in exercising its audit rights under this Clause. The purpose of this audit pursuant to this Clause is to verify processing of personal data is conducted in accordance with CDNetworks obligations under this DPA. Such audit shall consist solely of: (i) the provision by CDNetworks of written information (including, without limitation, questionnaires and information about security policies) that may include information relating to sub-processors; and (ii) interviews with CDNetworks IT personnel. Such audit may be carried out by Customer or an inspection body composed of independent members and in possession of the required professional qualifications bound by a duty of confidentiality. For the avoidance of doubt, no access to any part of CDNetworks IT systems, data hosting sites or centers, or infrastructure will be permitted. And;

b) additional information in CDNetworks' possession or control to the relevant supervisory authority when it requests or requires additional information in relation to the processing of Personal Data carried out by CDNetworks under this DPA.

7. Data Transfers

7.1. To the extent any processing of Personal Data by CDNetworks takes place in any country outside the EEA (except if in an Adequate Country), the Parties agree that the standard contractual clauses approved by the EU authorities under EU Data Protection Laws and set out in Annex I will apply in respect of that processing, and CDNetworks will comply with the obligations of the 'data importer' in the standard contractual clauses and the Customer will comply with the obligations of the 'data exporter'.

7.2. The Customer acknowledges and accepts that the provision of the Service under the Agreement may require the processing of Personal Data by sub-processors in countries outside the EEA.

7.3. If, in the performance of this DPA, CDNetworks transfers any Personal Data to a sub-processor located outside of the EEA (without prejudice to clause 5), CDNetworks shall in advance of any such transfer ensure that a legal mechanism to achieve adequacy in respect of that processing is in place, such as: (a) the

requirement for CDNetworks to execute or procure that the sub-processor execute to the benefit of the Customer standard contractual clauses approved by the EU authorities under EU Data Protection Laws and set out in Annex I; (b) the requirement for the sub-processor to be certified under the EU-U.S. Privacy Shield Framework; or (c) the existence of any other specifically approved safeguard for data transfers (as recognised under EU Data Protection Laws) and/or a European Commission finding of adequacy.

7.4. The following terms shall apply to the standard contractual clauses set out in Annex I: (a) The Customer may exercise its right of audit under clause 5.1(f) of the standard contractual clauses as set out in, and subject to the requirements of, clause 6.2 of this DPA; and (b) CDNetworks may appoint sub-processors as set out, and subject to the requirements of, clauses 4 and 7.3 of this DPA.

8. General

8.1. This DPA is without prejudice to the rights and obligations of the Parties under the Agreement which shall continue to have full force and effect. In the event of any conflict between the terms of this DPA and the terms of the Agreement, the terms of this DPA shall prevail so far as the subject matter concerns the processing of Personal Data.

8.2. CDNetworks' liability under or in connection with this DPA (including under the standard contractual clauses set out in Annex I) is subject to the limitations on liability contained in the Agreement.

8.3. This DPA does not confer any third-Party beneficiary rights, it is intended for the benefit of the Parties hereto and their respective permitted successors and assigns only, and is not for the benefit of, nor may any provision hereof be enforced by, any other person.

8.4. This DPA and any action related thereto shall be governed by and construed in accordance with the laws of the State of California, without giving effect to any conflicts of laws principles.

8.5. Any dispute arising out of this DPA shall be brought to the Superior Court of California in Santa Clara County, or the United States District Court for the Northern District of California in San Jose, and the Parties hereby submit and consent to the exclusive jurisdiction and venue thereof.

8.6. This DPA is the final, complete and exclusive agreement of the Parties with respect to the subject matter hereof and supersedes and merges all prior discussions and agreements between the Parties with respect to such subject matter. Other than in respect of statements made fraudulently, no other representations or terms shall apply or form part of this DPA. No modification of, amendment to, or waiver of any rights under the DPA will be effective unless in writing and signed by an authorised signatory of each Party. This DPA may be executed in counterparts, each of which shall be deemed to be an original, but all of which, taken together, shall constitute one and the same agreement. Each person signing below represents and warrants that he or she is duly authorised and has legal capacity to execute and deliver this DPA. Each Party represents and warrants to the other that the execution and delivery of this DPA, and the performance of such Party's obligations hereunder, have been duly authorised and that this DPA is a valid and legally binding agreement on each such Party, enforceable in accordance with its terms.

IN WITNESS WHEREOF, the Parties have each caused this DPA to be signed and delivered by its duly authorised representative.

Customer		**CDNetworks Europe, Co. Ltd.**	
By		**By**	
Name		**Name**	Bowie Chen
Title		**Title**	VP of Sales, Americas and EMEA
Address		**Address**	85 Gresham St, London EC2V 7NQ, UK
Date		**Date**	

ANNEX

STANDARD CONTRACTUAL CLAUSES

SECTION I

Clause 1

Purpose and scope

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

(b) The Parties:

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

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

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

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

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

Clause 2

Effect and invariability of the Clauses

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

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

---

[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 […].

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); Module Four: Clause 8.1 (b) and Clause 8.3(b);

(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); Module Four: Clause 18.

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

Clause 4

Interpretation

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

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

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

Clause 5

Hierarchy

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

Clause 6

Description of the transfer(s)

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

Clause 7 - Optional

Docking clause

(a) An entity that is not a Party to these Clauses may, with the agreement of the Parties, accede to these Clauses at any time, either as a data exporter or as a data importer, by completing the Appendix and signing Annex I.A.

(b) Once it has completed the Appendix and signed Annex I.A, the acceding entity shall become a Party to these Clauses and have the rights and obligations of a data exporter or data importer in accordance with its designation in Annex I.A.

(c) The acceding entity shall have no rights or obligations arising under these Clauses from the period prior to becoming a Party.

SECTION II – OBLIGATIONS OF THE PARTIES

Clause 8

Data protection safeguards

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

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 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.

[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.

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.

(f)

Clause 9

Use of sub-processors

MODULE TWO: Transfer controller to processor

OPTION 2: 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 one month 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.

(g) 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.

(h) 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.

(i) 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.

(j) 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 -

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

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 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.

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.

[OPTION: The data importer agrees that data subjects may also lodge a complaint with an independent dispute resolution body[4] at no cost to the data subject. It shall inform the data subjects, in the manner set out in paragraph (a), of such redress mechanism and that they are not required to use it, or follow a particular sequence in seeking redress.]

MODULE TWO: Transfer controller 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.

[4] The data importer may offer independent dispute resolution through an arbitration body only if it is established in a country that has ratified the New York Convention on Enforcement of Arbitration Awards.

(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 TWO: Transfer controller 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 TWO: Transfer controller to processor

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.

(h) 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 TWO: Transfer controller 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 safeguards[5];

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

(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.

---

[5] 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.

(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

MODULE TWO: Transfer controller 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.

(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) 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 TWO: Transfer controller to processor

(for Modules Two and Three): 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

MODULE TWO: Transfer controller 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

EXPLANATORY NOTE:

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

ANNEX I

A. LIST OF PARTIES

MODULE TWO: Transfer controller to processor

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

1. Name: …

Address: …

Contact person's name, position and contact details: …

Activities relevant to the data transferred under these Clauses: …

Signature and date: …

Role (controller/processor): …

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

1. Name: CDNetworks Europe, Co. Ltd.

Address: 85 Gresham St, London EC2V 7NQ, UK

Contact person's name, position and contact details: …

Activities relevant to the data transferred under these Clauses: processes Personal Data upon the instruction of the data exporter in accordance with the terms of the agreement between the data exporter and CDNetworks

Signature and date: …

Role (controller/processor): processor

B. DESCRIPTION OF TRANSFER

MODULE TWO: Transfer controller to processor

Categories of data subjects whose personal data is transferred

Data subjects of the data exporter who have signed the MSA with CDNetworks and use CDNetworks Services.

Categories of personal data transferred

i. identification data;

ii. professional life data;

iii. connection data; *and/or*

iv. localisation data (including IP addresses).

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).

On a continuous basis.

Nature of the processing

The data is transferred through the API channels to Importer to enable the provision of the relevant Services

Purpose(s) of the data transfer and further processing

For the provision of Services to customer.

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

In accordance with the privacy policies and data retention practices of the data importer, subject to the applicable data protection laws.

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

Please refer to our reply in Annex III.

C. COMPETENT SUPERVISORY AUTHORITY

MODULE TWO: Transfer controller to processor

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

The competent supervisory authority shall be the supervisory authority of Ireland

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

MODULE TWO: Transfer controller to processor

EXPLANATORY NOTE:

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

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

A. Data importer/sub-processor has implemented and shall maintain a security programme in accordance with industry standards.

B. More specifically, data importer/sub-processor's security programme shall include:

Access Control of Processing Areas

Data importer/sub-processor implements suitable measures in order to prevent unauthorised persons from gaining access to the data processing equipment (namely telephones, database and application servers and related hardware) where the personal data are processed or used, including:

- establishing security areas;
- protection and restriction of access paths;
- establishing access authorisations for employees and third Parties, including the respective documentation;
- all access to the data centre where personal data are hosted is logged, monitored, and tracked; and
- the data centre where personal data are hosted is secured by a security alarm system, and other appropriate security measures.

Access Control to Data Processing Systems

- Data importer/sub-processor implements suitable measures to prevent their data processing systems from being used by unauthorised persons, including:
- use of adequate encryption technologies;
- identification of the terminal and/or the terminal user to the data importer/sub-processor and processing systems;
- automatic temporary lock-out of user terminal if left idle, identification and password required to reopen;
- automatic temporary lock-out of the user ID when several erroneous passwords are entered, log file of events, monitoring of break-in-attempts (alerts); and
- all access to data content is logged, monitored, and tracked.

Access Control to Use Specific Areas of Data Processing Systems

Data importer/sub-processor commits that the persons entitled to use their data processing system are only able to access the data within the scope and to the extent covered by their respective access permission (authorisation) and that personal data cannot be read, copied or modified or removed without authorisation. This shall be accomplished by various measures including:

- employee policies and training in respect of each employee's access rights to the personal data;
- allocation of individual terminals and /or terminal user, and identification characteristics exclusive to specific functions;

- monitoring capability in respect of individuals who delete, add or modify the personal data;
- release of data only to authorised persons, including allocation of differentiated access rights and roles;
- use of adequate encryption technologies; and
- control of files, controlled and documented destruction of data.

Availability Control

Data importer/sub-processor implements suitable measures to ensure that personal data are protected from accidental destruction or loss, including:

- infrastructure redundancy; and
- backup is stored at an alternative site and available for restore in case of failure of the primary system.

Transmission Control

Data importer/sub-processor implements suitable measures to prevent the personal data from being read, copied, altered or deleted by unauthorised Parties during the transmission thereof or during the transport of the data media. This is accomplished by various measures including:

- use of adequate firewall, VPN and encryption technologies to protect the gateways and pipelines through which the data travels;
- certain highly confidential employee data (e.g., personally identifiable information such as National ID numbers, credit or debit card numbers) is also encrypted within the system; and
- providing user alert upon incomplete transfer of data (end to end check); and
- as far as possible, all data transmissions are logged, monitored and tracked.

Input Control

Data importer/sub-processor implements suitable input control measures, including:

- an authorisation policy for the input, reading, alteration and deletion of data;
- authentication of the authorised personnel;
- protective measures for the data input into memory, as well as for the reading, alteration and deletion of stored data;
- utilisation of unique authentication credentials or codes (passwords);
- providing that entries to data processing facilities (the rooms housing the computer hardware and related equipment) are kept locked;
- automatic log-off of user ID's that have not been used for a substantial period of time; and
- proof established within data importer/sub-processor's organisation of the input authorisation; and
- electronic recording of entries.

Separation of Processing for Different Purposes

Data importer/sub-processor implements suitable measures to ensure that data collected for different purposes can be processed separately, including:

- access to data is separated through application security for the appropriate users;
- modules within the data importer/sub-processor's data base separate which data is used for which purpose, i.e. by functionality and function;
- at the database level, data is stored in different normalised tables, separated per module, per Controller Customer or function they support; and
- interfaces, batch processes and reports are designed for only specific purposes and functions, so data collected for specific purposes is processed separately.

Documentation

Data importer/sub-processor will keep documentation of technical and organisational measures in case of audits and for the conservation of evidence. Data importer/sub-processor shall take reasonable steps to ensure that persons employed by it, and other persons at the place of work concerned, are aware of and comply with the technical and organisational measures set forth in this Appendix 2.

Monitoring

Data importer/sub-processor shall implement suitable measures to monitor access restrictions to data importer/sub-processor's system administrators and to ensure that they act in accordance with instructions received. This is accomplished by various measures including:

- individual appointment of system administrators;
- adoption of suitable measures to register system administrators' access logs to the infrastructure and keep them secure, accurate and unmodified for at least six months;
- yearly audits of system administrators' activity to assess compliance with assigned tasks, the instructions received by the data importer/sub-processor and applicable laws;
- keeping an updated list with system administrators' identification details (e.g. name, surname, function or organizational area) and tasks assigned and providing it promptly to data exporter upon request.

For transfers to (sub-) processors, also describe the specific technical and organisational measures to be taken by the (sub-) processor to be able to provide assistance to the controller and, for transfers from a processor to a sub-processor, to the data exporter

ANNEX III – LIST OF SUB-PROCESSORS

MODULE TWO: Transfer controller to processor

EXPLANATORY NOTE:

This Annex must be completed for Modules Two and Three, in case of the specific authorisation of sub-processors (Clause 9(a), Option 1).

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

1. Name: Salesforce, Inc.

Address: Salesforce Tower, 415 Mission Street, 3rd Floor, San Francisco, California, 94105, U.S.A.

Contact person's name, position and contact details: …

Description of processing (including a clear delimitation of responsibilities in case several sub-processors are authorised): Salesforce is engaged as sales and account management platform, information maintained on Salesforce: customer contact, occupation, and contract information. Purpose: for sales and account management and archiving.