

# MEGAPORT REGULATORY, INFORMATION SECURITY & PRIVACY STATEMENT

## 1. Megaport's Services and Regulatory Context

Megaport Limited (ASX: MP1) and each of its related entities and subsidiaries ('Megaport', 'we', 'us' or 'our') is a global leading Network as a Service (NaaS) provider. Using Software Defined Networking (SDN), Megaport's platform enables customers to rapidly connect to services across the Megaport network. Services can be directly controlled by customers through Megaport's web-based portal or the open Application Programming Interface (API).

Megaport Limited is incorporated in Australia pursuant to the Corporations Act 2001 (Cth) and is listed on the Australian Securities Exchange (ASX), and is therefore required to comply with the ASX Listing Rules.

Megaport's services are governed by various laws and regulations specific to the telecommunications industry (Telco Laws), with Megaport holding a licence, being registered with and/or overseen by the relevant telecommunications regulatory body in each country in which it operates, where required.

Megaport's Information Security Management System (ISMS) is certified to the ISO/IEC 27001:2013 standard, as detailed below.

## 2. Data Processing

### 2.1 Our Customers' Transmission Data

Customers control what data is transmitted across Megaport Services and by what methods (i.e. protocol and encryption), its origins and destinations. Megaport provides the transport mechanism, only reading IP packet headers in instances required route and forward packets appropriately.

Megaport does not collect, store, or view customer transmission data. We do not know what type of data our customers are sending. Our role is limited to being a mere conduit for the data. Megaport only retains certain metadata for billing and troubleshooting purposes, in accordance with relevant Telco Laws.

The infrastructure that facilitates the provision of Megaport services resides in securely managed data centres operated by established providers who implement environmental, physical, and logical controls in compliance with Megaport standards. In the event of service disruptions, outages and/or suspected security incidents, our internal policies dictate that our Security, Regulatory, and/or Privacy teams be involved to ensure that the appropriate investigation, remediation, and statutory notification actions are taken.

## 2.2 Personal Data

As we provide business-to-business services to corporate customers, the personal data Megaport collects from customers is limited to what is required for our own basic account administration purposes, like any other organisation would (e.g. customer representatives' contact details and interactions with customer support). Also, like any other organisation, we process some personal information as part of our marketing, sales, vendor administration and human resources processes. You can read more about how we process such personal data in Megaport's [Privacy Policy](#).

Megaport has a dedicated Privacy Team and has adopted an internal Personal Data Protection Policy and related procedures designed to protect privacy, comply with various privacy laws, and accommodate the following:

- Privacy screenings on all new projects, processes, systems, products and services, and where required, comprehensive privacy impact assessments carried out by the relevant Department Head (or delegate) in conjunction with the Privacy Officer;
- Assessing the adequacy of the privacy and security measures of our vendors, suppliers and partners and ensuring that the appropriate contractual protections are incorporated in their contracts (including EU/UK GDPR-required Data Processing Addenda and EU/UK cross-border standard contractual clauses/UK Addendum);
- Ensuring the Privacy Team's involvement in security incident investigations where personal data is impacted; and
- Keeping records of our personal data processes, disclosures, breaches, and requests for access and information.

## 2.3 Data Protection Addendum (DPA)

Megaport recognises that even our automatic passive transmission of your binary data might be regarded as 'processing' of 'personal data', and so we do accommodate a customer-facing DPA which we've made available online within our online [Global Services Agreement](#), specifically:

- clause 6(f) ('Services') - which explains the nature of our data transmission services to give you proper context; and
- clause 12(c) ('Personal Information') - which deals with any personal data potentially processed as part of our service, and which includes the link to our DPA.

More information about our internal privacy & security practices is set out in our Cloud Star Alliance (CSA) - Consensus Assessment Initiative Questionnaire (CAIQ) document, which can be provided upon request.

### 3. Information Security

Megaport manages an Information Security Management System (ISMS) compliant with the ISO/IEC 27001:2013 standard. Certification was received on 9 December 2020 and renewed on 9 December 2023.

Additional security-related information can be provided upon request including a copy of Megaport's ISO/IEC 27001 Certificate and Statement of Applicability (SoA).

*Michael Reid*

Michael Reid (Dec 20, 2023 19:36 GMT+10)

Michael Reid

CEO

20 December 2023