HP DaaS Analytics und Proactive Management

Häufig gestellte Fragen zum Datenmanagement

In diesem Dokument werden die häufigsten Fragen zur Erfassung, Übertragung, Speicherung, Aufbewahrung und Vernichtung von Daten im Rahmen von HP Device as a Service (HP DaaS) Analytics und Proactive Management beantwortet.

Inhalt

HP DaaS Analytics und Proactive Management – häufig gestellte Fragen zum Datenmanagement

Cloud-Technologie/Rechenzentren

F: Welche Cloud-Technologie und welche Rechenzentren werden von der HP DaaS Analytics und Proactive Management-Plattform verwendet?

A: Die HP DaaS Analytics und Proactive Management-Plattform wird über Amazon Web Services (AWS) gehostet. Dabei handelt es sich um eine skalierbare Computing-Infrastruktur und einen anerkannten führenden Anbieter für Cloud-Hosting.

Für die HP DaaS Analytics und Proactive Management-Plattform werden Rechenzentren im US-amerikanischen Oregon (AWS-OR) und in Frankfurt (AWS-DE) unterhalten. Daten für Kunden in EMEA-Ländern können im deutschen Rechenzentrum gehostet werden. Daten für Kunden in allen anderen Ländern lassen sich im US-Rechenzentrum hosten. Alle Daten für einen einzigen „Tenant“ werden in einem zentralen Rechenzentrum gehostet. Kunden, die separate Tenants in verschiedenen Rechenzentren haben möchten, um Daten für verschiedene Geschäftseinheiten zu hosten, können diese Option anfordern.

Weitere Informationen zu AWS finden Sie unter https://aws.amazon.com.

F: Welche Rollen erfüllen die jeweiligen Rechenzentren hinsichtlich Aufgaben und Kunden?

A: Die Rechenzentren in den USA und in Deutschland können differenziert nach Kunden aus unterschiedlichen Regionen eingesetzt werden und dienen als regionale Rechenzentren. Kunden in der EU bevorzugen möglicherweise das regionale Rechenzentrum in Deutschland, während den Kunden in allen anderen Ländern vielleicht das regionale Rechenzentrum in den USA lieber ist. Durch die beiden Rechenzentren lassen sich im Rahmen des HP DaaS Analytics und Proactive Management-Service personenbezogene Daten in jeder der Regionen lokalisieren.

Die Datenanalysen für HP DaaS Analytics und Proactive Management-Services erfolgen im Analytics-Rechenzentrum in den USA. Zu Datenschutzzwecken werden alle personenbezogenen Daten vor der Übertragung an das Analytics-Rechenzentrum in den USA und der Speicherung in diesem Rechenzentrum anonymisiert.

F: Wie stellt sich der Datenfluss zwischen dem Gerät und verschiedenen Komponenten von HP DaaS Analytics und Proactive Management dar?

A: Der Datenfluss entspricht dem folgenden Prozess:

1. Nach Erstellung eines Kontos registriert sich der HP DaaS-Kunde im cloudbasierten Portal von HP DaaS Analytics und Proactive Management, das in den regionalen Rechenzentren in den USA und in Deutschland gehostet wird.
2. Die Analytics und Proactive Management-Software gelangt dann per Push-Übertragung auf die Geräte des Kunden, um die einzelnen Geräte zu registrieren, die im Rahmen von Analytics und Proactive Management im regionalen Rechenzentrum in den USA oder in Deutschland verwaltet werden.
3. Das cloudbasierte Portal von HP DaaS Analytics und Proactive Management sowie die Analytics und Proactive Management-Software auf den Geräten erfassen Daten und senden sie an die regionalen Rechenzentren in den USA und in Deutschland.

4. Die in den Rechenzentren in den USA und in Deutschland vorgehaltenen personenbezogenen Daten werden vor der Übertragung an das Analytics-Rechenzentrum in den USA, wo sie zu Analysezwecken genutzt werden, anonymisiert.
5. HP DaaS Analytics und Proactive Management nutzt das cloudbasierte Portal zur Bereitstellung des angebotenen Funktionsspektrums – Gerätemanagement sowie Analyseservices (z. B. Statusüberwachung für die Geräteflotte, aussagekräftige Berichte, Vorfälle und Warnhinweise). Dazu werden anonymisierte Analysedaten aus dem Analytics-Rechenzentrum in den USA mit personenbezogenen Daten und Informationen aus den regionalen Rechenzentren kombiniert.

Datenerfassung

F: Welche Daten werden im Rahmen des HP DaaS Analytics und Proactive Management-Service erfasst und wie werden sie verwendet?

A: Die vom HP DaaS Analytics und Proactive Management-Service erfassten „Datentypen“ werden vom Kunden direkt bereitgestellt oder automatisch in dem cloudbasierten Portal von HP DaaS Analytics und Proactive Management sowie der Analytics und Proactive Management-Software auf den Geräten gesammelt.

HP DaaS Analytics und Proactive Management – häufig gestellte Fragen zum Datenmanagement

HP DaaS Analytics und Proactive Management erfasst die folgenden Daten, um die vertraglich vereinbarten Services zu erbringen:

Zweck der Datenerfassung	Erfasste Daten	Beschreibung der erfassten Daten
Kontoverwaltung	Kontodaten	Informationen z. B. zum Erwerb von HP DaaS Analytics und Proactive Management durch den Kunden oder zur Anmeldung des Kunden, Support-Protokolle hinsichtlich Vorfällen, die von HP DaaS Analytics und Proactive Management generiert wurden, und Aktionen im Zusammenhang mit dem HP DaaS Analytics und Proactive Management-Konto für die Durchführung von Transaktionsservices wie der Kontoverwaltung.
Sicherstellung der ordnungsgemäßen Funktionsweise der HP DaaS Analytics und Proactive Management-Software und -Services	Anwendungsdaten	Version der Analytics und Proactive Management-Software, Installationsstatus, ausgewählte Optionen hinsichtlich der Datenweitergabe und Update-Details.
Kontoeinrichtung und Berechtigungsprüfung	Kontaktdaten	Private und/oder geschäftliche Kontaktdaten, u. a. Vorname, Nachname, Postadresse, Telefonnummer, Faxnummer, E-Mail-Adresse und weitere Kontaktinformationen für die Kontoeinrichtung und -prüfung im Rahmen von HP DaaS Analytics und Proactive Management, die Serviceberechtigung und E-Mail-Benachrichtigungen rund um Vorfälle und Services.
Durchführung proaktiver Wartungs- und Verwaltungsarbeiten für den IT-Service sowie Bereitstellung kundenorientierter Berichte/Dashboards	Gerätedaten	Grundlegende Hardwareinformationen zum Gerät: Computer, Betriebssystem, Arbeitsspeicherkapazität, Region, Sprache, Zeitzone, Modellnummer, Datum des ersten Starts, Alter des Geräts, Herstellungsdatum des Geräts, Browserversion, Computerhersteller, Garantiestatus, eindeutige Gerätekennungen und weitere technische Informationen, die je nach Produkt variierer
		Hardwarekomponenten wie Batterie, Festplatte, BIOS, HP SureStart, Bildschirm und Grafik, Plug-and-play-Geräte und Treiber, Treiberfehler und Treiberabstürze, Arbeitsspeicher, Echtzeituhr, Prozessor, System-Slots, Umgebungsvariablen, Wärmemanagement, Betriebssystem, Netzwerkschnittstelle, Betriebssystem- und Drittsystempatches, Status und Anwendungen von Antivirussystem und Firewall, Sicherheitsprofil des Windows-Geräts sowie Gerätemanagementprofile und ihr Status.
		Auf dem Gerät installierte Softwareanwendungen. Hinweis: Die Inhalte von angezeigten Dateien oder Informationen in einer Anwendung werden weder durchsucht noch gespeichert.
		Leistungsdaten: Akku, Festplatte, CPU, Arbeitsspeicher und Wärmeentwicklung
		Nutzung der Softwareanwendung: Häufigkeit und Zeit der Nutzung sowie Auswirkungen der Softwarenutzung auf die Hardwareleistungsdaten (Akku, Festplatte, CPU, Arbeitsspeicher und Wärmeentwicklung).
		Daten zur Netzwerkauslastung: Raten der Netzwerkübertragung aus dem Gerät.

Zweck der Datenerfassung	Erfasste Daten	Beschreibung der erfassten Daten
Proaktive Servicewartung und Geräteverwaltung durch Erkennung des Standorts eines vermissten Geräts	Standortdaten	Geografische Daten zur Durchführung von standortbasierten Services. Diese Funktion ist für alle Kunden standardmäßig abgeschaltet. Es gibt eine Option, über die Kunden standortbasierte Services in HP DaaS Analytics und Proactive Management aktivieren oder inaktivieren können.
Authentifizierung und Autorisierung von Benutzerzugriff auf HP DaaS Analytics und Proactive Management-Konten und -Services	Berechtigungsnachweise	Benutzer-IDs, Kennwörter, Kennworthinweise und ähnliche Sicherheitsinformationen, die zur Authentifizierung erforderlich sind, damit Benutzer für den Zugriff auf die HP DaaS Analytics und Proactive Management-Konten und -Services autorisiert werden können.

F: Welche Datentypen werden von HP DaaS Analytics und Proactive Management nicht erfasst?

A: HP DaaS Analytics und Proactive Management erfasst nicht die folgenden Datentypen:

- Demografische Informationen (mit Ausnahmen von Land oder Sprachvorgaben)
- Finanzielle Kontoinformationen, Kredit- oder Debitkartennummern, kreditbezogene Informationen oder Zahlungsdaten
- Social-Media- oder Web-Browsing-Informationen
- Behördlich ausgegebene Identitätsnachweise wie Sozialversicherungsnummer oder amtliche Ausweise
- Gesundheitsinformationen
- Sensible Daten wie ethnische Herkunft, politische Ansichten, Gewerkschaftszugehörigkeit, Gesundheitsdaten, sexuelle Orientierung und genetische Daten

Sicherheit

F: Welche Sicherheitsmaßnahmen werden im Rahmen von HP DaaS Analytics und Proactive Management ergriffen, um personenbezogene Daten zu schützen?

A: Bei der Erfassung, Übertragung und Speicherung von Daten werden im Rahmen von HP DaaS Analytics und Proactive Management verschiedene Sicherheitstechnologien und -verfahren genutzt, um Ihre personenbezogenen Daten vor unbefugtem Zugriff, nicht autorisierter Nutzung oder unerlaubter Offenlegung zu schützen. Hierzu zählen:

1. Daten, die in den regionalen Rechenzentren in den USA und in Deutschland gespeichert sind:
   - Datenbanken mit personenbezogenen Daten in den regionalen Rechenzentren in den USA und in Deutschland sind verschlüsselt.
   - Berechtigungsnachweise (wie Kennwörter für HP DaaS Analytics und Proactive Management-Konten) werden in diesen regionalen Rechenzentren auf Anwendungsebene im Rahmen von HP DaaS Analytics und Proactive Management sowie SHA256-Hashing verschlüsselt.
   - Kontaktdaten (d. h. private und/oder geschäftliche Kontaktdaten wie Vorname, Nachname, Postadresse, Telefonnummer, Faxnummer, E-Mail-Adresse und weitere ähnliche Kontaktinformationen eines Kunden und/oder Benutzers für HP DaaS Analytics und Proactive

Management-Konten) werden in den regionalen Rechenzentren in den USA und in Deutschland in Klartext gespeichert.
   - Standortdaten (d. h. der von HP DaaS Analytics und Proactive Management erfasste geografische Echtzeitstandort des Geräts) wird auf Anwendungsebene im Rahmen von HP DaaS Analytics und Proactive Management sowie SHA256-Hashing verschlüsselt.
2. Daten, die im Analytics-Rechenzentrum in den USA gespeichert sind: Geräte-, Anwendungs- und Standortdaten werden anonymisiert und lassen sich nicht mit einer bestimmten Person in Zusammenhang bringen, bevor sie an das Analytics-Rechenzentrum in den USA übertragen und dort gespeichert werden.

Datenübertragung und -speicherung

F: Welche Datentypen werden im Rahmen von HP DaaS Analytics und Proactive Management an die verschiedenen Rechenzentren übertragen und dort gespeichert?

A: Die folgenden Datentypen werden an die verschiedenen Rechenzentren übertragen und dort gespeichert:

Datenkategorie	Regionales Rechenzentrum in den USA (für Kunden außerhalb Europas)	Regionales Rechenzentrum in Deutschland (für Kunden in Europa)	Analytics-Rechenzentrum in den USA (für alle Kunden)
Kontodaten	Ja	Ja	Nein
Anwendungsdaten	Ja	Ja	Ja
Kontaktdaten	Ja	Ja	Nein
Gerätedaten	Ja	Ja	Ja
Standortdaten	Ja	Ja	Ja
Berechtigungsnachweise	Ja	Ja	Nein

F: Bei welchen Daten kann ein Kunde durch Opt-out der Weitergabe an den HP DaaS Analytics and Proactive Management-Service widersprechen?

A: Die folgende Tabelle enthält Opt-out-Informationen:

Datenkategorie	Opt-out	Zusätzliche Kommentare
Kontodaten	Nein	
Anwendungsdaten	Nein	
Kontaktdaten	Siehe zusätzliche Kommentare	Der Vor- und Nachname sowie die E-Mail- und Landesinformationen eines Kunden müssen von ihm zwingend angegeben werden. Postadresse und Telefonnummer sind optional.
Gerätedaten	Nein	
Standortdaten	Ja	
Berechtigungsnachweise	Nein	

F: **Wo und mit welcher Methode werden Daten erfasst und wie häufig werden sie an HP DaaS Analytics und Proactive Management übertragen?**

A: In der folgenden Tabelle finden Sie Informationen zu den Quellen und Methoden der Datenerfassung und zur Häufigkeit der Datenübertragung:

Datenkategorie	Quelle	Methodik	Häufigkeit der Übertragung
Kontodaten	Cloudbasiertes Portal von HP DaaS Analytics und Proactive Management	Die Daten werden vom Kunden bereitgestellt und entweder vom Support-Spezialisten für HP DaaS Analytics und Proactive Management oder direkt vom Kunden im cloudbasierten Portal von HP DaaS Analytics und Proactive Management eingegeben.	Dies erfolgt in Echtzeit bei Änderung der Kontodaten.
Anwendungsdaten	Cloudbasiertes Portal und Software von HP DaaS Analytics und Proactive Management	Automatisch	Alle 15 Minuten bei Änderung der Anwendungsdaten.
Kontaktdaten	Cloudbasiertes Portal von HP DaaS Analytics und Proactive Management	Die Daten werden vom Kunden bereitgestellt und entweder vom Support-Spezialisten für HP DaaS Analytics und Proactive Management oder direkt vom Kunden im cloudbasierten Portal von HP DaaS Analytics und Proactive Management eingegeben.	Dies erfolgt in Echtzeit bei Änderung der Kontaktdaten.
Gerätedaten	Analytics und Proactive Management-Software	Automatisch	• Gerätedaten werden einmal am Tag zur Analyse übertragen. • Gerätedaten für die Einstellung und Überwachung von Gerätemanagementprofilen und -status werden entweder in Echtzeit oder einmal am Tag bei Änderung der Gerätedaten übertragen.
Standortdaten	Geografische Echtzeitdaten zum Gerätestandort werden von der Analytics und Proactive Management-Software erfasst.	Automatisch	In Echtzeit oder einmal in 12 Stunden bei Änderung der geografischen Standortdaten.
Berechtigungsnachweise	Cloudbasiertes Portal von HP DaaS Analytics und Proactive Management	Die Daten werden vom Kunden im cloudbasierten Portal von HP DaaS Analytics und Proactive Management eingegeben.	Dies erfolgt in Echtzeit bei Änderung der Berechtigungsnachweise.

F: **Welche Standortdaten werden im Rahmen von HP DaaS Analytics und Proactive Management erfasst, übertragen und gespeichert?**

A: **Kundenadressdaten**

- Bei HP DaaS Analytics und Proactive Management kann ein HP DaaS-Kunde, der das cloudbasierte Portal von HP DaaS Analytics und Proactive Management nutzt, seine Adressdaten zur Angabe der Kundenadresse bereitstellen. Beispiele: Land, Ort, PLZ, Anschrift etc.
- Diese Informationen werden vom Kunden manuell im cloudbasierten HP DaaS Portal eingegeben.
- Diese Informationen sind nicht zwingend erforderlich.
- Diese Informationen werden nur an die regionalen Rechenzentren in den USA oder in Deutschland übertragen und dort gespeichert.

Länderbezogene Daten des Betriebssystems

- Die länderspezifischen Angaben des Betriebssystems auf den Geräten, die für HP DaaS Analytics und Proactive Management registriert sind.
- Diese Angaben werden automatisch im Gerät über die HP DaaS Analytics und Proactive Management-Software auf dem Gerät erfasst.
- Diese Informationen werden nur an die regionalen Rechenzentren in den USA und in Deutschland sowie an das Analytics-Rechenzentrum in den USA übertragen und dort gespeichert.

Echtzeitdaten zum Gerätestandort

- Die geografischen Echtzeitdaten des Gerätestandorts (z. B. Breiten- und Längengrad des Geräts).
- Diese Daten werden nur erfasst, wenn ein HP DaaS-Kunde standortbasierte Services im cloudbasierten Portal von HP DaaS Analytics und Proactive Management für seine Geräteflotte in Analytics und Proactive Management aktiviert.
- Diese Daten werden im Gerät über die HP DaaS Analytics und Proactive Management-Software auf dem Gerät erfasst.
- Die standortbasierten Services für die Verfolgung des geografischen Gerätestandorts im Rahmen von HP DaaS Analytics und Proactive Management ist standardmäßig für alle Kunden abgeschaltet. Die Kunden haben die Option, im cloudbasierten Portal von HP DaaS Analytics und Proactive Management die standortbasierten Services zu aktivieren oder zu inaktivieren. Auch wenn die standortbasierten Services aktiviert sind, erlaubt HP DaaS Analytics und Proactive Management die Erfassung von Standortdaten des Geräts nicht für Geräte, die als mitarbeitereigene oder persönliche Geräte klassifiziert sind (im cloudbasierten Portal von HP DaaS Analytics und Proactive Management).
- Diese Daten werden an die regionalen Rechenzentren in den USA und in Deutschland übertragen und dort gespeichert. Personenbezogene Daten im Zusammenhang mit Standortdaten (d. h. die im Rahmen von HP DaaS Analytics und Proactive Management zu Analysezwecken erfassten geografischen Echtzeitdaten zum Gerätestandort) werden vor der Übertragung an das Analytics-Rechenzentrum in den USA und der Speicherung in diesem Rechenzentrum anonymisiert.

Standortdaten zur Assetverfolgung

- Im Rahmen von HP DaaS Analytics und Proactive Management können die Kunden die Standortadresse eines Assets über das cloudbasierte Portal von HP DaaS Analytics und Proactive Management eingeben. Dabei handelt es sich nicht um die Echtzeitdaten zum Gerätestandort, sondern um einen Kennsatz zur Identifizierung des physischen Asset-Standorts. Beispiel: Gebäude 1, 1. Stock.

- Diese Informationen werden vom Kunden manuell im cloudbasierten Portal von HP DaaS Analytics und Proactive Management eingegeben. Diese Informationen werden an die regionalen Rechenzentren in den USA oder in Deutschland und an das Analytics-Rechenzentrum in den USA übertragen und dort gespeichert.

F: **Wie geht HP DaaS Analytics und Proactive Management mit personenbezogenen Daten in den Gerätedaten um, die in den Umgebungsvariablen enthalten sind?**

A: Bei Umgebungsvariablen können personenbezogene Namen in manchen Werten enthalten sein. Analytics und Proactive Management liest den Namen des angemeldeten Windows-Benutzers im Gerät aus. Ist er in den Werten der Umgebungsvariablen enthalten, wird er vor der Übertragung an das Analytics-Rechenzentrum und der Speicherung in diesem Rechenzentrum entfernt.

Hat ein Benutzer jedoch einen Benutzernamen im Wert der Umgebungsvariablen angegeben, bei dem es sich nicht um den Namen des angemeldeten Windows-Benutzers handelt, kann der Service diesen vor der Übertragung der Umgebungsvariable an das Analytics-Rechenzentrum in den USA und ihrer Speicherung in diesem Rechenzentrum nicht entfernen.

Handelt es sich beim Benutzernamen beispielsweise um Franz Meier und der angemeldete Windows-Benutzer lautet fmeier und einer der Werte der Umgebungsvariablen ist C:\Benutzer\fmeier\Dokumente, dann überträgt und speichert die Analytics und Proactive Management-Software auf dem Gerät diese Daten als C:\Benutzer\benutzername\Dokumente. Ist der Wert der Umgebungsvariable jedoch C:\Benutzer\franz\Dokumente, dann überträgt und speichert Analytics und Proactive Management diese Daten als C:\Benutzer\franz\Dokumente im Analytics-Rechenzentrum in den USA.

F: **Wie geht HP DaaS Analytics und Proactive Management mit personenbezogenen Daten in den Gerätedaten um, die in Windows Event Logs enthalten sind?**

A: Windows Event Logs auf Geräten können personenbezogene Daten enthalten. Aufgrund des Umfangs und der Vielfalt der Daten ist es schwierig, sich ein Bild aller personenbezogenen Daten in Windows Event Log-Daten, die an das Analytics-Rechenzentrum in den USA übertragen und dort gespeichert werden, zu machen, sie zu entfernen und/oder zu bereinigen. Analytics und Proactive Management nutzt personenbezogene Daten aus Windows Event Logs nicht in seinen Analysen oder Ausgaben.

Datenschutz

F: Werden Daten über öffentliche Netzwerke übertragen, die TLS 1.1 oder höher, IPsec oder andere Standardtechnologien mit starker Verschlüsselung übertragen?

A: HP DaaS Analytics und Proactive Management nutzt TLS 1.2 zur Übertragung von Daten zwischen dem Gerät und den regionalen Rechenzentren in den USA und in Deutschland sowie dem Analytics-Rechenzentrum in den USA.

F: Werden Daten (in Datenbanken, Protokollen, Konfigurationsdateien, Sicherungsmedien etc.) auf sichere Weise gespeichert?

A: Alle Datenbanken in den regionalen Rechenzentren in den USA und in Deutschland, die personenbezogene Daten speichern, sind verschlüsselt.

Alle Datenbanken und der gesamte unstrukturierte Speicher im Analytics-Rechenzentrum in den USA werden in der ersten Jahreshälfte 2018 verschlüsselt.

F: Werden personenbezogene Daten (in Datenbanken, Protokollen, Konfigurationsdateien, Sicherungsmedien etc.) in Klartext gespeichert?

A: Alle Datenbanken in den regionalen Rechenzentren in den USA und in Deutschland, die personenbezogene Daten speichern, sind verschlüsselt.

Darüber hinaus bietet HP DaaS Analytics und Proactive Management in den regionalen Rechenzentren in den USA und in Deutschland Verschlüsselung auf Anwendungsebene sowie SHA256-Hashing für Berechtigungsnachweise (z. B. Kontokennwörter und Echtzeitdaten zum Gerätestandort).

Kontaktdaten (private und/oder geschäftliche Kontaktdaten mit Vornamen, Nachnamen, Postadresse, Telefonnummer, Faxnummer, E-Mail-Adresse etc. eines Kunden und/oder Benutzers für DaaS Analytics und Proactive Management-Konten) werden in den regionalen Rechenzentren in den USA und in Deutschland in Klartext gespeichert.

F: Werden Daten auf sichere Weise vernichtet, wenn sie nicht mehr gebraucht werden?

A: Sämtliche Daten in den regionalen Rechenzentren in den USA und in Deutschland werden innerhalb von dreißig Tagen nach der Kundeninaktivierung dauerhaft aus dem HP DaaS Analytics und Proactive Management-Service gelöscht.

Daten im Analytics-Rechenzentrum in den USA werden fünf Jahre nach der Datenerstellung gelöscht. (**Hinweis:** Zu Datenschutzzwecken werden alle personenbezogenen Daten vor der Übertragung in das Analytics-Rechenzentrum in den USA und der Speicherung in diesem Rechenzentrum anonymisiert.)

F: Wie wird der Datenzugriff eingeschränkt?

A: Sämtliche Daten, die erfasst und in den regionalen Rechenzentren in den USA und in Deutschland sowie im Analytics-Rechenzentrum in den USA gespeichert werden, sind durch Amazon Web Services (AWS) über IAM-Rollen, authentifizierte Benutzer und Bucket-Richtlinien geschützt.

F: Gibt HP DaaS Analytics und Proactive Management seine Daten an seine HP Lieferanten weiter und wenn ja, gehören dazu personenbezogene und anonymisierte Informationen?

A: Ja, HP DaaS Analytics und Proactive Management gibt Leistungsdaten (Festplatte, CPU, Arbeitsspeicher) an einige wichtige HP Lieferanten weiter, damit die Leistung von HP Produkten optimiert werden kann. HP stellt nur aggregierte, anonymisierte Daten ohne Bezug auf den jeweiligen HP DaaS Analytics und Proactive Management-Kunden bereit.

F: Bietet HP DaaS Analytics und Proactive Management separate, dedizierte Datenbanken an, die von den Kunden exklusiv für ihre Daten verwenden können?

A: Nein.

F: Werden Kundendaten und -informationen zusammen mit den Daten anderer Organisationen oder Unternehmen auf denselben physischen Servern gehostet?

A: Ja.

4AA7-2191DEE, 8. Februar 2018