# PRIVACY AND INFORMATION SECURITY DESCRIPTION

25th August 2020

## Granite platform and services


Granite

Kauppakatu 3 A
33200 Tampere
Finland

Pieni Rooberinkatu 9
00130 Helsinki
Finland

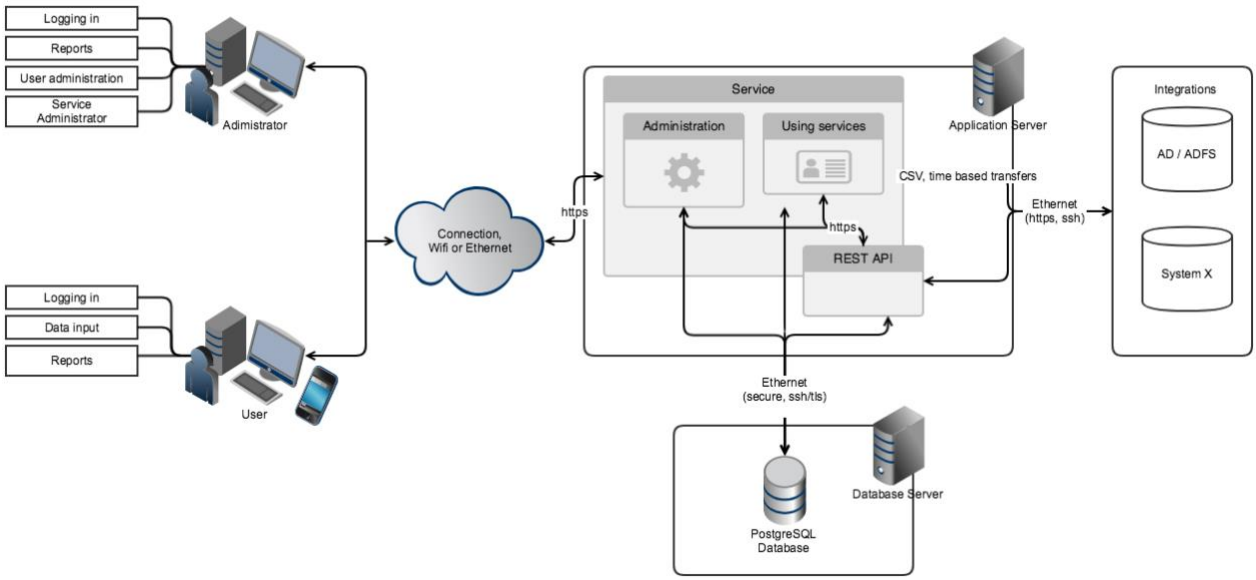
# 1. Privacy

The privacy of the customer, user and personal data on Granite services is one the key aspects to secure for Granite's whole organization. The customer's data processed by Granite is used for the purposes of providing the agreed service to the customer. The intended uses for personal data are therefore defined by the customer. We don't use the sensitive data in any way other than securing the promised service level for the customer. It's not used in the marketing and we don't provide that data to anybody outside the company - customer data is customer's data. Data center service provider nor Granite transfers personal data outside the EU/EEA area. Any sub-processor we utilize, will process the personal data in the EU/EEA area.

Our privacy guidelines are based on EU's General Data Protection Regulation (GDPR). We conduct Privacy Impact Assessment (PIA) annually to the whole Granite platform to ensure that all the regulations are taken into account in the service and product development. Granite's own PIA service is utilized for this and it consists of compliance and risk assessments.

Regular data protection training is organised for the entire personnel, and the training is a part of the orientation for new personnel. The training is organised via Granite's own online training system, where the performances are registered and can be monitored.

With regards to the software platform provided as a service to Granite's customers, Granite is a data processor and the customers are data controllers. General level data flow is descripted in the picture below. Controllers users input the personal data to the Granite system through browser (https) based user interface which is connected to the Internet. Application server and database server are connected with secure SSH/TLS connection. When Granite is integrated to another system it is done though https and SSH connections. Personal data can also be transferred via API integrations. External email service provider is utilized for the automatic email notifications sent by Granite system.



The personal data inputted to the Granite system by the customer is deleted after 3 months once the customer agreement period ends. Backups are deleted after 6 months when a new backup overwrites the previous ones.

## 2. Information security on a product development level

The information security for Granite services originates from product development, and information security is a fixed part of product development. Product development abides with the principles of secure programming, e.g. analysing and restricting user inputs, the influence of user access right levels and known vulnerabilities will be checked and taken into account. Mandatory training of secure programming practices is held every six months.

Product development is based on Agile methodologies. In product development, each new system feature has an owner, who verifies that the feature functions properly after it has been developed. The product development team explains how they have implemented the feature and what other functions/features it may affect. The owner will approve or, if needed, return the feature back to product development for amendments.

Product development will release a new software version approximately every 2-6 weeks. At first, the new software version will be tested both manually and with automatic testing tools in product development and beta environments, after which it will be transferred to the general demo environment. All system demos and presentations will be performed in the environment in question, so it is in active use. The aim is to notice possible software errors as quickly and early as possible. The customer and production environments will be updated three times per year, and the latest version that has been tested and tried in practice and found functional will always be installed during the update, which minimises the probability of error situations.

## 3. Information security on a data centre level

The server platforms are located in the data centres of a reliable third party, which fulfil at minimum the requirements for “important device facilities” or “very important device facilities”, depending on the data centre, issued by the Finnish Communications Regulatory Authority. The data centres have e.g. secured backup power supply and cooling and 24/7 access control. The data centres, server platforms and data for Granite services are located in Finland, regardless of the service provider, and they are subject to Finnish and EU regulation. Currently our data centre provider is Equinix (Finland) Oy which is ISO27001 certified.

The software for the server platform is based on open source code. The database server is PostgreSQL, the operating system Linux and the server software Apache with PHP extensions. The operating system can also be Microsoft Windows Server. The software for the server platform is updated regularly, especially in terms of information security properties.

Unnecessary services and communication ports on the server platform have been removed from use and only the necessary ones are operational, in order to minimise possible errors and leaks. All traffic between the system and the users' workstations is SSL encrypted (HTTPS protocol) with an official certificate, as in online banking.

## 4. Information security on system level

The user access management in the system observes the principle of minimum access rights, in other words the user has no default rights unless it is separately added through automatic specifications or manually. The system supports e.g. user access management based on AD/LDAP groups and roles as well as Single-Sign-On.

The system functions have been divided into three views in order to facilitate monitoring the user access: basic view, summary view and administration view. The basic view is for performing assessments and other content. The summary view is for reporting. The administration view manages the system and its content.

Personal user accounts are primarily always used to identify for the system. However, it is possible to create a direct web link in the basic view, e.g. in order to answer an assessment or a survey. The access for the summary and administration views will always be separately defined and restricted. Administrator rights will be granted for the administration view.

It is possible to use strong authentication in the system with personal USB keys, in addition to personal user IDs/password pairs or AD/LDAP identification and Single-Sign-Ons. The USB keys produce one-time passwords, and their authenticity will be verified with a separate key server. USB keys will be delivered by Granite's technology partner.

Backup copies of the system and database are done every day and are encrypted and saved on a different server platform. Daily backups are saved covering the last 30 days.

## 5. Information security on a corporate level

Granite's information security policy is approved by the management, and it describes e.g. the general principles and the target state for information security.

In terms of its own personnel, Granite observes the minimum access rights principle in all its operations, e.g. in terms of customer environments, product development environments and access to physical spaces. Access to the service providers' data centres is restricted in terms of Granite's personnel to a few key members of personnel.

Security investigations for all of Granite's personnel have been conducted by the Finnish Police. The whole personnel have signed confidentiality agreements regarding Granite and its customers' data. Regular information security training is organised for the entire personnel, and information security training is a part of the orientation for new personnel. The training is organised via Granite's own online training system, where the performances are registered and can be monitored.

Some of the larger and/or more demanding customers have audited the service providers for both the system and the server platform as well as the data centre. When needed, data centre visits can be performed through Granite, as well as audits for the service providers.

Granite has made separate security and confidentiality agreements per customers' demands, also on personnel level when needed.

## 6. Separate information security testing for software

Granite performs its own separate information security testing using Acunetix software, which automatically performs extensive testing every time a new software version (beta) is released for Granite. The reports produced by Acunetix are reviewed, and detected errors corrected at the latest by the next released software version. The software versions released for customers have therefore undergone an automatic information security scan several times.

In addition to its own information security testing, Granite has passed multiple external mechanical and manual security audits. Granite can provide the criteria and audit reports on request. Granite has committed to conducting an external information security audit at least every 12 months.