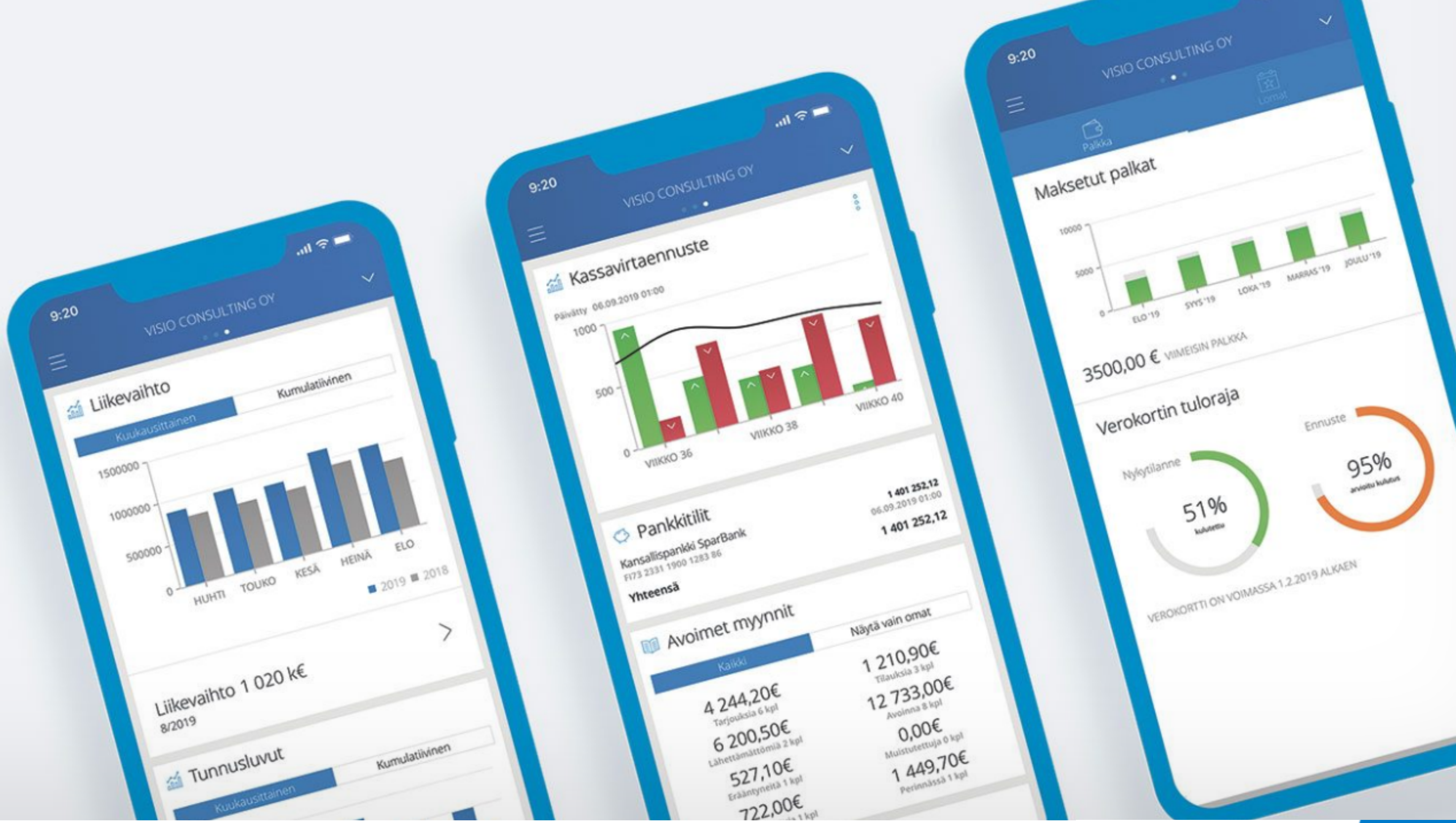

Netvisor Service technology and security statement

Updated on 26.10.2023

Table of contents

For the Reader

Netvisor is a financial management system produced using the SaaS (Software as a Service) model. Visma Solutions Oy owns the service and is responsible for providing the service. Visma Solutions Oy is part of the Visma Group and therefore Netvisor, like other Visma services, complies with Visma's general data security and data protection regulations.

This document describes the technical implementation of the Netvisor service. In addition, the document shows how information security and data protection have been implemented in Netvisor. At the end of the document there is also a section that discusses the most common questions regarding the technology of the Netvisor service and the answers to them. The document also contains several links to sites that provide additional information, both on Netvisor's own support pages and on other Visma sites.

The latest version of this document can be found at https://netvisor.fi/tietoturva and at the link “Security” at the bottom of Netvisor's https://netvisor.fi/ pages.

1. Technical implementation of Netvisor

Netvisor (hereinafter referred to as “Service”) is a browser-based web service.

Our goal is to be available 24/7. Exceptions to this are pre-planned service windows requiring downtime, which we inform in advance in the Visma Solutions Community's announcements, as well as urgent maintenance operations that ensure the security and performance of the service.

Visma Solutions Oy uses subcontractors to provide the service. The service's data center and continuity services are mostly provided by our technology partner Elisa Oyj. Elisa Corporation's data centers are located in Finland and are certified with ISO27001 certification. Part of the service is provided by Amazon Web Services and Microsoft Azure cloud service providers, on which we store customer data in European Availability Areas. A comprehensive list of service providers and subcontractors used to provide the service is documented in Visma Solutions' privacy policy.

1.1. Netvisor architecture

Netvisor has technically been implemented as a web service since the beginning of its history. The service is mainly implemented using Microsoft technologies and using the current industry standards and recommended practices.

Netvisor's service architecture is built to be scalable, that is, the service utilizes multiple application and database servers, and traffic to these is distributed via a load balancer. In the design of the service, fault tolerance has been taken into account, so that the functionality can be maintained even in the event of disturbances. The systems in production use are physically duplicated. Netvisor's production environment is protected on multiple levels; all traffic to the service is filtered multiple times, including but not limited to the firewall, load balancer and volumetric protection against denial of service attacks.

1.2. Kirjautuminen Netvisoriin

The Netvisor user account is personal and the user is responsible for the actions taken in the service using their own account. Login to the Netvisor service is always done with strong 2FA authentication. The available logon methods are:

- Netvisor mobile app
- Open ID authentication with personal banking credentials or mobile authentication
- Signicat authentication with Estonian ID card or Swedish or Norwegian BankID

Access to the service is not possible with just a username-password combination. It is possible to access individual parts of the service via a direct link, through which a one-time identification code is sent to the user by SMS when accessing the service. However, only predefined actions (such as fact-checking invoices) can be carried out in the service.

1.3. Integrations

The Netvisor service is bundled with a number of third-party services that provide users with additional features such as automations. Some connections are built into Netvisor with their traffic, performance and security monitored by Netvisor. Such connections include, for example:

- Web Service connections to the largest Finnish banks
- Connections to public services, e.g. income register
- Connections to print and scan services and e-invoicing operator

In addition to built-in integrations, Netvisor spans a Web Service API available to integration partners allowing third-party software to be connected to the system. Ready-made integrations can be found in the Netvisor Marketplace. All integration partners are validated by Netvisor, interface traffic is monitored and secured, and authentication is multi-layered. Each external integration is individually connectable to our customers and the customer user authorizes their operation with their own user account. It is also possible to limit the access of integration partners on a per-resource basis.

2. Netvisor Security

Netvisor's security is based on Visma Group's own security program (Visma Security Program), which is mandatory for all Visma products. Netvisor's security is divided into technical and administrative security. As an essential part of the operation and security of the service, we also adopt Visma's application delivery model (Visma Cloud Delivery Model), which ensures high standardization and efficient operation of the systems.

2.1. Technical Information Security

There are three levels of responsibility for technical information security. Netvisor's specialized product development teams are responsible for parts of the service and its operation. A separate platform team responsible for the platform of the service in collaboration with its technology partners. In addition, the overall security of the service is supported by specialized security teams under the Visma Security Operations Centre, responsible for, among other things, mapping the general security environment and preventive monitoring.

Netvisor's technical security is built in layers and different areas of information security have been taken into account using generally recommended practices. Secure communication between users and Netvisor as well as within the service complies with the following principles, for example:

- Data is always encrypted in transit
- Access control in the system is based on multi-layer authentication and access roles (RBAC)
- The network infrastructure of the server environment is built in accordance with industry best practices and security standards

As part of Netvisor's technical information security, a comprehensive security and audit log is exported from the service to a separate Visma Security Operations Center log source (SIEM, Security Information and Event Management). The log is analyzed both manually and based on artificial intelligence to detect possible anomalies. No personal data is provided to the log source and the analysis is carried out only to ensure the security of the service.

Software used in server environments (operating system, antivirus software, other software needed to provide the service) is regularly updated and any security vulnerabilities in this software are promptly responded to. At the application level, the Netvisor service is developed with security as the first priority, taking into account, among other things, the OWASP top 10 threats.

2.2. Administrative Information Security

The administrative security of the Netvisor service is based on Visma Group's own security program, which is mandatory for all Visma products. Visma's information security program includes continuous security metrics, internal security audits, and regular audits of administrative processes. These components consist of a dedicated Security Maturity Index for each Visma product, which provides a real-time view of the security level of each Visma product. Visma's security software has ISO27001 certification. More information about Visma's security program can be found at the Visma Trust Centre.

Visma Solutions' administrative security is based on Visma Group's data security regulations and complies with Visma's data security program. All Visma employees are required to regularly complete the Group's information security and data protection training. Confidentiality agreements have been signed with all Visma employees and partners.

Visma has a group-level Responsible Disclosure program, through which anyone can confidentially communicate to Visma information about a potential vulnerability in any Visma product or service.

3. Maintenance and control of the service

Netvisor is maintained by Netvisor's Product Development Unit, which has several teams. The infrastructure of the service is handled by a dedicated team that takes care of the availability of the Netvisor service, the security of the service infrastructure and the scalability of the solution. Netvisor's product development teams are responsible for developing and updating the Netvisor service functionalities.

3.1. Service monitoring

The supervision of the service is carried out by the entire Netvisor product development unit, depending on the area of specialization. In addition, the continuity of the service is ensured by a virtual monitoring team, which is responsible for the implementation of monitoring and troubleshooting outside office hours.

3.2. Service performance

The performance of Netvisor for the user is based on many different factors, including the speed of the user's own internet connection, the performance of the client's own hardware and the performance of the service's server environments. As with all online services, the customer's usage patterns are important for the speed of the system — for example, by limiting the size of the reports to be retrieved, the service processes requests faster. The system is optimized to guarantee a good customer experience for a wide user base and we do not prioritize or limit the normal use of the service per customer or operator.

As a rule, all page downloads on Netvisor occur on average in less than 0.8 seconds. However, for individual operations, the system may be slower if there is an exceptional amount of data to be loaded on the page compared to the average amount of data for companies, or when there is a simultaneous anomalous use in the corporate environment (for example, unusually heavy integration usage or load caused by a robotic process automation). In the event of a significant and long-term slowdown in a basic function, the customer should contact customer service to resolve the root cause of the problem. This can be, for example, scheduling integrations outside office hours.

3.3. Updates to Netvisor

Netvisor is a SaaS service used on an Internet browser, so customers themselves do not have to worry about updating the software to a new version. The new features of the Netvisor service are automatically available to customers and there is no separate cost for updates. Updates to Netvisor are made at least once a week with backwards compatibility and primarily without interruptions. Maintenance breaks requiring service outages are allocated to the weekend of the third full week of each month. Urgent security or troubleshooting updates may be executed daily. Updates and fixes will be announced in the weekly update bulletin.

3.4. Backup and data recovery

We implement the 3-2-2 principle when it comes to backing up Netvisor databases. Our customers' data is backed up incrementally to the primary assurance system at least once an hour and from there to the secondary assurance system once a day. There are at least three instances of data at all times; local backups are duplicated, and secondary backups are performed both physically & geographically to different locations and to different media. In addition, we implement an additional offsite backup once a week to a cloud-based location [f].

In the event of recovery due to for example data loss or corruption, the loss of data is a minimum of five minutes and a maximum of a week, depending on the following factors:

- when and how the failure situation arose
- how much time has elapsed since the event was discovered
- how widely the failure situation also affects tiered assurance systems

In a normal situation, if the effect is only on active data, we can make a recovery in the interval of 5min — 1h. If there is a need to restore the data to a time other than the previous backup situation, the possibility of recovery should always be assessed on a case-by-case basis. Please note that we do not recover data at the request of the customer, but only to guarantee the operations of the service and to secure customer data in case of disruption. We always execute the recovery on a case-by-case basis to the best of our ability.

4. Data protection

Visma complies with applicable data protection legislation and local recommendations in all its operations. In Visma Group, data protection responsibilities are shared between Visma Group and local Visma companies so that Visma Group is generally responsible for Visma's data protection processes and group-level data protection. The local Visma company is responsible for data protection in relation to the services provided by its own company. The Data Protection Officer of Visma Solutions Oy is Head of Data Protection and Data Protection Riku Tarkiainen. The email address of Visma Solutions' data protection officer is privacy.solutions@visma.com. Visma cooperates with local data protection and data security authorities on data protection issues. More information about Visma's data protection work can be found at https://www.visma.com/trust-centre .

Visma Group's privacy statement can be found at https://www.visma.com/privacy-statement . The website contains information in accordance with the GDPR on how Visma processes personal data both as controller and processor of personal data, as well as information on the rights of data subjects.

Visma Solutions has its own privacy website https://privacy.vismasolutions.com/ , which contains information about all Visma Solutions products (incl. Netvisor). On this site you will find an up-to-date list of subcontractors used to provide the Netvisor service. The same page also explains how Visma Solutions processes personal data in the role of both data controller and data processor in relation to our products and services.

Attached to the Netvisor Terms of Service is the Data Protection appendix, which acts as a Data Protection Agreement (DPA). This appendix defines the obligations under the GDPR for both the provider of the service and the customer and describes how the use of subcontractors has been implemented. The latest Netvisor Service Agreement and Terms of Service can be found at https://netvisor.fi/yhteystiedot/netvisor-kayttoehdot/ .

5. Frequently Asked Questions

Question: How is the login to Netvisor done in practice, are the passwords protected?
Answer: Authentication with username and password is not possible, but the login is always done with a strong 2FA authentication instead.

* * *

Question: Can I use SSO or Azure AD implementations to login to Netvisor?
Answer: No. The login methods used are described in section 1.2 of this document.

* * *

Question: When the access to Netvisor is allowed from any location and device, how do you ensure security?
Answer: The use of the Netvisor service is safe because the login to the service is always through strong authentication and the connection to the service always uses encrypted data transfer. If the customer organization has a special need to restrict access to Netvisor only from certain IP addresses, this functionality can be activated for the customer's environment through the Netvisor customer service.

* * *

Question: Can a Netvisor customer planning a software exchange receive the data stored in the service as a "database dump"?
Answer: We do not hand over customer data as a database dump. Netvisor's data export service allows you to download the materials that the company must keep for the period specified by law.

* * *

Question: Netvisor pages load slowly, not at all, or errors occur when using the service. What should I do?
Answer: If you experience problems using the service, we recommend first to check the functionality of your internet connection and hardware. Various business network settings may also affect Netvisor's user experience if the site is used, for example, in office environments.

* * *

Question: Is Netvisor performing automated security scanning with some tools? Can the client company itself perform such a scan on the Netvisor service using an automated tool?

Answer: Netvisor, like other Visma services, is regularly scanned with many security scanners by the Visma Product Security team. Any findings will be corrected by Netvisor's product development team on a prioritized basis. However, due to the nature of the service (a cloud service common to all), we are not able to give our customer companies permission to carry out their own security scans against the Netvisor service at this time. If you have a special need for a separate security audit of Netvisor, please contact Netvisor customer service.

* * *

Question: How are liability questions defined in a situation where the availability or performance of the Netvisor service has been degraded?

Answer: Netvisor does not have any general SLA promises or reimbursements based on them. Compensation matters are handled on a case-by-case basis and in accordance with Netvisor's general terms and conditions.

* * *

Question: How can a Netvisor customer track events in the service? How can log data be accessed if a customer needs to analyze a transaction?

Answer: Some of the transactions are logged so that customers can see the transactions and their authors directly in Netvisor. In addition to the information that is visible in Netvisor, log information about the events of the service is made available only to the Netvisor platform team. This information can be used in situations where a request has been issued by a public authority. Information has been disclosed, for example, on the basis of a tax audit or a criminal investigation. Requests are submitted to the product development team via Netvisor customer service.

Question: A third party requires separate clearance or certification from us in relation to Netvisor's operations. Can we conduct an audit of the service for its intended purpose?

Answer: The technology and security programs implemented by Visma Group are designed according to industry standards and modern requirements and cover the needs of even our most demanding customers. We rely on the coverage of the programmes and do not carry out external audits as a matter of principle. We recommend that you familiarize yourself with the content of the programs at Visma Trust Center to ensure that you also have coverage for your own needs.

* * *

6. Additional information

Further information regarding Visma and Netvisor's data security and data protection can be found at the following links:

Visma Trust Centre:
https://www.visma.com/trust-centre/

Visma Privacy Statement:
https://www.visma.com/privacy-statement/

Visma Solutions' privacy website:
https://privacy.vismasolutions.com/

Netvisor Terms and Conditions of Use:
https://netvisor.fi/yhteystiedot/netvisor-kayttoehdot/

Netvisor releases in Visma Community:
https://community.visma.com/t5/Netvisor-uutiset/bg-p/fi_sl_Netvisor_Uutiset/label-name/julkaisutiedotteet

Important announcements from Netvisor in Visma Community:
https://community.visma.com/t5/Tarkeat-tiedotteet/bg-p/fi_sl_tarkeat_tiedotteet

Netvisor Support Site:
https://support.netvisor.fi/

Netvisor Contact Information:
https://netvisor.fi/yhteystiedot/

Visma Solutions Data Protection Officer Email:
privacy.solutions@visma.com

VISMA