

HPE VERTRAGSANHANG DATENSCHUTZ UND DATENSICHERHEIT

HPE Support und sonstige Dienstleistungen (“Services”)
Stand: August 2020

Dieser Vertragsanhang Datenschutz und Datensicherheit (“Anhang”) regelt die Vertraulichkeit und Sicherheit personenbezogener Daten, die HPE im Zusammenhang mit der Erbringung der Services verarbeitet. Der Anhang ist Bestandteil des Vertrags zwischen HPE und dem Kunden, oder in Ermangelung eines Vertrages, der Allgemeinen Geschäftsbedingungen von HPE (“Vertrag”). HPE und der Kunde werden jeweils „Partei“, gemeinsam „Parteien“ genannt.

1. Dieser Anhang ist Bestandteil des Vertrags. Soweit Widersprüche zwischen den Bestimmungen dieses Anhangs und des Vertrags bestehen, hat der Anhang Vorrang. Die englisch- und deutschsprachigen Versionen dieses Anhangs sind jeweils einsehbar unter hpe.com/h20195/v2/Getdocument.aspx?docname=a50000759enw und hpe.com/h20195/v2/Getdocument.aspx?docname=a50000759dee. Im Fall von Abweichungen oder Widersprüchen ist die deutsche Version maßgeblich.
2. **Begriffsbestimmungen**
 - 2.1. “Personenbezogene Daten” oder “Personenbezogene Kundendaten” bezeichnen (Kunden-) Daten, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen, soweit hiervon abweichend gilt die Definition der einschlägigen Datenschutzgesetze.
 - 2.2. “Geschäftliche Kontaktdaten” meint (i) Kontaktinformationen von Kundenvertretern für Rechnungsstellung, Abrechnung und sonstige geschäftliche Anfragen, (ii) Informationen für die Nutzung der Services durch den Kunden und (iii) sonstige Informationen, die HPE erhebt und benötigt, um mit dem Kunden zu kommunizieren.
 - 2.3. “Datenschutzgesetze” bezeichnet alle einschlägigen Gesetze und Vorschriften der relevanten Rechtsordnungen in Bezug auf Verarbeitung und Schutz Personenbezogener Daten.
 - 2.4. “Verantwortlicher” bezeichnet die natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die nach geltendem Datenschutzrecht allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung Personenbezogener Daten entscheidet.
 - 2.5. “Auftragsverarbeiter” bezeichnet eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die Personenbezogene Daten im Auftrag des Verantwortlichen oder auf Weisung eines anderen Auftragsverarbeiters, der im Auftrag des Verantwortlichen handelt, Verarbeitet.
 - 2.6. “Verarbeiten”, “Verarbeitung” oder “Verarbeitet” bezeichnet jeden mit oder ohne Zuhilfenahme automatisierter Verfahren ausgeführten Vorgang oder jede solche Vorgangsreihe im Zusammenhang mit Personenbezogenen Daten (einschließlich Zugriff, Erheben, Erfassen, Organisation, Aufbewahrung, Speicherung, Anpassung oder Veränderung, Auslesen, Abfragen, Verwendung, Offenlegung, Bereitstellung, Abgleich, Verknüpfung, Sperrern, Löschen oder Vernichtung von Personenbezogenen Daten) und entsprechende Begriffsbestimmungen in einschlägigen Datenschutzgesetzen, soweit eine solche von dieser Definition abweicht.
 - 2.7. „Sensible Daten“ bezeichnet Personenbezogene Daten aus denen rassische und ethnische Herkunft, politischen Meinungen, religiöse oder weltanschauliche Überzeugungen oder die Gewerkschaftszugehörigkeit einer Person hervorgehen, sowie genetische Daten, biometrische Daten (soweit diese zur Identifikation einer Person Verarbeitet werden), Gesundheitsdaten oder Daten zum Sexualleben oder der sexuellen Orientierung einer Person.

3. Beauftragung und Weisungen

- 3.1. HPE Verarbeitet Personenbezogene Kundendaten in dem Umfang, der für die Erbringung der Services und die Erfüllung der Pflichten von HPE im Rahmen dieses Anhangs, des Vertrags und der anwendbaren Datenschutzgesetze als Erbringer der Services und Auftragsverarbeiter erforderlich ist. Einzelheiten der Verarbeitung, einschließlich Gegenstand, Zweck und Dauer der Verarbeitung, Arten Personenbezogener Daten und Kategorien betroffener Personen, auf die sich die Daten beziehen, sind in Anlage A aufgeführt.
- 3.2. HPE Verarbeitet Personenbezogene Kundendaten gemäß den in diesem Anhang oder dem Vertrag festgelegten oder auf sonstige Weise dokumentierten Weisungen des Kunden. Mögliche Kosten und Gebühren im Zusammenhang mit diesen zusätzlichen Weisungen sind gemäß den Vorgaben des Vertrags zu vereinbaren.
- 3.3. HPE darf Personenbezogene Kundendaten auf andere Weise als gemäß den Weisungen des Kunden Verarbeiten, sofern HPE hierzu gesetzlich verpflichtet ist. In einem so gelagerten Fall informiert HPE den Kunden vor der Verarbeitung über diese Pflicht, sofern das Gesetz eine solche Information nicht aus wichtigen Gründen des öffentlichen Interesses untersagt. Ist HPE aufgrund von Gesetzesänderungen oder aus anderen Gründen nicht in der Lage, die Weisungen des Kunden oder die Bestimmungen dieses Anhangs einzuhalten, oder ist HPE der Auffassung (ohne dass HPE insoweit eine umfassende rechtliche Analyse durchzuführen hat), dass eine Weisung des Kunden gegen geltendes Recht verstößt, informiert HPE den Kunden unverzüglich schriftlich.
- 3.4. HPE erkennt an, dass HPE keine Rechte an Personenbezogenen Kundendaten hat (einschließlich der darin enthaltenen Informationen zu geistigem Eigentum oder geschützten Informationen). HPE darf Personenbezogene Kundendaten nicht verkaufen, vermieten oder verleihen.
- 3.5. Nutzt der Kunde die Services, um Arten von Personenbezogenen Kundendaten zu Verarbeiten, die nicht ausdrücklich von diesem Anhang umfasst sind, handelt der Kunde auf eigenes Risiko und HPE ist für sich aus dieser Nutzung möglicherweise ergebende Compliance-Mängel nicht verantwortlich.

4. Einhaltung von Gesetzen

- 4.1. Die Parteien kommen zu jedem Zeitpunkt ihren jeweiligen Pflichten im Rahmen dieses Anhangs und der einschlägigen Datenschutzgesetze nach, die für ihre jeweilige Verarbeitung Personenbezogener Daten gelten. Sollte HPE durch den Kunden mit geschützten Gesundheitsdaten – gemäß der Definition im US-Health Insurance Portability and Accountability Act – umgehen, vereinbaren die Parteien darüber hinaus, die Bedingungen des Business Associate Agreements einzuhalten, der unter [hpe.com/info/customer-privacy](https://www.hpe.com/info/customer-privacy) eingesehen werden kann.
- 4.2. HPE hält außerdem sämtliche einschlägigen Gesetze und die unter [hpe.com/de/de/privacy/master-policy.html](https://www.hpe.com/de/de/privacy/master-policy.html) einsehbare Datenschutzrichtlinie von HPE in Bezug auf die Verarbeitung Geschäftlicher Kontaktdaten ein und verwendet Geschäftliche Kontaktdaten ausschließlich für berechtigte geschäftliche Zwecke, einschließlich Rechnungsstellung, Beitreibung, Überwachung und Optimierung der Nutzung der Services, Service-Verbesserung, Wartung, Support, Mitteilungen bezüglich Vertragsverlängerungen (direkt oder über einen im Auftrag von HPE tätigen Unterauftragsverarbeiter, oder über einen HPE Channel Partner) und Informationen über neue und weitere Services.
- 4.3. Personenbezogene Daten von HPE-Mitarbeitern, die HPE einem Kunden offenbart oder die der jeweilige HPE-Mitarbeiter selbst Kunden zur Verfügung stellt, Verarbeitet der Kunde um seine Service-Nutzung zu verwalten gemäß seinen Datenschutzrichtlinien und einschlägigen Datenschutzgesetzen. Eine solche Offenlegung durch HPE erfolgt nur, sofern sie für Sicherheitszwecke, Zwecke des Vertrags- und Service-Managements oder einer angemessenen und rechtmäßigen Verifizierung von Background-Screenings durch den Kunden zulässig ist.

5. Sicherheit

- 5.1. HPE implementiert und führt die in Anlage A aufgeführten physischen, technischen und organisatorischen Sicherheitsmaßnahmen durch, die im jeweiligen Vertrag ergänzt oder geändert werden können, um die Personenbezogenen Kundendaten vor unbeabsichtigter oder unrechtmäßiger Vernichtung oder unbeabsichtigtem Verlust, Veränderung, unbefugter Offenlegung oder unbefugtem Zugriff zu schützen.
- 5.2. Der Kunde erkennt an, dass HPE die Sicherheitsmaßnahmen durch die Einführung neuer oder verbesserter Sicherheitstechnologien verändern kann, und gestattet HPE, diese Änderungen vorzunehmen, sofern sie das Schutzniveau nicht mindern. HPE stellt auf Verlangen dem Kunden Informationen über die aktuellsten, auf die Services anwendbaren Maßnahmen zur Datensicherheit zur Verfügung.



6. Unterauftragsverarbeitung und Ort der Verarbeitung

- 6.1. Der Kunde gestattet HPE, verbundene und nicht verbundene Unterauftragsverarbeiter ("Unterauftragsverarbeiter") zu beauftragen, die einige oder alle der vertraglichen Pflichten von HPE erfüllen. HPE gewährt seinen Unterauftragsverarbeitern nur insoweit Zugang zu Personenbezogenen Kundendaten, wie dies für die Erbringung der Services erforderlich ist.
- 6.2. Die Unterauftragsverarbeiter, die für die Services eingesetzt werden können, und die Orte der Verarbeitung sind im Vertrag („Projektspezifische Unterauftragsverarbeiter“), unter hpe.com/info/customer-privacy.html („allgemeine Unterauftragsverarbeiter“) oder unter hpe.com/h20195/v2/Getdocument.aspx?docname=a50000760enw („DACH-Unterauftragsverarbeiter“) aufgeführt. Alle vorgenannten Unterauftragsverarbeiter gelten als vom Kunden genehmigt („genehmigte Unterauftragsverarbeiter“). Der Kunde abonniert auf den oben genannten Websites die jeweils anwendbaren Benachrichtigungen von HPE zu beabsichtigten Änderungen der eingebundenen Unterauftragsverarbeiter (jeweils einer für die allgemeinen Unterauftragsverarbeiter und einen für die DACH Unterauftragsverarbeiter). HPE benachrichtigt den Kunden mittels solcher Benachrichtigungen, wenn sich die allgemeinen- oder die DACH-Unterauftragsverarbeiter ändern. Der Kunde kann jederzeit einer Einbindung oder dem Austausch eines Unterauftragsverarbeiters widersprechen. Die Parteien unternehmen alle zumutbaren Anstrengungen, um auf den Widerspruch des Kunden hin eine einvernehmliche Lösung zu finden. Gelingt dies nicht innerhalb einer angemessenen Zeit, wird die Angelegenheit gemäß dem im Vertrag geregelten Streitbeilegungsverfahren behandelt. Können sich HPE und der Kunde nicht auf eine einvernehmliche Lösung verständigen, ist HPE berechtigt, den Vertrag ohne weitere Verpflichtungen zu kündigen.
- 6.3. HPE prüft seine Unterauftragsverarbeiter sorgfältig und schließt mit den Unterauftragsverarbeitern wirksame, durchsetzbare und schriftliche Verträge, nach denen die Unterauftragsverarbeiter verpflichtet sind, Bedingungen einzuhalten, die in Bezug auf die Verarbeitung und den Schutz Personenbezogener Kundendaten mindestens den Schutz vorsehen wie dieser Anhang (einschließlich der EU-Standardvertragsklauseln in Bezug auf Datenimporteure im Fall einer Weiterübermittlung Personenbezogener Daten aus der EU, dem EWR oder der Schweiz in ein Drittland ohne angemessenes Schutzniveau).
- 6.4. HPE haftet für Handlungen und Unterlassungen der von HPE mit der Erbringung der Services für die Kunden beauftragten Unterauftragsverarbeiter, die einen Verstoß gegen diesen Anhang darstellen, wie für eigene Handlungen oder Unterlassungen.

7. Prüfung und Zusicherung

- 7.1. HPE veranlasst Prüfungen der HPE-Datenverarbeitungs- und Datenschutzmaßnahmen durch namenhafte Prüfer, um die Einhaltung einschlägiger Datenschutzgesetze zu bestätigen und überlässt dem Kunden auf dessen Verlangen hin einen zusammenfassenden Bericht und weitere Informationen.
- 7.2. Nach Maßgabe des Vertrages ist der Kunde berechtigt, die Einhaltung der Pflichten aus dem Anhang durch HPE zu überprüfen. Die Prüfungsrechte werden in Absprache mit HPE und zu HPE-Geschäftszeiten ausgeübt. HPE ist verpflichtet, den Kunden oder die zuständige Datenschutzbehörde bei diesen Prüfungen zu unterstützen. Die Prüfungen sind unter Berücksichtigung der Betriebsabläufe und der Erfordernisse von HPE an Sicherheit und Vertraulichkeit durchzuführen.
- 7.3. Bei bestimmten Informationen zu den Sicherheitsmaßnahmen und -praktiken bei HPE handelt es sich um besonders schützenswerte vertrauliche Informationen, die HPE dem Kunden nicht offenlegen wird. HPE erklärt sich damit einverstanden, auf Verlangen und nicht mehr als einmal pro Jahr einen angemessenen Fragebogen zur Informationssicherheit in Bezug auf solche Sicherheitsmaßnahmen zu beantworten, die sich speziell auf die gemäß diesem Anhang erbrachten Services beziehen.
- 7.4. Auf Verlangen des Kunden stellt HPE innerhalb angemessener Zeit dem Kunden Informationen in angemessenem Umfang zu Verfügung, um die Einhaltung der geltenden Datenschutzgesetze nachzuweisen, sofern nicht diese Informationen dem Kunden ohne weiteres direkt durch die Nutzung der Services zugänglich sind.

8. Unterstützung des Kunden

- 8.1. Auf Verlangen des Kunden arbeitet HPE mit dem Kunden zusammen und gewährt diesem diejenige Unterstützung, die erforderlich ist, um die Verarbeitung der Personenbezogenen Kundendaten im Einklang mit den für den Kunden geltenden Datenschutzgesetzen in Bezug auf die HPE Services zu ermöglichen, beispielsweise durch:
 - 8.1.1. soweit möglich, Unterstützung des Kunden durch geeignete technische und organisatorische Maßnahmen bei dessen Pflicht, Anträgen natürlicher Personen nachzukommen, die ihre Rechte gemäß der für den Kunden geltenden Datenschutzgesetze ausüben;
 - 8.1.2. angemessene Unterstützung des Kunden bei der Beurteilung und Implementierung angemessener technischer und organisatorischer Maßnahmen, um ein Datenschutzniveau herzustellen, das für die mit der Datenverarbeitung verbundenen Risiken und die Art Personenbezogener Kundendaten angemessen ist;



- 8.1.3. Meldung von Sicherheitsvorfällen gemäß Anlage A;
- 8.1.4. angemessene Unterstützung des Kunden (i) bei der Durchführung einer Datenschutz-Folgenabschätzung und (ii) bei der Konsultation der Datenschutzaufsichtsbehörde.
- 8.2. Verlangt der Kunde Zusammenarbeit oder Unterstützung gemäß dieser Klausel, so hat er HPE die Anforderungen und Weisungen schriftlich mitzuteilen. HPE reagiert innerhalb einer angemessenen Zeit und lässt dem Kunden eine ungefähre Zeit- und Kostenschätzung für die Implementierung der Änderungen zukommen, die erforderlich sind, um die Compliance-Anforderungen des Kunden umzusetzen. Soweit die Einhaltung dieser Klausel eine Änderung des Umfangs der Services bedeutet, werden die Parteien in angemessener Weise einen entsprechenden Änderungsauftrag vereinbaren.
- 9. Datenqualität, Auslesen und Vernichtung, Reparatur- oder Austausch-Service**
- 9.1. Soweit es dem Kunden nicht selbst möglich ist, auf Personenbezogene Kundendaten zuzugreifen, wird HPE auf schriftliches Verlangen des Kunden (i) Personenbezogene Kundendaten aktualisieren, berichtigen oder löschen und/oder (ii) Kopien der Personenbezogenen Kundendaten zur Verfügung stellen.
- 9.2. Bei Beendigung des Vertrags gibt HPE nach Wahl des Kunden die Personenbezogenen Kundendaten zurück oder löscht sie. HPE behält keine Kopien der Personenbezogenen Kundendaten zurück, sofern nicht mit dem Kunden etwas anderes vereinbart ist oder HPE nach geltendem Recht dazu verpflichtet ist; in diesem Fall stellt HPE die aktive Verarbeitung der Daten ein und wahrt die Sicherheit und Vertraulichkeit der Daten.
- 9.3. In Bezug auf die Reparatur oder den Austausch von Datenträgern (Servern, Festplatten, SSD, Flash-Disks, Speichern etc.) kauft der Kunde entweder den optionalen (C)DMR Service oder löscht die Datenträger bzw. die sich darauf befindlichen Daten ausreichend (nach NIST-Standard), bevor er sie HPE überlässt.
- 10. Datenübermittlungen**
- 10.1. Um die Übermittlung von Personenbezogenen Daten aus der EU, dem EWR, dem Vereinigten Königreich (bis Ablauf der Übergangszeit des Brexit-Abkommens) oder der Schweiz durch den Kunden oder ein mit dem Kunden verbundenes Unternehmen an HPE oder ein mit HPE verbundenes Unternehmen zu regeln, der/das in einem Land ansässig ist, dem von der Europäischen Kommission nicht ein hinreichender Schutz Personenbezogener Daten gemäß Art. 25 Abs. 6 der Richtlinie 95/46/EG oder Art. 45 Abs. 3 der Datenschutz-Grundverordnung bestätigt wurde, kann sich der Kunde auf HPE's Binding Corporate Rules – Processors (BCR-P) oder einen EU-Standardvertrag gemäß den Standardvertragsklauseln für die Übermittlung personenbezogener Daten an Auftragsverarbeiter in Drittländern ("EU-Standardvertragsklauseln") berufen. Eine Auflistung der Services, die durch BCR-P geregelt sind, können auf der BCR Internetseite unter hpe.com/de/de/privacy/binding-corporate-rules.html eingesehen- oder auf Anforderung zur Verfügung gestellt werden.
- 10.2. In Übereinstimmung mit den BCR-P kann HPE (und jedes HPE Unternehmen sowie Unterauftragsverarbeiter, die vom Kunden zur Verarbeitung Personenbezogener Daten gemäß Ziffer 6 dieses Anhangs genehmigt wurden) Personenbezogene Daten in jedes Land übertragen oder Personenbezogene Daten von dort empfangen. Der Kunde hat dafür zu sorgen, dass betroffene Personen, vor der Übermittlung von sie betreffenden Sensiblen Daten, über diese Übermittlung informiert wurden oder vor der Übermittlung informiert werden, dass Sensible Daten in ein anderes Land übermittelt werden können. Der Kunde ist gemäß Abschnitt 4.1 der BCR-P berechtigt, die Rechte aus den BCR-P gegenüber HPE geltend zu machen und durchzusetzen. Die BCR-P umfassen eine Konzernvereinbarung sowie die anwendbaren Leitlinien und Anweisungen und ergeben damit die verbindlichen internen Datenschutzvorschriften für Auftragsverarbeiter in Bezug auf den Kunden; von Zeit zu Zeit werden diese in Übereinstimmung mit den anwendbaren Dokumenten der Artikel-29-Datenschutzgruppe (bzw. dem nachfolgend eingerichteten Europäischen Datenschutzausschuss), weiterentwickelt und/oder angepasst. Eine Kopie der die BCR-P bildenden Dokumente, auf die verwiesen wird und die Bestandteil dieses Anhangs sind, kann vom Kunden schriftlich angefordert werden. Der Kunde informiert die betroffenen Personen über die sich außerhalb der EU/EWR/Schweiz befindlichen Auftragsverarbeiter und darüber, dass hierfür in Einklang mit Datenschutzgesetzen auf BCR-P zurückgegriffen wird. Der Kunde stellt den betroffenen Personen auf Anfrage einen Link zu den BCR-Rechtshinweisen von HPE unter hpe.com/de/de/privacy/binding-corporate-rules.html zur Verfügung.
- 10.3. In Bezug auf die Übermittlung Personenbezogener Daten auf Basis eines EU-Standardvertrages, den HPE mit einem Unterauftragsverarbeiter abgeschlossen hat, räumt HPE dem Kunden diejenigen Rechte ein, als hätte der Kunde den EU-Standardvertrag direkt mit dem Unterauftragsverarbeiter abgeschlossen. Der Kunde stimmt der Übernahme der Rechte und Pflichten aus diesem EU-Standardvertrag zu.
- 10.3.1. Bei der Auslegung der EU-Standardvertragsklauseln ist der Begriff "Mitgliedsstaat, in dem der Datenexporteur niedergelassen ist" so auszulegen, dass damit (je nachdem) die Schweiz oder der EU-Mitgliedsstaat oder die Partei des EWR- Abkommens gemeint ist, in dem der Datenexporteur (wie in den EU-Standardvertragsklauseln definiert) niedergelassen ist.
- 10.3.2. Im Fall eines Widerspruchs zwischen EU-Standardvertragsklauseln, diesem Anhang und dem Vertrag, haben, soweit HPE Personenbezogene Daten von Einwohnern des EWR oder der Schweiz verarbeitet, die EU-Standardvertragsklauseln Vorrang, allerdings nur soweit zur Beseitigung des Widerspruchs erforderlich.



- 10.3.3. Prüfungen gemäß der EU-Standardvertragsklauseln sind nach den im Vertrag und Anlage A vorgesehenen allgemeinen Verfahren für Prüfungen durchzuführen, soweit sie nicht von einer Aufsichtsbehörde oder den Datenschutzgesetzen ausdrücklich abweichend vorgeschrieben sind. Der Kunde unternimmt wirtschaftlich zumutbare Anstrengungen, um der Aufsichtsbehörde die Prüfanforderungen des Vertrags mitzuteilen und zu verlangen, dass die Prüfung gemäß diesen Anforderungen durchgeführt wird.
- 10.3.4. Von den Parteien oder ihren jeweiligen verbundenen Unternehmen im Rahmen der EU-Standardvertragsklauseln erlittene Verluste sind so zu behandeln, als ob sie der Kunde bzw. HPE erlitten hätte und sie sind in allen Fällen unter Geltung der Haftungsbeschränkungen dieser Partei im Vertrag zu erstatten. Keine Bestimmung dieser Ziffer begrenzt die Haftung einer Partei in Bezug auf einen Anspruch einer betroffenen Person im Rahmen der EU-Standardvertragsklauseln.
- 10.3.5. Für den Fall, dass die EU-Standardvertragsklauseln keinen gültigen Übermittlungsmechanismus mehr darstellen, oder wenn HPE einen alternativen wirksamen Übermittlungsmechanismus einsetzt (z.B. verbindliche interne Datenschutzvorschriften für Auftragsverarbeiter – sog. Binding Corporate Rules Processorfor Processors), teilt HPE dem Kunden den Mechanismus mit und holt dessen Zustimmung ein, anstatt der EU-Standardvertragsklauseln diesen Mechanismus einzusetzen.

ANLAGE A – DATENVERARBEITUNG SUPPORT UND SONSTIGE DIENSTLEISTUNGEN („SERVICES“)

In dieser Anlage stellt HPE die für Services spezifischen Bestimmungen dar, einschließlich seiner Verpflichtung zu technischen und organisatorischen Sicherheitsmaßnahmen, um die Personenbezogenen Kundendaten zu schützen.

HPE nimmt im Rahmen der Services die folgende Verarbeitung personenbezogener Daten vor	Im Rahmen der Erbringung von Support Services zur Hardware- und Software-Wartung oder sonstigen Dienstleistungen vor Ort und per Remote-Zugriff hat HPE möglicherweise Zugang zu Daten, die in den Geschäftsanwendungen, der IT und Netzwerk-Infrastruktur des Kunden gespeichert sind, inklusive Metadaten. Diese Daten können Personenbezogene Kundendaten enthalten.
Art der Verarbeiten Personenbezogenen Kundendaten	Die Art der Verarbeiteten Personenbezogenen Daten hängt von den Daten ab, die der Kunde in den Geschäftsanwendungen, der IT und Netzwerk-Infrastruktur, inklusive in Metadaten gespeichert hat ab, und kann Sensible Daten umfassen.
Kategorien betroffener Personen	Jede betroffene Person, deren Personenbezogene Daten vom Kunden in den Geschäftsanwendungen, der IT und Netzwerk-Infrastruktur, inklusive in Metadaten gespeichert werden, einschließlich Kunden des Kunden, Endnutzern, Mitarbeitern, Auftragnehmern und Leiharbeitnehmern.
Dauer der Verarbeitung	HPE verarbeitet die Personenbezogenen Kundendaten für die Dauer des jeweiligen Vertrags.
Sicherheitsmaßnahmen	HPE unterhält das folgende Informationssicherheit- und physische Sicherheitsprogramm zum Schutz der Personenbezogenen Kundendaten ("HPE Sicherheitsprogramm").

- 1.1. Im Rahmen des HPE Sicherheitsprogramms führt HPE regelmäßige Überprüfungen der Sicherheitsmaßnahmen nach Industriestandards wie z.B. NIST, ISO 27001 und SOC durch. HPE bewertet das HPE Sicherheitsprogramm regelmäßig neu und aktualisiert es, wenn sich die Branche fortentwickelt, neue Technologien aufkommen oder neue Bedrohungen festgestellt werden.
- 1.2. Das HPE Sicherheitsprogramm umfasst mindestens Folgendes:
 - 1.2.1. HPE unterhält physische Sicherheitsstandards, die so ausgelegt sind, unbefugten physischen Zugang zu HPE Einrichtungen und Geräten zu verhindern, indem Folgendes angewandt wird:
 - der physische Zugang zu den Standorten ist auf HPE-Mitarbeiter, Unterauftragnehmer und befugte Besucher beschränkt;
 - für HPE-Mitarbeiter, Unterauftragnehmer und befugte Besucher werden Ausweise erstellt, die während des Aufenthalts auf dem Betriebsgelände zu tragen sind;
 - Überwachung des Zugangs zu HPE-Einrichtungen, einschließlich der zugangsbeschränkten Bereiche und der Geräte innerhalb der Einrichtungen;
 - der Zugang zum Rechenzentrum, in dem die Personenbezogenen Kundendaten gehostet werden, wird registriert, überwacht und verfolgt und
 - die Rechenzentren sind mit Alarmanlagen und Videokameras gesichert.



- 1.2.2. HPE unterhält folgende Standards zur Zugangskontrolle und -verwaltung der relevanten IT-Umgebung:
 - Administratorkonten sollten nur für den Zweck der Erbringung von Administratortätigkeiten genutzt werden.
 - Jedes Konto mit Administratorenrechten muss einer eindeutig identifizierbaren Person zugeordnet werden können.
 - Der gesamte Zugriff auf Computer und Server muss authentifiziert werden und darf nur im Rahmen des Aufgabengebiets eines Mitarbeiters erfolgen.
 - Initialpasswörter müssen vom Nutzer bei der ersten Nutzung geändert werden.
 - Anzeige und Drucken von Passwörtern muss verborgen, unterdrückt oder ansonsten unkenntlich gemacht werden, sodass unbefugte Parteien nicht in der Lage sind, sie zu sehen und anschließend wiederherzustellen.
 - Passwörter müssen einer Person eindeutig zugeordnet werden können.
 - Passwörter müssen bei der Übermittlung verschlüsselt sein.
 - Passwörter sollten so komplex sein, dass sie immer aus mindestens 3 von 4 Zeichenkategorien zusammengesetzt sind; als Zeichenkategorien müssen Großbuchstaben, Kleinbuchstaben, Ziffern oder Sonderzeichen zur Auswahl stehen.
 - Die Länge des Passworts muss mindestens 8 Zeichen betragen.
 - Die Passwörter müssen alle 90 Tage ablaufen.
 - Der Zugriff auf Computer und Server wird automatisch unterbrochen, wenn diese nicht genutzt werden; für den erneuten Zugriff ist eine Passwortauthentifizierung erforderlich.
 - Die Konten müssen nach mehreren fehlerhaften Anmeldeversuchen auf "gesperrt" gesetzt werden.
- 1.2.3. Computer und Server verfügen über angemessene aktuelle Versionen von Systemsicherheitssoftware, die eine Hostfirewall, Virenschutz sowie aktuelle Patches und Virendefinitionen enthalten können. Die Software ist so konfiguriert, dass sie nach bestimmten Ergebnissen sucht und diese umgehend entfernt oder berichtigt. HPE führt Protokolle über die verschiedenen Komponenten der Infrastruktur und unterhält ein System zur Erkennung von Eindringlingen, um Missbrauchsmuster, verdächtige Aktivitäten, unbefugte Nutzer und sonstige tatsächliche oder drohende Sicherheitsrisiken zu überwachen, festzustellen und zu melden.
- 1.3. Auf Verlangen prüft HPE mit dem Kunden eine Zusammenfassung der Schwachstellenbeurteilungen. Schwachstellenbeurteilungen berechtigen den Kunden nicht, Aufzeichnungen und/oder Verfahren einzusehen oder in irgendeiner Weise darauf zuzugreifen, wenn (a) sie nicht in unmittelbarem Bezug zu den Services stehen, (b) dadurch gegen geltende Gesetze verstoßen wird und/oder (c) dadurch gegen von HPE Dritten geschuldeten Vertraulichkeits- und Sicherheitspflichten verstoßen wird.
- 1.4. Mitarbeiter und Auftragnehmer werden zu HPE-Datenschutz- und Sicherheitsrichtlinien geschult und auf ihre Verantwortung in Bezug auf die Datenschutz- und Sicherheitspraktiken hingewiesen. HPE-Mitarbeiter und Auftragnehmer sind vertraglich zur Wahrung der Vertraulichkeit Personenbezogener Kundendaten und Einhaltung der geltenden HPE-Richtlinien, Standards oder Anforderungen in Bezug auf die Verarbeitung Personenbezogener Kundendaten verpflichtet. Eine Nichteinhaltung dieser Richtlinien, Standards oder Anforderungen wird einer Untersuchung unterzogen und kann Disziplinarmaßnahmen bis hin zur Beendigung des Arbeitsverhältnisses oder der Beauftragung durch HPE zur Folge haben.
- 1.5. Bestätigt HPE einen Sicherheitsverstoß, der zu unbeabsichtigter oder unrechtmäßiger Vernichtung, Verlust, Veränderung oder unbefugter Offenlegung von oder unbefugtem Zugang zu Personenbezogenen Kundendaten führt ("Sicherheitsvorfall"),
 - 1.5.1. informiert HPE den Kunden unverzüglich über den Sicherheitsvorfall. HPE hält den Kunden über den Stand des Sicherheitsvorfalls auf dem Laufenden, bis die Angelegenheit behoben ist. Die Berichte umfassen unter anderem eine Beschreibung des Sicherheitsvorfalls, die ergriffenen Maßnahmen und Maßnahmenpläne. Erlangt der Kunde Kenntnis von einem Sicherheitsvorfall, der sich auf die Services auswirkt, meldet der Kunde den Sicherheitsvorfall umgehend an HPE und teilt HPE den Umfang des Sicherheitsvorfalls mit.
 - 1.5.2. gewährt HPE auf Verlangen und auf Kosten des Kunden dem Kunden angemessene Unterstützung, (i) bei der Meldung eines Sicherheitsverstoßes an die nach den für den Kunden geltenden Datenschutzgesetzen zuständige Aufsichtsbehörde und (ii) bei der Benachrichtigung der von der Verletzung des Schutzes Personenbezogener Daten betroffener Personen in den Fällen, in denen die Verletzung des Schutzes Personenbezogener Daten voraussichtlich ein hohes Risiko für die persönlichen Rechte und Freiheiten natürlicher Personen zur Folge hat.



Entscheiden Sie sich für das richtige Produkt.
Kontaktieren Sie unsere Presales-Experten.



Chat



E-Mail



Telefon



Updates abrufen