General Data Protection Regulation

As of May 25th 2018, the EU General Data Protection Regulation (GDPR) will become applicable with the purpose to regulate the processing of personal data of the EU member states and its citizens. Under the GDPR, you, as a customer, will be the controller of personal data and APSIS will be your processor. This means that it is our responsibility to take action in order to ensure that the data we store on your behalf is accessed and protected in compliance with the GDPR.
For the purpose of comfort and transparency, we have created this FAQ relating to the GDPR and your use of our services.

GDPR

How has Apsis prepared for the implementation of GDPR?

In order to comply with GDPR, Apsis has conducted a full assessment of impacts in our infrastructure, business and development setup.

What kind of information that Apsis stores will be affected by GDPR?

Data created and/or uploaded by customers (such as email).

The data is controlled by, and only known by, the customer. Resultantly, our customers can fully control the deletion process themselves.

Logs and backups are cleaned/deleted in cycles taking requirements under the GDPR into consideration..

Does Apsis use any third-party partners that are relevant in regards to GDPR?

Apsis partners with Amazon AWS (www.aws.amazon.com) and Rackspace LTD (www.rackspace.com) for Cloud and hosting services.

DATA

Where is the data that is created by customers stored physically?

The data is stored at facilities in the EU.

How much data is there and for how long is it stored?

The amount of stored data depends on the customer's use of an application. We do not measure an individual customer's data size.

For further information, please read our backup policy.
All policies ensure that Apsis complies with GDPR.

DATA cont.

Is the data storage separated or shared with other Apsis customers?

Apsis is a multitenant cloud offering. Consequently, our customers have unique access to their own data. Security frameworks assure that a customer's data can only be viewed and handled by the customer.

Who can access the data?

The customer is the only one who can access his or her own data. However, with permission from the customer, Apsis Support and Development staff can access the data. Purpose built security logins are used.

How many copies/Backups exist?

Data is backed up every day and stored according to the Apsis backup policy. In compliance with the GDPR, backups are freed from data after deletion in the running environment.

Are there one or more sources and backups?

At Apsis, we have one source and several backups.

Is the data encrypted?

Data is stored behind encrypted communication. Data at rest is not encrypted. Backups are encrypted.

Is the data used for other purposes than what we as customers use it for?

No.

SECURITY

How do you work in order to ensure security at Apsis?

At Apsis, we actively work to ensure security (data, physical etc.). As an effect, we frequently review our security procedures.
In addition, Apsis works with partners whose sole focus is to protect Apsis and its customer's data.

Do you keep logs on data?

Yes, we do.

Describe your monitoring and incident handling.

Incidents are logged, documented and communicated to those concerned.

How do you handle application intrusion security?

By monitoring systems and immediate security patching.

Our in-house DevOps team is required to take immediate action if there are any sudden changes in our systems. Our third-party partners, Amazon and Rackspace, take immediate action in the event of threats to our Apsis environments.

PROCESSES

Describe your incident process.

Incidents are documented and handled by an incident team that includes C-Level participation.

Describe your process for accessing Apsis systems.

Please read our policy on login security levels.

Describe your backup and restore routines

Please read our backup policy.

Architecture

Describe your architecture in an easy format.