INFORMATION SECURITY AND DATA PROTECTION DESCRIPTION

18th November 2024

Granite platform and services

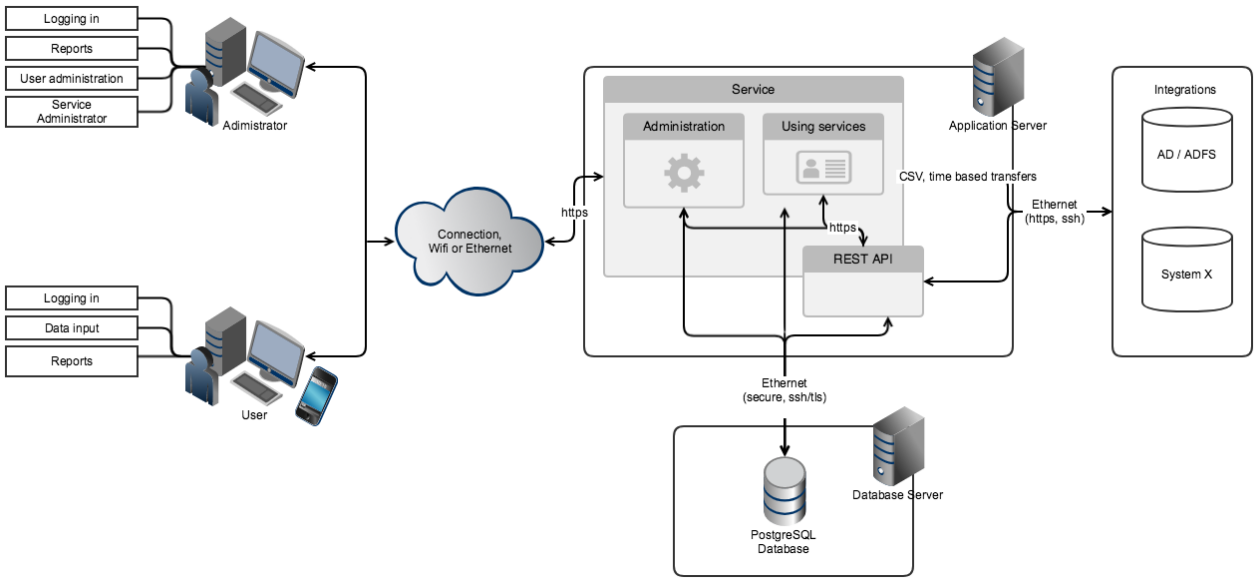
1. Data protection

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 strictly used only 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 data protection guidelines are based on EU's General Data Protection Regulation (GDPR). We conduct Data Protection Impact Assessment (DPIA) annually to the whole Granite platform to ensure that all the regulations are considered in the service and product development. Granite's own DPIA 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.



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. 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 errors.

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 (EU/EEA), regardless of the service provider, and they are subject to EU regulation. Currently our data center provider is Equinix.

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”).

The server platform is hardened based on CIS Benchmarks. 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.

4. Information security on a system level

The user access management in the system is based on 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.

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 administration view will always be separately defined and restricted. 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.

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 clearance for all of Granite's personnel have been conducted by the Finnish Security and Intelligence Service (SUPO). The whole personnel have signed confidentiality agreements regarding Granite and 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 are 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.

6. Separate information security testing for software

Granite performs its own separate information security testing using automated tools, which perform extensive testing every time a new software version (beta) is released for Granite. The reports produced by security testing tools 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 conducts an external security audit and penetration testing every 12 months.