PREPARING FOR GDPR WITH RAPIDRESPONSE

European Union General Data Protection Regulation (GDPR) is a set of regulations governing the management and storage of personal data.

For information about how Kinaxis uses personal data, review the Personal Data Protection Policy.

This document covers how you can use RapidResponse to comply with GDPR requests and individual rights.

Right to be informed

RapidResponse provides updates to administrators and can be configured to provide information to any user to alert them of a data issue. Administrators can send notifications to their users.

For more information:

- Alerts
- Notifying users

Right to access

For RapidResponse users, personal information such as the user's name, email address, profile picture, job title and contact information is provided in the user's properties. All this information is optional. Users can access and modify their own contact information and profile picture as required, however, the user's name and email address must be modified by a RapidResponse user administrator.

kinaxis®

If you maintain contact information for partners, customers or suppliers in your RapidResponse database, reports can be generated to provide this information, or you can export the data to provide people with access to their information.

For more information:

- User information
- User identification
- Generating reports
- Exporting data

Right to rectification and erasure

RapidResponse users can modify or remove identifying information if they need to correct an error or no longer want to be identified. A RapidResponse administrator can also remove a user's name and email address if they no longer want to be identifiable through RapidResponse. However, removing the email address also removes the ability to have reports sent to that user's inbox.

If contact information is stored in database tables, a RapidResponse data administrator can modify or remove this information by modifying data extracts to either provide different values for the contact information or to stop providing the relevant information. During the next data update, if a record is not presented, that record is automatically deleted or, if a record is different, it is modified.

For more information:

- User information
- User identification
- Updating data

Right to data portability

All data in RapidResponse can be exported or extracted as needed, including user data and contact information for partners, customers or suppliers stored in database tables. This data can be provided to the recipient in many common formats, including text files, Microsoft Excel files or XML documents.

Data can be extracted from RapidResponse using reports, exporting data as files, automated tasks, web services and scripts. How you extract the data depends on your requirements.

For more information:

- Exporting data
- Extracting data
- Generating reports
- Retrieving data using web services

Right to restrict processing / object / decision-making and profiling

If user data or contact information is present in your RapidResponse database, you might be asked to stop processing that data or stop including it in external-facing processes, such as closed loop data configurations or partner relationships.

Any data in your RapidResponse database can be removed by modifying the field values or removing the record. Modifications to your data extracts remove or modify the values the next time you perform a data update.

For more information:

- Closed loop configuration
- Updating data

Security

Kinaxis has implemented security by design into the RapidResponse Service. The infrastructure provides replication, backup and disaster recovery planning. RapidResponse network services include encryption in transit and advanced threat detection. The RapidResponse application implements identity, authentication and user permissions.

For more information:

- RapidResponse Security Guide