

Data Act Information

Version 1.0 · Effective October 5th, 2026

This page is the Information Page referred to in the Teraswitch [Data Act Addendum](#), for customers established in the European Union to whom Regulation (EU) 2023/2854 (the Data Act) applies.

1. Switching and deletion

How switching and deletion work is set out in the Data Act Addendum. To make a request, email support@teraswitch.com with two months' notice.

2. What can and cannot be exported

Sections 2.1 and 2.2 together list the categories of Exportable Data and Digital Assets that you can take with you. Section 2.3 lists what is excluded.

2.1 What you move yourself. Everything on your metal servers and instances, including operating systems, applications and data, is yours and under your control. You keep your access through the transitional and data retrieval periods and move it with your own tools. We keep that access in place. Standard service fees apply during these periods. We do not impose switching charges, including excess egress charges attributable to transferring Exportable Data and Digital Assets under the Data Act. To help us identify that egress, let us know your new provider's destination network ranges. If you switch before the end of a committed term, fees for the remainder of that term are payable as set out in the Addendum.

2.2 What we provide. Your account details, including projects, users, and SSH keys. The configuration of your services in our console, including server specifications and network and IP configuration records. Invoices, usage details and history, audit logs, and support ticket history for as long as we keep them. All of these are self-service accessible.

2.3 What we do not provide. Data specific to the internal functioning of our platform (internal network, security and monitoring configuration and data), which we exempt because disclosing it would risk our trade secrets. Passwords and API secrets, for security. Teraswitch-assigned IP addresses themselves; you get the configuration details, but the addresses stay with Teraswitch. Teraswitch-supplied operating system images, templates and software licences, which stay with Teraswitch; you will need to relicense with your new provider.

3. Formats

Data	Format	How to get it
Data on your metal servers and instances	As you stored it	Your own tools (SSH/RDP/virtual console/others)
Service configuration and usage details	HTML (via Console), JSON (via API)	Console or API

Data	Format	How to get it
SSH keys, and audit logs	HTML (via Console), JSON (via API)	Console or API
Invoices, including usage history	PDF / CSV (via Console), JSON (via API)	Console or API
Account details and configuration, including projects and users	HTML	Console
Support tickets	HTML	Console

Full data structures and formats for data retrievable via the Teraswitch API, including applicable limitations, are published in our API documentation [here](#), including a downloadable OpenAPI specification.

Other limitations: Hardware-level settings (RAID, BIOS) don't carry over to another provider and must be recreated. Transfer speed is limited by your server's port speed and network path. Invoices, usage, audit logs, and support ticket history are subject to our retention periods.

4. Where our infrastructure is, and government requests

Teraswitch, Inc. is incorporated in Pennsylvania, United States, and is subject to United States law. Your services run in the region you choose when you deploy them, as shown in the console and API, and we do not move them to another region. Our infrastructure is located in facilities operated by colocation partners in Canada, France, Germany, Ireland, Japan, the Netherlands, Singapore, South Korea, the United Kingdom and the United States. Infrastructure in each location is subject to the law of the jurisdiction where the facility is located.

You administer the operating systems, applications and data on your servers; we do not. Access to our own management systems is restricted to authorized personnel and logged. Our contractual confidentiality and security obligations also restrict access to and disclosure of customer data. Regarding government requests for customer data, we act only on valid, binding legal process and disclose only what it requires. We do not give any government direct or standing access to our systems or customer data. We will inform you of a request for your data before complying with it, unless we are legally prohibited from doing so or the request serves law enforcement purposes and notice would compromise it. Where a request conflicts with EU or Member State law, we raise the conflict and use the legal means reasonably available to narrow or resist it. These commitments apply to all customer data, whether personal or non-personal; for personal data, see also our [Data Processing Addendum](#).