Technical and Organisational Measures (TOMs) and Technical Solution Description

Version 2.1, October 2024

Version approval: Group CTO, General Counsel

Table of Contents

1 Purpose of this document

The purpose of this document is to describe key technical and organisational measures (TOMs) to comply with the requirements resulting from Art. 32 of the General Data Protection Regulation (GDPR) and additionally under Netigate's ISMS 27001 procedures, to ensure the security of personal data and other data inNetigate's services.

1.1 Measures implemented across the group

The TOMs outlined in this document are implemented in all Netigate group companies that develop and provide its software and services. The measures taken fulfil the requirements regarding confidentiality, integrity, availability, risk assessment, review and resilience according to Art. 32 GDPR.

1.2 Summary of measures per Art 32 GDPR

Netigate has – at a minimum – implemented the following measures according to Art. 32 GDPR:

a) access control and access review on least-privilege policy and per customer's instruction.
b) anonymisation functionality is available upon request in the platform
c) data encryption during transfer/transport and at rest.
d) regular, verified backups and restores
e) regular security tests (penetration tests and vulnerability analysis)

2 Product/Service introduction

Netigate and its group companies provide SaaS (Software-as-a-service) services used to collect, analyze and visualize feedback data from Customer's customers or employees. For example, such feedback may come from digital surveys, public sources (e.g. review sites, online stores, app store) or customer's internal systems (e.g. emails from CRM system, calls from call center or chat conversations from chat tool). Netigate also offers functions to create and distribute digital surveys to collect feedback through customer, employee, and market research from a selected or collective group of respondents. REST APIs and a broad selection of integrations allows for automation of workflows. These services are browser,based and available through the public internet.

In addition to the SaaS services, Netigate also provides professional consulting services through a team of in-house consultants skilled within customer experience (CX) and employee experience (EX), who can be hired to help customers design, interpret or apply insights and results from the collected feedback.

3 Risk management

Netigate's services are considered a "normal risk" service. If used only for analyzing data from 3rd party systems, the service does not need personal information to process the data. To distribute surveys through SMS or emails, the service needs respondents contact details. Data delivered to the platform is always controlled by the customer.

Netigate's Information Security Management System (ISMS)is based on and certified for ISO27001. The standard is risk driven using a continuously updated risk list to capture, prioritize and monitor mitigation of identified risks.

All exceptions shall be handled through defined risk in that security risks are reported or detected through monitoring and the resulting risk list is a key driver in Netigate's continuous risk mitigation and elimination work. The risk process is managed by the Netigate's Security team and reviews as part of a monthly security and privacy meeting.

4 Privacy controls

Privacy controls are described in the Netigate group company's privacy policies:

- For analyzing, visualizing and sharing results: https://lumoa.me/en/privacy-policy.
- For collecting feedback: https://www.netigate.net/legal/

5 Resilience

Latest measures on resilience are described in the *Trust Center* section of Netigate's website.

5.1 Change management

Netigate updates the SaaS platform continuously and all updates are made available to all customers. Significant features or changes that are significant are communicated to customers prior to deployment. Netigate uses a well-defined Secure Development Lifecycle (SLDC) including mandatory manual and automated testing as well as OWASP vulnerability scans before release.

5.2 Hardened configuration standard(s)

Configuration hardening is done by default for all environments but also driven using Security monitoring CIS benchmarks for Kubernetes. Azure cloud services has high security rating. Netigate only deploys its service to Azure West Europe (Netherlands, EU)

A majority of servers are automatically managed in Azure Kubernetes Services (AKS). Access to production environment is limited byt the principle of least privilege and only individual, named and identified users can access it Multi-Factor Authentication.

Development, Test, Stage and Production Environments are separated.

5.2.1 Regular, documented validation of configuration

The development and operations team uses an automated tool to perform regular, documented validation of the configuration for all servers and infrastructure changes. Any exceptions to the standard require CTO approval. An end-of-support procedure is in place and considered in risk assessments.

5.3 Vulnerability management

5.3.1 Patching

Netigate patches its core software frameworks as soon as possible when a new long time support (LTS) version is available. We do not take in use beta versions in production but keep with latest LTS version. Patch planning is done along normal development/operations planning process. This process occurs in 2-week sprint cycles where planning meeting starts new sprint.

5.3.1.1 Regular patching

Regular patching of production environment is done continuously for those patches that do not cause any interruptions to system use, patching window for patches that can cause down within maintenance window or communicated planned outage.

Patching of TEST environment needs to be completed minimum 24 hours prior to beginning of patching window for production environment. Acceptance criteria for patching is our automated and manual tests, typically new software version patch is kept in TEST environment for several days minimum before applying the patch to production.

5.3.1.2 Emergency patching

In case of critical vulnerability detected / announced by vendor where impact caused by waiting for regular patching window is considered as high, emergency patching window is scheduled. Decision whether to implement patch(es) in emergency patching window is done by Netigate CTO.

5.3.1.3 Regular validation of patching

Server configurations and patch levels are reviewed on a regular . Validation is done by development and operations team, using automated tooling to detect and monitor for vulnerabilities. .

5.3.1.4 Exceptions in patching

In case of need for exception of patch, it must be approved by development team via Netigate CTO.

5.3.2 Virus / malware detection

Netigate's Information Security Policy requires all Netigate's computers have an up to date antivirus/malware software installed and up to date. All our workloads are located in Azure and are protected by Azure Defender. This includes storage scanning for potential malware, container registry for vulnerable images, monitoring for suspicious activity on both virtual machines, Kubernetes clusters, etc.

5.3.3 Vulnerability scanning

OWASP Code and dependency Vulnerability scanning is performed regularly for each software build. In addition 3rd party penetration testing and security audit done by human resources is done minimum once per year. Infrastructure vulnerability scanning ist done using Azure Security Center.

Any validated findings that could be found and are critical/high vulnerabilities will be mitigated immediately and permanent fix for them will be developed. Lower security issues are also prioritized over functionality in order to keep system security high.

Report(s) are stored as per Netigate ISMS. In last performed security testing, scanning + intrusion testing. Process for 3rd party is done so that 2 testing rounds are performed and any found issues are fixed or system behavior is explained to 3rd party with end goal of having no issues. Reports are available upon request.

Netigate is committed to perform regular internal vulnerability scans and for internally found vulnerabilities we strive to follow fixing schedule as follows

- Zero-day vulnerability: As soon as possible
- Critical Risk: 30 days
- High Risk: 90 days
- Medium Risk: No time limit

5.4 Log management and Audit trails

Below is defined how user access (e.g. view, modify, delete access) is logged and monitored on a regular basis, and unauthorized access or suspicious user activity is flagged accordingly.

5.4.1 Operating system

Logs inside Netigate operation system are configured according to industry best practices and Netigate is following ISO27001.

5.4.2 Application

Netigate logs all events in centralized logging system which is located in EU.

As an example, a log file typically includes:

- DATE + timestamp
- LEVEL, “warning, error, info”
- HOST
- SERVICE
- CONTENT (actual text of the log)

Application logs are not deleted at all, for reviewing the data in case of incidents. We also do not log sensitive data there (see chapter Personal data in logs). Access to logs is only granted to selected operations personnel and they require 2-factor authentication and personal users.

Netigate logs user activities like login and data export or uploads. All services log their actions in info level logs and should there be warnings or errors, those are also stored.

Netigate has setup necessary alarms based on logs. These are monitored on a daily basis.

5.4.3 Time synchronization

All integration servers have time synchronization type set to synchronize with domain controller in UTC time.

5.4.4 Personal data in logs

Personal data are not put into our logs, we use an internal user id instead of usernames, email etc. mail. For survey responses, web proxy logs store public IP for 1 week to identify and mitigate attacks. IP addresses are never stored in combination with other data.

6 Personal data protection

6.1 Encryption policy

We are following https://github.com/ssllabs/research/wiki/SSL-Server-Rating-Guide to assess TLS ciphers that are used to secure communications between our servers and customer browsers/integrations. Although we strive to provide the best possible backward compatibility, we also don't support ciphers that are considered weak. Netigate currently supports TLS 1.2 and TLS 1.3

6.2 Encryption at rest and pseudonymisation

As per Netigate's Information Security Policy, Netigate encrypts all Restricted user data at rest through secure encryption algorithms and libraries.

As an example, User created passwords are encrypted through a one-directional BCrypt-encryption utilizing at least 2048 iterations and unique user specific salt. Besides incorporating a salt to protect against rainbow table attacks. It is not possible decrypt the passwords to return them to their original shape. Access to customer data is restricted on a strict need basis.

All data-at-rest uses at least 256-bit AES disk encryption and where possible, we restrict access to managed instances for cloud provider personnel.

6.3 Encryption in transit

All communication to and from Netigate services, external services and users are through HTTPS protocol.

API Key is used for authentication of incoming requests to Netigate's service in order to access Netigate's public endpoints per client and collection basis. Each client is provided with a company and collection specific id, administrators can have access to list of API Keys

7 Confidentiality

The following sections describe the levels and nature of access that will be provided to users based on the sensitivity of the data and users legitimate business need to access personal data.

7.1 Admin rights management

Access to servers is managed by Netigate, personal accounts are always used. Usage of shared accounts is not allowed and privileges are given on the principle of least privilege.

Normally, only members of the infrastructure team has access to servers but temporarily elevated privileges can be given for time limited efforts. In this case, access is only given to a specific environment (test, stage, prod).

7.1.1 Regular validation of admin rights

Elevated access is reviewed on a recurring basis as part of Netigate's ISMS in the Security and Privacy meetings. Roles are reviewed and removed if it is not longer required. Validation is done by using manual user termination action.

Reports from individual validations are stored in meeting minutes of recurring security meetings.

7.2 Privileged user management

An individual token is created for API access for each data set/tenant. For analytics, each user is granted access to a specific dataset. Netigate does not require 2-factor authentication at this time but it can be setup through SSO.

7.3 Monitoring

Netigate uses a combination of services to provide logging, monitoring and alerts. Alerts are configured to provide warnings when both overall system, specific components or processes fail or are about to fail or failed login attempts as an example.

Web proxy is used process and log all incoming requests coming to the servers. Additionally, Netigate logs failed login attempts and all API requests. Netigate stores both activity logs and resource logs of operations done in the cloud provider and on the resources in the cloud provider.

Monitoring and logs are restricted to privileged users on different levels depending on need to access them to provide a functional and secure service.

8 Integrity

Data integrity is a wide concept and a set of different measures are taken to ensure it. First, data is validated when it is transferred to Netigate. Second, access and write operations to databases are restricted and, third backups ensure that data can be restored to its original status.

9 Availability

Data availability is ensured through redundancy of most (but not all) of our services. All services are monitored and alerted to product teams for remedy.

10 Ability to restore availability and access to personal data

Below is defined how availability, unauthorized or accidental destruction of personal data is controlled

10.1 Business continuity and disaster recovery

Business continuity and disaster recovery is described in Netigate's Business Continuity Plan and Incident Management Procedure which are part of Netigate's ISMS documentation.

10.1.1 Validation of disaster recovery testing

Disaster recovery tests are performed bi-yearly and results are stored in the Netigate ticketing system.

10.2 Data backup and restore

Database servers are backed up at least with the following configuration:

- Weekly full backups
- Incremental hourly backups
- Retention:
    - Short-term: 7 days
    - Long-term, cold storage: 6 months
- Redundancy: 2nd region

All product and infrastructure data is stored separately and all environments can be recreated in a new region if necessary.

10.2.1 Validation of Data backup and restore testing

Restore tests are performed at least every 6 months as part of the ISMS.

11 Software management and vulnerability management

11.1 Application environment

11.1.1 Dependencies and malware

Dependencies on 3rd party and Open Source Software for application development and runtime are defined in code and scanned during builds before deploy to production.. These dependencies are scanned by Github Dependabot, continuity Sonarcloud and Azure Container Registry to detect potential vulnerabilities.

11.1.2 Vulnerability management

Potential vulnerabilities are reported during build and vulnerable build is cancelled. Critical vulnerabilities must be patched in testing and staging environment in 1 working day and in 2 working days in production environment.

Existing builds are scanned daily by Azure Security Center and critical vulnerabilities are reported.

11.2 Server environment

11.2.1 Code review on installed software

If any software is installed on servers this should be defined in code that is subject to code reviews in configuration management software I.e., Puppet, Chef, Ansible.

11.2.2 Installation and versioning

Installation and versions of software-as-a-service are defined with infrastructure as code software Terraform and changes are subject to review.

11.2.3 Vulnerability monitoring

Vulnerabilities are monitored using Azure Security Center. Critical vulnerabilities must be patched in testing and staging environment in 1 working day and in 2 working days in production environment.

11.3 Employee workstation and mobile devices

Software installation and vulnerability management is defined in Mobile device policy.

12 Communication security

12.1 Network security management

12.1.1 Network controls

All network configuration and policies are defined with infrastructure as code software Terraform and changes are subject to review.

Applications environments (testing, staging and production) only include features strictly necessary for application functionality.

Employee access of CI/CD tooling, application environment, database access in possible only over VPN with audit log. Additionally, all internal and external communication to applicationauth environments should be secured over TLS.

Internal network security is actively protected with Azure Defender Intrusion detection.

12.1.2 Security of network services

Application environment network security follows Azure Security center recommendations which includes multiple standard compliance reports. These reports are regularly reviewed, and necessary recommendations are implemented by development team.

12.1.3 Segregation in networks

VPN server, CI/CD tooling, Production, Staging and Testing environments are divided in separate networks. These networks are isolated form other networks that are used for day-to-day daily tasks – employee internet access, document storage, etc.

Public HTTPS termination for application environment are centralized for all applications through Kubernetes ingress controller. This allows for centralized public TLS certificate management and configurations.

12.2 Sessions

Session management varies depending on sensitivity of data. For access to non-PII functions, session expiry is 30 days (of inactivity or logout)

In administrative parts where PII data is collected, standard session time is 30 minutes.

12.3 Information transfer

12.3.1 Information transfer policies and procedures

Messaging between application services, parts of application infrastructure and between Netigate applications and users are only performed over encrypted channels. Preferred encryption should be TLS with protocol version 1.3 or 1.2 with well-known and secure cipher suites.

All email communication, including attachments, is subject spam protection to malware scanning. All documents uploaded through Netigate applications is subject to malware scanning.

12.3.2 Agreements on information transfer

There are two main external APIs available to Netigate customers:

- for providing external data to the insights and analytics part of the platform or export data https://help.lumoa.me/en/articles/525-api-documentation
- surveys, respondent and response data can be accessed and added using the Feedback Customer API: https://api.netigate.net/v1.2/index.html.

Customers can also import and export data to/from Netigate UI from/to Excel manually if needed.

Netigate can also help to setup custom integration if needed and separate contract for that can be made. Custom integration can be used to fetch data from customer provided end point.

12.3.3 Electronic messaging

Communication external from Netigate CX application to users can be done via e-mail, GSM or landline phone communications.

12.3.4 Confidentiality or nondisclosure agreements

Vast majority of contracts between Netigate group companies and customers are based on company template/standard terms, not those of the customer, and contain market-standard confidentiality clauses. For contractor and employees a Netigate group company, a standard template is used which also contains a market-standard confidentiality clause that includes protection of all customer data.

13 Physical security

Access to Netigate physical facilities is protected by personal key cards + secret pin. In addition, senstivie areas such as network, legal documents and internal IT are protected by additional electronic locks. All access (successful or attempted) is monitored, alerted and logged.

Netigate utilizes multiple cloud providers such as Azure and Aiven for server, network and storage infrastructure. All are certified to the ISO 27001 Standard with its clear focus on e.g. access control, physical security and handling of physical media and devices.

For more details on Azures physical security and handling of physical storage see:

- https://learn.microsoft.com/en-us/azure/security/fundamentals/physical-security
- https://learn.microsoft.com/en-us/compliance/assurance/assurance-data-bearing-device-destruction

14 Anonymization

Netigate's Privacy Policy describes how we respondent personally identifiable data (PII) collected by Netigate.

- respondent information provided by the company conducting the survey (the Controller), most often your email and phone number but can also be additional information such as organisational or regional belonging
- survey responses or other forms of feedback
  meta-data regarding survey answers such as time and date of response

Netigate's products offer many ways to prevent personal data from being collected, anonymous results being connected to an individual and assuring GDPR-compliant removal of personal data. Some examples are:

- anonymous survey links
- minimum number of 3 team members to show aggregate data
- scheduled removal of all answer data or contact data and open answers only
- automated removal of personal data before processing by public ML-models.

In addition, personally identifiable network data, such as I Paddresses are separated from and never stored with PII data.

15 Sub-processors

Netigate engages sub-processors such as data center operators to deliver the services and to process data on Netigate's and its customers' behalf. The sub-processor's data centers are as a minimum ISO 27001-certified. Netigate's current sub-processors are listed in the List of Sub-Processors available at www.netigate.net/legal. Documentation of technical and organisational measures of the respective sub-processor are available on request.