BRIDGE® management technologies

GDPR - General Data Protection Regulation

BRIDGE Management Technologies

May 16th, 2018

Does our website store any information from you?

Yes, our main website is only for contact and presentation purposes, the only information that we use is the one that you give us, through the contact form, where you insert your mail, first and last name, phone number and your contact message.

At the moment you click on the send button, our server will send your message to our e-mail with the data that you entered, and all data collected on the website will be erased, and sent to our e-mail.

Also, we have an analytic tool, that stores your IP and access location. This information is anonymous and used only for access metrics.

What information do we collect?

We only collect information from our clients when they feed it into our Bridge's service. And all this information is given for work purposes, and stored in ours servers, or theirs. It is the client's decision whether to keep the data in their infrastructure or in ours.

Internal Infrastructure

The client is responsible for all data stored, updates and security of the servers. We can only give maintenance on the service. The access is usually made through a VPN connection, which is provided by the client.

Bridge's Infrastructure

When the decision is to use our service, for which we are responsible for maintenance, update and data security, we always choose to use AWS services. We have been working with them for years, and no risks or problems have been detected so far. All servers in AWS are located in Frankfurt, Germany.

All AWS services are only accessed by the server that is running our software, and by authorized employees. This server can only access services which are related to a specific client, this way it makes it impossible for clients to access content from other clients. The only way to access the server is by using an encrypted file key.

All the content is secured with HTTPS, user accounts and passwords with strong password policies.

All the data collected with Bridge's software is related to your personal and business information, and of course, it is provided by you. This kind of information is just used for work purposes, it will not be shared with anyone, it will stay safely stored in our infrastructure, and only you will be able to access it.

Where is this information stored/kept?

As said before, it depends on what you aligned in our contract: if the software will be in your infrastructure or ours.

If you decide to keep it in your infrastructure, all the data and content will only be accessed by you, we will only be able to access it if you let us do it. Many clients decide to take all the process under control, where we only need to send the software to them, and all they do is download it.

We also keep all client data saved, making backups twice a day, storing all files, history, log files and database content, which are only accessible with an internal connection configured, making it impossible to access this data from an external network and unauthorized people.

How do we proceed with instance deletion required by clients?

Unfortunately, it happens for the customer to decide to finish the partnership with our services. And then it is time to make the deletion procedure: we start by making all backup from our software and client data stored. Then, we delete all content and server related to this customer, make it available only for the customer to download it, and then delete it. All content inserted by the client is now in their hands. And they are the only ones who have it. When it is decided to delete the service, we delete all client files and information that we once stored.

How do we transfer information we collect internally?

Sometimes, we are asked to work directly with our clients, accessing their IT, and sometimes this requires a more suitable structure where we can work and solve their bugs.

When this occurs, it is a good practice to download some of their data, so the problem is fixed.

All the transferences are made with good practice and encrypted connection, so there is no risk of data loss, or of exploitation of personal and important data.

When the transference is done, we keep it in our internal computers, and all contents are manipulated with encrypted machines, with good security policies. Also, our employees are fully qualified to keep important client data safe and prevent all sorts of external access to these computers. All machines are only accessed by authorized personnel.

How do we store and secure information we collect?

When it is necessary to download some content from our clients in our internal infrastructure, we do it by using the best security practices available. All the transactions are made with a secure encrypted channel, through the server and our machines.

Once the content is downloaded, we move it into our internal server, where it can be accessed only via an internal connection - never via internet. As soon the fix is concluded, we update the server and delete all data downloaded and used.