Data security in the Targito platform

Data security
The Targito platform (further referred to as „Targito") is based on working with big data. This means that we put maximum focus into ensuring that our customers' data are safe. Our customers include not only leading czech e-commerce, but also banks and insurance companies, where security requirements are amongst the most thoroughly tested features of the platform. For this reason, Targito has been designed from the ground up to meet even the strictest security requirements.

Data in motion
All communication in Targito, including the exchange of any type of data, takes place only via encrypted communication channels. All channels require authentication, most often via a username and password, but the authentication process may also contain additional security measures (for example, only allowed IP addresses). These channels include:

- SFTP, used for batch data exchange via SSH connection.
- API, using exclusively HTTPS as a protocol for communication.
- User interface using exclusively HTTPS as the communication protocol

Data at rest
As one of the few platforms on the market, Targito provides encryption of all customer data completely automatically. Customer data stored in the file storage and also data stored directly in the database are encrypted using the symmetric cipher AES-256. The platform uses logical data segregation and all data accesses are logged.

Data location and backup
All data is located on the Amazon Cloud (AWS) in the European Union. The data is primarily located in the Frankfurt region. Ireland is used as a backup region. Targito performs automatic backups, including versioning of files uploaded by the customer. This works on the following basis:

- File storage - uses file versioning, where the history of all versions and even the deleted files is stored for 30 days (with the possibility of increase)
- Database - utilises the "time travel" function which can be used to find out the status of data at any time in the last 24 hours (with the possibility of increasing to 90 days)

Note: Requests to increase the limits mentioned above may affect the license price. The reduction is not possible to maintain the basic security requirements of Targito.

Approaches and logging
Each Targito user has their own access to the user interface with individually assigned rights, which, among other things, can deny access of the user to personal data. This ensures that the client's employees can, for example, only have assigned an analytical role and not have access to customer data. At the same time, all accesses to customer data are logged.

Individual requirements
Targito is ready to meet various individual security requirements such as using a dedicated architecture for customer data, logging into the user interface through an LDAP client, using customer-managed encryption keys or other various security measures. Thanks to the architecture of the Targito platform, it is possible to use another cloud provider (such as Microsoft Azure or Google Cloud) in the case of a dedicated architecture.

Note: Requests to increase the limits mentioned above may affect the license price.