Your Data, Our Responsibility

As an OTRS Customer, you get easy, flexible access to your data through our private cloud. That means your business can be as agile as it needs to be every single day – work from anywhere, at any scale, any time.

It also means that OTRS accepts responsibility: Your data security is our number one priority. Take a look at our four-pronged approach to keeping your data under lock and key.

Always Use Certified Data Centers

For years, OTRS has worked closely with OVH, building a trustworthy and reliable relationship with their team to safely serve our customers. OTRS can provide two data centers in Northern America, one in Virginia, USA and one in Beauharnois, Canada.

All OVH data centers are a member of CIS (Center of Information Security) and has the following certifications:

- ISO 27001
- PCI-DSS (Level 1 provider)
- SSAE16
- SOC 1

Complete details of OVH data security policies are available at https://www.ovh.com/world/us/support/termsofservice/.

Employ Dedicated, Encrypted Servers

OTRS fully-managed solutions include dedicated servers for those using a GOLD or higher service package.

This means:

- No shared databases or file systems between customer systems.
- Full access control.
- No one else can access your data.

Also, servers run a hardened operating system to minimize attack possibilities.

Backup for of each OTRS instance is stored on a dedicated server and, if possible, the backup server is located in a separate fire zone.

Guard Against Vulnerabilities

OTRS uses a variety of internal processes to make sure that your data and OTRS system are protected from the greatest number of threats.

- Risk management
- Data protection plan
- Security vulnerability processes
- Internal emergency plan to counteract threats quickly
- External data protection office – to ensure independence of the data protection office from OTRS interests.

Strictly Manage Physical Access to Customer Data

- Only approved OTRS employees have access to core functions of your system.
- All team members are vetted against local labor and data protection laws.
- Team members use only SSH keys to login to OTRS instances.
- SSH keys are changed frequently to avoid man-in-the-middle attacks.
- All security-relevant traffic (e.g. email and AD connection) is routed via a VPN tunnel, protecting this traffic from unauthorized access.

OTRS environment is compliant with all GDPR regulations

GDPR specifies data protection regulations for companies working in the European Union. It is currently the strictest data protection standard worldwide. OTRS ensures compliance with GDPR regulations through the assignment of an external data protection officer who oversees all necessary implementation of the regulations. Additional information about GDPR can be found at eugdpr.org.

Author: Mathias Roehl