Technical and Organisational Measures for Data Protection

of

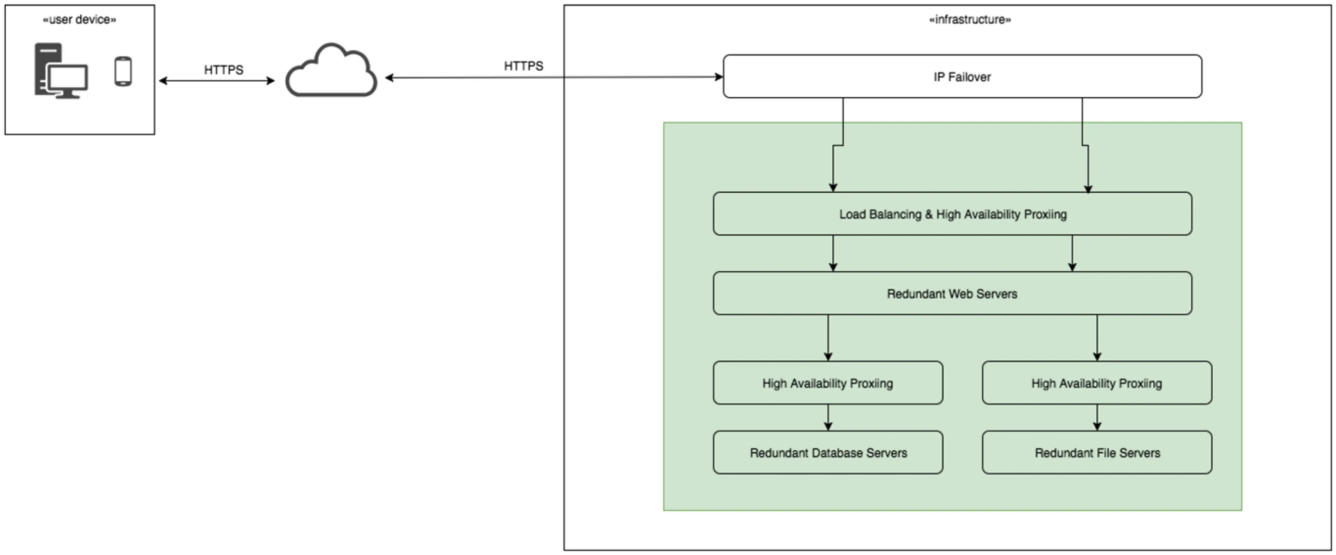
fynk GmbH
Heinrichsgasse 2/8
A-1010 Wien

1. Introduction

This document is intended to provide an overview of the technical and organisational measures that fynk takes as part of its role as a commissioned data processor to protect the data of the contractual partner. The structure of the document adheres to the requirements resulting from the GDPR. General information is provided in advance to facilitate understanding of the further details.

1.1 System Architecture

fynk mainly uses the infrastructure and services of Amazon Web Services EMEA Sarl, 38 avenue John F. Kennedy, L-1855, Luxembourg (hereinafter referred to as 'AWS') and Microsoft Deutschland GmbH, Walter-Gropius-Straße 5, 80807 Munich (hereinafter referred to as 'Azure') to operate the application. AWS and Azure are ISO27001 certified. To ensure data security, fynk uses software-based encryption of all data carriers that contain customer data. The architecture is designed for security, scalability and high availability, and every component that is absolutely necessary for operation has at least single redundancy. The system architecture is shown in the following diagram.



1.2 Roles at fynk with Data Access

From an organisational perspective, there are several use cases that require fynk to access customer data. A distinction must be made between the form in which the data is accessed:

1.2.1 Access in the Application

To help customers set up the account and to be able to track errors, account managers and, if necessary, developers can log into the customer's company account. Every action (e.g. data access and data modification) performed by the individual user is logged.

1.2.2 Database Access

To be able to track errors some specially trained developers can connect to the database. Individual users are used for this purpose and the database queries are logged.

1.2.3 Server Access

For maintenance work and infrastructure measures, fynk system administrators can access the servers on which the customer data is stored. Personal users are used (no collective users) and login and logout times are logged on the servers.

2. Confidentiality

2.1 Physical Access Control

fynk uses the infrastructure and services of AWS and Azure to operate the application. The following security measures are currently used for access control in the AWS and Azure data centres:

- electronic access control system with logging
- documented key allocation to employees and colocation customers for colocation racks (each client exclusively for their own colocation rack)
- guidelines for escorting and labelling guests in the building
- 24/7 staffing of the data centres
- video surveillance at the entrances and exits

2.2 Authentication

2.2.1 Users

fynk offers several types of authentication for users. In principle, the customer can configure the level of protection themselves. There is the option of simple authentication via email and password. There is also the option of activating two-factor authentication using the Authenticator app.

The password can be reset by accessing the email address provided during registration. Depending on the settings, a password is automatically generated during registration or you can choose your own password. The password can be reset by accessing the email address provided during registration.

The password guideline for users is: At least 8 characters

2.2.3 Account Managers

The login of customer advisors is secured with email, password and two-factor authentication. The default password guideline of fynk is:

- at least 11 characters
- at least three types of characters (upper case letter, lower case letter, number, special character)
- password rotation every 6 months
- the last 10 passwords must not be used

2.2.4 Server Administrators

fynk prevents unauthorised access to the fynk infrastructure through the use of RSA keys. Authorised fynk administrators have a personal key with which they can connect to the servers they need for their work. When assigning keys, we follow the principle of least privilege; employees are only given access to systems that they absolutely need. On the other hand, access to the fynk infrastructure is secured by means of end-to-end two-factor authentication using FIDO keys.

2.3 Access Control

2.3.1 Users

Access control is implemented by the system according to the customer's configuration. fynk offers a role and authorisation system which customers can configure themselves in the application. The customer is responsible for assigning and periodically checking the assigned authorisations. Access by users in the application is logged.

2.3.2 Account Managers

Access control for customer advisors is the responsibility of fynk. Organisational onboarding and offboarding processes ensure that assigned authorisations are up to date.

In addition, all assigned authorisations are checked regularly. Access by account managers is logged.

2.3.3 System Administrators

For system administrators, access control is the responsibility of fynk. Organisational onboarding and offboarding processes for new employees and departures ensure that assigned authorisations are up to date. In addition, all assigned authorisations are checked on a monthly basis. Login times of system administrators are logged on all servers.

All fynk employees are obliged to maintain data confidentiality; this obligation remains in effect even after termination.

3. Integrity

3.1 Transfer Control

fynk follows the least-privilege principle for transfer control: data is not passed on wherever possible. Production data is stored exclusively in the production and backup system. In exceptional cases, production data is imported into a test system. In this case, there is a defined process that ensures that the data is deleted as soon as the necessary tests have been completed. Data is always transferred via encrypted channels, which technically prevent unauthorised reading, copying, modification or removal. Backups are encrypted before transmission.

3.2 Input Control

Every request from logged-in users is logged in the application. This allows changes or deletions of data to be tracked. This also applies to fynk employees. The login times of system administrators are logged on the servers.

4. Availability and Resilience

4.1 Availability

High availability is critical to the success of fynk. AWS and Azure offer the highest standards of availability at both hardware and software level.

The architecture of the application is designed for high availability. ‘Single points of failure’, i.e. software and hardware components that limit the availability of fynk in the event of a failure, are avoided thanks to redundant infrastructure.

A tried and tested backup strategy enables us to avoid data loss as far as possible. Database backups are stored every 2 hours, files every 24 hours. We combine full backups with incremental backups. Backups are replicated on 3 different machines and tested on a test system at least every six months.

Thanks to the services of AWS, fynk fulfils the highest requirements in terms of network security and DDoS prevention.

4.2 Resilience

The resilience of fynk is ensured by regular capacity and resource planning in the infrastructure.

5. Procedures for Regular Review, Assessment and Evaluation

5.1 Data Protection Management

fynk uses software for data protection management. Relevant documents are stored here and any changes to data protection are documented.

Employees are trained at least once a year or whenever there are relevant changes.

5.2 Incident-Response-Management

Incidents relevant to data protection law are handled according to a defined process. If customer data is affected, customers are notified in accordance with the contractual provisions. If the incident gives rise to official reporting obligations, fynk will comply with these.

5.3 Privacy-Friendly Default Settings

The application supports data protection processes in many areas. The default settings provide for minimal data collection and automated data deletion after appropriate periods. Fynk supports customers in configuring the system according to their specific data protection requirements.

6. Order Control

To ensure order control, i.e. that fynk uses the customer's data exclusively in the interests of the customer, an order data processing contract is concluded in which the rights and obligations of both parties are defined.