CDNetworks Data Processing Addendum

This Data Processing Addendum ("**DPA**") is incorporated into and made a part of the Master Services Agreement, Service Order Form, and other written or electronic agreement (together, the "**Agreement**"), by and between CDNETWORKS EUROPE, CO. LTD. ("**CDNetworks**") and the undersigned entity that has subscribed Services from CDNetworks ("**Customer**").

In the course of providing Services to Customer pursuant to the Agreement, CDNetworks may process Personal Data as a Processor (or sub-Processor, as applicable) on behalf of Customer. CDNetworks and Customer are individually referred to as a "Party" and collectively as the "Parties".

This DPA will take effect, and will replace and supersede any previously applicable terms relating to their subject matter (including any data processing agreement or addendum relating to the Services), from the date on which Customer signed or the Parties otherwise agreed to this DPA.

1. Definitions

Capitalized terms used in this DPA shall have the meanings given to them below:

a) "**Applicable Data Protection Law**" means all laws and regulations (including decisions and guidelines issued by competent supervisory authorities) relating to data protection, the processing of personal data, and privacy protection applicable to CDNetworks and Customer in respect of the processing of Customer Personal Data to provide the Services, including such laws, by way of example and without limitation, the General Data Protection Regulation, the Data Protection Act, and the California Consumer Privacy Act;

b) "**Controller**" means the entity determines the purposes and means of the processing of Personal Data.

c) "**Customer Personal Data**" means all Personal Data processes by CDNetworks as a Processor on behalf of Customer, as specified in Appendix 1;

d) "**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);

e) "**Personal Data**" means personal data, personal information, personally identifiable information or other equivalent term (each as defined in Applicable Data Protection Law);

f) "**Personal Data Breach**" means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, Customer Personal Data transmitted, stored or otherwise processed.

g) "**Processor**" means the entity processes Personal Data on behalf of the Controller.

h) "**Standard Contractual Clauses**" means standardised and pre-approved model data protection clauses which can be used as a ground for data transfers from European Economic Area to third countries.

i) "**Services**" means all services provided by CDNetworks as set forth in the Service Order Form(s), including, but not limited to: Web & Network Performance, Media Delivery, Cloud Security, Zero Trust Security, Edge Computing, Storage, Cloud DNS+, Colocation Services, and other professional services.

j) "**Sub-Processor**" means the additional Processor, appointed by CDNetworks to carry out the processing activities, even in part, and mandated as Processor when the conditions referred to in Section 5 of this DPA are met.

2. Status of the Parties

2.1 Scope and Roles. This DPA applies when Customer Personal Data is processed by CDNetworks on Customer's behalf. In this context, Customer will act as a Controller (or a Processor processing Personal Data on behalf of a third-party Controller, as applicable), CDNetworks will act as a Processor (or sub-processor, as applicable).

2.2 Details of Personal Data Processing. The subject matter and duration of the processing, the nature and purpose of the processing, the type of personal data and categories of data subjects, are as described in Appendix 1 Description of Data Processing.

2.3 Compliance with Laws. Each Party warrants that it will comply with all laws, rules and regulations applicable to it and binding on it in the performance of this DPA, including Applicable Data Protection Law. As between the Parties, the Customer shall have sole responsibility for the accuracy, quality, and lawfulness of Personal Data and the means by which the Customer acquired Personal Data.

2.4 Controller Authorisation. If Customer is a data processor, Customer warrants to CDNetworks that Customer's instructions and actions with respect to the data processing activities, including its appointment of CDNetworks as a processor and concluding this DPA as well as the Standard Contractual Clauses, have been authorised by the relevant controller.

3. Data Processor Terms

3.1 Documented Instructions.

3.1.1 The Parties agree that this DPA and the Agreement, as well as the instructions provided by Customer via email and/or customer console for administration of the Services (collectively, "**Documented Instructions**"), constitute Customer's Documented Instructions regarding CDNetworks' processing of Customer Personal Data.

CDNetworks shall process Customer Personal Data only in accordance with Documented Instructions from Customer, unless otherwise provided by applicable laws or valid binding orders to which CDNetworks is subject.

3.1.2 Taking into account the nature of the processing, Customer agrees that it is unlikely CDNetworks can form an opinion on whether Documented Instructions infringe Applicable Data Protection Law. If CDNetworks forms such an opinion, it will immediately inform Customer upon becoming aware, in which case, Customer is entitled to withdraw or modify its Documented Instructions.

3.2 Confidentiality.

3.2.1 CDNetworks warrants that it will not access, use or disclose to any third party, any Customer Personal Data, except, in each case, as necessary to maintain or provide the Services, or as necessary to comply with the applicable laws or a valid binding order of a governmental body. If a governmental body sends CDNetworks a demand for Customer Personal Data, CDNetworks will attempt to redirect the governmental body to request that data directly from Customer. As part of this effort, CDNetworks may provide Customer's basic contact information to the governmental body. If compelled to disclose Customer Personal Data to the governmental body, CDNetworks will give Customer reasonable notice of such demand unless CDNetworks is legally prohibited from doing so.

3.2.2 CDNetworks shall take reasonable steps to ensure that all persons authorized to process Customer Personal Data have committed themselves to appropriate confidentiality obligations in relation to Customer Personal Data or are under an appropriate statutory obligation of confidentiality.

3.3 Processor Assistance with Personal Data Breach.

3.3.1 CDNetworks shall (i) notify the Customer of a Personal Data Breach without undue delay after becoming aware; *and* (ii) take appropriate measures to address the Personal Data Breach, including measures to mitigate its possible adverse effects resulting from such incident.

3.3.2 In order to enable Customer to report a Personal Data Breach to supervisory authorities or data subjects (as applicable), CDNetworks shall provide the Customer with appropriate cooperation and assistance in respect of a Personal Data Breach, including all reasonable information in CDNetworks' possession concerning such Personal Data Breach insofar as it affects Customer Personal Data.

3.4 Processor Assistance with Data Subject Requests.

3.4.1 Taking into account the nature of the processing, CDNetworks will assist Customer in fulfilling Customer's obligation to respond to data subject's requests under Applicable Data Protection Law. If CDNetworks receives a request from a data subject to exercise any rights, such as access, rectification or erasure, CDNetworks will promptly forward such request to the Customer once CDNetworks has identified that the request is associated with the Customer.

3.4.2 In the event that the Customer is unable to address a data subject request without CDNetworks' assistance, then upon Customer's request, CDNetworks shall provide Customer with reasonable assistance in responding to the data subject request to the extent CDNetworks is able and in line with Applicable Data Protection Law. Customer shall cover all costs incurred by CDNetworks in connection with such assistance (if any).

3.5 Processor Assistance with Data Protection Impact Assessment and Prior Consultation. Taking into account the nature of the processing and the information available to CDNetworks, CDNetworks will assist Customer in complying with Customer's obligations in respect of data protection impact assessment and prior consultation under Applicable Data Protection Law. Customer shall cover all costs incurred by CDNetworks in connection with such assistance (if any).

3.6 Return or Deletion of Customer Personal Data. CDNetworks shall, at the choice of Customer and where appropriate, delete or return all Customer Personal Data after the end of Services provision, and securely delete any remaining copies, unless otherwise provided by Applicable Data Protection Law.

4. Security

CDNetworks shall implement necessary technical and organisational measures at a minimum to the standard set out in Appendix 2 Security Measures to ensure a level of security appropriate to the risk presented by processing of Customer Personal Data, including as appropriate:

i the pseudonymisation and encryption of Customer Personal Data;

ii the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and Services;

iii the ability to restore the availability and access to Customer Personal Data in a timely manner in the event of a physical or technical incident; *and*

iv a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.

Customer acknowledges that the Security Measures are subject to technical progress and that CDNetworks may update or modify the Security Measures from time to time provided that the level of protection of Customer Personal Data is not undermined or degraded.

5. Sub-Processing

5.1 Authorized Sub-Processor. Customer grants a general written authorisation to CDNetworks to engage Sub-Processors for carrying out specific processing activities on behalf of Customer. Customer hereby approves the authorized Sub-Processors that CDNetworks uses to provide the Services, listed at https://www.cdnetworks.com/sub-processors/. Further, to the extent that any Applicable Data Protection Law would deem a CDNetworks affiliate to be a Sub-Processor for purposes of this DPA, Customer hereby authorizes CDNetworks' use of such affiliates as authorized Sub-Processors.

5.2 Changes of Sub-Processor. CDNetworks shall maintain the Sub-Processors list available on CDNetworks official website and provide Customer with advanced notice of any intended changes concerning the addition or replacement of Sub-Processor. If the Customer has a reasonable objection to the engagement of any Sub-Processor, Customer shall inform CDNetworks of such objections within ten (10) days after receiving the notice and the Parties shall seek to resolve the matter in good faith. If the Parties are unable to agree upon a decision, Customer can: (i) terminate the Agreement pursuant to its terms; *or* (ii) cease using the Services for which CDNetworks has engaged the Sub-Processor.

5.3 Sub-Processing Activity. Where CDNetworks engages a Sub-Processor as described in Section 5:

5.3.1 CDNetworks will restrict the Sub-Processor's access to Customer Personal Data only to what is necessary to provide or maintain the Services, and prohibit the Sub-Processor from accessing Customer Personal Data for any other purpose;

5.3.2 CDNetworks will ensure the same data protection obligations as set out in this DPA are imposed on the Sub-Processor by way of a contract between CDNetworks and that Sub-Processor. Where the Sub-Processor fails to fulfil its data protection obligations, CDNetworks will remain responsible to the Customer for the performance its obligations.

6. Data Transfers

In connection with the Services, the Parties anticipate and accept that the provision of Services may require the transfer of Customer Personal Data to countries or regions outside the European Economic Area ("**EEA**"). To the extent any processing of Customer Personal Data by CDNetworks (and its Sub-Processors) takes place in any country outside the EEA (except if in an

adequate country under the GDPR), the Parties agree that the Standard Contractual Clauses attached and set out in Annex will apply in respect of such transfer.

7. Audit

7.1 Periodic Audit. CDNetworks shall conduct periodic audits of its processing activities, typically on an annual basis, and in accordance with Applicable Data Protection Law, shall make available to the Customer all necessary information in CDNetworks' possession or control, in relation to the processing of Customer Personal Data, to demonstrate CDNetworks' compliance with its obligations as a Processor.

7.2 Customer Audit. CDNetworks shall allow for and contribute to audits conducted by Customer or an independent third-party auditor mandated by the Customer in accordance with Applicable Data Protection Law, provided that conditions of confidentiality have been mutually agreed prior to initiation of such audit.

7.2.1 CDNetworks may fulfil Customer's right to audit by providing an audit report or similar compliance documentation not older than thirteen (13) months, prepared by an independent external body, demonstrating that the technical and organisational measures adopted by CDNetworks are appropriate and in accordance with an accepted industry audit standard.

7.2.2 In the event that Customer reasonably believes the information provided pursuant to the Article 7.2.1 warrants further examination to confirm CDNetworks' compliance with its obligations, upon Customer's request not less than thirty (30) days in advance, CDNetworks shall enable Customer to conduct one (1) onsite audit per annual period during the term set forth in the Agreement.

7.2.3 CDNetworks may charge a fee, based on CDNetworks' reasonable costs, for any audit under Article 7.2.2. CDNetworks will provide Customer with further details of any applicable fees and the basis of its calculation, in advance of any such audit. Customer shall be responsible for any fees charged by any auditor mandated by Customer to perform any such audit.

8. General

8.1 Conflict. 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 Liabilities. CDNetworks' liability under or in connection with this DPA (including under the Standard Contractual Clauses set out in Annex) is subject to the exclusions and limitations on liability contained in the Agreement. In no event does CDNetworks exclude or limit its liability towards data subject or competent supervisory authorities.

8.3 Term. This DPA is effective from the date on which it is entered into by the Parties and will continue in force until the expiration or termination of the Agreement.

8.4 Governing Law and Jurisdiction. This DPA and any action related thereto shall be governed by and construed in accordance with the laws of England and Wales, without giving effect to any conflicts of laws principles. All disputes arising under this DPA shall be brought in the courts of England and Wales, and the Parties hereby submit and consent to the exclusive jurisdiction and venue thereof.

8.5 Counterparts. This DPA may be executed in counterparts, each of which shall be deemed to be an original, and all of which 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.

Appendix 1: Description of Data Processing

This Appendix 1 forms part of the DPA and describes the processing activities that CDNetworks will perform on behalf of Customer.

Categories of data subject

The data subjects, whose personal data is processed under this DPA, are End Users. To be specific, End Users refer to natural persons who (i) login, access, or use CDNetworks services and/or Customer's systems embedded with CDNetworks services; *or* (ii) access the content uploaded by Customer to CDNetworks services.

Type of personal data being processed

Depending on the services that Customer subscribed from CDNetworks, the following categories of personal data may be processed, collective referred to as "Customer Personal Data".

(1) Customer Content Personal Data

When CDNetworks provides Content Delivery Networks (CDN) Service for Customer, personal data (if any) contained in Customer Content is processed ("Customer Content Personal Data").

"Customer Content" means all content (including, but not limited to, audio, video, live streaming graphs, texts, scripts), applications or information of Customer that are hosted, cached, transmitted, or displayed through CDNetworks services.

CDNetworks has no control over what content Customer chooses to upload to the services (irrespective of whether it contains personal data/sensitive data or not), unless Customer Content violates applicable laws.

Upon Customer's and/or End User's choice, the Customer Content Personal Data may include data such as:

a) End User's name, image and contact information.

b) Login credentials.

c) Information tailored for End User.

d) Other personal data embedded in Customer Content.

(2) Security Solution Personal Data

When CDNetworks provides Security Solutions for Customer, personal data provided by Customer or collected through End Users' activities is processed ("Security Solution Personal Data").

The Security Solution Personal Data may include:

a) Credentials information: username and password (and similar security information) used for authentication.

b) IP address of End User.

c) Device Information: device type, browser type, operating system, online identifiers, and other similar information.

d) Behaviour Information: access history, URL of sites visited.

(3) Log Support Personal Data

When Customer subscribes CDNetworks services, CDNetworks provides Customer with dedicated support. During the service provision period, personal data embedded in logs or traffic information is processed ("Log Support Personal Data").

The Log Support Personal Data may include:

a) IP address of End User.

b) Geographic location based on IP address and CDNetworks servers.

c) URLs visited with time stamps.

d) Device Information: device type, browser type, operating system, online identifiers, and other similar information.

Purpose and nature of the processing

The purpose of the processing is to provide and secure the services that Customer subscribed from CDNetworks.

The processing activities are as follows:

(1) Customer Content Personal Data

Customer Content Personal Data is uploaded by Customer. Depending on the choice of Customer and the location of End User, Customer Content Personal Data is cached (without being stored) on the optimal CDN edge PoPs (Points of Presence) of CDNetworks and transmitted via CDNetworks network, to enable a nearby content delivery.

(2) Security Solution Personal Data

Security Solution Personal Data is collected, transferred, stored and analysed to shield Customer's online business from cyber threats.

(3) Log Support Personal Data

Log Support Personal Data is collected, transferred, stored and analysed to monitor service provision and to launch incident management.

Duration of the processing

As between CDNetworks and Customer, the duration of data processing under this DPA is the service period as stipulated in the Agreement.

Appendix 2: Security Measures

CDNetworks has implemented and shall maintain the following technical and organisational measures, which in conjunction with the security commitments in this DPA, to safeguard personal data processed by CDNetworks.

Measures of pseudonymisation and encryption of personal data

CDNetworks implements state-of-the-art encryption standards and pseudonymisation techniques to minimize the exposure of personal data by:

- Transport Layer Security (TLS) encryption protocols, which provide secure end-to-end encryption as data moves between Customers, CDNetworks infrastructure, and the End Users' environment;
- trustworthy Public-Key Infrastructure and Certification Authority, ensuring the authenticity and security of communication with CDNetworks services;
- strong encryption algorithms for data both in transit and at rest;
- formalized key management policies covering the lifecycle of key, including generation, storage, recovery, use, rotation and destruction; *and*
- replacing personal data with pseudonyms or codes, that additional information is kept separately and can only be accessed by strictly authorized personnel for necessary purpose.

Additionally, CDNetworks performs continuous monitoring and management to the encryption systems, ensuring ongoing protection against evolving cybersecurity threats.

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

CDNetworks employs a multi-layered security and resilience strategy designed to ensure the continuous protection and performance of CDNetworks systems and services.

- Secure code development and testing: conduct thorough vulnerability assessments during the development and testing phases, prior to official deployment, as well as during operation, including automated and manual testing methodologies to identify potential weaknesses in the code.
- High-availability systems: CDNetworks leverages high-availability systems distributed across geographically diverse regions to enhance service resilience. These systems are designed to ensure minimal downtime, providing failover capabilities and load balancing to maintain continuous service delivery in the event of localized failures.

- Data backup and recovery: execute backup plans with regular intervals, ensuring data redundancy and enabling quick recovery in case of failure. The backup system undergoes frequent testing, and includes secure storage as well as managed destruction of backup media when no longer required.
- Strict authentication and authorization controls: enforce role-based access controls (RBAC) and support multi-factor authentication (MFA), only authorized personnel can access critical systems, minimizing the risk of unauthorized access.
- Incident management plan: a robust incident management plan is in place, allowing for rapid detection, containment, and mitigation of incidents. This includes real-time monitoring, logging, and alerting mechanisms, as well as predefined workflows for handling incidents to minimize disruption and protect data integrity.
- Network, Application, Host security and monitoring: CDNetworks infrastructure is fortified with cutting-edge network, application, host security measures, including advanced anti-DDOS firewalls, intrusion detection/prevention system (IDS/IPS), Web Application and API Protection (WAAP), Host-based Intrusion Detection System (HIDS), etc. These facilities actively monitor and defend against malicious attacks, preventing unauthorized access, and ensuring the ongoing integrity of network operations.

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

CDNetworks has established a comprehensive data backup, incident management and recovery framework designed to safeguard the data availability and minimize downtime in the event of any physical or technical disruption. This framework encompasses:

- meticulously defined data retention schedules, backup types and frequencies, and backup methods;
- a full-lifecycle incident management approach, including incident detection and notification, containment, risk classification and execution of response plan, ongoing updates, post-incident review;
- proactively identifying a range of potential internal and external threats, including malware insertion, cyberattacks, information destruction, and equipment or facility failures. Incidents are categorized and ranked by severity, and each category has predefined response protocols, supported by dedicated incident response teams and CDNetworks geographically distributed data centres;
- in the event of a physical or technical incident, the team is expected to respond and execute the predefined response actions without undue delay upon awareness to mitigate damage, restore access and minimize downtime; *and*

- regular drills and simulations of data recovery plans to validate their effectiveness, ensuring that the systems and personnel are well-prepared to respond quickly and efficiently in real-world scenarios.

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

CDNetworks' technical and organizational measures undergo rigorous and systematic testing and evaluation, including external third-party audits and internal security audits.

- External third-party audits: CDNetworks' technical and organizational measures are regularly tested and evaluated by independent third-party auditors as part of CDNetworks security and privacy compliance program, including ISO 27001, SOC 2, K-ISMS, PCI DSS and other external audits.
- Internal security audits: CDNetworks conducts regular manual and automated vulnerability scans and assessments on all IT assets integrated on the platform, in order to identify and address any potential security gap. These approaches include host-based assessments, network-based scans, and application-based evaluations.

Measures for user identification and authorisation

CDNetworks implements effective measures for user authentication and privilege management by:

- mandatory access control and authentication policies;
- a zero-trust model for user identification and authorization, providing secure and flexible Identity and Access Management (IAM) features through Console and APIs;
- unique credentials and Multi-Factor Authentication (MFA), with advanced options like time-based one-time passwords (TOTP), SMS-based and email-based MFA, as well as IP whitelisting to control login sources;
- supporting Federated Identity Authentication to streamline and secure user access across multiple systems;
- access permissions assigned based on the user's role, data classification and tiered management, as well as approval processes in place for exceptional access requests;
- in adherence with the principle of least privilege and time-limited access; *and*
- login auditing and abnormal login alerts.

Measures for the protection of data during transmission

CDNetworks employs a comprehensive set of measures to ensure the security during data transmission:

- using Transport Layer Security (TLS) protocols to encrypt data in transit, ensuring that information exchanged between systems is protected from interception and tampering;
- IP whitelist and IP blacklist, API authentication and additional encryption technologies protecting data as it travels through gateways and communication channels;
- employing effective encryption algorithms and parameters, such as 2048-bit RSA encryption for data in transit; *and*
- audit logging, monitoring and tracking.

Measures for the protection of data during storage

CDNetworks utilizes a comprehensive framework for the protection of data during storage, including:

- a secure, access-controlled environment, with physical and digital safeguards in place;
- using state-of-the-art encryption protocols and effective encryption algorithms, such as employing AES with a key length of 128-bits or longer;
- regular testing for software vulnerabilities and potential backdoors within data storage systems; *and*
- audit logs, abnormal behaviour detection and alerts mechanism.

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

The physical security of CDNetworks' data processing equipment (namely database, servers and related hardware) is achieved through multi-layered protective measures.

- Strict access restrictions for personnel and visitors, including secure entry systems such as key cards or biometric authentication, and on-site security personnel monitoring access.
- 24/7 surveillance systems are employed, ensuring continuous monitoring of all sensitive areas. Video cameras record all access points and critical zones to detect and respond to any potential unauthorized activity in real time.
- Specialized environmental controls, such as temperature and humidity controls, are implemented to ensure the optimal operation of hardware.
- Comprehensive access logs are maintained that every access to the data

centre is recorded, ensuring a full audit trail of personnel or visitors who enter and leave the premises.

- Security alarm systems and additional safeguards.

Measures for ensuring events logging

CDNetworks maintains a comprehensive events logging and monitoring system to ensure traceability of any data access and processing activities, including:

- zero-trust model for identity verification and authorization to ensure only legitimate users are granted access. Event logs are tied to verified identities, providing an accurate record of all actions taken;
- automated alerting systems notifying relevant personnel when suspicious activities or security breaches are detected;
- systematically reviewing all event logs and analysing any deviation from normal behaviour; *and*
- annual testing of the logging configurations, monitoring systems, alert mechanisms and incident response workflows.

Measures for ensuring system configuration, including default configuration

CDNetworks adheres to industry-leading configuration baselines for all data processing systems deployed in production environments. Key measures include:

- utilizing automated monitoring tools that continuously oversee configurations to prevent unauthorized modifications. Only authorized personnel are granted the privilege to make any changes to system configurations;
- implementing stringent change management process that mandates a rigorous review and approval for any modifications, ensuring all changes are logged for audit purposes;
- conducting regular audits to identify and rectify any deviation from approved configurations, maintaining ongoing system integrity;
- enforcing access control measures based on the principle of least privilege. By default, access is denied until explicitly authorized; *and*
- applying centralized management of system time synchronization to ensure accurate timekeeping.

Measures for internal IT and IT security governance and management

CDNetworks implements a robust governance framework for internal IT and IT security management by:

- establishing internal policies that set the foundation for secure system

operation and data processing, which include but not limited to, access control, incident response, IT assets management, security baselines, etc.;

- organizing regular IT and security training programs. Key personnel responsible for data protection receive targeted training to address their specific responsibilities;
- members of the information security and data protection team holding certifications in relevant security frameworks; *and*
- regular internal audits, risk assessments, and policy reviews to ensure compliance and adapt to emerging threats.

Measures for certification/assurance of processes and products

CDNetworks ensures that the services and products are consistently aligned with globally recognized standards by maintaining continuous certification to industry-leading framework. CDNetworks certifications include:

- ISO 27001 is an industry-wide accepted information security certification that focuses on the implementation of an Information Security Management System (ISMS) and security risk management processes.
- PCI DSS (Payment Card Industry Data Security Standard) is an information security standard for organizations that handle branded credit cards from the major card schemes.
- K-ISMS is a Korea government-backed certification that ensures safe management of important information assets such as “corporate information, industrial secrets, and personal information” held by companies and organizations.
- SOC 2 report is designed to assure service organizations’ clients, management and user entities about the suitability and effectiveness of the service organization's controls relevant to security, availability, processing integrity, confidentiality and privacy.

These certifications are upheld through regular audits, ongoing assessments, and continuous updates to adapt to emerging threats and meet evolving compliance requirements.

Measures for ensuring data minimisation

CDNetworks adheres strictly to the principle of data minimization by collecting only the personal data necessary for specific, legitimate purposes. Data is processed only for the purposes for which it was collected, and any unnecessary or excessive data is either deleted or anonymized.

Measures for ensuring limited data retention

CDNetworks has established data retention policies that strictly limit the storage of personal data to the duration necessary to fulfil the processing purposes. Personal data is automatically deleted or anonymized after the service period, or sooner upon Customer's request, unless otherwise required by applicable laws. Regular reviews of stored data are conducted to ensure compliance with retention guidelines and prevent unnecessary retention.

Measures for ensuring accountability

CDNetworks promotes accountability through a well-defined governance structure and clear assignment of roles and responsibilities in data processing. Regular internal and external audits ensure adherence to data protection policies. Breach reporting mechanisms and thorough documentation of all processing activities allow for transparent oversight and foster accountability in data processing operations.

Measures for allowing data portability and ensuring erasure

CDNetworks enables data portability by providing Customer with easy, secure access to their personal data in a structured, commonly used, and machine-readable format. At all times, CDNetworks will adhere to the instructions given by Customer in respect of retrieval or deletion of personal data, unless otherwise provided by applicable laws.

ANNEX

STANDARD CONTRACTUAL CLAUSES

MODULE TWO: Transfer 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) for the transfer of personal data to a third country.

(b) The Parties:

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

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

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

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

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

Clause 2

Effect and invariability of the Clauses

(a) These Clauses set out appropriate safeguards, including enforceable data subject rights and effective legal remedies, pursuant to Article 46(1) and Article 46 (2)(c) of Regulation (EU) 2016/679 and, with respect to data transfers from controllers to processors and/or processors to processors, standard contractual clauses pursuant to Article 28(7) of Regulation (EU) 2016/679,

provided they are not modified, except to select the appropriate Module(s) or to add or update information in the Appendix. This does not prevent the Parties from including the standard contractual clauses laid down in these Clauses in a wider contract and/or to add other clauses or additional safeguards, provided that they do not contradict, directly or indirectly, these Clauses or prejudice the fundamental rights or freedoms of data subjects.

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

Clause 3

Third-party beneficiaries

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

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

(ii) Clause 8 - 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.

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[1] (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

[1] 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.

(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.[2] The Parties agree

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

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) 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.

(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[3];

(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.

---

[3] 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

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

Clause 18

Choice of forum and jurisdiction

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

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

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

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

APPENDIX

ANNEX I

A. LIST OF PARTIES

Data exporter(s):

1. Name: the entity identified as “Customer” in the DPA.

Address: the address of Customer specified in the DPA.

Contact person’s name, position and contact details: the contact information specified in the DPA or the Agreement.

Activities relevant to the data transferred under these Clauses: the data exporter (also referred as “**Customer**”) subscribes, purchases and receives services from data importer.

Signature and date: this ANNEX shall be deemed executed upon execution of the DPA.

Role (controller/processor): controller

Data importer(s):

1. Name: CDNetworks as identified in the DPA.

Address: the address of CDNetworks specified in the DPA.

Contact person’s name, position and contact details: the contact information specified in the DPA or the Agreement.

Activities relevant to the data transferred under these Clauses: the data importer provides services to data exporter as ordered by the data exporter.

Signature and date: this ANNEX shall be deemed executed upon execution of the DPA.

Role (controller/processor): processor

B. DESCRIPTION OF TRANSFER

Categories of data subjects *whose personal data is transferred*

The data subjects are “End Users” as defined in Appendix 1 of the DPA.

Categories of personal data transferred

The personal data transferred is “Customer Personal Data” as described in Appendix 1 of the DPA.

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.

Customer Content may include sensitive data, which is determined and controlled by Customer in its sole discretion. Any such sensitive data shall be protected in accordance with the TOMs as described in Annex II.

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

The data is transferred on a continuous basis when CDNetworks is performing services provision to Customer.

Nature of the processing

The nature of processing is described in Appendix 1 of the DPA.

Purpose(s) of the data transfer and further processing

The purpose of data transfer and further processing is to provide and secure the services that Customer subscribed from CDNetworks.

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

Personal data will be retained during the service provision period as stipulated between Customer and CDNetworks, unless otherwise provided by applicable laws.

The Log Support Personal Data will be retained for 180 days after service termination.

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

When providing services to Customer, CDNetworks may engage the sub-processors listed at https://www.cdnetworks.com/sub-processors/.

C. COMPETENT SUPERVISORY AUTHORITY

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

The competent supervisory authority shall be the authority to which the Customer is subject, as determined in accordance with the GDPR.

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

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

The technical and organisational measures implemented by CDNetworks, including the certifications held by CDNetworks, are described in Appendix 2 Security Measures of the DPA.

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

When sharing personal data with sub-processors, CDNetworks will share it only if the recipient agrees to comply with CDNetworks' data processing policies or has adopted a substantially similar technical and organisational measures regarding the treatment of personal data.