XENETA

Data Security

General

Xeneta does not store mission-critical data from our customers:

- Only basic data for user accounts is stored by Xeneta — we do not store any private information
- We do not store any sensitive customer data — only past and current Requests for Quotations (RFQs) and contracted prices are stored within our system

General

Xeneta's user account control, infrastructure access, and data encryption follows industry standards.

- Data in transit is encrypted using TLS v1.2 with modern ciphers
- An independent third-party performs monthly vulnerability scans and we correct any detected vulnerabilities
- An independent third-party performs penetration tests on the system to verify its security
- Password policy is industry-standard as verified by an independent third-party
- Internal access to customer data is on a need-to-know basis

Disaster Recovery

Xeneta aims to provide service reliability and we have a number of disaster recovery and infrastructure redundancies in place.

- Our uptime service-level agreement (SLA) is 99% as measured per month
- All parts of our infrastructure have redundancies
- Part of our infrastructure is hosted on Amazon Web Services (AWS) to increase reliability
- We deploy in multiple AWS Availability Zones to mitigate disaster risk
- AWS provides us with automated backups of our databases
- AWS provides us with off-site backups
- Physical access to the data centers is tightly controlled by Amazon