

HPE Fraud Risk Management as-a-Service

Anhang II: Beschreibung der Datenverarbeitung

1.	Beschreibung der Datenverarbeitung	Im Rahmen der Dienstleistungen, die darin bestehen, (i) die HPE Fraud Risk Management (FRM)-Plattform des Verarbeiters zur Verfügung zu stellen und (ii) Software-Wartungssupport und professionelle Dienstleistungen zu erbringen, kann der Verarbeiter Zugang zu den in der FRM-Plattform gespeicherten personenbezogenen Daten des Verantwortlichen erhalten.
2.	Art der verarbeiteten personenbezogenen Daten	Die Art der verarbeiteten personenbezogenen Daten hängt von den Daten ab, die der Verantwortliche in der FRM-Plattform des Verarbeiters gespeichert hat, und kann folgende personenbezogenen Daten umfassen: (i) Anruferdatensätze (IMSI, MSISDN, Geräte-ID, IMEI, EID, ICCID usw.); (ii) Teilnehmerdaten (demografische Daten und Zahlungsdaten der Teilnehmer der Kontrollstelle, z. B. Name des Benutzers, Adresse, Kontakttelefonnummer/E-Mail, Bankkonten/Kreditkarten usw.)
3.	Kategorien der verarbeiteten personenbezogenen Daten	Jede betroffene Person, deren personenbezogene Daten von dem für die Verarbeitung Verantwortlichen in den Geschäftsanwendungen (einschließlich Metadaten), der IT- und der Netzinfrastruktur gespeichert werden, einschließlich der Daten von Anruferdatensätzen und Teilnehmerdaten.
4.	Dauer der Verarbeitung	Der Verarbeiter verarbeitet die personenbezogenen Daten des Verantwortlichen für die Dauer der Vereinbarung und der geltenden Transaktionsdokumente. Alle personenbezogenen Daten werden auf der FRM-Plattform für maximal 12 Monate gespeichert.
5.	Technische und organisatorische Maßnahmen	Der Verarbeiter unterhält ein Sicherheitsprogramm auf Informations- und physikalischer Ebene zum Schutz der personenbezogenen Daten des Verantwortlichen, wie in Anhang III beschrieben.

HPE Fraud Risk Management as-a-Service

Anhang III: Technische und organisatorische Maßnahmen einschließlich technischer und organisatorischer Maßnahmen zur Gewährleistung der Sicherheit der Daten

1. Im Rahmen des Sicherheitsprogramms des Verarbeiters auf informations- und physikalischer Ebene zum Schutz der personenbezogenen Daten des Verantwortlichen („Sicherheitsprogramm des Auftragsverarbeiters“) führt der Verarbeiter regelmäßige Überprüfungen der Sicherheitspraktiken anhand von Branchenstandards wie NIST, ISO 27001 und SOC durch. Der Verarbeiter führt parallel zur Weiterentwicklung der Branche, dem Aufkommen neuer Technologien oder der Identifizierung neuer Bedrohungen regelmäßig Neubewertungen und Aktualisierungen des Sicherheitsprogramms durch.

2. Auf Anfrage überprüft der Verarbeiter gemeinsam mit dem Verantwortlichen eine Zusammenfassung der Schwachstellenbewertungen. Schwachstellenbewertungen berechtigen den Verantwortlichen nicht dazu, Aufzeichnungen und/oder Prozesse einzusehen oder in irgendeiner Weise darauf zuzugreifen, (a) die nicht direkt mit den Services zusammenhängen, (b) wenn damit gegen geltendes Recht verstoßen wird und/oder (c) wenn damit die Vertraulichkeits- und Sicherheitsverpflichtungen des Verarbeiters gegenüber einem Dritten verletzt werden.
3. Mitarbeiter des Verarbeiters und Auftragnehmer werden in den Datenschutz- und Sicherheitsrichtlinien des Verarbeiters geschult und über ihre Verantwortung in Bezug auf Datenschutz- und Sicherheitspraktiken aufgeklärt. Die Mitarbeiter und Auftragnehmer des Verarbeiters sind vertraglich verpflichtet, die Vertraulichkeit der personenbezogenen Daten des Verantwortlichen zu wahren und die geltenden Richtlinien, Normen oder Anforderungen des Verarbeiters in Bezug auf die Verarbeitung der personenbezogenen Daten des Verantwortlichen einzuhalten. Verstöße gegen diese Richtlinien, Normen oder Anforderungen werden untersucht und können zu disziplinarischen Maßnahmen bis hin zur Beendigung des Beschäftigungsverhältnisses oder der Beauftragung durch den Verarbeiter führen.
4. Wenn der Verarbeiter eine Sicherheitsverletzung feststellt, die zur versehentlichen oder unrechtmäßigen Zerstörung, zum Verlust, zur Änderung oder zur unbefugten Weitergabe von personenbezogenen Daten des Verantwortlichen oder zum unbefugten Zugriff auf diese führt (jeweils ein „Sicherheitsvorfall“), ergreift der Verarbeiter die folgenden Maßnahmen:
 - 4.1 Er informiert den Verantwortlichen unverzüglich über den Sicherheitsvorfall. Bis die Angelegenheit behoben ist, informiert der Verarbeiter den Verantwortlichen über den aktuellen Status des Sicherheitsvorfalls. Die Meldungen werden unter anderem eine Beschreibung des Sicherheitsvorfalls, der ergriffenen Maßnahmen und der Abhilfepläne beinhalten. Erlangt der Verantwortliche Kenntnis von einem Sicherheitsvorfall, der die Services betrifft, muss er den Verarbeiter unverzüglich darüber informieren und ihm den Umfang des Sicherheitsvorfalls mitteilen. Die Benachrichtigung erfolgt an das Security Operations Center des Verarbeiters per E-Mail an soc@hpe.com und/oder unter 1-877-762-6139.
 - 4.2 Er wird auf Ersuchen und auf Kosten des Verantwortlichen: (i) den Verantwortlichen in angemessener Weise bei der Meldung einer Sicherheitsverletzung an die nach den für den Verantwortlichen geltenden Datenschutzgesetzen zuständige Aufsichtsbehörde unterstützen und (ii) den Verantwortlichen in angemessener Weise bei der Unterrichtung der betroffenen Personen über eine Datenschutzverletzung unterstützen, wenn der Verstoß voraussichtlich wahrscheinlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen zur Folge hat.

HPE.com besuchen

[Jetzt chatten](#)

© Copyright 2026 Hewlett Packard Enterprise Development LP. Die hier enthaltenen Informationen können jederzeit ohne vorherige Ankündigung geändert werden. Neben der gesetzlichen Gewährleistung gilt für Produkte und Services von Hewlett Packard Enterprise ausschließlich die Herstellergarantie, die in den Garantieerklärungen für die jeweiligen Produkte und Services explizit genannt wird. Die hier enthaltenen Informationen stellen keine zusätzliche Garantie dar. Hewlett Packard Enterprise haftet nicht für technische oder redaktionelle Fehler oder Auslassungen.

a50005126DEE - Anhang a50009449DEE

HEWLETT PACKARD ENTERPRISE

hpe.com

