



PRIVACY AND INFORMATION SECURITY DESCRIPTION

15th October 2021

Granite platform and services



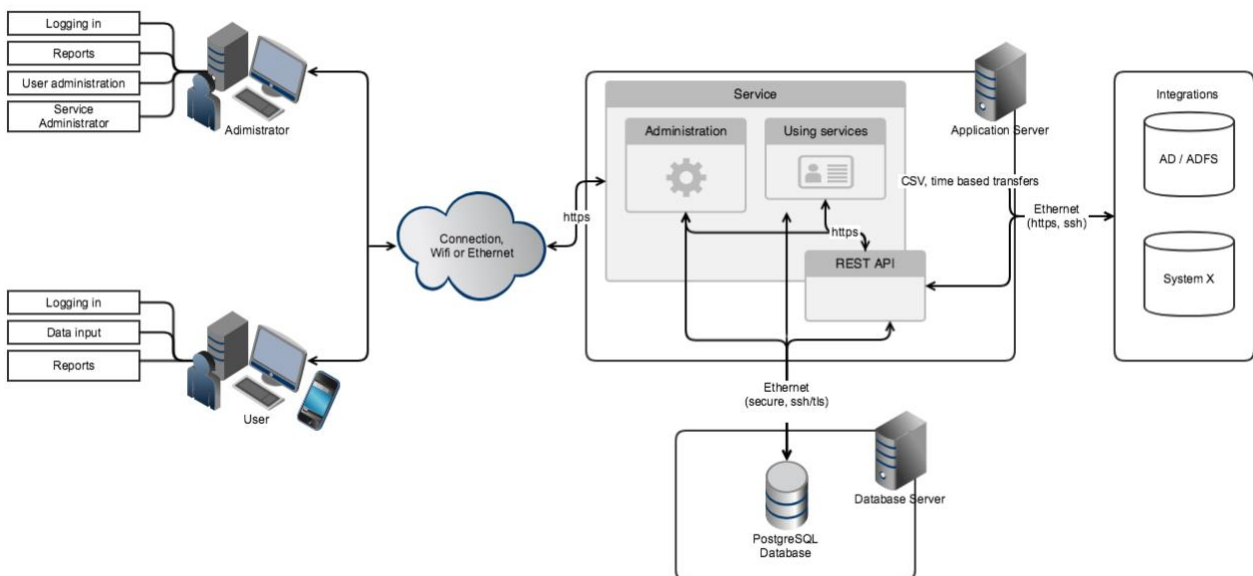
1. Privacy

The privacy of the customer, user and personal data on Granite services is one of 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 described 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 through 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 12 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 monthly. 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 at least 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 center level

The server platforms are located in the data centers of a reliable third party, which fulfil at minimum the requirements of ISO27001 standard. The data centers have e.g. secured backup power supply and cooling and 24/7 access control. The data centers, 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 center provider is Equinix (Finland) Oy.

The software for the server platform is based on open source code. The database server is PostgreSQL, the operating system is Linux and the server software is 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. All data storage partitions for the whole platform are encrypted using strong industry standard encryption algorithms ("data at rest encryption").

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 file an anonymous report using one-time session identifier. The access for the summary and administration views will always be separately defined and restricted. Administrator rights will be granted for the administration view.

The system logs user activities and automated integration events that are additional to the server, firewall and network logs. User activity logs are accessible through administration view of the system. Passed and rejected user login attempts are logged. All the activities from identified user are logged with time stamps, identifiers and performed activities.

Activities done using a direct web link described above or the IP addresses from this type of access, are not logged in to the system as the purpose for direct web link is to provide anonymous access for example to file whistleblowing reports. The server, firewall and network devices will create logs from this type of access for the security purposes, but these logs are not accessible for the customer and only very limited number of Granite's employees have access to these logs.

It is possible to use strong authentication in the system with personal 2FA authenticator mobile app, in addition to personal user IDs/password pairs or AD/LDAP identification and Single-Sign-On.

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

All the storage devices like servers' hard drives are handled securely in terms of life cycle management. Devices are wiped/overwritten multiple times based on best security practices before they are disposed.

5. Information security on a corporate level

Granite has ISO27001 certified Information Security Management System (ISMS). It covers the whole company and all the operations. 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 centers 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.

Granite's personnel is classified in terms of granting access to customer environments and customer data. Access to customer data is restricted to service and production employees only based on the minimum access rights principle.

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.