MEGAPORT SERVICES - DATA PROCESSING ADDENDUM ("DPA")

WHEREAS Megaport's Services constitute 'Network-as-a-Service' and essentially involve the provision of a software-defined network along which raw data in the form of data packets ("**Packets**") can be transmitted, Megaport having no knowledge of what such Packets relate to; AND WHEREAS the Customer (as defined below) envisages the Services being used to transmit Packets which ultimately relate to individuals,

NOW THEREFOR IT IS AGREED that, to the extent applicable Privacy Laws regard such individuals as being 'identifiable' from the Packet alone and Megaport's passive transmission of such Packet along its network as being 'processing' subject to such Privacy Law, this DPA will apply and be incorporated into Customer's Agreement (as defined below), with effect from the date on which a counter-signed copy hereof is returned via email to privacy@megaport.com. (Note that if the 'Customer' entity signing this DPA is not yet party to an effective Agreement, this DPA will be of no force and effect, not until such Agreement is entered into.)

1. INTERPRETATION

Capitalised terms herein bear the same meanings as given to them in the Agreement, save for the following terms which, for purposes of this DPA, bear the following meanings:

1.1 "**Agreement**" means the agreement governing Customer's use of Megaport's Services, comprising one or more Orders as read with the terms of the relevant 'General Services Agreement' and/or 'General Reseller Agreement', 'Privacy Policy' and 'Acceptable Use Policy';

1.2 "**Controller**", "**Data Subject**", "**Personal Data Breach**", and "**Processing**" shall have the same meaning as in the EU's General Data Protection Regulation 2016/679;"**Controller Clauses**" means the Module One of the Standard Contractual Clauses for Controllers as approved by the European Commission and available at https://eur-lex.europa.eu/eli/dec_impl/2021/914/oj (as amended, superseded or updated from time to time), and excluding any illustrative/optional clauses;

1.3 "**Customer**" means the signing party specified as such below, if and to the extent that it is also party to a valid Agreement;

1.4 "**Data Exporter**" means the entity transferring the personal data to a Data Importer in a third country.

1.5 "**Data Importer**" means the entity receiving the personal data transferred by the Data Exporter.

1.6 "**Group**" means the Megaport Ltd group of companies;

1.7 "**Megaport**" means the relevant Group entity providing the Services to Customer;

1.8 "**PI**" means '**Personal Information**' as defined in the Agreement and under Privacy Law;

1.9 "**Privacy Laws**" means any laws and regulations governing the processing of PI, including but not limited to the EU's General Data Protection Regulation 2016/679 ("**GDPR**") , the UK's Data Protection Act 2018, and California's Consumer Privacy Protection Act, as amended.

1.10 "**Standard Contractual Clauses**" or "**SCCs**" means the standard contractual 'model clauses' approved by the European Commission for purposes of Restricted Transfers between data controllers– Module 1 (available at https://eur-lex.europa.eu/eli/dec_impl/2021/914/oj) (as amended, superseded, or updated from time to time), and excluding any illustrative/optional clauses;

1.11 "**Restricted Transfer**" means any transfer of PI to, or access of PI from a country where the European Commission does not regard as having adequately protective Privacy Laws, each, where the processing of PI is subject to Privacy Laws.

1.12 **"UK Addendum"** means the International Data Transfer Addendum to the EU Commission Standard Contractual Clauses approved by the United Kingdom's Information Commissioner's Office. (available at https://ico.org.uk/media/for-organisations/documents/4019539/international-data-transfer-addendum.pdf) (as amended, superseded or updated from time to time), and excluding any illustrative/optional clauses.

1.13 "**UK Data**" means PI subject to UK's Privacy Laws.

2. PI PROCESSING.

2.1 **Scope:** This DPA only applies if and to the extent that Packets relate to individuals and applicable Privacy Law regards (a) such individuals as being 'identifiable' from the Packet; and (b) Megaport's passive transmission thereof along its network as being 'processing' subject to such Privacy Law. For clarity, because the Services are used by corporate entities, not individuals, any metadata relating to Service usage (like Packet routing information, dates, times, quantities transmitted etc.) ("**Metadata**") does not constitute PI.

2.2 **Processing Details:** As detailed in the Agreement, Customer controls the use of the Services in that (as between the parties), it alone determines the type, quantity and routing of data it transmits using the Services. Megaport only processes Packets (a) as instructed by Customer (as reflected in this DPA, the Agreement, the configurations set via Customer's Megaportal account, and any instructions given via support tickets) or (b) as otherwise required by law (e.g. to comply with a court order to intercept or retain any Packets), in which case Megaport shall to the extent permitted by those laws, give Customer prior notice thereof. Megaport agrees that they will not sell, share, retain, use, or disclose PI for any purpose except as permitted in the Agreement. Megaport will not combine any PI received from Customer with any other PI it receives from other sources. If Megaport is no longer able to meet obligations under relevant Privacy Laws, it will notify the Customer as soon as possible, and Customer may take reasonable and appropriate steps to stop any unauthorized use of the PI.

2.3 **Authorised Personnel**: As detailed in the Agreement, the Services involve automatic transmission of Packets by Megaport's systems. Manual processing is only applied to the Metadata, and only for purposes of troubleshooting and to detect and prevent unlawful use of the Services. Nevertheless, in doing so, Megaport ensures that Metadata is only processed by those individuals who need to know and access it for such purposes and takes reasonable steps to ensure the reliability of those individuals.

2.4 **Cross-border transfers**: Enabling data transfer (potentially including across borders) is the essence of Megaport's Services and because (as between the parties) Customer alone controls the data types, origins, destinations and recipients, Customer alone is responsible for implementing any legally required appropriate safeguards for any PI it chooses to send to recipients in countries which the relevant Privacy Law regards as not having adequately protective PI-related laws.

2.4.1 **Restricted Transfers**: In the event Megaport, in its capacity as a Controller, receives Customer employee and other representative PI whose processing would be subject to GDPR, the SCC are hereby incorporated by way of reference, and in this regard (a) PI will be processed in accordance with the undertaking set forth therein; (b) Customer is the 'data exporter' and Megaport is the 'data importer'; (c) the data subjects, data categories, types, purposes and contact points for queries would all be as indicated in each of their 'privacy policy' as published online; ; (d) the technical and organisational security measures implemented by the data importer are those specified in Appendix 1; and (e) each signature to this DPA shall be considered a signature to the SCC for purposes of any Controller-Controller Restricted Transfer between them. Mutatis mutandis, the UK Addendum is hereby deemed to be incorporated to this DPA in addition to the SCC when a Restricted Transfer includes UK Data.

2.4.2 **Change in Law**: Should either of the above mechanism change to require either a specific method to allow for international transfers of PI (such as an addendum that makes reference to laws, courts, and authorities in that jurisdiction) or use of a different form of standard contractual clauses (or an equivalent agreement), the Parties will update this DPA without undue delay to implement an approach that is valid under the relevant Privacy Law for Customer PI that is subject to it.

2.4.3 **Cooperation**: All costs of cooperation and assistance by Data Importer to Data Exporter to enable Data Exporter to comply with its obligations under GDPR under Clause 8.6.(d), 8.9.(c), 10 shall be borne by Data Exporter.

2.4.4 **Effective Date**: The SCC and/or the UK Addendum shall come into force on the date of signature of the DPA by the Parties or the first transfer of the PI from the Data Exporter to the Data Importer, whichever the earlier. It shall be automatically terminated when the DPA terminates or expires for any reason, notwithstanding the survival of the relevant provision for as long as PI related to a Party is retrained by the other Party. In

any case, the processing by the Data Importer shall only take place for the duration specified in Annex 1.B of the SCC, or the SCC, whichever the earlier.

2.4.5 **Governing law:** The Data Exporter not being established in the EEA, the governing law of the Irelandhas been selected. For data processing operations subject to the UK Privacy Laws, the governing law shall be that of England and Wales.

2.4.6 **Choice of forum and jurisdiction:** The Data Exporter not being established in the EEA, the courts of Ireland have been elected as competent jurisdiction in the occurrence of any dispute between the Parties relating to the SCC. For data processing operations subject to the UK Privacy Laws, the courts of London shall have exclusive jurisdiction over any dispute arising out of the UK Addendum.

2.4.7 **Option**: Optional language contained in Clause 7 of the SCC ("Docketing Clause") and the second paragraph of Clause 11 ("Redress") is hereby waived.

2.5 **Security**: Megaport implements appropriate technical and organisational measures to secure its Services against the risk of unauthorised or accidental Packet processing or other similar risks, including measures specifically identified in the Agreement. This includes ensuring the confidentiality, integrity, availability, and resilience of its processing systems and services; restoring availability and access to Packets in a timely manner in the event of any incident; and regularly assessing the effectiveness of its security measures. Note specifically, however, that as Megaport does not encrypt the Packets (as doing so would leave the decryption keys under Megaport's control), as between the parties, **Customer is solely responsible for ensuring that the Packets are encrypted and none of Megaport, its Affiliates and officers will be liable whatsoever for any loss, harm, damages or third-party claims suffered by Customer or anyone else which arise from the Packets not having been properly encrypted.**

2.6 **Co-operation**: The Parties shall reasonably co-operate with each other to enable each other to discharge their Privacy Law obligations (including compulsory data protection impact assessments and data subject access requests), as may be applicable. It is noted however that due to the nature of the Services, Megaport does not retain any Packets to update, correct or grant access to data in any event.

2.7 **Data Breach**: Without detracting from Megaport's notification and remediation obligations under the Agreement and relevant telecommunications laws, if Megaport becomes aware that a Packet-related incident also constitutes a Personal Data Breach, Megaport shall notify the Customer without undue delay and reasonably cooperate and assist Customer in its investigation, mitigation and remediation thereof, as well as with any reporting obligations Customer may have under Privacy Law.

2.8 **Return or Deletion**: In accordance with telecommunications laws, Packets are not retained by Megaport in any form for longer than needed to provide the Services, it being noted that the Services involve mere split-second Packet transmission, not storage. Consequently, at cessation of the Services, there will be no Packets under Megaport's possession to return or destroy. Nevertheless, Megaport may provide written certification of this if requested by the Customer within 30 days of Agreement termination.

2.9 **Liability**: As this DPA forms part of the Agreement, each party's liability under this DPA is still subject to the aggregate liability limitations and exclusions provided for under the Agreement, if any.

2.10 **Order of precedence**: This DPA will prevail in the event and to the extent of any inconsistencies between it and the Agreement; provided that nothing in this DPA serve to reduce Megaport's obligations to protect PI under, or to permit PI Processing in a manner otherwise prohibited by, the Agreement.

IN WITNESS WHEREOF the Parties hereto have duly executed and delivered this DPA on the date of last signature below.

CUSTOMER: _____
Legal Name of Customer

Signature: _____

Signatory Name:

Signatory Title:

DATE:

MEGAPORT

Signature: Michael Reid
Michael Reid (Jul 13, 2023 13:14 GMT+10)

Signatory Name: Michael Reid

Signatory Title: CEO

DATE: Jul 13, 2023

APPENDIX 1
intended to supplement Annex 2 of the SCC and/or UK Addendum

SECURITY MEASURES

Megaport to ensure the following basic security measures:

Governance

- Megaport has an Information Security Policy which is aligned with industry standards and which is reviewed periodically.
- Organisational roles and responsibilities for Information Security are clearly defined and staffed appropriately.
- The Megaport's Information Security strategy has executive leadership approval.

Access Control

- Megaport ensures access to information is restricted to authorised users. Account permissions are granted based on the principle of least privilege, where accounts are only given permissions necessary for job function.
- Strong passwords are enforced and multi factor authentication is used where practical.
- Administrative or privileged accounts are separate from a user's non-privileged account.

Physical Controls

- Megaport will ensure security controls exist that prevent unauthorised access to areas (e.g. offices, datacentres) containing equipment performing IT functions.

Cryptographic Controls

- Megaport will ensure that when sensitive data is in storage or in transit that it is encrypted by industry best practice ciphers (e.g. AES-128, TLS 1.2).
- Megaport will ensure that cryptographic keys are managed via documented standards and procedures. Cryptographic keys will be protected from unauthorised access or misuse.

Business Continuity

- Megaport has instituted and maintains a Business Continuity Plan or necessary Disaster Recovery controls.
- Backups of essential data are performed on a regular basis and validated regularly.

Incident Response

- Megaport has a documented incident response procedure aligned with industry best practice, that covers the response, notification and remediation of Security Incidents.
- Megaport's Incident Response policy defines and allocates the roles and responsibilities of staff during an incident.

Network Security

- Megaport will implement industry best practice network security controls to ensure network traffic is monitored and unauthorised traffic is blocked.
- Remote access into the Megaport's network must be restricted to authorised connections only. Remote access connections will be controlled by secure protocols and appropriate encryption.

Endpoint Security

- Megaport will utilise malware protection on systems where it is feasible. Megaport will ensure anti-malware software will receive the latest software updates and is functional.

- Megaport will ensure systems are deployed and maintained to configuration “hardening” standards that follow industry best practices (e.g. CIS Microsoft Windows Server Benchmarks).

- Megaport will ensure that software used on its systems maintains up-to-date patching.

Vulnerability Management

- Megaport implements and maintains a vulnerability management process that applies security patches to known vulnerabilities.
- Vulnerabilities are classified based on severity and timeframes to address vulnerabilities are defined and adhered to.

More details about Megaport’s security practices and measures can be found on Megaport’s Information and Privacy Security Statement