ADDENDUM ZUR VERARBEITUNG VON KUNDENDATEN

Dieses Addendum zur Datenverarbeitung (Data Processing Addendum, „DPA“) und die geltenden Anhänge regeln alle Situationen, in denen HP als Auftragsverarbeiter handelt und im Auftrag des Kunden personenbezogene Daten des Kunden im Rahmen der Erbringung der gemäß dem/den geltenden Vertrag/Verträgen („Dienstleistungsvertrag“) zwischen HP und dem Kunden vereinbarten Leistungen verarbeitet. Dieses DPA betrifft nicht jene Fälle, in denen HP und der Kunde als eigenständige Verantwortliche erachtet werden. Hier verwendete, kursiv gedruckte [in der englischen Version großgeschriebene] Begriffe haben die im Dienstleistungsvertrag vereinbarte Bedeutung. Im Falle eines Konflikts zwischen den Bestimmungen des Dienstleistungsvertrags, soweit sich diese sich auf die Verarbeitung personenbezogener Daten beziehen, und des DPA hat das DPA Vorrang.

1 DEFINITIONEN

1.1 **„Kunde“** bezeichnet die Endkunden der HP Services;

1.2 **„Personenbezogene Daten des Kunden“** bezeichnet die personenbezogenen Daten, für die der Kunde der Verantwortliche ist und die durch HP als Auftragsverarbeiter oder den Unter – Auftragsverarbeiter von HP im Rahmen der Erbringung der Leistungen verarbeitet werden;

1.3 **„Verantwortlicher“** bezeichnet die natürliche oder juristische Person, Behörde, Einrichtung oder jede andere Stelle, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung personenbezogener Daten bestimmt; wo die Zwecke und Mittel der Verarbeitung von nationalen oder gemeinschaftlichen Rechtsvorschriften oder Verordnungen durch Unionsrecht oder das Recht der Mitgliedsstaaten bestimmt werden, kann der Verantwortliche oder die spezifischen Kriterien für seine Benennung durch Unionsrecht oder das Recht der Mitgliedsstaaten bestimmt werden;

1.4 **„Auftragsverarbeiter“** bezeichnet eine natürliche oder juristische Person, Behörde, Einrichtung oder jede andere Stelle, die personenbezogene Daten im Auftrag des Verantwortlichen oder auf Anweisung eines anderen Verantwortlichen, der im Auftrag eines Verantwortlichen handelt, verarbeitet;

1.5 **„Gesetze zum Schutz der Daten und der Privatsphäre“** bezeichnet alle gegenwärtigen und zukünftigen Gesetze und Vorschriften im Zusammenhang mit der Verarbeitung, Sicherheit, dem Schutz und der Aufbewahrung personenbezogener Daten sowie der Privatsphäre, die in den entsprechenden Rechtsgebieten existieren und zu denen u. a. die Richtlinie 95/46/EG zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr, die Richtlinie 2002/58/EG über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation sowie alle nationalen Gesetze und Vorschriften zur Umsetzung der vorstehenden Richtlinien, die DSGVO (sofern geltend) und alle sonstigen Datenschutzgesetze von Norwegen, Island, Liechtenstein, der Schweiz oder Großbritanniens (sobald Großbritannien nicht mehr länger Teil der EU ist) sowie alle Änderungen an diesen Gesetzen und Vorschriften und als Ersatz an deren Stelle tretenden Gesetze und Vorschriften gehören;

1.6 **„Betroffene Person“** hat die dem Begriff „betroffene Person“ in den jeweils geltenden Gesetzen zum Schutz der Daten und der Privatsphäre zugewiesene Bedeutung und umfasst mindestens alle identifizierten oder identifizierbaren natürlichen Personen, auf die sich die personenbezogenen Daten beziehen;

1.7 **„EU“** bezeichnet die Europäische Union sowie zusammen alle Länder, die Mitglieder dieser Union sind;

1.8 **„Europäisches Land“** bezeichnet einen Mitgliedstaat der EU, Norwegen, Island, Liechtenstein, die Schweiz und Großbritannien, sobald Großbritannien nicht mehr länger ein Mitgliedstaat der EU ist;

1.9 **„EU-Standardvertragsklauseln“** bezeichnet die EU-Standardvertragsklauseln für die Übermittlung personenbezogener Daten an Auftragsverarbeiter (2010/87/EU) oder den Nachfolger dieses Beschlusses;

1.10 **„EU-US Privacy Shield“ oder „EU-US-Datenschutzschild“** bezeichnet den unter der Bezeichnung EU-US Privacy Shield durch das US-Handelsministerium und die Europäische Kommission etablierten Rechtsrahmen in seiner jeweils gültigen Fassung;

1.11 **„DSGVO“** bezeichnet die Datenschutz-Grundverordnung (EU) 2016/679 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr;

1.12 **„HP Group“** bezeichnet HP Inc. (1501 Page Mill Road, Palo Alto, CA 94304) und alle in deren Mehrheitsbesitz befindlichen und unter deren Kontrolle stehenden Tochtergesellschaften, ungeachtet des jeweiligen Rechtsgebiets, in dem Gründung oder Geschäftstätigkeiten erfolgen;

1.13 **„Personenbezogene Daten“** bezeichnen alle Informationen, die sich auf eine identifizierte oder identifizierbare lebende natürliche Person beziehen sowie jene, wie sie anderweitig durch geltende Gesetze zum Schutz der Daten und der Privatsphäre definiert sind. Eine identifizierbare Person ist eine Person, die direkt oder indirekt identifiziert werden kann, insbesondere durch Zuordnung zu einem Kennzeichen, wie beispielsweise zu einem Namen, zu einer Kennziffer, zu Standortdaten, zu einer Online-Kennung oder zu einem oder mehreren besonderen Merkmalen, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität sind;

1.14 **Ein „personenbezogene Daten betreffender Zwischenfall“** hat die Bedeutung, die jeweils dem Begriff „Sicherheitsvorfall“, „Sicherheitslücke“ oder „Verletzung des Schutzes personenbezogener Daten“ durch die geltenden Gesetze zum Schutz der Daten und der Privatsphäre zugewiesen wurden, und schließt dabei jede Situation ein, in der HP feststellt, dass auf Personenbezogene Daten des Kunden durch unbefugte Personen bzw. auf eine unbefugte Weise zugegriffen wurde, diese Personenbezogenen Daten des Kunden durch unbefugte Personen bzw. auf eine unbefugte Weise offengelegt, geändert, verloren, zerstört oder genutzt wurden bzw. dass derartige Geschehnisse wahrscheinlich sind;

1.15 **„Verarbeiten“**, **„verarbeitet“**, **„Verarbeitung“** oder **„verarbeitet“** bezeichnet jeden Vorgang oder jede solche Vorgangsreihe im Zusammenhang mit personenbezogenen Daten wie das Erheben, das Erfassen, die Organisation, das Ordnen, die Speicherung, die Anpassung oder Veränderung, das Auslesen, das Abfragen, die Verwendung, die Offenlegung durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung, den Abgleich oder die Verknüpfung, die Einschränkung, das Löschen oder die Vernichtung sowie alle gleichartigen Definitionen in geltenden Gesetzen zum Schutz der Daten und der Privatsphäre, sofern derartige Definitionen über diese Definition hinausgehen;

1.16 **„Entsprechendes Land“** bezeichnet alle anderen Länder als diese europäischen Länder und andere Länder in Hinblick auf welche eine Angemessenheitsfeststellung im Rahmen von Artikel 25 Absatz 6 der europäischen Datenschutzrichtlinie bzw. von Artikel 45 DSGVO besteht;

1.17 **„Leistungen“** bezeichnen Leistungen einschließlich von Produkten und Kundendienst, die durch HP im Rahmen des Dienstleistungsvertrags erbracht werden;

1.18 **„Dienstleistungsvertrag“** bezeichnet den Vertrag zwischen HP und dem Kunden über den Erwerb von Leistungen von HP; und

1.19 **„Unter-Auftragsverarbeiter“** bezeichnet jede durch HP bzw. durch jeden anderen Unter-Auftragsverarbeiter von HP beauftragte Einrichtung, die Personenbezogene Daten des Kunden für Verarbeitungstätigkeiten erhält, die im Auftrag des Kunden durchgeführt werden sollen.

2 GELTUNGSBEREICH & EINHALTUNG GELTENDEN RECHTS

2.1 Dieses DPA regelt lediglich die Verarbeitung der personenbezogenen Daten des Kunden durch HP im Zusammenhang mit der Erbringung von Leistungen durch HP und jene Fälle, in denen HP als Auftragsverarbeiter im Auftrag des Kunden, der selbst Verantwortlicher ist, handelt. Dieses DPA betrifft nicht jene Fälle, in denen HP und der Kunde als eigenständige Verantwortliche erachtet werden.

2.2 Die Kategorien von betroffenen Personen, der Arten verarbeiteter personenbezogener Daten des Kunden und der Verarbeitungszwecke sind in Anlage 1 dieses DPA dargelegt. HP wird Personenbezogene Daten des Kunden für die Dauer des Dienstleistungsvertrags (oder darüber hinaus, soweit dies gemäß geltendem Recht erforderlich ist) verarbeiten.

2.3 Der Kunde allein trägt mit seiner Inanspruchnahme der HP-Leistungen die alleinige Verantwortung für die Einhaltung aller geltenden Gesetze zum Schutz der Daten und der Privatsphäre in Hinblick auf die Richtigkeit, Qualität und Rechtmäßigkeit der personenbezogenen Daten des Kunden, die von HP im Zusammenhang mit den Leistungen verarbeitet werden sollen. Der Kunde muss des Weiteren Sorge tragen, dass seine an HP erteilten Anweisungen in Bezug auf die Verarbeitung der personenbezogenen Daten des Kunden unter Einhaltung der geltenden Gesetze zum Schutz der Daten und der Privatsphäre erfolgt und darf HP nicht in eine Situation bringen, in welcher HP gegen seine Pflichten im Rahmen der geltenden Gesetze zum Schutz der Daten und der Privatsphäre verstößt.

2.4 Wenn der Kunde die Leistungen für die Verarbeitung von Kategorien personenbezogener Daten in Anspruch nimmt, die nicht ausdrücklich Gegenstand dieses DPA sind, handelt der Kunde auf eigene Gefahr hin und HP trägt keinerlei Verantwortung für etwaige Defizite bezüglich der Rechtmäßigkeit im Zusammenhang mit einer solchen Inanspruchnahme.

2.5 Sofern HP etwaige personenbezogene Daten von HP-Mitarbeitern dem Kunden gegenüber offenlegt oder ein HP-Mitarbeiter personenbezogene Daten direkt dem Kunden zur Verfügung stellt, weil dieser die personenbezogenen Daten administrative Zwecke in Bezug auf die Inanspruchnahme der Leistungen verarbeitet, muss der Kunde diese personenbezogenen Daten gemäß seinen Datenschutzbestimmungen sowie gemäß den geltenden Gesetzen zum Schutz der Daten und der Privatsphäre verarbeiten. Derartige Offenlegungen erfolgen durch HP nur dann, wenn diese für die Zwecke der Vertragsverwaltung, des Leistungsmanagements oder einer angemessenen Sicherheitsüberprüfung vonseiten des Kunden oder für Sicherheitszwecke gesetzlich zulässig sind.

3 PFLICHTEN DES AUFTRAGSVERARBEITERS

3.1 Ungeachtet anderslautender Bestimmungen in dem Dienstleistungsvertrag wird HP im Zusammenhang mit personenbezogenen Daten des Kunden:

3.1.1 Personenbezogene Daten des Kunden nur gemäß der dokumentierten Anweisungenen des Kunden verarbeiten (die spezifischer oder allgemeiner Natur sein können, gemäß den Festlegungen des Dienstleistungsvertrags oder wie in anderer Form durch den Kunden mitgeteilt). Ungeachtet des Vorstehenden wird HP ggf. Personenbezogene Daten des Kunden, so wie gemäß geltendem Recht erforderlich, verarbeiten. In dieser Situation wird HP angemessene Schritte zur Information des Kunden über derartige Erfordernisse ergreifen, bevor HP die Daten verarbeitet, es sei denn, dass dies gesetzlich verboten ist;

3.1.2 Sorge tragen, dass nur befugte Mitarbeiter, die angemessen im Schutz und in der Handhabung personenbezogener Daten geschult worden sind und zur Wahrung der Vertraulichkeit der personenbezogenen Daten des Kunden verpflichtet wurden, Zugang zu diesen erhalten.

3.1.3 angemessene technische und organisatorische Sicherheitsmaßnahmen umsetzen, um sich gegen eine unbeabsichtigte oder rechtswidrige Zerstörung, einen Verlust, eine Abänderung, nicht autorisierte Weitergabe, oder einen Zugriff auf personenbezogene Daten zu schützen.

Diese Maßnahmen sind im Verhältnis zu dem Schaden, der aus unbefugter oder rechtswidriger Verarbeitung, versehentlichem Verlust, der Zerstörung, Beschädigung oder dem Diebstahl personenbezogener Daten des Kunden erwachsen kann, angemessen und berücksichtigen die Natur der personenbezogenen Daten des Kunden, welche damit geschützt werden sollen. Anlage 2 enthält eine Zusammenfassung der Sicherheitsmaßnahmen von HP.

3.1.4 ohne Verzögerung und im gesetzlich zulässigen Umfang den Kunden über alle Anfragen von betroffenen Personen informieren, die ihre Rechte gemäß den geltenden Gesetzen zum Schutz der Daten und der Privatsphäre ausüben möchten. Auch wird HP soweit wie möglich auf schriftliches Ersuchen und Kosten des Kunden sowie unter Berücksichtigung der Verarbeitungsart den Kunden in der Umsetzung angemessener technischer sowie organisatorischer Maßnahmen unterstützen, um bei der Erfüllung der Pflichten des Kunden bezüglich der Erwiderung auf derartige Anfragen zu helfen. Soweit diese personenbezogenen Daten des Kunden für den Kunden nicht über die im Rahmen des Dienstleistungsvertrags erbrachten Leistungen zugänglich sind, wird HP, soweit dies gesetzlich zulässig ist und auf Ersuchen des Kunden hin, wirtschaftlich vertretbare Anstrengungen unternehmen, um dem Kunden bei der Erwiderung auf solche Ersuchen zu unterstützen, wenn diese Erwiderungen auf solche Anfragen durch die geltenden Gesetze zum Schutz der Daten und der Privatsphäre vorgeschrieben sind;

3.1.5 auf schriftliches Ersuchen und auf Kosten des Kunden sowie unter Berücksichtigung der Verarbeitungsart bzw. der HP zur Verfügung stehenden Informationen den Kunden hinsichtlich seiner Pflichten gemäß Artikel 32 bis 36 DSGVO bzw. gemäß vergleichbaren Bestimmungen im Rahmen geltender Gesetze zum Schutz der Daten und der Privatsphäre unterstützen. HP behält sich das Recht vor, eine Verwaltungsgebühr für die im Rahmen dieser Klausel 3.1.5 bzw. der Klauseln 3.1.3 und 3.1.4 erbrachten Unterstützung zu berechnen; und

3.1.6 auf schriftliches Ersuchen des Kunden hin, nach der beendeten Leistungserbringung solche personenbezogenen Daten des Kunden zu löschen oder an den Kunden zurückzugeben, es sei denn, dass das geltende Recht die Aufbewahrung der personenbezogenen Daten des Kunden verlangt.

4 UNTERAUFTRAGSVERARBEITUNG

4.1 Der Kunde erteilt HP die Befugnis, Personenbezogene Daten des Kunden an Unternehmen der HP Inc. Group bzw. an externe Parteien in ihrer Eigenschaft als Unter-Auftragsverarbeiter zu übermitteln bzw. diesen Zugriff darauf zu gewähren (und die Ernennung von Unter-Auftragsverarbeitern gemäß Klausel 4.1 zu gestatten), sodass die Leistungserbringung bzw. die Umsetzung der anderen im Abschnitt „Verarbeitungstätigkeiten“ in der Anlage 1 benannten Zwecke möglich wird. HP trägt die Verantwortung dafür, dass seine Unter-Auftragsverarbeiter die sich aus diesem DPA ergebenden Pflichten erfüllen. HP wird Sorge tragen, dass jeder Unter-Auftragsverarbeiter, an den HP Personenbezogene Daten des Kunden übermittelt, eine schriftliche Vereinbarung mit HP abschließt, die vorschreibt, dass die Unter-Auftragsverarbeiter sich an Bestimmungen halten, deren Schutzwirkung mindestens so hoch sind wie jene ist, die in diesem DPA festgelegt sind. HP wird dem Kunden die aktuelle Liste von Unter-Auftragsverarbeitern für die Leistungen, die in dem Dienstleistungsvertrag geregelt sind, zur Verfügung stellen.

4.2 HP kann jederzeit und ohne Rechtfertigung einen neuen Unter-Auftragsverarbeiter ernennen, sofern dem Kunden dies mindesten zehn (10) Tage im Voraus mitgeteilt wird und der Kunde nicht berechtigterweise solchen Änderungen innerhalb dieser Frist widerspricht. Berechtigte Einwendungen müssen angemessene und dokumentierte Gründe in Bezug auf die Verstöße eines Unter-Auftragsverarbeiters gegen die geltenden Gesetze zum Schutz der Daten und der Privatsphäre enthalten. Wenn entsprechend der begründeten Auffassung von HP derartige Einwendungen berechtigt sind, wird HP davon Abstand nehmen, einen solchen Unter-Auftragsverarbeiter im Zusammenhang mit der Verarbeitung personenbezogener Daten des Kunden einzusetzen. In solchen Fällen wird HP

angemessene Anstrengungen unternehmen um (i) dem Kunden eine Änderung in den Leistungen von HP zu ermöglichen oder um (ii) dem Kunden eine Änderung hinsichtlich seiner Konfiguration oder Inanspruchnahme der Leistungen zu empfehlen, sodass die Verarbeitung personenbezogener Daten des Kunden durch den abgelehnten Unter-Auftragsverarbeiter vermieden werden kann. Sollte HP nicht zu solchen Änderungen innerhalb einer angemessenen Frist in der Lage sein, die nicht mehr als neunzig (90) Tage betragen darf, kann der Kunde durch schriftliche Mitteilung an HP die Leistungen kündigen, welche von HP nicht ohne die Inanspruchnahme des abgelehnten Unter-Auftragsverarbeiters erbracht werden können.

5 PERSONENBEZOGENE DATEN BETREFFENDE ZWISCHENFÄLLE

5.1 HP wird den Kunden unverzüglich informieren, sobald ihm ein personenbezogene Daten betreffender Zwischenfall, der Personenbezogene Daten des Kunden betrifft, bekannt wird, und wird die Maßnahmen innerhalb einer angemessenen Frist ergreifen, die der Kunde jeweils vernünftigerweise verlangen kann, um den personenbezogene Daten betreffenden Zwischenfall zu beheben, und weitere Informationen weiterleiten, soweit sie der Kunde vernünftigerweise verlangen kann. HP behält sich das Recht vor, eine Verwaltungsgebühr für die im Rahmen dieser Klausel 5.1 erbrachte Unterstützung zu berechnen, es sei denn, dass der Kunde nachweist, dass eine solche Unterstützung aufgrund der Nichteinhaltung dieses DPA durch HP erforderlich ist, wobei auch der Umfang, in dem dieser Nachweis erbracht wird, zu berücksichtigen ist.

6 INTERNATIONALE ÜBERMITTLUNGEN PERSONENBEZOGENER DATEN DES KUNDEN

6.1 HP wird ggf. Personenbezogene Daten des Kunden in andere Länder als das Land übermitteln, in dem die Daten ursprünglich erhoben wurden, vorausgesetzt, dass eine solche Übermittlung im Zusammenhang mit den Leistungen erforderlich ist und diese Übermittlung gemäß den geltenden Gesetzen zum Schutz der Daten und der Privatsphäre erfolgt.

6.2 EUROPASPEZIFISCHE VORSCHRIFTEN

6.2.1 Sofern Personenbezogene Daten des Kunden aus einem europäischem Land in ein entsprechendes Land übermittelt werden, wird HP mitteilen, welche der nachstehend aufgelisteten Übermittlungsmechanismen dabei in gemäß der in Klausel 6.2.2 festgelegten Rangfolge für derartige Übermittlungen gemäß den geltenden Gesetzen zum Schutz der Daten und der Privatsphäre Anwendung finden:

6.2.1.1 EU-U.S. Privacy Shield: HP ist im Rahmen des EU-U.S. Privacy Shield für Personenbezogene Daten des Kunden zertifiziert und garantiert, dass HP weiterhin über diese Zertifizierung verfügen wird. HP wird den Kunden umgehend informieren, sollte HP die Zertifizierungen nicht verlängern oder verlieren bzw. die Zertifizierungen so ändern, dass die Verarbeitung personenbezogener Daten des Kunden nicht länger Gegenstand der Zertifizierung ist.

6.2.1.2 EU-Standardvertragsklauseln: Die EU-Standardvertragsklauseln werden hiermit in Gänze in dieses DPA aufgenommen und HP wird, soweit zutreffend, Sorge tragen, dass seine Unter-Auftragsverarbeiter die Pflichten eines Datenimporteurs (wie in den EU-Standardvertragsklauseln definiert) erfüllen werden. Soweit ein Konflikt zwischen diesem DPA und den EU-Standardvertragsklauseln bestehen sollten, haben die Bestimmungen der EU-Standardvertragsklauseln Vorrang.

6.2.2 Falls für die Leistungen mehr als ein Übermittlungsmechanismus zutrifft, unterliegt die Übermittlung personenbezogener Daten des Kunden einem einzigen Übermittlungsmechanismus unter Beachtung der folgenden Rangfolge: 1) EU-U.S. Privacy Shield-Zertifizierung von HP; und 2) die EU-Standardvertragsklauseln.

7 PRÜFUNGEN

7.1 Auf schriftliches Ersuchen des Kunden hin, wird HP dem Kunden alle Informationen zur Verfügung stellen, die für den Nachweis über die Einhaltung der in den geltenden Gesetzen zum Schutz der Daten und der Privatsphäre festgelegten Pflichten erforderlich sind, vorausgesetzt, dass HP nicht verpflichtet wird, vertrauliche Geschäftsdaten vorzulegen. Höchstens einmal jährlich und auf Kosten des Kunden wird HP des Weiteren Prüfungen und Inspektionen durch den Kunden bzw. dessen beauftragten externen Prüfer, bei dem es sich nicht um einen Wettbewerber von HP handeln darf, gestatten und an diesen mitwirken. Der Umfang etwaiger Prüfungen dieser Art, einschließlich der Vertraulichkeitsbestimmungen, ist einvernehmlich zwischen den Parteien vor der Prüfung zu vereinbaren.

8 HAFTUNG

8.1 Die Haftung von HP, welche aus bzw. im Zusammenhang mit seiner Verarbeitung personenbezogener Daten des Kunden gemäß DPA erwächst (ungeachtet der Frage, ob in Bezug auf den Vertrag, aus unerlaubter Handlung oder im Rahmen einer anderen Haftungstheorie), ist Gegenstand aller etwaigen Bestimmungen zur Haftungsbeschränkung, die in dem Dienstleistungsvertrag festgelegt sind.

Anlage 1

Angaben zur Verarbeitung

HP kann diese Anlage 1 periodisch aktualisieren, um Änderungen bei den Verarbeitungstätigkeiten Rechnung zu tragen.

Kategorien von betroffenen Personen

- Mitarbeiter des Kunden, Vertreter des Kunden und Unterauftragnehmer.

Arten personenbezogener Daten

Die personenbezogenen Daten des Kunden, welche durch HP im Zusammenhang mit der Erbringung der Leistungen verarbeitet werden, werden durch den Kunden in seiner Eigenschaft als Verantwortlicher sowie gemäß der entsprechenden Leistungsbeschreibung und/oder dem Kaufauftrag/Änderungsauftrag festgelegt und kontrolliert, können dabei jedoch zum Beispiel Folgende enthalten:

- *Kontaktdaten* – wie beispielsweise Name, dienstliche Telefonnummer, dienstliche E-Mail-Adresse und Adresse des Dienstsitzes;
- *Daten zu Berechtigungsnachweisen und sicheren Anmeldung* – wie beispielsweise Mitarbeiterkennung oder Ausweisnummer;
- *Daten zur Produktnutzung* – wie beispielsweise gedruckte Seiten, Druckmodus, verwendete Medien, Marke der Tintenpatrone oder des Toners, Typ der gedruckten Datei (.pdf, .jpg usw.), für den Druck verwendete Anwendungssoftware (Word, Excel, Adobe Photoshop usw.), Dateigröße, Zeitstempel, sowie Nutzung und Status weiteren Druckerzubehörs;
- *Leistungsdaten* – Druckvorgänge, Funktionen und verwendete Warnmeldungen, wie beispielsweise „Wenig Tinte"-Warnungen, Verwendung von Fotokarten, Fax, Scanner, integriertem Webserver und zusätzliche technische Informationen, die je nach Produkt unterschiedlich sein können;
- *Gerätedaten* – Informationen über Computer, Drucker und/oder Geräte, wie beispielsweise Betriebssystem, Speichergröße, Region, Sprache, Zeitzone, Modellnummer, Datum der Inbetriebnahme, Gerätealter, Herstellungsdatum des Geräts, Browserversion, Computerhersteller, Verbindungsschnittstelle, Garantiestatus, eindeutige Gerätekennungen, Werbungkennungen und zusätzliche technische Informationen, die je nach Produkt unterschiedlich sein können;
- *Daten zu Anwendungssoftware* – Informationen im Zusammenhang mit der HP-Anwendungssoftware, wie beispielsweise Standort, Sprache, Softwareversion, Einstellung zur gemeinsamen Datennutzung und Angaben zur Aktualisierung; und
- Weitere durch die betroffene Person bereitgestellte personenbezogene Daten, wenn diese persönliche, online oder telefonisch bzw. per E-Mail mit den Kundendienstzentren, Help Desks oder weiteren Kundensupportkanälen interagiert, um die Erbringung von HP Services zu ermöglichen oder in Reaktion auf Anfragen des Kunden und/oder der betroffenen Person.

Verarbeitungstätigkeiten

Die im Zusammenhang mit dem Dienstleistungsvertrag verarbeiteten personenbezogenen Daten des Kunden werden von HP zur Betreuung der Beziehung mit dem Kunden bzw. zur Erbringung der Leistungen für den Kunden verwendet. HP kann die personenbezogenen Daten des Kunden verarbeiten, um:

- Leistungen zum Geräteparkmanagement zu erbringen, wie beispielsweise Managed Print Services und Device as a Service;
- seine Kontakt- und Registrierungsdaten zu pflegen, sodass die Erbringung umfassender Support- und Wartungsleistungen, einschließlich Care Pack und erweiterter Gewährleistungssupport, sowie die Durchführung von Reparaturen und Rücksendungen möglich sind;
- um Zugang zu Portalen für die Bestellung und Durchführung von Aufträgen für Produkte bzw. Dienstleistungen zu gewähren, zur Kontenverwaltung und die Organisation von Versand bzw. Lieferungen;

- um die Leistung und die Bedienung von Produkten, Lösungen, Diensten und Support zu verbessern, einschließlich des Gewährleistungssupports und sowie rechtzeitiger Firmware- und Softwareaktualisierungen bzw. Warnungen, die den kontinuierlichen Betrieb bzw. die kontinuierliche Erbringung der Leistung gewährleisten;
- zur Durchführung verwaltungstechnischer Kommunikation mit den Kunden in Bezug auf die Leistungen. Zu den Beispielen verwaltungstechnischer Kommunikation gehören u. a. Antworten auf Anfragen oder Ersuchen des Kunden, Kommunikation in Bezug auf den Abschluss von Leistungserbringungen oder Gewährleistungen, Mitteilungen über Produktrückrufe aus Sicherheitsgründen oder relevante Mitteilungen über Fusionen, Unternehmensübernahmen bzw. Veräußerungen;
- die Integrität und Sicherheit der Internetseiten, Produkte, Funktionen und Dienste von HP aufrechtzuerhalten, sowie zur Verhinderung und Aufdeckung von Sicherheitsbedrohungen, Betrugsversuchen und sonstigen kriminellen bzw. böswilligen Handlungen, die eine Gefahr für die Daten des Kunden darstellen;
- um die Identität des Kunden zu kontrollieren, einschließlich Aufforderung zur Nennung des Anrufernamens bzw. der Mitarbeiteridentifikationsnummer oder Ausweisnummer für die Erbringung von Remote-Wartungsleistungen durch HP;
- um geltende gesetzliche Bestimmungen bzw. Vorschriften, Gerichtsbeschlüsse, Forderungen staatlicher Behörden sowie von Rechtspflegeorganen zu erfüllen und um Mitarbeiter sowie andere Kunden zu schützen und um Streitigkeiten beizulegen; und
- auf Kundenbedürfnisse zugeschnittene Leistungen zu erbringen, um Dienste sowie Kommunikationen zu personalisieren und um Empfehlungen zu erstellen.

Anlage 2

SUMMARY OF HP SECURITY MEASURES

To protect Customer data, HP abides by a robust set of information security controls including policies, practices, procedures and organizational structures to protect the confidentiality, integrity and availability of its own and its Customers' information (including Personal Data as defined in HP's Customer and Data Processing Addenda). The following sets forth an overview of the technical/organizational security measures deployed by HP throughout the company.

1. Security Policy

HP maintains globally applicable policies, standards, and procedures intended to protect HP and Customer data. The detail of HP's security policies are confidential to protect the integrity of HP's data and systems. However, summaries of our key policies are included below.

2. Information Security Organization

HP has an Information Security Organization that is responsible for directing and managing the information security strategy and controls adopted by the organization. An Information Security Framework/Management System is put in place to ensure compliance with HP's security policies and controls as well as to confirm that the security requirements of its Customers are complied with. This Framework is structured in alignment with the NIST Cybersecurity Framework and is reviewed annually.

3. Asset Management

HP has a process in place for identifying technical information assets and through this process HP identifies all assets under its responsibility and categorizes the critical assets. HP further maintains a set of documented handling procedures for each information classification type including those assets that contain Personal Data. Handling procedures address storage, transmission, communication, access, logging, retention, destruction, disposal, incident management, and breach notification.

4. Access Control

The principle of least privilege is used for providing logical access control. User access is provided via a unique user ID and password. HP's password policy has defined complexity, strength, validity and password-history related controls. Access rights are reviewed on a periodic basis and revoked upon personnel departure.

User account creation and deletion procedures as have been mutually agreed upon are implemented, for granting and revoking access to client systems that are used during the course of the engagement.

5. Personnel Training

HP employees are required to complete the Integrity at HP training which is designed to ensure that new employees are familiar with the program, policies, and resources that govern HP expectations for ethical behavior, excellence, and compliance. Integrity at HP features modules on security and data privacy and employees also are required to take an annual "refresher" course. HP employees also undergo a periodic security awareness training focused on essential security policies and emphasizing the user responsibilities related to incident management, data privacy and information security.

6. Third Parties and Subcontractors

HP has processes in place to select sub-contractors that are able to comply with comprehensive contractual security requirements.

7. Systems Security

By policy, development of systems and supporting software within HP follow a secure development methodology to ensure security throughout the system/software lifecycle. The Software Development Lifecycle defines initiation, development/acquisition, implementation, operations, and disposal requirements. All system components, which include modules, libraries, services, and discrete components, are evaluated to determine their impact on the overall system security state.

HP has defined controls for the protection of application service transactions. These controls include: validating and verifying user credentials, mandating digital signatures and encryption, implementing secure communication protocols, storing online transaction details on servers within the appropriate network security zone.

Internal vulnerability scans are performed both on a quarterly basis and after any significant change.

8. Physical and Environmental Security

HP facilities are secured using various combinations of physical and electronic access controls and surveillance capabilities. Depending on the facility, this could include security guards, electronic access control and closed-circuit television (CCTV).

All HP personnel are registered and are required to carry appropriate identification badges.

Facilities have required infrastructure support with temperature control and power backups where required, using UPS and / or diesel generators to support critical services.

9. Operations Management

HP has defined a minimum set of hardening requirements for technology infrastructure which includes workstations, servers and network equipment. Workstation / servers images contain pre-hardened operating systems. Hardening requirements vary depending on the type of operating system and applicable controls implemented.

HP has deployed Network Intrusion Detection / Prevention Systems (NIDS/ NIPS) within the network and are monitored and managed 24*7.

HP security policies and standards mandate secure disposal of media.

10. Cryptography

HP has defined a set of robust processes for cryptography to ensure the confidentiality, integrity, and availability of information assets. Approved protocols require encryption for certain assets including those that contain personal data.

12. Information Security Incident Management

HP follows a developed Cyber Incident Management Process that addresses purpose, scope, roles, responsibilities, management commitment, organizational coordination, implementation procedures, and compliance checking. HP reviews and updates this process on an annual basis.

A Cyber Incident Response Team, which includes HP Cybersecurity personnel trained in incident response and crisis management, is assembled for regular table-top reviews of process and any incident or event.

13. Business Continuity Management

HP maintains a global Continuity of Operations program. This program takes a holistic, company-wide approach for end-to-end continuity through a set of collaborative, standardized, and internally documented planning processes.

HP periodically exercises its business continuity plans to ensure effectiveness of the plans. HP currently tests and updates all plans at least yearly, as well as ensures that people with a role in the business continuity plan are trained.