Data Security and Privacy Statement

Overview

EXCENTIA is a passionate Atlassian Partner since 2009 with deep knowledge in Atlassian plugin development. The aim of this documentation is to cover all of relevant information about the Data Security & Privacy Statement of EXCENTIA CONSULTORIA S.L. to help our customer see clearly what we do and what we really don't with their data.

Data storage terms and data storage location

This section explains where our application will store data from our customers and where (physically) the data will be stored to comply with all local laws.

- EXCENTIA uses a private server located on France
- We do not store personal information (e.g. name, e-mail, address).
- We store only the unique ID number of your Atlassian Cloud products.
- EXCENTIA does not store user passwords for Atlassian Cloud products, this includes all forms of storage such as databases or files.
- EXCENTIA stores a password token create on SonarQube server that can be revoked by user at any time
- Please read the documentation of the product for further details

Backups

This section explains our backup and recovery policy for customer data.

- Our backup data is securely stored, unauthorized access of backup data is not possible.
- We backup at least once a day, and we keep the backups at least for a month.
- Please read the documentation of the product for further details

Account removal and data retention

This section explains how a customer can close an account and completely remove their data from our service.

- Customer accounts may be removed any time by uninstalling the AddOn from Cloud product.
- Customer account information is retained by EXCENTIA for 30 days, after this period account information is unrecoverable deleted.
- Please read the documentation of the product for further details

Application and infrastructure security

This section explains what security measures we've taken in our application and infrastructure.

- EXCENTIA support team accesses addon data only for purposes of application health monitoring and performing system or application maintenance, and upon customer request for support purposes.
- Only authorized EXCENTIA employees have access to server data.
- Customers are responsible for maintaining the security of their own Confluence and JIRA Cloud login information.
- Communication between the Cloud products and the AddOn server is done using web requests. All web requests are digitally signed, authenticated and authorized.
- AddOn server is only accessible through secure protocols (e.g. https).
- Please read the documentation of the product for further details.

Security disclosure

This section explains how and under what circumstances we notify our customers about security breaches or vulnerabilities and indicate how a user or security researcher should disclose a vulnerability found in our add-on to us.

- Security breaches or vulnerabilities with the proposed solution of the problem are published on our website.
- Customers can report security breaches or vulnerabilities using security@excentia.es e-mail address.
- Please read the documentation of the product for further details.

Privacy

Data collected during the use of our add-on will not be shared with third parties except if required by law.