Ramboll RamApp and RIMS Service Description

Thank you for your interest in Ramboll RamApp and RIMS and welcome to the service. The service is provided by Ramboll Finland Oy (The Service Provider).

A short description of what the Ramboll RamApp service provides:

Ramboll RamApp, a mobile version, and RIMS, the desk-top version of the same web-based service (the Service) allow users to manage the progress of work sites, run inventories, gather perceptions and data and manage feedback. Work site management includes editing site properties (status, dates, descriptions), managing work phases and quantities, and managing billing information. Inventory includes both updating existing data and adding new data. Gathering Perceptions and data includes the ability to collect information (odor observations, precipitation, water pH) and to present the collected data in tables and graphs. Feedback management involves submitting and processing feedback. The service also enables real-time location of machines or users.

A link to the Service can be found at: https://ramapp.ramboll.fi/

Availability of the Service

The Service is essentially always available as in there are no time restrictions as to when it can be used. Despite the efforts of the Service Provider, there may be temporary or short-term interruptions due to, inter alia, maintenance, general system or data communication malfunctions, or due to force majeure. The user is therefore, not absolutely guaranteed uninterrupted access to the Service.

User IDs and Customer Accounts

The administrator’s master IDs are used to manage user IDs based on contract between The Service Provider and Customer.

The administrator's root user IDs can, if needed, manage accounts for all users and clients, as well as basic configuration, user accounts, user rights, and account information for accounts.

Advice and Support Services

The Service includes phone and email support to Customers main users (on weekdays from 8am to 4pm EET) on issues related to the Service and its content. The advice covers essential questions that do not require special research or investigation. However, more extensive agreements requiring special research or investigation may be agreed upon separately.

The Service advice includes such questions as:

- The benefits of using the Service and how it can best be utilized in your projects
- Creating new user IDs
- Solving issues with Service

Content Provided by Third Parties

Links to third party websites may be included in the Service. All content, services and any applications provided by such third parties are subject to the terms and conditions defined by such parties and the Service Provider is not responsible for content or services supplied by third parties.

Customer Information and Personal Data

In this service description Customer Information refers to any information that a customer enters into the Service when using it. Personal Data refers to any information relating to an identified or identifiable natural person (Data Subject). An identifiable natural person is a person who can be identified, directly or indirectly, in particular, by their identifying information such as name, personal identification number, location information or domain identifier information.

Customer Information may include Personal Data relating to the users of the Service or to other people if the customer discloses such information within the Service.

Personal Data to be Processed

The customer decides what Personal Data to disclose to the Service, the purpose for which the Personal Data is processed, and what Service functionality it uses for processing the Personal Data. Whenever possible, the customer should avoid entering Personal Data that is sensitive by nature or threatens the privacy of the Data Subjects. The customer should also try to minimize the processing of Personal Data in the Service to only what is necessary, as required by data protection legislation.

It is possible to process at least the following types of Personal Data in the Service:

- Personal contact information such as name, email address and phone, name of employer, location of employer
- Information recorded by the system user in the system such as messages, comments, reminders, and notes
- Users' electronic identification and address information such as username and IP address

The Personal Data in the Service relates to the following groups of registered persons:

- Registered users such as employees of customers and partners
- Personal Data relating to other users or persons, provided the customer furnishes such information to the Service
- People who develop and maintain the service

Processing of Personal Data

The Service Provider treats the Personal Data provided by the customer to the Service in accordance with current data protection legislation, in particular with regard to the requirements of the EU General Data Protection Regulation (Regulation 679/2016 / EU, GDPR).

As regards the processing of Personal Data, the customer acts as a Data Controller within the meaning of the GDPR and thus determines the purposes and the means of the collection of Personal Data and is responsible for providing proper information to the Data Subjects allowing the Data Subjects to exercise their rights as well as taking care of other obligations imposed by the law.

The Service Provider processes Personal Data as a Data on behalf of the customer in order to be able to provide the Service to the customer in accordance with the service contract and the necessary data processing agreement. The Service Provider's right to process Personal Data that the customer has entered into the Service is always subject to the customer's right to processing.

If the customer's business is subject to special provisions concerning processing of information or Personal Data, Customer shall inform and instruct the Service Provider of such specific obligations.

Access to Customer Information

Access to Customer Information is provided by the customer and by users authorized by the customer, as well as by those employees who maintain the Service Provider's system or provide support or counselling on the Service on behalf of the Service Provider.

Helping the customer

The Service Provider will assist the customer separately on request eg. in the following cases in connection with the Service:

- in matters relating to the rights of data subjects
- about adding / removing authorisations of registered users
- in requests concerning investigations or notifications on personal data breaches

To provide the service, the Service Provider acquires content production, data processing and IT services from its external contract partners. The Service Provider will use only qualified service providers who are assessed or certified, who have committed themselves to confidentiality and where the subcontractors process personal data as sub-processors they also have a DPA in place with the Service Provider and provide sufficient guarantees to implement technical and organizational measures to protect Personal Data under the GDPR. The suitability of the subcontractors shall be regularly reviewed and audited.

Services that may be subcontracted may include, for example, advisory and support services, deployment and management of enterprise and end user services, telecommunications and data services, data backup, server management, and service maintenance. Details of subcontracted services and their suppliers are available upon request. The use of subcontractors is based on the prior authorization of customers and any information on possible changes in the use of subcontractors is communicated to customers.

Customer Information will not be disclosed to third parties unless otherwise instructed by the customer or unless otherwise required by law.

Cookies and web analytics

The website of the Service uses cookies and web analytics. For more information on network traffic privacy and cookie policies, visit: https://ramboll.com/legal-information

Physical location of Customer Information

For machine, platform and backup services, the location of devices and the physical location of data is in EU. Customer Information will not be transferred to other services (maintenance, data recovery, data destruction).

Retention time for Customer Information

Customer Information is retained for as long as the Customer contract account is active, after which it is automatically removed from the service after six months retention period. In addition, backups and logs are permanently deleted from the systems within 6 months of the data being removed from the service. Deleted information cannot be recovered.

Data security and data protection related logs are kept as long as deemed necessary in case they are needed to identify or resolve potential data breaches

Service requests and other messages sent to the support service will be retained for the purpose of resolving possible contingency situations after the end of the contract or freeze period.

Documents maintained by the Service Provider

The Service Provider maintains a log on processing activities in accordance with Article 30 (2) of the GDPR and makes it available to the customer and the authorities as appropriate. The document is available on request.

Potential privacy breaches

Any potential data breaches of Personal Data will be notified in accordance to Article 33 without undue delay to the customer's data protection contact person or other recipient the customer has specifically named for this purpose.

Data Protection

Data Protection refers to the protection of Personal Data, information systems and services from threats and from harm to the business or customers. Personal Data is processed in manner ensuring appropriate security in order to protect systems from unauthorized access, any illegal, unintentional or accidental processing, modification, transfer, disclosure or deletion by using appropriate technical or organizational measures (integrity and confidentiality)

The Personal Data is accessible only to the customer and users authorized by customer, accurate, and where necessary, kept up to date, and rectified or deleted without delay when the purposes of processing no longer exist.

These security principles apply to all Customer Information, regardless of whether they contain Personal Data or not. In addition to the principles outlined herein, the general security policies of the Service Provider are available upon request.

Organization and management of information security

The service provider has a designated person responsible for coordinating and supervising the processing of Personal Data in accordance to GDPR. The roles and responsibilities of the maintenance of equipment and systems containing Personal Data and customer data have been defined and the responsibilities associated with data security have been taken into account in the assignments of those processing the data.

Country Data Protection Manager:

Seppo Mattila
TIETOHALLINTOJOHTAJA, TIETOSUOJA-ASIAT
P: +358 (40) 7347070
seppo.mattila@ramboll.fi

RamApp Data Protection Contact:

Ari Hyvönen
Projektipäällikkö
P: +358 (40) 5025664
ari.hyvonen@ramboll.fi

Staff security

The confidentiality of the Personal Data and other information and the nature of the duties are taken into account in the assignment of processing duties. The importance of maintaining confidentiality is emphasized through the employment contracts of employees and/or through a separate confidentiality agreement, where necessary.

The rules on processing Personal Data and Customer Information and security instructions are available to everyone. Personnel is trained and familiarized with and directed to information-safe practices and the safe handling and protection of Personal Data and Customer Information as well as information security. Personnel is informed about security risks (related to terminal equipment, network connections, e-mail, software, network services).

Physical security

Attention has been paid to the installation of server equipment used to process Personal Data and Customer Information, and the equipment is positioned in appropriate and purpose-built premises, taking into account dust, air temperature and humidity, fire and water damage prevention and lock and burglary protection. The power supply of the devices is secured and protected against power surges and power outages.

Access to premises containing Personal Data or information systems containing Customer Information is restricted to designated authorized persons only.

Hardware Security

Processing of Personal Data and Customer Information is only done in enterprise-specific devices that meet the requirements (such as compatibility, security and control) and whose security features are ensured. The security of the usage of server, network and terminal equipment is ensured by careful installation and controlled deployment and continuous maintenance. Improper access to the devices is blocked by password protection.

Critical server and network devices have been duplicated and, if necessary, available terminal equipment. All available devices are listed and their lifecycle is reviewed from time to time, taking into account manufacturer's warranty and maintenance agreements. Security is taken into account when the equipment is being serviced and the devices are removed when used and recycled.

Software Security

Only reliable software and versions are available for your operating system, communications software, and applications. Program security features such as authentication and security features as well as control and logging procedures are utilized in accordance with the necessary level of protection.

Attacks by viruses and malicious code are centrally prevented with managed security software, which is constantly updated. Devices are in continuous maintenance and security updates run for the operating system and applications, and the success of the security updates and the security of the devices is monitored. The software license and agreement management ensures that software is available and supported.

Data connections

The Service is generated and Client information is stored behind firewalls on a secure private network. All connections are protected by SSL / TLS encryption.

Continuity and extraordinary circumstances management

A plan is in place for restoring data back-ups and it is regularly tested. The operation and availability of the Service is monitored by monitoring software. Risks are regularly re-evaluated based on the information and experience gathered and proactive measures are taken to minimize risks as part of the service maintenance and development work.

Contact

All contact information on the use of the Service or agreements can be found at:

ari.hyvonen@ramboll.fi

If you want to contact Ramboll Finland Oy regarding eg. exercising the rights of Data Subjects or accessing documents:

info@ramboll.fi