Hewlett Packard Enterprise

HPE Device Entitlement Gateway (DEG) as-a-Service

Anhang II: Beschreibung der Datenverarbeitung

1.	Beschreibung der Datenverarbeitung	Im Rahmen der Erbringung von Softwarewartungssupport und professionellen Dienstleistungen kann der Verarbeiter Zugang zu den in der Processor Device Entitlement Gateway (DEG)-Plattform gespeicherten Daten (einschließlich Metadaten) haben. Diese Daten können personenbezogene Daten des Verantwortlichen umfassen.
2.	Art der verarbeiteten personenbezogenen Daten	Die Art der verarbeiteten personenbezogenen Daten hängt von den Daten ab, die der Verantwortliche in den Geschäftsanwendungen (einschließlich Metadaten), der IT und der Netzwerkinfrastruktur gespeichert hat, und kann sensible personenbezogene Daten umfassen. IMSI, MSISDN, Geräte-ID (IMEI, EID, ICCID), IP-Adresse, Cookie.
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 Netzinfrastruktur gespeichert werden, einschließlich Geräteidentifikationsdaten, Metadaten der elektronischen Kommunikation und Authentifizierungsdaten.
4.	Dauer der Verarbeitung	Der Verarbeiter verarbeitet die personenbezogenen Daten des Verantwortlichen für die Dauer der Vereinbarung und/oder der geltenden Transaktionsdokumente. Alle personenbezogenen Daten werden auf der DEG-Plattform für maximal 6 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 Device Entitlement Gateway (DEG) 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“) führt HPE 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. Das Sicherheitsprogramm des Verarbeiters umfasst mindestens Folgendes:
   a. Der Verarbeiter hält mit den folgenden Praktiken physische Sicherheitsstandards ein, die jeden unbefugten physischen Zugang zu den Einrichtungen und Anlagen des Verarbeiters verhindern sollen:
      i. Der physische Zugang zu den Standorten ist auf Mitarbeiter des Verarbeiters, Unterauftragnehmer und autorisierte Besucher beschränkt
      ii. Angestellte des Verarbeiters, Subunternehmer und autorisierte Besucher erhalten Ausweise, die bei Anwesenheit vor Ort getragen werden müssen
      iii. Überwachung des Zugangs zu den Einrichtungen des Verarbeiters, einschließlich der Bereiche mit Zugangsbeschränkung und der Ausrüstung innerhalb der Einrichtungen
      iv. Der Zugriff auf das Rechenzentrum, in dem die personenbezogenen Daten des für die Verarbeitung Verantwortlichen gespeichert sind, wird protokolliert, überwacht und nachverfolgt; und
      v. Die Rechenzentren sind mit Alarmanlagen und Videokameras gesichert.
   b. Der Verarbeiter unterhält Zugangskontrollen für die maßgebliche IT-Umgebung in Übereinstimmung mit den bewährten Verfahren der Branche. Zu diesen Kontrollen gehören unter anderem Anforderungen bezüglich des Grundsatzes zur Erteilung minimaler Berechtigungen und Anforderungen an die Komplexität und Verwendung von Passwörtern.
   c. Die Infrastruktur des Verarbeiters ist mit angemessenen aktuellen Versionen von Systemsicherheitssoftware ausgestattet, die eine Host-Firewall, einen Virenschutz sowie aktuelle Patches und Virendefinitionen umfassen kann. Der Verarbeiter führt Protokolle über Ereignisse, die die Infrastruktur betreffen, wozu auch Systeme zur Angriffserkennung zur Überwachung, Erkennung und Meldung von Missbrauchsmustern, verdächtigen Aktivitäten, nicht autorisierten Benutzern und anderen Sicherheitsrisiken gehören.
3. 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.
4. Mitarbeiter 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.
5. 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:
   a. 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.
   b. 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.

Hewlett Packard Enterprise

a50000032DEE - Anhang a50009392DEE