Certificate

The certification body of TÜV Informationstechnik GmbH
hereby awards this certificate to the company

finAPI GmbH
Adams-Lehmann-Straße 44
80797 München, Germany

for the processing of the

Processes within the context of the provision of services in connection with account information services and payment initiation services

fulfils all requirements of criteria

Trusted Site Privacy, Version 2.1

of TÜV Informationstechnik GmbH. The requirements are summarised in the appendix to the certificate.
The appendix is part of the certificate and consists of 7 pages.
The certificate is valid only in conjunction with the evaluation report.

Privacy
TÜViT®
2022
Trusted Site

Certificate ID: 5548.22

Certificate validity:
2022-04-27 - 2024-04-27

Essen, 2022-04-27

Dr. Christoph Sutter
Head of Certification Body

TÜV Informationstechnik GmbH
TÜV NORD GROUP
Am TÜV 1
45307 Essen, Germany
www.tuvit.de

TO CERTIFICATE

Certification Scheme

The certification body of TÜV Informationstechnik GmbH performs its certification on the basis of the following certification scheme:

- German document: "Zertifizierungsprogramm (nicht akkreditierter Bereich) der Zertifizierungsstelle der TÜV Informationstechnik GmbH", version 1.1 as of 2020-03-01, TÜV Informationstechnik GmbH

Evaluation Report

- German document: "Trusted Site Privacy – Gutachten Technik – Prozesse im Rahmen der Erbringung von Dienstleistungen in Zusammenhang mit Kontoinformationsdiensten und Zahlungsauslösediensten", version 1.4 as of 2022-04-11, TÜV Informationstechnik GmbH, Fachstelle Datenschutzsachverständige

- German document: "Trusted Site Privacy – Gutachten Recht – Prozesse im Rahmen der Erbringung von Dienstleistungen in Zusammenhang mit Kontoinformationsdiensten und Zahlungsauslösediensten", version 1.4 as of 2022-04-11, TÜV Informationstechnik GmbH, Fachstelle Datenschutzsachverständige

Evaluation Requirements

- German document: "TÜViT Trusted Site Privacy, Version 2.1”, document version 4.0 as of 2018-01-04, TÜV Informationstechnik GmbH

Target of Evaluation

The target of evaluation "Processes within the context of the provision of services in connection with account information services and payment initiation services" of finAPI GmbH is specified in the document:

- German document: "Trusted Site Privacy – Target of Audit – Prozesse im Rahmen der Erbringung von Dienstleistungen in Zusammenhang mit Kontoinformationsdiensten und Zahlungsauslösediensten", version 1.3 as of 2022-04-11, finAPI GmbH

Within the processes the following processing is carried out (target of evalution):

1 finAPI Access

The processing finAPI Access realises the account information service (KID) and the payment initiation service (ZAD) for customers of finAPI GmbH. End-customers, i.e. customers of the customers of finAPI GmbH, can initiate payment orders via the customer product they have selected. Data input takes place via a web form.

2 finAPI GiroCheck

With the processing finAPI GiroCheck, end-customers can transmit to their desired contractual partner, the provider of a desired service or product, a credit rating check, with the help of an account information analysis carried out by finAPI GmbH.

3 finAPI DebitFlex

The processing finAPI DebitFlex optimises the receivables management of companies. Instead of initiating a dunning procedure, it enables the customer of finAPI GmbH to offer defaulting end-customers various payment options (immediate payment, payment deferral or instalment payment) for the settlement of receivables accompanied. The processing of finAPI DebitFlex is a pilot project and is carried out exclusively by finAPI GmbH as a processor in accordance with Art. 28 GDPR.

4 finAPI Data Intelligence

The finAPI Data Intelligence processing can be used to categorise retrieved account information. For this purpose, the account information is categorised according to individual markers (labelling) after it has been retrieved. Various reports are created on the basis of these labels.

5 RuleEngine

After retrieving and categorising the data with the finAPI Data Intelligence processing, the categorised data are reduced to the level necessary for the finAPI GiroCheck service with the RuleEngine application.

The target of evaluation does not include the frontends to the GiroCheck and DebitFlex services of finAPI GmbH's customers.

Evaluation Result

The target of evaluation fulfils all applicable requirements from the evaluation requirements: German document: "Trusted Site Privacy, Version 2.1".

Remarks of certification body

The certificate is not a certificate within the meaning of the EU General Data Protection Regulation (EU-GDPDR – Regulation 2016/679).

Certification according to the EU-GDPR by an accredited conformity assessment body requires, pursuant to Art. 42 (5) EU-GDPR, that the competent federal or state data protection authorities or the European Data Protection Board pursuant to Art. 63 EU-GDPR have approved the criteria for certification – i.e.

the certification scheme in the sense of ISO/IEC 17065 in conjunction with ISO/IEC 17067.

Summary of the Evaluation Requirements

1 Data protection audit

Legal requirements

Based on the defined target of evaluation, it must be evaluated which legal requirements apply to the processing of personal data and how these are integrated into the context of application of the target of evaluation. In this context, data protection must also be sufficient where laws, regulations and case law leave gaps and room for manoeuvre.

Lawfulness of processing

After identifying the data types relevant to the audit, it is evaluated for each data type whether the processing is permissible with regard to the purpose of the data processing. The requirements for data economy with regard to the state of the art are also taken into account.

Affected Persons Friendliness

Here, the consideration of the legitimate interests of the persons, whose data are processed, are reviewed. The affected persons have the right to know what data relating to them is being processed, how it is being processed and whether there is a possibility to protect their own data, i.e. to intervene in the processing of their data.

Affected persons should be informed about which of their data is processed and by which processes. It must be made transparent to affected persons what rights and what information options they have and how their personal data are secured. Data protection has to be an important aspect even in the phase of drafting contracts.

When using an IT product, the user must be informed about which functions the product has in order to be able to process personal data securely and in compliance with data protection. This includes, for example, suitable product descriptions and installation instructions or also appropriate training or information possibilities by a company that introduces and uses a product that processes information.

Transparency

The data protection policy, the data protection concepts as well as the technical and organisational measures that implements data protection in the company or in the process should be made transparent and understandable to all those affected. The focus of the evaluation is aligned to that the measures taken to ensure durable data protection must be designed in a transparent manner.

Data protection quality management

Changes in the area of information technology and the legal basis usually have an impact on the concept for meeting data protection requirements. They must be evaluated and implemented regularly and in a timely manner with regard to the effects on data protection. If necessary, analyses and action models must be adapted. The quality management measures based on this are the subject of consideration.

Data security

The information systems used can only meet data protection requirements if appropriate technical and organisational measures have been taken with regard to data security. Appropriate concepts must be in place and corresponding trustworthy components should be used when setting up the systems.

- Access control to premises and facilities

Access to data processing systems with which personal data are processed or used shall be effectively prevented to unauthorised persons by appropriate measures.

- Access control to systems

The use of data processing systems by unauthorised persons shall be effectively prevented by appropriate measures.

- Access control to data

The persons authorised to use a data processing system shall only be able to access the data subject to their access authorisation. It must not be possible to read, copy, modify or remove personal data without authorisation during processing, use and after storage.

- Disclosure control

It shall not be possible for personal data to be read, copied, modified or removed without authorisation during electronic transmission or during their transport or storage on data carriers. It shall be possible to verify and identify the entities to which personal data are intended to be transmitted by data transmission equipment.

- Input control

It must be possible to subsequently check and determine whether and by whom personal data have been entered into data processing systems, changed or removed.

- Processing control

Personal data processed on behalf of controller may only be processed in accordance with the controller's instructions. A processor may only collect, process or use the data within the framework of the controller's instructions.

- Availability control

Personal data must be protected by appropriate measures against accidental destruction or loss.

- Segregation control

Appropriate measures must be taken to ensure that data collected for different purposes can be processed separately.

2 Security inspection

Security of the components used as well as network and transport security

For all sub-components that implement security functionalities, it was possible to verify that they can be classified as trustworthy on the basis of formal evaluations already carried out and/or publicly available information.

Network and transport security are state of the art.

Measures of system management

Suitable configuration options exist, as well as appropriate monitoring and logging, which contribute to a secure operating state. Tools used for this purpose are subject to the same security requirements as the IT product / IT system itself.

Tests and inspections

Extensive penetration tests for exploitable vulnerabilities, as well as analyses of the defence mechanisms at application level and checks of the authentication/authorisation procedures used are carried out. The vulnerabilities identified during the tests and the analyses are assessed according to their degree of risk.