Xledger Data Center Fact Sheet 2025

Last updated February 2025

Table of contents

1 Introduction

Xledger is a 100% cloud-based ERP vendor with more than 20 years of experience within cloud computing. Thousands of organizations in 80 countries use Xledger as their financial system globally. Xledger has offices in Norway, Sweden, Finland, United Kingdom, and USA.

2 Summary

Both the application and physical infrastructure (i.e., servers and internal network infrastructure) is solely operated by a limited number of Xledger employees. The physical servers are located at two highly secured external data centers. These provide power, conditioned modules and redundant WAN links. All data centers that host and process customer data are located in Norway.

Xledger has conducted an annual International Standard on Assurance Engagements (ISAE) 3402 Type II audit of the operational center, in which the security controls were audited and verified by an independent third auditor. See appendix 1 for further details about ISAE 3402.

Xledger has also conducted an annual International Standards Organization (ISO) 27001 audit of the data centers, processes, and operation procedures, in which the data centers operation and the staff operating the infrastructure is ISO 27001 certified by an independent third auditor. See appendix 2 for further details about ISO 27001.

Xledger complies with all aspects of current data protection legislation and is committed to compliance with the EU General Data Protection Regulation (GDPR), ensuring all personal data is handled in line with the principles in the regulations. See appendix 3 for further details about GDPR.

3 Data Center Infrastructure

3.1 Facilities

The data center is constructed of a concrete frame with conditioned modules above and below the ground. All modules have advanced fire detection and protection apparatus. The center is equipped with electromagnetic protection.

3.2 Backup Power Systems

An energy center is located contiguously to the main building and provides the majority of the backup power generation plant, its uninterruptible power supply (UPS) equipment, and chilled water pumping systems.

3.3 HVAC System

Conditioned modules are supported by redundant IMV chillers, feeding in-module redundant close control units permitting the center to operate within an acceptable temperature range.

3.4 Facility security

On site 24/7/365 manned security operates from a purpose-built security bunker. Internal and external advanced security surveillance camera systems, intruder detection and card access systems are placed throughout the site. In addition, there is a 360-degree boundary fencing with secured access control. All the above-mentioned ensures a high security level.

3.5 Certification

The data center provider is committed to quality, and certified according to ISO/IEC 27001, ISO 9001, ISO 14001 and OHSAS 18001.

3.6 Energy Efficiency

The data center deploys cost-reducing, environment-protecting, green energy management systems. These economies of scale mean that customers' power requirements, costs and associated carbon footprint are substantially reduced.

4 Application Infrastructure

4.1 Multi-tenancy

Xledger is a true multi-tenant application, meaning that all customer data is stored in the same database. User access is based on application control where users are given access based on a key list. Each entity has a key list.

5 Operations

5.1 Continuous Monitoring

Xledger is solely operated by internal employees. All monitored system exceptions are notified to operational management through SMS and email.

5.2 Mirroring and Backup

Continuous mirroring ensures high application availability and scheduled backups secure system data. Mirroring of database and fileserver occurs continuously. Database backup occurs every 15 minutes. Backup of files occurs every fourth hour. The database is test restored bi-weekly and tested. Backups are stored offline at a secured facility.

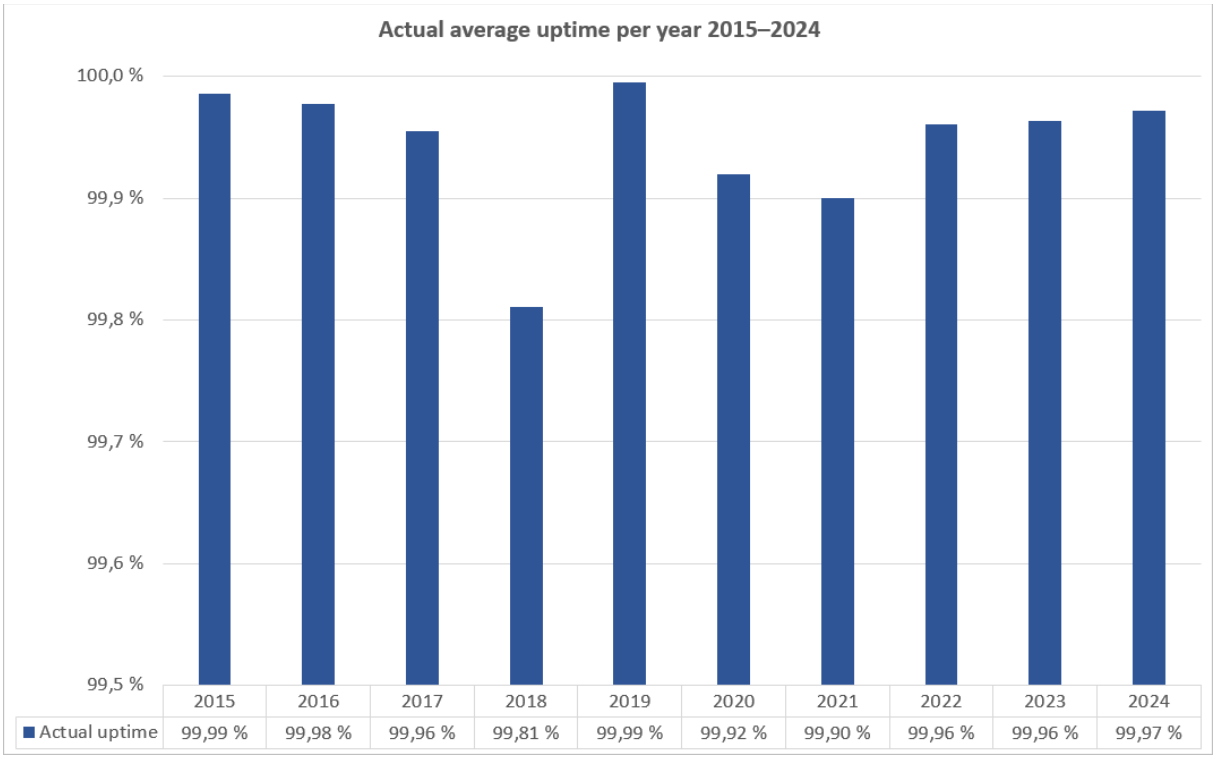
Our Business Continuity Plans are regularly tested against different (natural and hardware) scenarios to verify the integrity of our backups.

6 Availability

Two independent internet connections ensure a redundant internet connection and highly reliable availability. The Xledger application is continuously updated through high frequency product updates (patches) and technical maintenance. These are deployed at nighttime. The average uptime over the last 10 years, excluding planned product updates (patches) and technical maintenance, has been 99.94%.

Downtime is defined as unplanned downtime such as:

a) Technical downtime where the connection between our gateway and data center is unavailable.
b) Unexpected downtime in the data center (inside the firewall), e.g., the database is unavailable.
c) When we intentionally (not planned) take down the system and route the users to a static error page.



	2015	2016	2017	2018	2019	2020	2021	2022	2023	2024
Actual uptime	99,99 %	99,98 %	99,96 %	99,81 %	99,99 %	99,92 %	99,90 %	99,96 %	99,96 %	99,97 %

7 Security and compliance

7.1 Encryption

All data traffic between the user's web browser and the Xledger web server requires HTTPS with 256-bit encrypted secure connection using a 2048-bit SSL Certificate.

7.2 User Login and Application Access

Application login requires a username, a password and a security code which is sent to the user via e-mail, SMS or Authenticator (Google or Microsoft). Security code is activated by default for all users and ensures two-factor authentication. The application access is role-based. Each user is assigned standard roles controlling access to application information and features. The user can only access the application layer and not the underlying database and other infrastructure components. The users are automatically logged out of the application after a certain inactive time period.

Xledger supports SSO with Microsoft Azure AD and Microsoft ADFS. By leveraging Xledger with Azure AD SSO the customer can use the conditional access policies in Azure AD to control from where and from which device the users can access Xledger.

7.3 Audit Trail

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

7.4 Vulnerability management

Xledger continuously monitor our internal environment and internet facing assets for vulnerabilities and security recommendations. Based on this we upgrade and update our assets and services to increase our security posture.

7.5 Penetration test

On an annual basis we have a penetration test on the Xledger application performed by an independent third-party security provider. The executive summary of this test is available upon request. New functions are also tested by a third-party provider before they are released.

7.6 GDPR

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. All Customer data is stored within the European Union.

We do not share your data with any partners/suppliers unless a signed data transfer agreement exists between Xledger and the third party, and you have a separate agreement with both parties.

Our test and development environment does not use customer data, but rather a generic data set.

7.7 Data access

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.

Xledger does not use any third-party resources in development of the application, nor does any third-party resources have access to the application infrastructure. Xledger does use third part suppliers for renting rack space and internet lines in our datacenters, but these do not have access to the application solution. We also use a third-party for off-site storage of our encrypted backups, but these are not accessible for the supplier.

The Xledger application can be integrated with external systems through different API technologies such as Web Services and GraphQL. When integrating through Web Services, external systems can access a set of Xledger data secured with Client Certificated over HTTPS in addition to username and password. When integrating through GraphQL, external systems can access a set of Xledger data secured with username and password.

Appendix 1: ISAE 3402

The International Standard on Assurance Engagements (ISAE) 3402 (Assurance Reports on Controls at a Service Organization) was issued in December 2009 by the International Auditing and Assurance Standards Board (IAASB), which is part of the International Federation of Accountants (IFAC).

ISAE 3402 was developed to provide an international assurance standard for allowing public accountants to issue a report for use by user organizations and their auditors (user auditors) on the controls at a service organization that are likely to impact or be a part of the user organization's system of internal control over financial reporting.

Benefits to the service organization
Service organizations receive significant value from having an ISAE 3402 engagement performed. A Service Auditor's Report with an unqualified opinion that is issued by an Independent Accounting Firm differentiates the service organization from its peers by demonstrating the establishment of effectively designed control objectives and control activities. A Service Auditor's Report also helps a service organization build trust with its user organizations (i.e. customers).

Without a current Service Auditor's Report, a service organization may have to entertain multiple audit requests from its customers and their respective auditors. Multiple visits from user auditors can place a strain on the service organization's resources. A Service Auditor's Report ensures that all user organizations and their auditors have access to the same information and in many cases, this will satisfy the user auditor's requirements.

Benefits to the customers
ISAE 3402 engagements are generally performed by control-oriented professionals who have experience in accounting, auditing, and information security. A ISAE 3402 engagement allows a service organization to have its control policies and procedures evaluated and tested (in the case of a Type II engagement) by an independent party. Very often this process results in the identification of opportunities for improvements in many operational areas.

User organizations that obtain a Service Auditor's Report from their service organization(s) receive valuable information regarding the service organization's controls and the effectiveness of those controls. The user organization receives a detailed description of the service organization's controls and an independent assessment of whether the controls were placed in operation, suitably designed, and operating effectively (in the case of a Type II report).

User organizations should provide a Service Auditor's Report to their auditors. This will greatly assist the user auditor in planning the audit of the user organization's financial statements. Without a Service Auditor's Report, the user organization would likely have to incur additional costs in sending their auditors to the service organization to perform their procedures.

Appendix 2: ISO 27001

The International Standards Organization (ISO) 27001:2022 was issued to Xledger in October 2023 by DNV GL and is valid until October 2026.

ISO 27001 (referred to as 'the standard' or 'ISO' in this article) is an information security standard, part of the larger ISO27000 family of standards, which provide best practice advice and guidance on the implementation and maintenance of an information security management systems (ISMS). An ISMS is a risk-based methodology for businesses to apply to protect the confidentiality, availability, and integrity (CIA) of its information assets and systems.

Implementing ISO 27001 demonstrate commitments to Information Security Management towards our customers. It shows that Xledger invest time and resources to have this certification and in our work with security. It provides us with a trusted framework to use in our Security Management work. It is an international standard that are known among our customers and shows our compliance towards customers' demands regarding security.

Verified and issued by a renowned third-party shows our continual improvements in our security work through systematically processes. To keep the certification, we must show continuous improvements in our security work.

Appendix 3: GDPR

Data protection in Xledger

Xledger shall meet the requirements for security measures as stipulated under applicable law, including (for so long as it has legal effect) GDPR, article 32 on Security of processing. The Customer shall use planned and systematic measures to ensure satisfactory data security with regard to confidentiality, integrity and accessibility. Xledger will report to the Customer all discrepancies in accordance with applicable law, including GDPR (for so long as it has legal effect). The Customer is responsible for reporting any discrepancies to the relevant supervisory authority and/or affected data subjects.

Customer requirements

Xledger customers are Data Controllers and the primary responsible subject to the GDPR regulation and need to consider what they need to do to be compliant with GDPR. For so long as Xledger is processing personal data on the Customer's behalf in a capacity as data processor, the Customer will:
a) be the data controller;
b) be responsible for inputting the personal data that it provides to Xledger for processing from time to time (inclusive of details about any special categories of personal data);
c) ensure that it has secured all necessary appropriate consents, registrations and notifications as may be required to enable the lawful transfer of the personal data to Xledger, and in order for Xledger to process such personal data to the extent required for, and for the duration of provision of services to the Customer under the terms of the agreement;
d) provide Xledger with documented instructions where necessary for processing of the personal data.

Xledger as a data processor/sub data processor will ensure compliance of the system as such and for the data that are in the basic system setup. However, we do not know or control what kind of data/data structures our customers put into Xledger.

The GDPR requirements does not overrule other legal requirements that customers have for storing necessary information related to accounting and payroll and related governmental reporting requirements.