// Raynet One

GDPR Compliance

Content

Records of Processing

The following information is typically processed in Raynet One. The actual processing highly depends on the configuration and setup during the product integration project.

Typical Categories of Data Subjects

- Staff of the customer, possibly including volunteers, agents, temporary, and casual workers.
- Advisors, consultants, and other professional experts working with the systems of the customer.
- Possibly staff of software suppliers.

Typical Categories of Personal Data

The "Personal Data" processed in Raynet One typically falls into the following categories of data:

- Employment details, such as last name, first name, preferred language.
- Personal business-related contact details such as email.
- Usage, Usage frequency, and dates of specific software products.
- Login to systems.
- User assignment (personal hardware or virtual devices).

Product Features with GDPR Relation

Anonymizing

Anonymization of user data in Raynet One is not considered feasible as it is often required to be able to identify a unique user record for purposes such as usage conciliation (Secondary use rights), optimization, or compliance (named user licenses).

Pseudonymizing

For protecting the confidential relation of user and used software, user-related data can be pseudonymized by running a hashing function on the user data in the databases. This is optional and will be discussed with the customer at the beginning of a project.

Built-in Encryption Features

All entered credentials are encrypted in the configuration. Raynet One can be configured to communicate via TLS only. This is optional and will be discussed with the customer at the beginning of a project.

Raynet One also supports operations on encrypted data partitions or encrypted tablespaces. This is optional and will be discussed with the customer at the beginning of a project.

User Data Cleanup

It is possible to configure a stored procedure which will erase the record history of user and account data from the databases after a defined period. This is optional and will be discussed with the customer at the beginning of a project.

Privacy by Default and by Design

Care has been taken to take the general privacy design guidelines into consideration. All features have been verified to work with the least amount of personal data required. It is up to the customer to actively opt in to additional processing if required.

Data Subject Rights

Section 2: Information and Access to Data

Article 13: Information to be Provided Where Personal Data Is Collected from the Data Subject

Before the project starts, the customer is required to inform the internal parties about the potential collection of personal data. This depends on which data is in scope. When the scanning process has been started, the data necessary for informing the data subject by the data controller are clearly identifiable within Raynet One.

Article 14: Information to be Provided Where Personal Data Has Not Been Obtained from the Data Subject

When the scanning process has been started, the data necessary for informing the data subject by the data controller are clearly identifiable within Raynet One.

Article 15: Right of Access by the Data Subject

Personal data can be uniquely assigned to the data subject through database foreign key relationships. This data can be easily exported to a common format via the built-in export functionality of Raynet One Data Hub and can thus be made available to the data subject.

Section 3: Rectification and Erasure

Article 16: Right to Rectification

Since Raynet One collects its data from other systems, a correction at the data source is recommended. However, the data can also be corrected by an intervention in the Raynet One databases.

Article 17: Right to Erasure ('Right to be Forgotten')

Personal data stored in Raynet One usually underlies a contractual retention period based on the licensing contract with the software manufacturer the data is related to. Regardless of this retention period, data from the databases can be manually deleted or automatically deleted after a defined period.

Article 18: Right to Restriction of Processing

Raynet One is configured to collect data only from objects in the defined scope. Subsequently, information can be manually removed from the database and thus excluded from further processing.

Article 19: Notification Obligation Regarding Rectification or Erasure of Personal Data or Restiction of Processing

Personal data can be uniquely assigned to the data subject through database foreign key relationships. This data can be easily exported to a common format via the built-in export functionality of Raynet One Data Hub and can thus be made available to the data subject.

Article 20: Right to Data Portability

Processing of personal data in the scope of a software asset management process is usually base on article 6, paragraph 1 letter c. A right to object therefore does not apply in these cases. Regardless of this, personal data attributed to a data subject is clearly identifiable by database foreign key relations and can be exported.

Section 4: Right to Object and Automated Individual Decision Making

Article 21: Right to Object

Processing of personal data in the scope of a software asset management process is usually based on article 6, paragraph 1 letter c or f. A right to object therefore does not apply in these cases.

Article 22: Automated Individual Decision-Making, Including Profiling

Claims resulting from paragraph 3 have to be ensured by the owner of the license management process.