Xledger Security and Privacy

Valid through Q3-Q4 2022[1]

1 Contact Xledger for an updated version after Q1 2023

Xledger passionately believes that a strong business reputation is based on a strong data protection and information security program.

We see data protection and information security as fundamental components of doing business. Xledger is committed to protecting information assets, personal data, and client information. We do passionately believe that solid data protection and information security programs are the essential components of a professional services organization.

The intention of this document is to summarize our approach to data protection and information security. It provides an overview of how we approach and secure client information and our information systems that support it. This work is that foundation for our certifications.

The specifics of these measures may vary depending on the services performed and applicable country regulatory requirements. Our data protection and information security programs and practices are focused on sharing information appropriately and lawfully while preserving confidentiality, integrity, and availability.

Data Privacy

GDPR

We take our data management responsibilities seriously. Xledger complies with all aspects of current data protection legislation and is committed to compliance with the GDPR, ensuring all personal data is handled in line with the principles outlined in the regulations.

Our data protection framework is based on the principles of the EU General Data Protection Regulation (GDPR). It addresses the issues raised by modern data management tools and systems. We apply a common set of personal data management principles to provide a framework for processing personal data in compliance with GDPR, local privacy laws and professional standards.

Customer Data

Xledger does passionately believe that your data is yours and only yours. From the first lines of code written it was in Xledger's DNA that a true multi-tenant solution is the best way to secure and segregate customer data.

Our test and development environment does not use customer data. The data used are a generic data set to facilitate a full and complete functional test and development.

In cases where the customers need a test environment with their own data this is aligned with our production environment. This means that the test environment is processed and stored in the same locations as the production environment and follows the same operational security procedures.

We do not share your data with any partners/suppliers, and your data is stored within the European Union.

Securing Xledger

MFA and SSO

Xledger does follow and support the latest security functions such as MFA. Currently we do support Google Authenticator, Microsoft Authenticator, SMS, and e-mail. We do highly recommend our customers to use MFA to protect their data.

Xledger usernames and passwords is compared against known breached credentials. This does give our customers increased security through forcing a mandatory password change if their credentials are known to the public.

SSO (Single Sign-On) to Xledger is supported through Azure and Microsoft ADFS. By using Azure as SSO platform this gives our users increased control and security by utilizing Azure's built-in functions (such as Conditional Access) to control access to their data.

Vulnerability Management/Penetration test

Xledger continuously monitor our internal environment and internet facing assets for vulnerabilities and security recommendations.

On an annually basis we do have a penetration test on the Xledger application performed by an independent third-party security provider.

Based on these scans and penetration tests we upgrade and update our assets to increase our security posture.

Logging

To comply with the audit requirement, customers' actions, and location (from where the changes are made) are logged in the application and can be audited.

Third party suppliers

Xledger does not use any third-party resources in development of the application, nor does any third-party resources have access to the application.

Xledger does use third part suppliers for renting rack space and internet lines in our datacenters, but these does not have access to the application solution.

We do as well use a third-party for off-site storage of our encrypted backups, but these are not accessible for the supplier.

These suppliers and underlying procedures are audited as a part of the ISO 27001 certification and the ISAE 3402 Type 2 certification.

Data protection

Data Storage

Xledger's cloud environment is situated in Norway in the greater Oslo area. Both locations are ISO 27001 certified for data center operations to increase operational security.

The reason for choosing to store and operate data in our own cloud is that it gives us better control and security. Since we operate our own cloud, it also makes us more independent and less dependable on third parties.

Access To data

Access to data is limited to employees in our DevOps and IT Operations, but only to the required level according to their role/function in Xledger.

Physical access to the hardware (that stores customer data) in data centers is limited to some but not all IT Operations staff.

These accesses are audited on demand or annually as a part of the ISO 27001 certification and the ISAE 3402 Type 2 certification.

BCP

Xledger recognize the importance of continuous operations and access to data for our customers in case of disasters. To facilitate this, we do have our own plans to continue or recover in case of a disaster.

Our BCP plans are regularly tested against different (natural and hardware) scenarios to verify the integrity of our backups. A complete functional restore test of the production database backup is done biweekly.

Compliance

Information security audits to provide us with a more complete view of our information security compliance, our global technology products, services, and data centers are subject to audits. We conduct several forms of audit:

Independent third-party compliance audits against ISO 27001:2013 to certify the Operations of cloudbased ERP solutions employed within our two data centers in Norway and local data rooms.

Independent third-party compliance audits against ISAE 3402/SOC 1, Type 2 attestation of our platform, operations and procedures of Xledger.net.

Network vulnerability scans, which focus on the technical aspects of our Global Information Security Policy, such as patch management, application security and infrastructure security Foundation audits, which review technical controls and build processes of components such as operating systems, databases, and infrastructure in compliance with CIS.