NEPTON SERVICE DESCRIPTION, SERVICE PRODUCTION, DPA AND OTHER TERMS

4.4.2024

Saarni Nepton Oy • Hatsinanpuisto 8, 02600 Espoo • support@nepton.com

Table of contents

1 Service description

1.1 General

Nepton is a comprehensive HR, worktime management, shift planning and payroll solution.

The service can be used with any device that has a modern browser. It does not depend on the operating system and no other software is required to access it.

Different entry terminals can be connected to Nepton. Entry terminals can be used for entering working time or lunch data.

Different payroll, personnel management and enterprise resource planning systems can be connected to Nepton. The customer can connect other systems to the service by utilising the service's interface connection (API).

The service provider is the company with whom the service contract was made.

1.1.1 Service modules and service levels

The customer's Nepton access right includes the use of the modules defined in the contract. Some of the modules are available at multiple service levels. The modules defined in the contract must always include the HR module at some service level.

HR – module contains

	Easy HR	Pro HR	Complete HR
Updating of own personal information	X	X	X
Viewing of own work relationship information	X	X	X
Custom permissions	X	X	X
Standard reports	X	X	X
Standard integrations for other solutions	X	X	X
Fixed person- and work relationship information	X		
Custom person- and work relationship information		X	X
Competence management and attaching competence to persons		X	X
Limited storage (5 files / person) for saving documents (work contracts, testimonials, certificates, etc)		X	
Unlimited storage (5 files / person) for saving documents (work contracts, testimonials, certificates, etc) *			X
Online forms (work contracts, development discussions, other forms)			X

*) Service includes normal usage. Normal usage does not cover using the service for other purposes than described in this service description.

Worktime management – module contains

	Easy Worktime	Pro Worktime	Complete Worktime
Managing own work and absence registrations	X	X	X
Worktime calculations that cover worktime law requirements	X	X	X
Possibility to automate work time calculations for person groups based on worktime law, union agreements or local agreements.	X	X	X
Standard reporting on work time calculations	X	X	X
Flexitime, worktime bank and overtime accruals	X	X	X
Possibility to create standard integrations	X	X	X
Worktime targeting to projects, cost centres, customers, etc		X	X
Holiday and absence accruals		X	X
Holiday and absence planning and reporting		X	X
Travel and expense registration and approval			X
Automatic calculation of allowances on travel registration			X
Unlimited storage for documents and images on events *			X

*) Service includes normal usage. Normal usage does not cover using the service for other purposes than described in this service description.

Shift planning – module contains

	Easy Shift planning	Pro Shift planning	Complete Shift planning
Shift planning and making lists public	X	X	X
Pre-planned absences and holidays	X	X	X
Shift planning for tasks	X	X	X
Communication of planned shifts	X	X	X
Shift list and levelling period calculation	X	X	X
Standard reporting of shifts	X	X	X
Competence requirements in planning and shift picking by employees		X	X
Shift picking by the employees		X	X
Shift calendars (schemas)			X

1.1.2 Basic service features

The following features are available to all customers:

- Service can be used on all kinds of devices
- Customer can enable single sign-on (SSO)
- User can synchronise events recorded with their own calendars (Outlook, Google, etc.)
- Nepton terminals can also be used as canteen terminal
- Customer can implement various integrations using the service's interface (API)
- Customer can schedule various data transfers (HR, payroll, invoicing, ERP, switchboard, etc.)

1.1.3 Single sign-on

Nepton supports several different single sign-on (SSO) methods. This means that users do not have to enter separate passwords into the service.

The service supports Google and Microsoft (Entra ID and M365) logins.

The service supports standard SAML 2.0 identity providers. Related SSO certificate is owned by the customer. For security reasons, the certificate typically needs to be renewed every few years. Provider tracks pending renewals and will request customer contact person to perform any necessary renewals before current certificate expires.

1.1.4 Integrations and interfaces

Integrations can be implemented using an interface connection (API), scheduled file transfer (SFTP) or manual file upload. The most appropriate method is always agreed upon together with the customer. Interface connections (API) enable real-time integrations with other information systems.

Integrations and interfaces are described in the Nepton support service. The service provider can assist in implementing desired integrations on standard commercial terms.

1.1.5 Supported browsers

The service works on modern browsers. Saarni Nepton does active development for new browser versions so that the service will always work as well and as fast as possible.

To get the best experience from the service and to maintain your security, you should use modern, actively maintained and developed browsers with the latest product version.

Saarni Nepton tracks the service usability specially across these browsers:

- Apple Safari
- Google Chrome
- Microsoft Edge

- Mozilla Firefox
- Opera

The service does not support Internet Explorer. Usage of Internet Explorer is not recommended.

The service does not use Flash or Java applets.

1.1.6 Updates, maintenance, and availability

Below are the typical times in Finnish time (UTC + 2 / UTC + 3 during summertime), when the service's routine maintenance procedures are performed. We recommend that scheduled activities are not placed during these periods. After some updates, it is possible that the users need to login to the service again. Please note that all integrations will be paused approximately 15 minutes before the scheduled maintenance window.

- **Quarterly release 03:00 - 05:30**
  Significant feature changes and longer maintenance jobs. Informed at least two weeks in advance.
- **Weekly patches 13:00 - 13:30**
  Weekly patches, fixes, minor changes, and maintenance jobs. Performed on Thursdays and possibly other days if critically needed. Thursday's release is informed at least 24 hours in advance.
- **Security updates 22:00 - 24:00**
  Monthly, weekly, and daily as necessary.

Critical data security updates can also be installed outside standard maintenance windows.

The service and its components are updated regularly and as needed. All updates are automated. Every new version can only be released after it has passed several automated tests. This enables continuous improvement of quality and functionality.

The availability objective of the service (outside maintenance windows) is 99.8%. Availability is measured from several outside measuring points at least 100,000 times a month.

Service availability target is defined in attachment SLA normal.pdf.

1.1.7 Data retainment service

Customer can at the service termination order a data retainment service. This enables the administrative login credentials to be kept active and customer data to be retained, but data modifications are not allowed. Data retainment service is invoiced separately and can be agreed for a fixed period.

1.2 Service production

The provider is not responsible for the customer's computers, devices, systems and telecommunications operation or information security.

1.2.1 Support and main user training

The provider offers an electronic support service, where the customer can get familiar with service instructions and features of the service. The support service is updated when service changes or extensions are made.

The support service is available on https://support.nepton.com/hc/en-gb

1.2.2 Customer communications

The customer is informed about changes and extensions to the service in the support service, or with letters. The customer must name the contact persons to whom the announcements will be sent.

In urgent situations, the parties named by the customer are informed by email or phone. Information is also provided outside the support service's opening hours if necessary.

1.3 Saarni Nepton data protection

1.3.1 Immaterial rights

Immaterial rights to the service will not be transferred to the customer.

The customer has ownership of the data they have added to the service, the customer-specific data added to the service on behalf of the customer, and data inferred from these.

The provider can use the data stored by the customer in the service to provide the service to the customer. The provider's employees process the data stored by the customer in the service only at the customer's request.

Saarni Nepton can anonymise the data stored by the customer in the service and use the data for developing the service, artificial intelligence training or statistical purposes.

1.3.2 Trusted service and other sub-processors

Trusted services are part of Nepton, and they are visible in the top-level navigation. Users have access to free lite versions of trusted services as part of Nepton.

The provider may transfer customer data to sub-processors if this is necessary for the functionality and development of the Nepton service. Personal data may also be included in these transfers. Only necessary data is transferred or processed by sub-processors. The provider is responsible for ensuring the realisation of information security and data protection with regards to the sub-processors. There is always a valid data protection agreement in place between the provider and the sub-processors.

Trusted services and other sub-processors handling personal data are listed on the https://support.nepton.com/hc/en/articles/360018646578 page. The person responsible for customer's data protection must register to Nepton support service and subscribe to this article (FOLLOW), so that she or he will receive notifications when a new version of this article (including changes to sub-processors) is published. Changes related to data protection and sub-processors will also be communicated in advance using other communication channels.

1.3.3 Principles of information management

The customer or the entity authorised by them saves the customer selected personal data to the service. Such data can include e.g. name, address, e-mail address, phone number, bank account number, ID number in the organisation, social security number, tax number, details of next of kin, title, employment information, salary, roles, identities of supervisors and subordinates, cost centre, the person's identification data in other systems, competence profiles, shift plans, sickness absences, annual holidays, work event stamps with comments, travel invoices, project allocations and other information that the customer needs to manage employment relationships and to fulfil their employer obligations. The customer or an entity authorised by them can also define new data fields.

Local legislation determines how long an employee's personal data must be kept after termination of employment.

The service does not automatically delete data stored by the customer or employees. The customer must delete, pseudonymise or anonymise such personal data for which there are no reasons for being kept. The service records personal data changes, deletions, pseudonymisations and anonymisations to a change log, which is kept for 12 months.

When the use of the service is ended, the customer can at the service termination order a data retainment service. This enables the administrative login credentials to be kept active and customer data to be retained, but data modifications are not allowed.

The customer has the right to request an independent copy of their own data. The method will be agreed together with the customer. The provider can charge for the work according to the price list or the contract.

The customer's data will be deleted after the end of the contract.

1.3.4 Data transfers to other systems

The service allows the customer to transfer data to other systems or receive data from other systems. The customer can order data transfer implementations from the provider. The provider gives technical support in matters related to data transfers.

The customer manages the data transfer credentials. The provider is not responsible for actions made with these credentials. The provider is not a party to the customer's contracts with third-party system suppliers.

1.3.5 Network identification data

Customer authorises Saarni Nepton to collect network identification data of users. This network identification data is collected to ensure service quality, prevent service abuse, and support forensics. The collected data (IP addresses and timestamps) can be stored for up to two years from collection.

1.4 Saarni Nepton information security

Saarni Nepton reviews and defines the security objectives of the service annually. The defined objectives are to ensure the integrity, continuity, usability, confidentiality, and sustainability of the service under all circumstances.

The information security management team implements and develops security according to the defined information security policy and the requirements of CSA CCM, ISO 27001, KATAKRI, OWASP, and VAHTI. In this regard, the provider has processes for quality management, risk management, continuity management, incident management, and crisis management, among others.

The development of security thinking is promoted at all levels and in all roles in the organisation. Regular security trainings are mandatory for all employees.

Several customers can use the service simultaneously. Security and data protection are central design principles of the service. The visibility of information and who has access to which functions is implemented through role-based access control and centralised security management. Technical separation of information is implemented at the application level.

Only designated individuals have access to the customer’s environment and information. The provider only reviews the customer’s information to ensure the functionality of the service or at the customer’s request.

The customer can use their own single sign-on in the service. Other login methods can be turned off. Logging into the service starts a user session. If the user is inactive in the service for a long time, the session will be terminated.

The service has different environments for development, testing, and production. The service and its parts are updated regularly and when needed. A new version must pass several automated tests before it can be deployed.

The security of the service is protected and monitored continuously. Methods used include firewalls, network segmentation, MFA, EDR, and various security scanners.

The service collects data about user activities. Part of the data is stored permanently, and logs are stored temporarily. Changes made are saved in the service. The customer's administrator can view basic log and change history in the service.

The service is produced, and customer data is processed only in EU/EEA countries. The provider can change data centre, telecommunications, and other operators. The provider ensures that operator change will not decrease security level of the service.

1.4.1 Data centre

The service is provided from a data centre based in Finland. The electricity used is renewable and carbon neutral. The data centre heats 25,000 households and thus decreases society's carbon dioxide emissions by 100,000 tons per year.

The data centre equipment and power inputs are duplicated in case of failures.
If necessary, the data centre can operate several days without external power supply with backup power generators.

Data centre design principles:

- TIER III EN 50600
- VAHTI
- ST III KATAKRI
- PUE < 1,2

Data centre standards and certifications:

- Energy Efficiency System (EES+)
- ISO 9001 Quality Management (for B2B services)
- ISO 14001 Environmental Management System
- ISO 22301 Business Continuity Management
- LEED Datacentre V4.0
- OHSAS 18001 Occupational Health and Safety Assessment Series
- PCI DSS (Payment Card Industry Data Security Standard)
- SOC 2 (Service Organisation Control report type II)

1.4.2 Private cloud

The service is produced from a private cloud managed by Saarni Nepton. Stored data is protected by strong encryption. The service can be transferred to other physical devices and to another location without interruption to the service availability.

1.4.3 Telecommunication

The data communication of the service is protected by encryption. Internal connections of the data centre are duplicated. There are four separate fibre connections from the data centre outward.

There are several networks inside the service for different purposes. Saarni Nepton can monitor network traffic and detect anomalies.

1.4.4 Backups

Saarni Nepton backs up the service and its data several times a day. All backups are kept for at least two weeks. Individual weekly backups are kept for at least eight weeks. Backups are encrypted and stored to several data centres. The integrity and immutability of backups are continuously monitored.

1.4.5 Disaster recovery

The provider maintains and develops various plans for exceptional situations. The goal is to prevent exceptional situations and ensure the fastest possible recovery under all circumstances. Various incident scenarios have been considered in the provider's recovery plan. Saarni Nepton has automated the recovery from certain exceptional situations.

If data centre or its most vital core systems are destroyed, the service has a:

- Recovery Point Objective (RPO) is 12 hours
- Recovery Time Objective (RTO) is 48 hours

1.4.6 Logging

Justification for storing logs include investigating technical errors, assisting in digital forensics, and complying with data protection regulation. Logs are stored as long as their storage is estimated to be necessary. Saarni Nepton data protection officer defines the principles for log collection, storage, and processing.

Logs are generated in several places, and they are retained for maximum of 14 months. The logs generated by the application servers are stored for at least two weeks. The logs generated by the service are stored for at least two months.

The customer can view certain logs directly in the service. Other logs can be requested from the provider's support service. Access to systems that collect logs is restricted and access is only granted to specific employees of Saarni Nepton.

2 Modification of contract attachments

If this document is referred to in the contract between the customer and the provider, this document is an attachment to the contract. The provider can unilaterally change the content of this contract attachment. However, the right to change does not apply to the following paragraphs:

- 1.2.1 Immaterial rights
- 2 Modification of contract attachments

The customer will be informed of significant changes to this contract attachment at least three months before the changes take effect. If the content of this contract attachment has been substantially changed to the customer's detriment, the customer has the right to terminate the contract within three months of notification.

If IT ETP, IT EHK or IT YSE contract terms are referred to in the contract between the customer and the provider or in this contract attachment, the provider has the right to update these contract terms to newer versions.

3 Delivery terms

3.1 Deployment

Nepton is a cloud service. The service includes the features that belong to the contractually agreed service level. Implementation does not include changes to the service's features, functionality, or capabilities, unless agreed upon in writing.

Deployment is typically carried out through the following steps:

During the **planning phase**, the customer must provide the requirements definitions and information necessary for this phase. Such information includes e.g. information about other systems to be integrated, technical interface documents, organisational structure, collective agreements, descriptions of working hours, and specifications related to raises, bonuses, vacations, and absences. The customer must approve the specification documents resulting from the design phase, after which the provider can start the implementation phase. The provider and the customer must also agree on both a start date and an end date for the acceptance testing.

In the **implementation phase**, the provider implements the service usage methods, settings, calculations, and interfaces according to the specification documents.

In **acceptance testing**, the customer ensures that the service works in accordance with the specification documents. Acceptance testing ends on the agreed date. The provider will correct the deficiencies found in the acceptance testing to conform to the agreed specifications. After this, the service is considered accepted, delivered, and taken into use.

During **production**, the provider offers training, customer support and advice to the customer’s main users. The provider's training catalogue includes various learning paths that offer the customer's employees the opportunity to acquire Nepton certifications as a sign of expertise in using the service. All main users must complete at least Nepton silver level training. The service fee includes support for trained main users in matters related to the use of the service, security, calculation, and error messages.

The charge of service fees begins in accordance with the contract or on a jointly determined date, however, at the latest at the start of production use.

The customer can postpone the start of production use to a later date than planned or agree on certain subset to be deployed after the start of production. However, this has no effect on the agreed start of service fees.

Requirements that have not been documented in the planning phase are change requests. Change requests are handled through change management. Agreed changes are scheduled and priced separately. Changes do not affect deployment acceptance testing or schedules, nor do they prevent the delivery acceptance or the start of service fees.

3.2 Entry terminals

Different entry terminals can be connected to the service. These terminals can be used for entering working time or lunch data.

The terminal comes with a wall mount, power cord and installation instructions. The customer is responsible for the cabling (electricity and network connection), the installation of the device in place, the costs related to the installation, and that the cabling and connections have been made in accordance with official requirements. A separately priced installation service offered by Nepton partners is available.

For terminals, a contract is in force for a fixed period of 36 (thirty-six) months, after which the contract continues as part of service contract. The provider or its subcontractor owns the terminals. The customer has the right to use the terminals and related software. At the end of the service contract, the customer is obliged to return the terminals to the provider.

If there is a fault in the terminal, the customer is obliged to deliver the faulty terminal to the provider. The customer is responsible for the delivery cost to the provider. The provider will repair or deliver a replacement terminal in similar condition within the next 5 (five) business days (Mon-Fri).

If it is determined that the fault was caused by, for example, vandalism, fire, faults or breakdowns caused by air conditioning, electricity or lightning, moisture damage or other similar reason, altered usage conditions or using the terminal in a way that is not appropriate, the repair costs of the terminal or the costs of an equivalent new terminal will be charged to the customer.

The provider has the right to deliver the customer a new terminal when, for example the provider's terminal model has been changed. The customer is responsible for returning the old terminal to the provider and the costs incurred by this.

The provider is responsible for the data security and operation of the terminals.

3.3 Managed service

The customer can order an additional managed service to ensure smooth Nepton use in a developing and changing work environment. The managed service includes making minor changes requested by the customer in relation to personal data, work time records, project list, roles, rights, person groups, offices, calculation rules, calculation groups, interface rules and other settings. The managed service does not include extensive changes, for example when the organisational structure changes or the salary system changes.

Requests from managed service customers are by default handled as high priority requests. The customer can for an individual change request suggest alternative priority. The customer appoints individuals who have the right to make managed service change requests.

The managed service includes:

Persons

- Adding persons
- Removing persons
- Personal data changes
- Employee role changes
- Employee setting group changes
- Employee person group changes
- Employee supervisor changes
- Employee unit changes
- Employee default project changes

Work time

- Accrual changes (balance and bank)
- Annual holiday balance changes
- Work time shortening leave changes
- Work obligation changes
- Person group changes and additions
- Role changes and additions
- Small-scale setting group changes and additions

Work shift planning

- Additions and changes to planning models (shift schedule and levelling period models)
- Unit changes
- Location changes and additions
- Shift template changes and additions
- Task management

Integrations

- Scheduling changes
- Parameter changes to integrations (for example salary code changes)

The managed service is ordered when the service contract is concluded or after the start of production use. The managed service is charged with other recurring charges. The customer can terminate the managed service, if the customer's main user has completed at least the Nepton silver level certification. Change requests that are not covered by the managed service are agreed upon and invoiced separately.

3.4 Change requests

The customer can order changes to the Nepton service. These may include, for example, changes to personal data, work time records, project list, roles, rights, personnel groups, locations, calculation rules, calculation groups, interface rules and other settings. Changes will be charged according to the provider's valid price list.

If the customer uses the provider's managed service, minor changes are included in the price of the service.

3.5 Main user trainings and certifications

The provider's training catalogue includes various learning paths that offer the customer's employees the opportunity to acquire Nepton certifications as a sign of expertise in using the service. All main users must complete at least Nepton silver level training.

3.6 Other services

Customer can use the following paid services:

- **Separate test environment** enables testing of changes in advance
- **Increased SLA** includes SLA conditions that are broader than normal
- **SFTP server** enables the implementation of integrations using scheduled transfer files

The provider assists with taking these services into use according to pricelist or to its price list or a separately agreed project contract.

3.7 Support service availability

The electronic support service is always available.

For trained customer main users, specialist support is available by email and phone on weekdays between 8 AM - 4 PM (UTC+2 / UTC+3 during DST). Support requests can be sent at any time via the support service or email.

Availability of specialist support is presented in the document "SLA normal.pdf".

New versions are announced in the support service or in a customer letter, which inform the customer about the service changes or expansions.

3.8 User rights

Every person who uses the service, or whose data is processed in the service, needs a user right. The customer and provider agree on the number of user rights and document this in the service contract.

The provider monitors the adequacy of user rights. If the number of user rights is exceeded, the provider may charge for the excess according to the unit price. The charge for exceeding user rights applies to those past periods that have been charged with an insufficient number

of user rights. The provider has the right to change the chargeable user rights for future billing periods to correspond to the actual usage.

If the customer's need for user rights varies seasonally, this can be considered at the customer's request. For example, if the customer needs 100 user rights in the summer season and 50 user rights in the winter season, the customer will be invoiced for 75 user rights annually.

3.9 Invoicing

The invoicing principles and payment terms are determined by the service contract, project contract or order confirmation.

The service fee is based on selected modules, service levels and the number of required user rights. The user rights of each module and service level are charged according to the agreed unit price.

If the customer has exceeded the number of user rights, and the excess is more than 5 %, the provider can charge the excess. However, the provider cannot charge excesses older than 24 months.

3.10 Termination

The conditions for terminating the service contract are specified in the service contract or in the order confirmation. A fixed-term contract cannot be terminated in the middle of the contract period.

3.11 Other terms

The provider has the right to mention the customer as a reference in accordance with the service contract, project contract or order confirmation.

If the customer intends to use the service for less than the number of user rights, the customer must notify the provider of this at least 30 days before the start of the next billing cycle.

The customer can audit the service or the source code of the service. The source code audit is performed under the guidance of the provider's employees. The customer is responsible for the costs related to the audit.

4 Data processing agreement (DPA)

The parties to this data processing agreement are:

(1) **Saarni Nepton Oy**, a company registered and operating in Finland, with a registered office at Hatsinanpuisto 8, 02600 Espoo, Finland, business ID FI16206791 (hereinafter "Provider" or "Processor")

(2) **The customer** who has entered into a commercial contract with the provider (hereinafter "Customer" or "Controller")

The data processing agreement concerns the processing of personal data carried out based on the commercial contract.

Sections **1.2 Saarni Nepton data protection** and **1.3 Saarni Nepton information security** in this service description are included in this data processing agreement. If there is a conflict between the aforementioned sections and this data processing agreement, this data processing agreement shall apply.

4.1 Contact persons

The parties agree to notify each other of any changes to the data protection contacts.
Contact details of the provider's data protection officer:

Vesa Kivistö
dpo@nepton.com

4.2 Definitions

Commercial contract refers to an agreement between a customer and a provider that enables the customer to use the Nepton service.

Data Protection Regulation refers to the General Data Protection Regulation (679/2016) of the European Union, other applicable data protection provisions, and instructions and orders issued by data protection authorities that affect the controller, data processor, sub-processor, or other sub-processors.

Personal data means any information that can be used to identify a natural person, either directly or indirectly. This includes obvious identifiers like name, phone number, and email address, as well as less obvious ones like location data, online identifiers, and biometric data.

Data subject means an individual who can be identified, directly or indirectly, based on identifying information such as name, personal identification number, location information, or factors related to the person's physical, physiological, genetic, mental, economic, cultural, or social characteristics.

Customer determines the purposes and means of processing personal data. The customer is the data controller or joint data controller under data protection legislation.

Provider processes personal data on behalf of the customer. The provider is a data processor under data protection legislation.

Sub-processor processes personal data on behalf of the provider.

4.3 Processing of personal data

The provider produces the service and processes the customer's data only in the countries within the European Economic Area (EEA). The provider does not transfer the customer's personal data outside these countries without the customer's authorisation.

The provider respects privacy and is committed to protecting personal data and complying with the requirements of the EU Data Protection Regulation. This data processing agreement describes how the provider processes personal data and how data subjects can exercise their rights.

The customer determines the scope and types of personal data to be stored in the service. The customer is responsible for complying with the Data Protection Regulation with respect to data subjects.

The provider processes personal data only to fulfil its commercial and legal obligations under the commercial contract. The provider undertakes to keep personal data confidential and to process personal data only at the customer's request.

For clarity, it is stated that the processing of personal data is subject to section 7 Confidentiality of the IT 2022 YSE contract terms. The provider's employees are regularly trained in information security and data protection, and employees have signed NDA's.

The provider ensures that service and service provisioning to customer are aligned with applicable data protection legislation, including data protection regulation requirements. The provider ensures the confidentiality, integrity, availability and resilience of the processed systems and services.

The provider agrees to:

a) process personal data only in accordance with documented guidelines from the customer, which also applies to transfer of personal data outside the EEA.
b) ensure that service provider's personnel authorised to process personal data are committed to complying with applicable confidentiality and non-disclosure obligations.
c) implement all actions required by article 32 of the Data Protection Regulation (Security of processing).
d) comply with the requirements of the Data Protection Regulation for data processors or sub-processors.
e) considering the nature of the processing operation, assist the customer with appropriate technical and organisational measures in fulfilling the customer's obligation to respond to requests from data subjects.
f) assist the customer to fulfil their obligations and to ensure compliance with Data Protection Regulation articles 32-36.
g) after the termination of the contract, and as decided by the customer, delete or return all personal data in the service to the customer, unless EU regulations or national legislation require the retention of personal data.
h) provide the customer access to all information necessary to demonstrate customer compliance with the controller's data protection requirements.

i) allow and assist the customer or independent third-party auditor in carrying out data protection audits.
j) immediately inform the customer if any guidance or instruction from the controller is deemed to violate the Data Protection Regulation or other data protection provisions of the law.

The provider will promptly notify customer about all suspected or confirmed data security breaches, personal data losses or other situations in which data protection of personal data is deemed to be under threat. The provider grants access to all necessary information about the data security breach and actions which have been taken after the breach. The notification will include at least following information if they are available:

a) The nature of the event
b) The number of registered persons related to the event
c) Descriptions of registered persons and personal data fields related to the event
d) Identified or suspected party that caused the event
e) Identified or suspected parties who have accessed personal data
f) Identified or estimated impact on registered persons, customers, and providers
g) Implemented and planned actions that the provider has taken to limit consequences of the event and to minimise possible damages, to prevent the continuation of the event, and to prevent the recurrence of similar events
h) Other information necessary for the customer

The provider agrees to defend the customer with regards to all lawsuits, claims, administrative penalties, fines, damages, or other repercussions caused by service provider or service provider subcontractor breaking their data protection obligations as defined in this service description or in applicable data protection legislation.

4.4 Built-in and default data protection, Article 25 (2)

Several customers can use the service at the same time. Information security and data protection are central design principles of the service. Information visibility and who can access what functions are realised with the help of role-based access authorisation and centralised security management. The technical differentiation of data is implemented at the application level.

4.5 Data minimisation, Article 25 (1) ja 32 (1)

The provider or service do not automatically delete the data stored by the customer or its employees. The customer must delete, pseudonymise or anonymise such personal data that there is no reason to be kept. The service logs changes, deletions, pseudonymisation and anonymisation of personal data in a change log, which is kept for 12 months.

4.6 Personal data sub-processors, Articles 28 (2) and (4)

The provider can transfer the customer's personal data to sub-processors if this is necessary for the production and development of the Nepton service. Only information necessary for the functionality of the Nepton service is transferred or processed by sub-processors.

The provider is responsible for the implementation of information security and data protection for sub-processors. A separate data processing agreement is always valid between the provider and the sub-processors.

Changes regarding data protection and sub-processors are always announced in advance.

4.7 Confidentiality and integrity, Article 32 (1) (b)

Physical Access Control
Data centres are protected by guards, access control devices, alarm systems and video surveillance. Office premises are also guarded and protected by lobby security, alarm systems and video surveillance at front doors.

Electronic Access Control
All passwords and certificates are under central lifecycle management.

Internal Access Control
Successful and failed logins to the service, and views or changes of personal data are always logged. Only authorised persons have the right to view and change data.

Isolation Control
The service is designed to offer excellent isolation properties. Users have access and visibility only to data and functionalities they have been granted access to according to their role. The isolation is implemented in the logical application layer of the service by utilising service architecture and testing methods suitable for this purpose and by implementing centralised security mechanisms.

Data protection
All traffic in operator networks is encrypted.

4.8 Availability and resilience, Article 32 (1) (b)

The data centre's equipment, network connections and power supplies are duplicated in case of malfunctions. The data centre has internal backup power generators, and if necessary, the data centre can operate for several days without external power supply.

The service is protected by security software, security devices and regularly executed vulnerability scans.

The service and its data are backed up several times a day with parallel procedures. Backups are stored encrypted and duplicated to several different data centres, their integrity is verified, and immutability is monitored.

4.9 Recovery plan, Article 32 (1) (c)

The provider maintains and actively develops various plans for exceptional situations.

The goal is to prevent exceptional situations and ensure recovery as fast as possible in all situations. Identified types of exceptional situations have been considered in the provider's recovery plan. Recovery from certain types of exceptional situations is automated.

4.10 Regular assessment, Articles 25 (1) and 32 (1) (d)

Data protection
The provider's data protection officer is responsible for data protection management, evaluates and, if necessary, modifies policies regularly, and assists with solving possible data protection incidents.

Information security
The provider's information security management determines and prioritises the objectives of information security, the ways to achieve them and oversees their execution based on risk assessment. Information security training materials are updated regularly. Employees are supported in increasing their knowledge of information security. Participation in mandatory trainings is monitored by supervisors and information security management.

Continuity
The provider's continuity management process is based on ISO 22301 practices. The continuity management plan is updated regularly. The provider's management team inspects and approves the continuity management plan.

Risk management
The provider's risk management process is based on ISO 31000 practices. Risks are assessed regularly and as comprehensively as possible. The relevant risks are regularly presented to the management team.

Quality management
The provider's quality management process is a mix of ISO 27001 and the practices that the provider has defined. Observed quality deviations are reported to and processed by quality management. The provider informs the management team of the types and amounts of deviations on a regular basis.