

# Zertifikat

Die Zertifizierungsstelle der TÜV NORD CERT GmbH  
bescheinigt hiermit dem Unternehmen

**finAPI GmbH**  
**Adams-Lehmann-Straße 44**  
**80797 München**

für die

## **Prozesse im Rahmen der Erbringung von Dienstleistungen in Zusammenhang mit Kontoinformationsdiensten und Zahlungsauslösediensten**

die Erfüllung aller Anforderungen der Kriterien

### **Trusted Site Privacy, Version 2.1**

der TÜV Informationstechnik GmbH. Die Anforderungen sind in der Anlage zum Zertifikat  
zusammenfassend aufgelistet.

Die Anlage ist Bestandteil des Zertifikats mit der ID 5558.25 und besteht aus 5 Seiten.

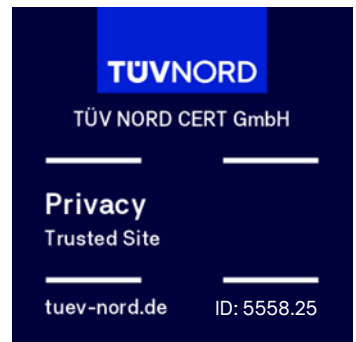
Essen, 06.10.2025

Sebastian Kessler,

Zertifizierungsstelle der TÜV NORD CERT GmbH

**TÜV NORD CERT GmbH**  
Am TÜV 1, 45307 Essen  
tuev-nord-cert.de

TÜV®



Zertifikatsgültigkeit:  
06.10.2025 – 06.10.2027

Zum Zertifikat



## Zertifizierungsprogramm

Die Zertifizierungsstelle der TÜV NORD CERT GmbH führt Zertifizierungen auf Basis des folgenden Zertifizierungsprogramms durch:

- „Zertifizierungsprogramm (nicht akkreditierter Bereich) Trusted Site Privacy“, Version 1.1 vom 01.03.2020

## Evaluierungsbericht

- „Trusted Site Privacy – Gutachten Recht –“, Version 1.1 vom 30.07.2025, TÜV Informationstechnik GmbH, Fachstelle für Datenschutzsachverständige
- „Trusted Site Privacy – Gutachten Technik –“, Version 1.1 vom 30.07.2025, TÜV Informationstechnik GmbH, Fachstelle für Datenschutzsachverständige

## Evaluierungsanforderungen

- „Trusted Site Privacy, Version 2.1 Kriterienkatalog“, Dokumentversion 4.0 vom 04.01.2018, TÜV Informationstechnik GmbH

## Evaluierungsgegenstand

Der Evaluierungsgegenstand „Prozesse im Rahmen der Erbringung von Dienstleistungen in Zusammenhang mit Kontoinformationsdiensten und Zahlungsauslösediensten“ der finAPI GmbH ist festgelegt in dem Dokument:

- „Trusted Site Privacy – Target of Audit – Beschreibung des Prüfgegenstandes“, Version 1.1 vom 14.04.2025, finAPI GmbH

## Evaluierungsergebnis

- Der Evaluierungsgegenstand, Prozesse im Rahmen der Erbringung von Dienstleistungen in Zusammenhang mit Kontoinformationsdiensten und Zahlungsauslösediensten, erfüllt alle anwendbaren Anforderungen aus den Kriterien Trusted Site Privacy, Version 2.1. .

Die im Evaluierungsbericht genannten Empfehlungen sind zu beachten.

## Hinweise der Zertifizierungsstelle

Das Zertifikat ist kein Zertifikat im Sinne der EU-Datenschutz-Grundverordnung (EU-DSGVO – Verordnung 2016/679).

Eine Zertifizierung nach der EU-DSGVO durch eine akkreditierte Konformitätsbewertungsstelle setzt gemäß Art. 42 Abs. 5 EU-DSGVO voraus, dass die zuständigen Bundes- oder Landesdaten-schutzbehörden oder der Europäische Datenschutzausschuss gemäß Art. 63 EU-DSGVO die Kriterien für die Zertifizierung – also das Zertifizierungsprogramm im Sinne der ISO/IEC 17065 i. V. m. ISO/IEC 17067 – genehmigt haben.

## Zusammenfassung der Evaluierungsanforderungen

### 1 Datenschutz-Audit

#### Rechtliche Anforderungen

Auf der Grundlage des festgelegten Evaluierungsgegenstands ist zu überprüfen, welche rechtlichen Anforderungen bei der Verarbeitung personenbezogener Daten zur Anwendung kommen und wie diese in den Anwendungszusammenhang des Evaluierungsgegenstands eingebunden werden. Dabei muss der Datenschutz auch dort genügen, wo Gesetze, Verordnungen und Rechtsprechung Lücken und Gestaltungsspielräume lassen.

#### Zulässigkeit der Verarbeitung

Nach Identifikation der prüfungsrelevanten Datentypen wird für jeden Datentyp untersucht, ob die Verarbeitung im Hinblick auf den Zweck der Datenverarbeitung zulässig ist. Dabei werden auch die Anforderungen an die Datensparsamkeit im Hinblick auf den Stand der Technik berücksichtigt.

#### Betroffenenfreundlichkeit

Hier wird die Berücksichtigung der schutzwürdigen Belange der Personen, deren Daten verarbeitet werden, überprüft. Die Betroffenen haben ein Recht darauf zu erfahren, was mit ihren personenbezogenen Daten geschieht, wie sie weiterverarbeitet werden und ob es eine Möglichkeit zum Selbstschutz, d. h. eine Einflussnahme auf die Verarbeitung der Daten, gibt.

Die Betroffenen sollten darüber informiert werden, welche ihrer Daten mit welchen Prozessen verarbeitet werden. Den Betroffenen muss transparent gemacht werden, welche Rechte und welche Auskunftsmöglichkeiten sie haben und wie ihre personenbezogenen Daten gesichert werden. Dabei muss der Datenschutz auch schon bei der Vertragsgestaltung eine wichtige Rolle spielen.

Bei Einsatz eines IT-Produktes muss der Anwender darüber informiert sein, welche Funktionen das Produkt hat, um personenbezogene Daten sicher und datenschutzkonform verarbeiten zu können. Dazu gehören z. B. geeignete Produktbeschreibungen und Installationsanleitungen oder auch entsprechende Einarbeitung bzw. Auskunftsmöglichkeit durch ein Unternehmen, das ein Produkt der Informationsverarbeitung einführt und einsetzt.

## **Transparenz**

Die Datenschutz-Policy, die Datenschutzkonzepte und auch die technischen und organisatorischen Maßnahmen, mit denen der Datenschutz im Unternehmen oder Prozess verwirklicht wird, sollten allen Betroffenen transparent und verständlich gemacht werden. Der Untersuchungsfokus ist darauf ausgerichtet, dass die getroffenen Maßnahmen zur Gewährleistung eines dauerhaften Datenschutzes durchschaubar gestaltet sein müssen.

## **Datenschutz-Qualitätsmanagement**

Veränderungen im Bereich der Informationstechniken und der Rechtsgrundlagen haben in der Regel Auswirkungen auf das Konzept zur Erfüllung der Datenschutzanforderungen. Sie müssen regelmäßig und rechtzeitig im Hinblick auf die Datenschutzauswirkungen untersucht und umgesetzt werden. Gegebenenfalls sind Analysen und Handlungsmodelle anzupassen. Die darauf aufbauenden Maßnahmen des Qualitätsmanagements sind Gegenstand der Betrachtung.

## **Datensicherheit**

Die eingesetzten Informationssysteme können Datenschutzanforderungen nur dann genügen, wenn entsprechende technische und organisatorische Maßnahmen in Bezug auf Datensicherheit ergriffen wurden. Es müssen entsprechende Konzepte vorliegen und es sollten entsprechende vertrauenswürdige Komponenten beim Aufbau der Systeme eingesetzt werden.

### ■ Zutrittskontrolle

Der Zutritt zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet oder genutzt werden, ist Unbefugten durch geeignete Maßnahmen wirksam zu verwehren.

### ■ Zugangskontrolle

Die Nutzung von Datenverarbeitungssystemen durch Unbefugte ist durch geeignete Maßnahmen wirksam zu verhindern.

### ■ Zugriffskontrolle

Die zur Benutzung eines Datenverarbeitungssystems Berechtigten sollen ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können. Personenbezogene Daten dürfen bei der Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können.

- **Weitergabekontrolle**

Personenbezogene Daten dürfen bei der elektronischen Übertragung oder während ihres Transports oder ihrer Speicherung auf Datenträger nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können. Es muss überprüft und festgestellt werden können, an welche Stellen eine Übermittlung personenbezogener Daten durch Einrichtungen zur Datenübertragung vorgesehen ist.

- **Eingabekontrolle**

Es muss nachträglich überprüft und festgestellt werden können, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind.

- **Auftragskontrolle**

Personenbezogene Daten, die im Auftrag verarbeitet werden, dürfen nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können. Ein Auftragnehmer darf die Daten nur im Rahmen der Weisungen des Auftraggebers erheben, verarbeiten oder nutzen.

- **Verfügbarkeitskontrolle**

Personenbezogene Daten müssen durch geeignete Maßnahmen gegen zufällige Zerstörung oder Verlust geschützt sein.

- **Trennungsgebot**

Durch geeignete Maßnahmen muss sichergestellt werden, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können.

## **2 Sicherheitstechnische Untersuchung**

### **Sicherheit der verwendeten Komponenten sowie Netzwerk- und Transport-Sicherheit**

Für alle Teilkomponenten, die Sicherheitsfunktionalitäten realisieren, konnte anhand von bereits durchgeführten formalen Evaluationen und/oder öffentlich zugänglichen Informationen nachvollzogen werden, dass sie als vertrauenswürdig eingestuft werden können. Die Netzwerk- und Transport-Sicherheit entsprechen dem Stand der Technik.

### **Mittel des Systemmanagements**

Es existieren geeignete Konfigurationsmöglichkeiten, sowie ein angemessenes Monitoring und Logging, die zu einem sicheren Betriebszustand beitragen. Dafür eingesetzte Werkzeuge unterliegen denselben Sicherheitsanforderungen, wie das IT-Produkt / das IT-System selbst.

## Tests und Inspektionen

Umfangreiche Penetrationstests auf ausnutzbare Schwachstellen, sowie Analysen der Abwehrmechanismen auf Applikationsebene und Prüfungen der eingesetzten Authentifizierungs-/Autorisierungs-Verfahren werden durchgeführt. Die bei den Tests und den Analysen ermittelten Schwachstellen werden entsprechend ihres Risikogrades bewertet.