Zertifikat

Die Zertifizierungsstelle der TÜV Informationstechnik GmbH
bescheinigt hiermit dem Unternehmen

finAPI GmbH
Adams-Lehmann-Straße 44
80797 München

für die Verarbeitungen der

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 und besteht aus 8 Seiten.
Dieses Zertifikat gilt nur in Verbindung mit dem Prüfbericht.

Privacy 2022 TÜViT® Trusted Site

Certificate ID: 5548.22

Zertifikatsgültigkeit:
27.04.2022 – 27.04.2024

Essen, 27.04.2022

Dr. Christoph Sutter
Leiter Zertifizierungsstelle

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

ZUM ZERTIFIKAT

Zertifizierungsprogramm

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

- „Zertifizierungsprogramm (nicht akkreditierter Bereich) der Zertifizierungsstelle der TÜV Informationstechnik GmbH“, Version 1.1 vom 01.03.2020, TÜV Informationstechnik GmbH

Prüfbericht

- „Trusted Site Privacy – Gutachten Technik – Prozesse im Rahmen der Erbringung von Dienstleistungen in Zusammenhang mit Kontoinformationsdiensten und Zahlungsauslösediensten“, Version 1.4 vom 11.04.2022, TÜV Informationstechnik GmbH, Fachstelle Datenschutzsachverständige
- „Trusted Site Privacy – Gutachten Recht – Prozesse im Rahmen der Erbringung von Dienstleistungen in Zusammenhang mit Kontoinformationsdiensten und Zahlungsauslösediensten“, Version 1.4 vom 11.04.2022, TÜV Informationstechnik GmbH, Fachstelle Datenschutzsachverständige

Prüfanforderungen

- „TÜViT Trusted Site Privacy, Version 2.1”, Dokumentenversion 4.0 vom 04.01.2018, TÜV Informationstechnik GmbH

Prüfgegenstand

Der Prüfgegenstand „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 – Prozesse im Rahmen der Erbringung von Dienstleistungen in Zusammenhang mit Kontoinformationsdiensten und Zahlungsauslösediensten“, Version 1.3 vom 11.04.2022, finAPI GmbH

In den Prozessen werden folgenden Verarbeitungen durchgeführt (Prüfungsumfang):

1 finAPI Access

Die Verarbeitung finAPI Access realisiert den Kontoinformationsdienst (KID) und den Zahlungsauslösedienst (ZAD) für Kunden der finAPI GmbH. Endkunden, d. h. Kunden der Kunden der finAPI GmbH, können über das jeweils von ihnen gewählte Kundenprodukt Zahlungsaufträge anstoßen. Die Dateneingabe erfolgt über eine Webform.

2 finAPI GiroCheck

Mit der Verarbeitung finAPI GiroCheck können Endkunden ihrem Wunschvertragspartner, dem Anbieter einer vom Endkunden begehrten Dienstleistung oder eines Produkts eine Kreditwürdigkeitsprüfung, mit Hilfe einer von der finAPI GmbH durchgeführten Analyse ihre Kontoinformationen übermitteln.

3 finAPI DebitFlex

Die Verarbeitung finAPI DebitFlex optimiert das Forderungsmanagement von Unternehmen. Sie ermöglicht dem Kunden der finAPI GmbH, anstelle der Einleitung eines Mahnverfahrens, den ggf. säumigen Endkunden verschiedene Zahlungsoptionen (Sofortzahlung, Zahlungsaufschub oder Ratenzahlung) zur Forderungsbegleichung anzubieten. Die Verarbeitung finAPI DebitFlex läuft als Pilotprojekt ausschließlich mit der finAPI GmbH als Auftragsverarbeiter nach Art. 28 DSGVO.

4 finAPI Data Intelligence

Mithilfe der Verarbeitung finAPI Data Intelligence können abgerufene Kontoinformationen kategorisiert werden. Dazu werden die Kontoinformationen nach ihrem Abruf nach individuellen Markern kategorisiert (Labeling). Auf Basis dieser Labels werden verschiedene Reports erstellt.

5 RuleEngine

Nach Abruf und Kategorisierung der Daten mit der Verarbeitung finAPI Data Intelligence werden die kategorisierten Daten mit der Anwendung RuleEngine auf das für den finAPI GiroCheck Dienst notwendige Maß reduziert.

Nicht vom Prüfungsumfang erfasst sind die Frontends zu den Diensten GiroCheck und DebitFlex der Kunden der finAPI GmbH.

Prüfergebnis

Der Prüfgegenstand erfüllt alle anwendbaren Anforderungen aus den Prüfkriterien „TÜViT Trusted Site Privacy, Version 2.1“.

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 Landesdatenschutzbehörden 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 Prüfanforderungen

1 Datenschutz-Audit

Rechtliche Anforderungen

Auf der Grundlage des festgelegten Prüfgegenstands ist zu überprüfen, welche rechtlichen Anforderungen bei der Verarbeitung personenbezogener Daten zur Anwendung kommen und wie diese in den Anwendungszusammenhang des Prüfgegenstands 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 Selbstdatenschutz, 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 Risikograde bewertet.