CUSTOMER DATA PROCESSING ADDENDUM
_____

This Data Processing Addendum ("DPA") and applicable Attachments apply when HP processes Customer Personal Data in order to provide the Services agreed to in the applicable agreement(s) between HP and Customer ("Services Agreement"). Capitalized terms not specifically defined herein shall have the meaning set out in the Services Agreement. In the event of a conflict between the terms of the Services Agreement as they relate to the processing of Personal Data and this DPA, the DPA shall prevail.

1   DEFINITIONS

1.1   **"CCPA"** means California Consumer Privacy Act of 2018, as amended by the California Privacy Rights Act ("CPRA"), Cal. Civ. Code 1798.100, *et seq.*, and any related regulations, each as amended and supplemented from time to time;

1.2   **"Customer"** means the end-user customer of HP Services;

1.3   **"Customer Personal Data"** means the Personal Data in relation to which the Customer is the Data Controller and which is processed by HP as a Data Processor or its Sub-processors in the course of providing the Services;

1.4   **"Data Controller"** means the natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purposes and means of the processing of Personal Data and includes a "business" as defined under the CCPA;

1.5   **"Data Processor"** means any natural or legal person, public authority, agency or any other body which processes Personal Data on behalf of a Data Controller or on the instruction of another Data Processor acting on behalf of a Data Controller;

1.6   **"Data Protection and Privacy Laws"** means all current and future applicable laws and regulations relating to the processing, security, protection, and retention of Personal Data and privacy that may exist in the relevant jurisdictions, including, but not limited to the CCPA, GDPR, PIPL and any applicable regulations and national standards protecting individuals' personal information in the People's Republic of China, UK General Data Protection Regulation, UK Data Protection Act 2018, Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector, any national laws or regulations implementing the foregoing Directives, and any data protection laws of Norway, Iceland, Liechtenstein and Switzerland and any amendments to or replacements for such laws and regulations;

1.7   **"Data Subject"** shall have the meaning assigned to the term "data subject" under applicable Data Protection and Privacy Laws and shall include, at the minimum, any and all identified or identifiable natural persons to whom the Personal Data relates;

1.8   **"De-Identify"** a process that transforms Personal data into data that cannot reasonably be used to infer information about, identify, locate, contact, relate to, describe, be capable of being associated with, or otherwise be linked, directly or indirectly to, a particular Individual or Household, or a device linked to an Individual or Household;

1.9   **"EU"** means the European Union and the countries which are members of that union collectively;

1.10 **"European Country"** means a member state of the EU, Norway, Iceland, Liechtenstein and Switzerland;

1.11 **"European-U.S. Approved Adequacy Mechanism"** means any adequacy mechanism approved under applicable Data Protection and Privacy Laws for the transfer of Personal Data from a European Country to the U.S.;

1.12 **"EU Standard Contractual Clauses"** means the EU standard contractual clauses for the transfer of Personal Data from Data Controllers to Data Processors and from Data Processors to Data Processors foreseen in the Commission Implementing Decision (EU) 2021/914 of 4 June 2021 or its successor with any necessary amendments for Switzerland;

1.13 **"GDPR"** means the General Data Protection Regulation (EU) 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data;

1.14 **"HP Group"** means HP Inc. (1501 Page Mill Road, Palo Alto, CA 94304) and all its majority owned and controlled subsidiaries irrespective of jurisdiction of incorporation or operation;

1.15 **"Personal Data"** means any information relating to an identified or identifiable individual or as otherwise defined by applicable Data Protection and Privacy Laws. An identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to his physical, physiological, genetic, mental, economic, cultural or social identity;

1.16 **"Personal Data Incident"** shall have the meaning assigned by applicable Data Protection and Privacy Laws to the terms "security incident", "security breach" or "personal data breach" but shall include any situation in which HP becomes aware that Customer Personal Data has been or is likely to have been accessed, disclosed, altered, lost, destroyed or used by unauthorized persons, in an unauthorized manner;

1.17 **"PIPL"** means the Personal Information Protection Law of the People's Republic of China;

1.18 **"process"**, **"processes"**, **"processing"** or **"processed"** means any operation or set of operations which is performed upon Personal Data whether or not by automatic means, including, without limitation, accessing, collecting, recording, organizing, structuring, retaining, storing, adapting or altering, retrieving, consulting, using, disclosing by transmission, disseminating or otherwise making available, aligning, combining, blocking, restricting, erasing and destroying Personal Data and any equivalent definitions in applicable Data Protection and Privacy Laws to the extent that such definitions should exceed this definition;

1.19 **"Processor Binding Corporate Rules"** mean binding corporate rules for Data Processor approved by certain Privacy Authorities in the EU;

1.20 **"Relevant Country"** means all countries other than those European Countries and other countries in respect of which there is an adequacy finding under Article 45 of the GDPR or the equivalent under Swiss law or UK law and includes the U.S. as long as any such adequacy finding is limited to require use of a European-U.S. Approved Adequacy Mechanism;

1.21 **"Sell"** and **"Sale"** shall have the meaning set out in CCPA;

1.22 **"Share"** shall have the meaning set out in CCPA;

1.23 **"Services"** means services, including products and support, provided by HP under the Services Agreement;

1.24 **"Services Agreement"** means the agreement between HP and Customer for the purchase of Services from HP; and

1.25 **"Sub-processor"** means any natural or legal person, public authority, agency or any other body which processes Personal Data on behalf of a Data Processor acting on behalf of a Data Controller.

2   SCOPE & COMPLIANCE WITH LAW

2.1 This DPA applies to the processing of Customer Personal Data by HP in connection with HP's provision of the Services and when HP acts as a Data Processor on behalf of the Customer as the Data Controller. All Parties shall comply with applicable Data Protection and Privacy Laws, Nothing in this Section 2.1 shall modify any restrictions applicable to either Party's rights to use or otherwise process Personal Data under the Agreement between the Parties.

2.2 The categories of Data Subjects, types of Customer Personal Data processed, and purposes of processing are set out in Attachment 1 of this DPA. HP shall process Customer Personal Data for the duration of the Services Agreement (or longer to the extent required by applicable law).

2.3 Customer, in its use of HP's Services, shall have sole responsibility for compliance with all applicable Data Protection and Privacy Laws regarding the accuracy, quality and legality of Customer Personal Data that is to be processed by HP in connection with the Services. Customer shall further ensure that the instructions it provides to HP in relation to the processing of Customer Personal Data will comply with all applicable Data Protection and Privacy Laws and shall not put HP in breach of its obligations under applicable Data Protection and Privacy Laws.

2.4 If the Customer uses the Services to process any categories of Personal Data not expressly covered by this DPA, Customer acts at its own risk and HP shall not be responsible for any potential compliance deficits related to such use.

2.5 Where HP discloses any HP employee Personal Data to the Customer or an HP employee provides Personal Data directly to the Customer, which the Customer processes to manage its use of the Services, Customer shall process that Personal Data in accordance with its privacy policies and applicable Data Protection and Privacy Laws. Such disclosures shall be made by HP only where lawful for the purposes of contract management, service management or the Customer's reasonable background screening verification or security purposes.

3   OBLIGATIONS OF DATA PROCESSOR

3.1 Notwithstanding anything to the contrary in the Services Agreement, in relation to Customer Personal Data, HP shall:

3.1.1 only process Customer Personal Data in accordance with Customer's documented instructions (which may be specific or general in nature as set out in the Services Agreement or as otherwise agreed between the Parties). Without limitation to the generality of the foregoing, to the extent the CCPA applies to the Customer Personal Data, HP shall not in a manner that is not consistent with the CCPA: Sell or Share Customer Personal Data; retain, use, or disclose Customer Personal Data for any purpose other than the specific business purposes of performing the Services or otherwise performing obligations under the

Agreement, which purposes are in the context of the direct business relationship between the Parties; or combine Customer Personal Data with Personal Data from any other source. HP will not retain or use Customer Personal Data or De-identified Customer Personal Data for any Other Purpose, including, but not limited to, its own purposes, re-identification or uses independent of HP's obligations. To the extent the CPPA applies to the Customer Personal Data, HP shall notify Customer if it cannot meet its obligations under the CCPA with respect to Customer Personal Data. Notwithstanding the foregoing, HP may process Customer Personal Data as required under applicable law. In this situation, HP will take reasonable steps to inform Customer of such a requirement before HP processes the data, unless the law prohibits this;

3.1.2   ensure only authorized personnel who have undergone the appropriate training in the protection and handling of Personal Data and are bound to respect the confidentiality of Customer Personal Data shall have access to the same;

3.1.3   implement appropriate technical and organizational measures to protect against unauthorized or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Customer Personal Data. These measures shall be appropriate to the harm which might result from any unauthorized or unlawful processing, accidental loss, destruction, damage or theft of Customer Personal Data and having regard to the nature of the Customer Personal Data which is to be protected;

3.1.4   without undue delay and to the extent permitted by law, notify Customer of any requests from Data Subjects seeking to exercise their rights under applicable Data Protection and Privacy Laws and, at Customer's written request and cost, taking into account the nature of the processing, assist Customer by implementing appropriate technical and organizational measures, insofar as this is possible, to assist with the Customer's obligation to respond to such requests;

3.1.5   at Customer's written request and cost, taking into account the nature of processing and the information available to HP, assist Customer with its obligations under Articles 32 to 36 of the GDPR or equivalent provisions under applicable Data Protection and Privacy Laws, to assist Customer to fulfil the Customer's obligations under PIPL; and obligations under CPRA;

3.1.6   upon written request by Customer, delete or return to Customer any Customer Personal Data after the end of the provision of the Services, unless applicable law requires storage of the Customer Personal Data and at HP's election between deletion or return of Customer Personal Data.

4   SUB-PROCESSING

4.1   Customer authorizes HP to transfer Customer Personal Data or give access to Customer Personal Data to members of the HP Group and third parties as Sub-processors (and permit Sub-processors to do so in accordance with Clause 4.1) for the purposes of providing the Services or other purposes identified in the 'Processing Activities' section of Attachment 1. HP shall remain responsible for its Sub-processor's compliance with the obligations of this DPA. HP shall ensure that any Sub-processors to whom HP transfers Customer Personal Data enter into written agreements with HP requiring that the Sub-processors abide by terms no less protective than those set forth in this DPA. HP shall make available to Customer the current list of Sub-processors for the Services covered by the Service Agreement.

4.2 HP can at any time and without justification appoint a new Sub-processor provided that Customer is given ten (10) days' prior notice and Customer does not legitimately object to such changes within that timeframe. Legitimate objections must contain reasonable and documented grounds relating to a Sub-processor's non-compliance with applicable Data Protection and Privacy Laws. If, in HP's reasonable opinion, such objections are legitimate, HP shall refrain from using such Sub-processor in the context of the processing of Customer Personal Data. In such cases, HP shall use reasonable efforts to (i) make available to Customer a change in HP's Services or (ii) recommend a change to the Customer's configuration or use of the Services to avoid the processing of Customer Personal Data by the objected-to Sub-processor. If HP is unable to make available such change within a reasonable period of time, which shall not exceed ninety (90) days, Customer may, by providing written notice to HP, terminate the Service which cannot be provided by HP without the use of the objected-to Sub-processor by providing written notice to HP. Where PIPL applies, HP shall request Customer's prior authorization to appoint a new Sub-processor. Customer must respond to HP's request within ten (10) days. If Customer objects to the change, HP shall refrain from using such Sub-processor in the context of the processing of Customer Personal Data. In such cases, HP shall use reasonable efforts to (i) make available to Customer a change in HP's Services or (ii) recommend a change to the Customer's configuration or use of the Services to avoid the processing of Customer Personal Data by the objected-to Sub-processor. If HP is unable to make available such change within a reasonable period of time, which shall not exceed ninety (90) days, Customer may, by providing written notice to HP, terminate the Service which cannot be provided by HP without the use of the objected-to Sub-processor by providing written notice to HP.

5   PERSONAL DATA INCIDENTS

5.1 HP shall notify Customer, without undue delay, if HP becomes aware of any Personal Data Incident involving Customer Personal Data and take such steps as Customer may reasonably require, within a reasonable period of time, to remedy the Personal Data Incident and provide such further information as Customer may reasonably require. HP reserves the right to charge an administrative fee for assistance provided under this Clause 5.1, unless and to the extent that Customer demonstrates that such assistance is required because of a failure by HP to abide by this DPA.

6   INTERNATIONAL TRANSFERS OF CUSTOMER PERSONAL DATA

6.1 HP may transfer Customer Personal Data outside the country from which it was originally collected provided that such transfer is required in connection with the Services and such transfers take place in accordance with applicable Data Protection and Privacy Laws, including, without limitation, completing any prior assessments required by Data Protection and Privacy Laws.

6.2 European Specific Provisions

6.2.1   To the extent that Customer Personal Data is transferred from a European Country to a Relevant Country, HP makes available the transfer mechanisms listed below which shall apply, in the order of precedence as set forth in Clause 6.2.2, to any such transfers in accordance with applicable Data Protection and Privacy Laws:

6.2.1.1 If applicable, HP Processor Binding Corporate Rules: HP has adopted Processor Binding Corporate Rules that cover the Customer Personal Data it processes. HP shall maintain such HP Processor Binding Corporate Rules and promptly notify Customer in the event that the HP Processor Binding Corporate Rules are no longer a valid transfer mechanism. HP Processor Binding Corporate Rules are available on this link: https://www.hp.com/uk-en/bcr-

6.2.1.2 European-U.S. Approved Adequacy Mechanism: Any transfer under a European-U.S. Approved Adequacy Mechanism must be made in accordance with the rules of the mechanism including, where required, the registration or certification of HP's Affiliate(s) located in the United States of America, which will process Customer Personal Data for purposes of the Services.

6.2.1.3 EU Standard Contractual Clauses, either Data Controller to Data Processor (Attachment 2) or Data Processor to Data Processor (Attachment 3), as applicable.

6.2.2 In the event that the Services are covered by more than one transfer mechanism, the transfer of Customer Personal Data will be subject to a single transfer mechanism in accordance with the following order of precedence: 1) HP Processor Binding Corporate Rules; 2) European U.S. Approved Adequacy Mechanism; 3) EU Standard Contractual Clauses.

6.3 Other Specified Transfer Mechanisms

6.3.1 Without prejudice to the generality of Clause 6.1 above, the Parties agree that the transfer mechanisms referred to in Attachment 4 (UK) and 5 (Argentina) shall be used to transfer Personal Data from the country in question to a Relevant Country.

6.4 China Specific Provisions

6.4.1 To the extent that any Customer Personal Data that is collected or generated within China is transferred from the People's Republic of China by HP to a country or region outside of China, HP makes available the transfer mechanisms listed below:

6.4.1.1 The security assessment: Where the security assessment conducted by the Cyberspace Administration of China (CAC) applies to the transfer of Customer Personal Data, the Customer shall apply for the security assessment and comply with the relevant requirement, and HP shall provide assistance if requested by Customer and deemed necessary by both Parties.

6.4.1.2 Standard Contract (Attachment 6): Where the security assessment does not apply, the Customer must enter into a standard contract published by the CAC, with the recipient of the Customer Personal Data.

6.4.2 Where the Data Controller transfers Personal Data from the People's Republic of China to the Data Processor in a country or region outside of China, the Data Controller shall be responsible for getting data subjects' consent to the transfer.

7 AUDITS

7.1 At Customer's written request, HP shall make available to Customer all information necessary to demonstrate compliance with the obligations set forth under applicable Data Protection and Privacy Laws, provided that HP shall have no obligation to provide commercially confidential information. On no more than an annual basis and at the Customer's expense, HP shall further allow for and contribute to audits and inspections by Customer or its authorized third-party auditor that shall not be a competitor of HP. The scope of any such audits, including conditions of confidentiality, shall be

mutually agreed upon by the Parties prior to initiation. To ensure Customer has the right to take reasonable and appropriate steps to stop and remediate any unauthorized use of Customer Personal Data by HP, the parties will confirm and develop a mutually approved remediation plan as necessary to address any audit findings that implicate such unauthorized use of Customer Personal Data.

List of Attachments

Attachment 1 – Details of Processing
Attachment 2 – EU Standard Contractual Clauses (Data Controller to Data Processor)
Attachment 3 – EU Standard Contractual Clauses (Data Processor to Data Processor)
Attachment 4 – International Data Transfer Agreement (IDTA) (UK)
Attachment 5 – Standard Contractual Clauses (Argentina)
Attachment 6 – Standard Contract for Personal Information Cross-Border Transfer (China)

Attachment 1

Details of Processing

HP may periodically update this Attachment 1 to reflect changes in processing activities.

Categories of Data Subjects

- Customer's employees, customers agents and subcontractors.

Types of Personal Data

The Customer Personal Data processed by HP in connection with HP's provision of the Services is determined and controlled by Customer as Data Controller and in accordance with the applicable statement of work and/or purchase/change orders, but may include as examples:

- *Contact data* – such as name, professional or personal phone number, professional or personal email address and professional office address;

- *Security credentials data* – such as employee identification or badge number;

- *Product usage data* – such as pages printed, types of devices that initiated print jobs, print mode, media used, ink or toner brand, file type printed (.pdf, .jpg, etc.), application used for printing (Word, Excel, Adobe Photoshop, etc.), file size, time stamp, and usage and status of printer supplies;

- *Performance Data* – Printing events, features, and alerts used such as "Low on Ink" warnings, use of photo cards, fax, scan, embedded web server, and additional technical information that varies by product;

- *Device Data* – Information about computers, printers and/or devices such as operating system, amount of memory, region, language, time zone, model number, first start date, age of device, device manufacture date, browser version, computer manufacturer, connection port, warranty status, unique device identifiers, advertising identifiers and additional technical information that varies by product;

- *Application Data* – Information related to HP applications such as location, language, software versions, data sharing choices and update details; and

- Other Personal Data provided by a Data Subject when she/he interacts in-person, online or by phone, or mail with service centers, help desks or other customer support channels to facilitate delivery of HP Services and to respond to Customer and/or Data Subject inquiries; or (ii) on devices received by HP.

Processing activities

Customer Personal Data processed in connection with the Services Agreement shall be used by HP to manage the relationship with and provide Services to the Customer. HP may process Customer Personal Data to:

- deliver fleet management services such as Managed Print Services and Device as a Service;

- maintain accurate contact and registration data to deliver comprehensive support and maintenance services, including care-pack and extended warranty support and facilitating repairs and returns;

- facilitate access to portals for viewing and managing data, managing devices, ordering and completing orders for products or services, for the purposes of administering accounts and arranging shipments and deliveries;

- improve the performance and operation of products, solutions, services and support, including warranty support and timely firmware and software updates and alerts to ensure the continued operation of the device or service;

- provide administrative communications to Customer about the Services. Examples of administrative communications may include responses to Customer inquiries or requests, product usage or performance reports, service completion or warranty-related communications, safety recall notifications, or applicable corporate updates related to mergers, acquisitions or divestitures;

- maintain the integrity and security of HP's websites, products, features and services and preventing and detecting security threats, fraud or other criminal or malicious activity that might compromise Customer's information;

- verify Customer identity, including requesting the caller's name and employee identification or badge number for the delivery of HP's remote maintenance services;

- comply with applicable laws, regulations, court orders, government and law enforcement requests and to protect employees and other customers and to resolve disputes; and

- deliver a tailored experience, personalize the Services and communications and create recommendations; and

- wipe data from devices returned to HP.

EU STANDARD CONTRACTUAL CLAUSES (DATA CONTROLLER TO DATA PROCESSOR)

SECTION I

Clause 1

Purpose and scope

(a)The purpose of these standard contractual clauses is to ensure compliance with the requirements of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) for the transfer of personal data to a third country.

(b)The Parties:

(i) the natural or legal person(s), public authority/ies, agency/ies or other body/ies (hereinafter 'entity/ies') transferring the personal data, as listed in Annex I.A (hereinafter each 'data exporter'), and

(ii) the entity/ies in a third country receiving the personal data from the data exporter, directly or indirectly via another entity also Party to these Clauses, as listed in Annex I.A (hereinafter each 'data importer')

have agreed to these standard contractual clauses (hereinafter: 'Clauses').

(c)These Clauses apply with respect to the transfer of personal data as specified in Annex I.B.

(d)The Appendix to these Clauses containing the Annexes referred to therein forms an integral part of these Clauses.

Clause 2

Effect and invariability of the Clauses

(a) These Clauses set out appropriate safeguards, including enforceable data subject rights and effective legal remedies, pursuant to Article 46(1) and Article 46(2)(c) of Regulation (EU) 2016/679 and, with respect to data transfers from controllers to processors and/or processors to processors, standard contractual clauses pursuant to Article 28(7) of Regulation (EU) 2016/679, provided they are not modified, except to select the appropriate Module(s) or to add or update information in the Appendix. This does not prevent the Parties from including the standard contractual clauses laid down in these Clauses in a wider contract and/or to add other clauses or additional safeguards, provided that they do not contradict, directly or indirectly, these Clauses or prejudice the fundamental rights or freedoms of data subjects.

(b) These Clauses are without prejudice to obligations to which the data exporter is subject by virtue of Regulation (EU) 2016/679.

Clause 3

Third-party beneficiaries

(a) Data subjects may invoke and enforce these Clauses, as third-party beneficiaries, against the data exporter and/or data importer, with the following exceptions:

(i) Clause 1, Clause 2, Clause 3, Clause 6, Clause 7;

(ii) Clause 8 – Clause 8.1(b), 8.9(a), (c), (d) and (e);

(iii) Clause 9 – Clause 9(a), (c), (d) and (e);

(iv) Clause 12 – Clause 12(a), (d) and (f);

(v) Clause 13;

(vi) Clause 15.1(c), (d) and (e);

(vii) Clause 16(e);

(viii) Clause 18 – Clause 18(a) and (b).

(b) Paragraph (a) is without prejudice to rights of data subjects under Regulation (EU) 2016/679.

Clause 4

Interpretation

(a) Where these Clauses use terms that are defined in Regulation (EU) 2016/679, those terms shall have the same meaning as in that Regulation.

(b) These Clauses shall be read and interpreted in the light of the provisions of Regulation (EU) 2016/679.

(c) These Clauses shall not be interpreted in a way that conflicts with rights and obligations provided for in Regulation (EU) 2016/679.

Clause 5

Hierarchy

In the event of a contradiction between these Clauses and the provisions of related agreements between the Parties, existing at the time these Clauses are agreed or entered into thereafter, these Clauses shall prevail.

Clause 6

Description of the transfer(s)

The details of the transfer(s), and in particular the categories of personal data that are transferred and the purpose(s) for which they are transferred, are specified in Annex I.B.

SECTION II – OBLIGATIONS OF THE PARTIES

Clause 8

Data protection safeguards

The data exporter warrants that it has used reasonable efforts to determine that the data importer is able, through the implementation of appropriate technical and organisational measures, to satisfy its obligations under these Clauses.

8.1 Instructions

(a) The data importer shall process the personal data only on documented instructions from the data exporter. The data exporter may give such instructions throughout the duration of the contract.

(b) The data importer shall immediately inform the data exporter if it is unable to follow those instructions.

8.2 Purpose limitation

The data importer shall process the personal data only for the specific purpose(s) of the transfer, as set out in Annex I.B, unless on further instructions from the data exporter.

8.3 Transparency

On request, the data exporter shall make a copy of these Clauses, including the Appendix as completed by the Parties, available to the data subject free of charge. To the extent necessary to protect business secrets or other confidential information, including the measures described in Annex II and personal data, the data exporter may redact part of the text of the Appendix to these Clauses prior to sharing a copy, but shall provide a meaningful summary where the data subject would otherwise not be able to understand the its content or exercise his/her rights. On request, the Parties shall provide the data subject with the reasons for the redactions, to the extent possible without revealing the redacted information. This Clause is without prejudice to the obligations of the data exporter under Articles 13 and 14 of Regulation (EU) 2016/679.

8.4 Accuracy

If the data importer becomes aware that the personal data it has received is inaccurate, or has become outdated, it shall inform the data exporter without undue delay. In this case, the data importer shall cooperate with the data exporter to erase or rectify the data.

8.5 Duration of processing and erasure or return of data

Processing by the data importer shall only take place for the duration specified in Annex I.B. After the end of the provision of the processing services, the data importer shall, at the choice of the data exporter, delete all personal data processed on behalf of the data exporter and certify to the data exporter that it has done so, or return to the data exporter all personal data processed on its behalf and delete existing copies. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit return or deletion of the personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process it to the extent and for as long as required under that local law. This is without prejudice to Clause 14, in particular the requirement for the data importer under Clause 14(e) to notify the data exporter throughout the duration of the contract if it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under Clause 14(a).

8.6 Security of processing

(a) The data importer and, during transmission, also the data exporter shall implement appropriate technical and organisational measures to ensure the security of the data, including protection against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access to that data (hereinafter 'personal data breach'). In assessing the appropriate level of security, the Parties shall take due account of the state of the art, the costs of implementation, the nature, scope, context and purpose(s) of processing and the risks involved in the processing for the data subjects. The Parties shall in particular consider having recourse to encryption or pseudonymisation, including during transmission, where the purpose of processing can be fulfilled in that manner. In case of pseudonymisation, the additional information for attributing the personal data to a specific data subject shall, where possible, remain under the exclusive control of the data exporter. In complying with its obligations under this paragraph, the data importer shall at least implement the technical and organisational measures specified in Annex II. The data importer shall carry out regular checks to ensure that these measures continue to provide an appropriate level of security.

(b) The data importer shall grant access to the personal data to members of its personnel only to the extent strictly necessary for the implementation, management and monitoring of the contract. It shall ensure that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

(c) In the event of a personal data breach concerning personal data processed by the data importer under these Clauses, the data importer shall take appropriate measures to address the breach, including measures to mitigate its adverse effects. The data importer shall also notify the data exporter without undue delay after having become

aware of the breach. Such notification shall contain the details of a contact point where more information can be obtained, a description of the nature of the breach (including, where possible, categories and approximate number of data subjects and personal data records concerned), its likely consequences and the measures taken or proposed to address the breach including, where appropriate, measures to mitigate its possible adverse effects. Where, and in so far as, it is not possible to provide all information at the same time, the initial notification shall contain the information then available and further information shall, as it becomes available, subsequently be provided without undue delay.

(d)   The data importer shall cooperate with and assist the data exporter to enable the data exporter to comply with its obligations under Regulation (EU) 2016/679, in particular to notify the competent supervisory authority and the affected data subjects, taking into account the nature of processing and the information available to the data importer.

8.7 Sensitive data

Where the transfer involves personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, or biometric data for the purpose of uniquely identifying a natural person, data concerning health or a person's sex life or sexual orientation, or data relating to criminal convictions and offences (hereinafter 'sensitive data'), the data importer shall apply the specific restrictions and/or additional safeguards described in Annex I.B.

8.8 Onward transfers

The data importer shall only disclose the personal data to a third party on documented instructions from the data exporter. In addition, the data may only be disclosed to a third party located outside the European Union (in the same country as the data importer or in another third country, hereinafter 'onward transfer') if the third party is or agrees to be bound by these Clauses, under the appropriate Module, or if:

(a) the onward transfer is to a country benefitting from an adequacy decision pursuant to Article 45 of Regulation (EU) 2016/679 that covers the onward transfer;

(b) the third party otherwise ensures appropriate safeguards pursuant to Articles 46 or 47 Regulation of (EU) 2016/679 with respect to the processing in question;

(c) the onward transfer is necessary for the establishment, exercise or defence of legal claims in the context of specific administrative, regulatory or judicial proceedings; or

(d) the onward transfer is necessary in order to protect the vital interests of the data subject or of another natural person.

Any onward transfer is subject to compliance by the data importer with all the other safeguards under these Clauses, in particular purpose limitation.

8.9 Documentation and compliance

(a) The data importer shall promptly and adequately deal with enquiries from the data exporter that relate to the processing under these Clauses.

(b) The Parties shall be able to demonstrate compliance with these Clauses. In particular, the data importer shall keep appropriate documentation on the processing activities carried out on behalf of the data exporter.

(c) The data importer shall make available to the data exporter all information necessary to demonstrate compliance with the obligations set out in these Clauses and at the data exporter's request, allow for and contribute to audits of the processing activities covered by these Clauses, at reasonable intervals or if there are indications of non‐compliance. In deciding on a review or audit, the data exporter may take into account relevant certifications held by the data importer.

(d) The data exporter may choose to conduct the audit by itself or mandate an independent auditor. Audits may include inspections at the premises or physical facilities of the data importer and shall, where appropriate, be carried out with reasonable notice.

(e) The Parties shall make the information referred to in paragraphs (b) and (c), including the results of any audits, available to the competent supervisory authority on request.

Clause 9

Use of sub-processors

(a) GENERAL WRITTEN AUTHORISATION The data importer has the data exporter's general authorisation for the engagement of sub-processor(s) from an agreed list. The data importer shall specifically inform the data exporter in writing of any intended changes to that list through the addition or replacement of sub-processors at least 90 days in advance, thereby giving the data exporter sufficient time to be able to object to such changes prior to the engagement of the sub-processor(s). The data importer shall provide the data exporter with the information necessary to enable the data exporter to exercise its right to object.

(b) Where the data importer engages a sub-processor to carry out specific processing activities (on behalf of the data exporter), it shall do so by way of a written contract that provides for, in substance, the same data protection obligations as those binding the data importer under these Clauses, including in terms of third-party beneficiary rights for data subjects. The Parties agree that, by complying with this Clause, the data importer fulfils its obligations under Clause 8.8. The data importer shall ensure that the sub-processor complies with the obligations to which the data importer is subject pursuant to these Clauses.

(c) The data importer shall provide, at the data exporter's request, a copy of such a sub-processor agreement and any subsequent amendments to the data exporter. To the extent necessary to protect business secrets or other confidential information, including personal data, the data importer may redact the text of the agreement prior to sharing a copy.

(d) The data importer shall remain fully responsible to the data exporter for the performance of the sub-processor's obligations under its contract with the data importer. The data importer shall notify the data exporter of any failure by the sub-processor to fulfil its obligations under that contract.

(e) The data importer shall agree a third-party beneficiary clause with the sub-processor whereby – in the event the data importer has factually disappeared, ceased to exist in law or has become insolvent – the data exporter shall have the right to terminate the sub-processor contract and to instruct the sub-processor to erase or return the personal data.

Clause 10

Data subject rights

(a) The data importer shall promptly notify the data exporter of any request it has received from a data subject. It shall not respond to that request itself unless it has been authorised to do so by the data exporter.

(b) The data importer shall assist the data exporter in fulfilling its obligations to respond to data subjects' requests for the exercise of their rights under Regulation (EU) 2016/679. In this regard, the Parties shall set out in Annex II the appropriate technical and organisational measures, taking into account the nature of the processing, by which the assistance shall be provided, as well as the scope and the extent of the assistance required.

(c) In fulfilling its obligations under paragraphs (a) and (b), the data importer shall comply with the instructions from the data exporter.

Clause 11

Redress

(a) The data importer shall inform data subjects in a transparent and easily accessible format, through individual notice or on its website, of a contact point authorised to handle complaints. It shall deal promptly with any complaints it receives from a data subject.

(b) In case of a dispute between a data subject and one of the Parties as regards compliance with these Clauses, that Party shall use its best efforts to resolve the issue amicably in a timely fashion. The Parties shall keep each other informed about such disputes and, where appropriate, cooperate in resolving them.

(c) Where the data subject invokes a third-party beneficiary right pursuant to Clause 3, the data importer shall accept the decision of the data subject to:

    (i) lodge a complaint with the supervisory authority in the Member State of his/her habitual residence or place of work, or the competent supervisory authority pursuant to Clause 13;

    (ii) refer the dispute to the competent courts within the meaning of Clause 18.

(d) The Parties accept that the data subject may be represented by a not-for-profit body, organisation or association under the conditions set out in Article 80(1) of Regulation (EU) 2016/679.

(e) The data importer shall abide by a decision that is binding under the applicable EU or Member State law.

(f) The data importer agrees that the choice made by the data subject will not prejudice his/her substantive and procedural rights to seek remedies in accordance with applicable laws.

Clause 12

Liability

(a) Each Party shall be liable to the other Party/ies for any damages it causes the other Party/ies by any breach of these Clauses.

(b) The data importer shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages the data importer or its sub-processor causes the data subject by breaching the third-party beneficiary rights under these Clauses.

(c) Notwithstanding paragraph (b), the data exporter shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages the data exporter or the data importer (or its sub-processor) causes the data subject by breaching the third-party beneficiary rights under these Clauses. This is without prejudice to the liability of the data exporter and, where the data exporter is a processor acting on behalf of a controller, to the liability of the controller under Regulation (EU) 2016/679 or Regulation (EU) 2018/1725, as applicable.

(d) The Parties agree that if the data exporter is held liable under paragraph (c) for damages caused by the data importer (or its sub-processor), it shall be entitled to claim back from the data importer that part of the compensation corresponding to the data importer's responsibility for the damage.

(e) Where more than one Party is responsible for any damage caused to the data subject as a result of a breach of these Clauses, all responsible Parties shall be jointly and severally liable and the data subject is entitled to bring an action in court against any of these Parties.

(f) The Parties agree that if one Party is held liable under paragraph (e), it shall be entitled to claim back from the other Party/ies that part of the compensation corresponding to its/their responsibility for the damage.

(g) The data importer may not invoke the conduct of a sub-processor to avoid its own liability.

Clause 13

Supervision

(a) Where the data exporter is established in an EU Member State: The supervisory authority with responsibility for ensuring compliance by the data exporter with Regulation (EU) 2016/679 as regards the data transfer, as indicated in Annex I.C, shall act as competent supervisory authority.

Where the data exporter is not established in an EU Member State, but falls within the territorial scope of application of Regulation (EU) 2016/679 in accordance with its Article 3(2) and has appointed a representative pursuant to Article 27(1) of Regulation (EU) 2016/679: The supervisory authority of the Member State in which the representative within the meaning of Article 27(1) of Regulation (EU) 2016/679 is established, as indicated in Annex I.C, shall act as competent supervisory authority.

Where the data exporter is not established in an EU Member State, but falls within the territorial scope of application of Regulation (EU) 2016/679 in accordance with its Article 3(2) without however having to appoint a representative pursuant to Article 27(2) of Regulation (EU) 2016/679: The supervisory authority of one of the Member States in which the data subjects whose personal data is transferred under these Clauses in relation to the offering of goods or services to them, or whose behaviour is monitored, are located, as indicated in Annex I.C, shall act as competent supervisory authority.

(b) The data importer agrees to submit itself to the jurisdiction of and cooperate with the competent supervisory authority in any procedures aimed at ensuring compliance with these Clauses. In particular, the data importer agrees to respond to enquiries, submit to audits and comply with the measures adopted by the supervisory authority, including remedial and compensatory measures. It shall provide the supervisory authority with written confirmation that the necessary actions have been taken.

SECTION III – LOCAL LAWS AND OBLIGATIONS IN CASE OF ACCESS BY PUBLIC AUTHORITIES

Clause 14

Local laws and practices affecting compliance with the Clauses

(a) The Parties warrant that they have no reason to believe that the laws and practices in the third country of destination applicable to the processing of the personal data by the data importer, including any requirements to disclose personal data or measures authorising access by public authorities, prevent the data importer from fulfilling its obligations under these Clauses. This is based on the understanding that laws and practices that respect the essence of the fundamental rights and freedoms and do not exceed what is necessary and proportionate in a democratic society to safeguard one of the objectives listed in Article 23(1) of Regulation (EU) 2016/679, are not in contradiction with these Clauses.

(b) The Parties declare that in providing the warranty in paragraph (a), they have taken due account in particular of he following elements:

(i) the specific circumstances of the transfer, including the length of the processing chain, the number of actors involved and the transmission channels used; intended onward transfers; the type of recipient; the purpose of processing; the categories and format of the transferred personal data; the economic sector in which the transfer occurs; the storage location of the data transferred;

(ii) the laws and practices of the third country of destination– including those requiring the disclosure of data to public authorities or authorising access by such authorities – relevant in light of the specific circumstances of the transfer, and the applicable limitations and safeguards;

(iii) any relevant contractual, technical or organisational safeguards put in place to supplement the safeguards under these Clauses, including measures applied during transmission and to the processing of the personal data in the country of destination.

(c)   The data importer warrants that, in carrying out the assessment under paragraph (b), it has made its best efforts to provide the data exporter with relevant information and agrees that it will continue to cooperate with the data exporter in ensuring compliance with these Clauses.

(d)   The Parties agree to document the assessment under paragraph (b) and make it available to the competent supervisory authority on request.

(e)   The data importer agrees to notify the data exporter promptly if, after having agreed to these Clauses and for the duration of the contract, it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under paragraph (a), including following a change in the laws of the third country or a measure (such as a disclosure request) indicating an application of such laws in practice that is not in line with the requirements in paragraph (a).

(f)   Following a notification pursuant to paragraph (e), or if the data exporter otherwise has reason to believe that the data importer can no longer fulfil its obligations under these Clauses, the data exporter shall promptly identify appropriate measures (e.g. technical or organisational measures to ensure security and confidentiality) to be adopted by the data exporter and/or data importer to address the situation. The data exporter shall suspend the data transfer if it considers that no appropriate safeguards for such transfer can be ensured, or if instructed by the competent supervisory authority to do so. In this case, the data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses. If the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise. Where the contract is terminated pursuant to this Clause, Clause 16(d) and (e) shall apply.

Clause 15

Obligations of the data importer in case of access by public authorities

15.1 Notification

(a)   The data importer agrees to notify the data exporter and, where possible, the data subject promptly (if necessary, with the help of the data exporter) if it:

   (i)   receives a legally binding request from a public authority, including judicial authorities, under the laws of the country of destination for the disclosure of personal data transferred pursuant to these Clauses; such notification shall include information about the personal data requested, the requesting authority, the legal basis for the request and the response provided; or

   (ii) becomes aware of any direct access by public authorities to personal data transferred pursuant to these Clauses in accordance with the laws of the country of destination; such notification shall include all information available to the importer.

(b)   If the data importer is prohibited from notifying the data exporter and/or the data subject under the laws of the country of destination, the data importer agrees to use its best efforts to obtain a waiver of the prohibition, with a view to communicating as much information as possible, as soon as possible. The data importer agrees to document its best efforts in order to be able to demonstrate them on request of the data exporter.

(c)   Where permissible under the laws of the country of destination, the data importer agrees to provide the data exporter, at regular intervals for the duration of the contract, with as much relevant information as possible on the requests received (in particular, number of requests, type of data requested, requesting authority/ies, whether requests have been challenged and the outcome of such challenges, etc.).

(d)   The data importer agrees to preserve the information pursuant to paragraphs (a) to (c) for the duration of the contract and make it available to the competent supervisory authority on request.

(e)   Paragraphs (a) to (c) are without prejudice to the obligation of the data importer pursuant to Clause 14(e) and Clause 16 to inform the data exporter promptly where it is unable to comply with these Clauses.

15.2   Review of legality and data minimisation

(a)   The data importer agrees to review the legality of the request for disclosure, in particular whether it remains within the powers granted to the requesting public authority, and to challenge the request if, after careful assessment, it concludes that there are reasonable grounds to consider that the request is unlawful under the laws of the country of destination, applicable obligations under international law and principles of international comity. The data importer shall, under the same conditions, pursue possibilities of appeal. When challenging a request, the data importer shall seek interim measures with a view to suspending the effects of the request until the competent judicial authority has decided on its merits. It shall not disclose the personal data requested until required to do so under the applicable procedural rules. These requirements are without prejudice to the obligations of the data importer under Clause 14(e).

(b)   The data importer agrees to document its legal assessment and any challenge to the request for disclosure and, to the extent permissible under the laws of the country of destination, make the documentation available to the data exporter. It shall also make it available to the competent supervisory authority on request.

(c)   The data importer agrees to provide the minimum amount of information permissible when responding to a request for disclosure, based on a reasonable interpretation of the request.

SECTION IV – FINAL PROVISIONS

Clause 16

Non-compliance with the Clauses and termination

(a)   The data importer shall promptly inform the data exporter if it is unable to comply with these Clauses, for whatever reason.

(b)   In the event that the data importer is in breach of these Clauses or unable to comply with these Clauses, the data exporter shall suspend the transfer of personal data to the data importer until compliance is again ensured or the contract is terminated. This is without prejudice to Clause 14(f).

(c)   The data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses, where:

(i)   the data exporter has suspended the transfer of personal data to the data importer pursuant to paragraph (b) and compliance with these Clauses is not restored within a reasonable time and in any event within one month of suspension;

(ii)   the data importer is in substantial or persistent breach of these Clauses; or

(iii)   the data importer fails to comply with a binding decision of a competent court or supervisory authority regarding its obligations under these Clauses.

In these cases, it shall inform the competent supervisory authority of such non-compliance. Where the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise.

(d)   Personal data that has been transferred prior to the termination of the contract pursuant to paragraph (c) shall at the choice of the data exporter immediately be returned to the data exporter or deleted in its entirety. The same shall apply to any copies of the data. The data importer shall certify the deletion of the data to the data exporter. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit the return or deletion of the transferred

personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process the data to the extent and for as long as required under that local law.

(e)   Either Party may revoke its agreement to be bound by these Clauses where (i) the European Commission adopts a decision pursuant to Article 45(3) of Regulation (EU) 2016/679 that covers the transfer of personal data to which these Clauses apply; or (ii) Regulation (EU) 2016/679 becomes part of the legal framework of the country to which the personal data is transferred. This is without prejudice to other obligations applying to the processing in question under Regulation (EU) 2016/679.

Clause 17

Governing law

These Clauses shall be governed by the law of one of the EU Member States, provided such law allows for third-party beneficiary rights. The Parties agree that this shall be the law of France.

Clause 18

Choice of forum and jurisdiction

(a)   Any dispute arising from these Clauses shall be resolved by the courts of an EU Member State.

(b)   The Parties agree that those shall be the courts of France.

(c)   A data subject may also bring legal proceedings against the data exporter and/or data importer before the courts of the Member State in which he/she has his/her habitual residence.

(d)   The Parties agree to submit themselves to the jurisdiction of such courts.

APPENDIX

ANNEX I

A. LIST OF PARTIES

Data exporter(s): [*Identity and contact details of the data exporter(s) and, where applicable, of its/their data protection officer and/or representative in the European Union*]

Name: See Customer's name in the Agreement

Address: See Customer's address in the Agreement

Contact person's name, position and contact details: See Customer's contact person's name, position and contact details in the Agreement

Activities relevant to the data transferred under these Clauses: Same as the Agreement

Signature and date: Same as the Agreement

Role (controller/processor): Controller

Data importer(s): [*Identity and contact details of the data importer(s), including any contact person with responsibility for data protection*]

Name: See HP's name in the Agreement

Address: See HP's address in the Agreement

Contact person's name, position and contact details: Zoe McMahon, DPO, https://www.hp.com/us-en/privacy/ww-privacy-form.html

Activities relevant to the data transferred under these Clauses: Same as the Agreement

Signature and date: Same as the Agreement

Role (controller/processor): Processor

B. DESCRIPTION OF TRANSFER

Categories of data subjects whose personal data is transferred

See Attachment 1.

Categories of personal data transferred

See Attachment 1.

Sensitive data transferred (if applicable) and applied restrictions or safeguards that fully take into consideration the nature of the data and the risks involved, such as for instance strict purpose limitation, access restrictions (including access only for staff having followed specialised training), keeping a record of access to the data, restrictions for onward transfers or additional security measures.

See attachment 1.

The frequency of the transfer (e.g. whether the data is transferred on a one-off or continuous basis).

See attachment 1.

Nature of the processing

See attachment 1.

Purpose(s) of the data transfer and further processing

See attachment 1.

The period for which the personal data will be retained, or, if that is not possible, the criteria used to determine that period

See Agreement and DPA.

For transfers to (sub-) processors, also specify subject matter, nature and duration of the processing

Subject matter: See Attachment 1.

Nature: See Attachment 1.

Duration of the processing: As long as the contract is in effect.

C. COMPETENT SUPERVISORY AUTHORITY

Commission Nationale de l'informatique et des Libertés (CNIL)

ANNEX II

TECHNICAL AND ORGANISATIONAL MEASURES INCLUDING TECHNICAL AND ORGANISATIONAL MEASURES TO ENSURE THE SECURITY OF THE DATA

To protect Customer data, HP abides by a robust set of information security controls including policies, practices, procedures, and organizational structures to safeguard 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 HP's technical/organizational security measures 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 is 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 responsible for directing and managing the organization's information security strategy and controls. An Information Security Framework/Management System is put in place to ensure compliance with HP's security policies and controls and 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 periodically and revoked upon personnel departure.

User account creation and deletion procedures, as have been mutually agreed upon, are implemented to grant and revoke access to client systems used during the engagement.

5. Personnel Training

HP employees must complete the Integrity at HP training designed to ensure that employees are familiar with the program, policies, and resources that govern HP's 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 must also complete an annually refreshed

dedicated security awareness training focused on essential security policies and emphasizing the employees' 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.

For applicable suppliers (suppliers that handle/store/transmit HP data and customer owned HP held data or have access to the HP network), HP Cybersecurity performs a risk assessment to verify the existence of an information security program. An adequate program must include physical, technical, and administrative safeguards. This assessment must be done before the supplier has access to HP information.

7.   Systems Security

By policy, the 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, including 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 regularly.

8.   Physical and Environmental Security

HP facilities are secured using various 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, including 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.

11.   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.

12.   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 their effectiveness. HP currently tests and updates all plans at least yearly and ensures that people with a role in the business continuity plan are trained.

For transfers to (sub-) processors, also describe the specific technical and organisational measures to be taken by the (sub-) processor to be able to provide assistance to the controller and, for transfers from a processor to a sub-processor, to the data exporter

Sub-processors only process: name, business email address, business phone number, business address. The purpose of transferring this data is to complete the contract.

For HP all of the above technical and organizational measures are flowed down to the sub-processors through the partner code of conduct and contract terms. Sub-processors are required to commit to following HP's requirements.

Attachment 3

EU STANDARD CONTRACTUAL CLAUSES (DATA PROCESSOR TO DATA PROCESSORS)

SECTION I

Clause 1

Purpose and scope

(a) The purpose of these standard contractual clauses is to ensure compliance with the requirements of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32021D0914&from=EN_-_ntr1-L_2021199EN.01003701-E0001for the transfer of personal data to a third country.

(b) The Parties:

   (i) the natural or legal person(s), public authority/ies, agency/ies or other body/ies (hereinafter 'entity/ies') transferring the personal data, as listed in Annex I.A (hereinafter each 'data exporter'), and

   (ii) the entity/ies in a third country receiving the personal data from the data exporter, directly or indirectly via another entity also Party to these Clauses, as listed in Annex I.A (hereinafter each 'data importer')

   have agreed to these standard contractual clauses (hereinafter: 'Clauses').

(c) These Clauses apply with respect to the transfer of personal data as specified in Annex I.B.

(d) The Appendix to these Clauses containing the Annexes referred to therein forms an integral part of these Clauses.

Clause 2

Effect and invariability of the Clauses

(a) These Clauses set out appropriate safeguards, including enforceable data subject rights and effective legal remedies, pursuant to Article 46(1) and Article 46(2)(c) of Regulation (EU) 2016/679 and, with respect to data transfers from controllers to processors and/or processors to processors, standard contractual clauses pursuant to Article 28(7) of Regulation (EU) 2016/679, provided they are not modified, except to select the appropriate Module(s) or to add or update information in the Appendix. This does not prevent the Parties from including the standard contractual clauses laid down in these Clauses in a wider contract and/or to add other clauses or additional safeguards, provided that they do not contradict, directly or indirectly, these Clauses or prejudice the fundamental rights or freedoms of data subjects.

(b) These Clauses are without prejudice to obligations to which the data exporter is subject by virtue of Regulation (EU) 2016/679.

Clause 3

Third-party beneficiaries

(a) Data subjects may invoke and enforce these Clauses, as third-party beneficiaries, against the data exporter and/or data importer, with the following exceptions:

   (i)   Clause 1, Clause 2, Clause 3, Clause 6, Clause 7;

(ii)   Clause 8 – Clause 8.1(a), (c) and (d) and Clause 8.9(a), (c), (d), (e), (f) and (g);

(iii)   Clause 9 – Clause 9(a), (c), (d) and (e);

(iv)   Clause 12 – Clause 12(a), (d) and (f);

(v)   Clause 13;

(vi)   Clause 15.1(c), (d) and (e);

(vii)   Clause 16(e);

(viii) Clause 18 – Clause 18(a) and (b).

(b) Paragraph (a) is without prejudice to rights of data subjects under Regulation (EU) 2016/679.

Clause 4

Interpretation

(a) Where these Clauses use terms that are defined in Regulation (EU) 2016/679, those terms shall have the same meaning as in that Regulation.

(b) These Clauses shall be read and interpreted in the light of the provisions of Regulation (EU) 2016/679.

(c) These Clauses shall not be interpreted in a way that conflicts with rights and obligations provided for in Regulation (EU) 2016/679.

Clause 5

Hierarchy

In the event of a contradiction between these Clauses and the provisions of related agreements between the Parties, existing at the time these Clauses are agreed or entered into thereafter, these Clauses shall prevail.

Clause 6

Description of the transfer(s)

The details of the transfer(s), and in particular the categories of personal data that are transferred and the purpose(s) for which they are transferred, are specified in Annex I.B.

SECTION II – OBLIGATIONS OF THE PARTIES

Clause 8

Data protection safeguards

The data exporter warrants that it has used reasonable efforts to determine that the data importer is able, through the implementation of appropriate technical and organisational measures, to satisfy its obligations under these Clauses.

8.1 Instructions

(a)   The data exporter has informed the data importer that it acts as processor under the instructions of its controller(s), which the data exporter shall make available to the data importer prior to processing.

(b) The data importer shall process the personal data only on documented instructions from the controller, as communicated to the data importer by the data exporter, and any additional documented instructions from the data exporter. Such additional instructions shall not conflict with the instructions from the controller. The controller or data exporter may give further documented instructions regarding the data processing throughout the duration of the contract.

(c) The data importer shall immediately inform the data exporter if it is unable to follow those instructions. Where the data importer is unable to follow the instructions from the controller, the data exporter shall immediately notify the controller.

(d) The data exporter warrants that it has imposed the same data protection obligations on the data importer as set out in the contract or other legal act under Union or Member State law between the controller and the data exporter.

8.2 Purpose limitation

The data importer shall process the personal data only for the specific purpose(s) of the transfer, as set out in Annex I.B., unless on further instructions from the controller, as communicated to the data importer by the data exporter, or from the data exporter.

8.3 Transparency

On request, the data exporter shall make a copy of these Clauses, including the Appendix as completed by the Parties, available to the data subject free of charge. To the extent necessary to protect business secrets or other confidential information, including personal data, the data exporter may redact part of the text of the Appendix prior to sharing a copy, but shall provide a meaningful summary where the data subject would otherwise not be able to understand its content or exercise his/her rights. On request, the Parties shall provide the data subject with the reasons for the redactions, to the extent possible without revealing the redacted information.

8.4 Accuracy

If the data importer becomes aware that the personal data it has received is inaccurate, or has become outdated, it shall inform the data exporter without undue delay. In this case, the data importer shall cooperate with the data exporter to rectify or erase the data.

8.5 Duration of processing and erasure or return of data

Processing by the data importer shall only take place for the duration specified in Annex I.B. After the end of the provision of the processing services, the data importer shall, at the choice of the data exporter, delete all personal data processed on behalf of the controller and certify to the data exporter that it has done so, or return to the data exporter all personal data processed on its behalf and delete existing copies. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit return or deletion of the personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process it to the extent and for as long as required under that local law. This is without prejudice to Clause 14, in particular the requirement for the data importer under Clause 14(e) to notify the data exporter throughout the duration of the contract if it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under Clause 14(a).

8.6 Security of processing

(a) The data importer and, during transmission, also the data exporter shall implement appropriate technical and organisational measures to ensure the security of the data, including protection against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access to that data (hereinafter 'personal data breach'). In assessing the appropriate level of security, they shall take due account of the state of the art, the costs of implementation, the nature, scope, context and purpose(s) of processing and the risks involved in

the processing for the data subject. The Parties shall in particular consider having recourse to encryption or pseudonymisation, including during transmission, where the purpose of processing can be fulfilled in that manner. In case of pseudonymisation, the additional information for attributing the personal data to a specific data subject shall, where possible, remain under the exclusive control of the data exporter or the controller. In complying with its obligations under this paragraph, the data importer shall at least implement the technical and organisational measures specified in Annex II. The data importer shall carry out regular checks to ensure that these measures continue to provide an appropriate level of security.

(b) The data importer shall grant access to the data to members of its personnel only to the extent strictly necessary for the implementation, management and monitoring of the contract. It shall ensure that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

(c) In the event of a personal data breach concerning personal data processed by the data importer under these Clauses, the data importer shall take appropriate measures to address the breach, including measures to mitigate its adverse effects. The data importer shall also notify, without undue delay, the data exporter and, where appropriate and feasible, the controller after having become aware of the breach. Such notification shall contain the details of a contact point where more information can be obtained, a description of the nature of the breach (including, where possible, categories and approximate number of data subjects and personal data records concerned), its likely consequences and the measures taken or proposed to address the data breach, including measures to mitigate its possible adverse effects. Where, and in so far as, it is not possible to provide all information at the same time, the initial notification shall contain the information then available and further information shall, as it becomes available, subsequently be provided without undue delay.

(d) The data importer shall cooperate with and assist the data exporter to enable the data exporter to comply with its obligations under Regulation (EU) 2016/679, in particular to notify its controller so that the latter may in turn notify the competent supervisory authority and the affected data subjects, taking into account the nature of processing and the information available to the data importer.

8.7 Sensitive data

Where the transfer involves personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, or biometric data for the purpose of uniquely identifying a natural person, data concerning health or a person's sex life or sexual orientation, or data relating to criminal convictions and offences (hereinafter 'sensitive data'), the data importer shall apply the specific restrictions and/or additional safeguards set out in Annex I.B.

8.8 Onward transfers

The data importer shall only disclose the personal data to a third party on documented instructions from the controller, as communicated to the data importer by the data exporter. In addition, the data may only be disclosed to a third party located outside the European Union https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32021D0914&from=EN_-_ntr6-L_2021199EN.01003701-E0006 (in the same country as the data importer or in another third country, hereinafter 'onward transfer') if the third party is or agrees to be bound by these Clauses, under the appropriate Module, or if:

(i) the onward transfer is to a country benefitting from an adequacy decision pursuant to Article 45 of Regulation (EU) 2016/679 that covers the onward transfer;

(ii) the third party otherwise ensures appropriate safeguards pursuant to Articles 46 or 47 of Regulation (EU) 2016/679;

(iii) the onward transfer is necessary for the establishment, exercise or defence of legal claims in the context of specific administrative, regulatory or judicial proceedings; or

(iv) the onward transfer is necessary in order to protect the vital interests of the data subject or of another natural person.

Any onward transfer is subject to compliance by the data importer with all the other safeguards under these Clauses, in particular purpose limitation.

8.9 Documentation and compliance

(a) The data importer shall promptly and adequately deal with enquiries from the data exporter or the controller that relate to the processing under these Clauses.

(b) The Parties shall be able to demonstrate compliance with these Clauses. In particular, the data importer shall keep appropriate documentation on the processing activities carried out on behalf of the controller.

(c) The data importer shall make all information necessary to demonstrate compliance with the obligations set out in these Clauses available to the data exporter, which shall provide it to the controller.

(d) The data importer shall allow for and contribute to audits by the data exporter of the processing activities covered by these Clauses, at reasonable intervals or if there are indications of non-compliance. The same shall apply where the data exporter requests an audit on instructions of the controller. In deciding on an audit, the data exporter may take into account relevant certifications held by the data importer.

(e) Where the audit is carried out on the instructions of the controller, the data exporter shall make the results available to the controller.

(f) The data exporter may choose to conduct the audit by itself or mandate an independent auditor. Audits may include inspections at the premises or physical facilities of the data importer and shall, where appropriate, be carried out with reasonable notice.

(g) The Parties shall make the information referred to in paragraphs (b) and (c), including the results of any audits, available to the competent supervisory authority on request.

Clause 9

Use of sub-processors

(a) GENERAL WRITTEN AUTHORISATION The data importer has the controller's general authorisation for the engagement of sub-processor(s) from an agreed list. The data importer shall specifically inform the controller in writing of any intended changes to that list through the addition or replacement of sub-processors at least 10 days in advance, thereby giving the controller sufficient time to be able to object to such changes prior to the engagement of the sub-processor(s). The data importer shall provide the controller with the information necessary to enable the controller to exercise its right to object. The data importer shall inform the data exporter of the engagement of the sub-processor(s).

(b) Where the data importer engages a sub-processor to carry out specific processing activities (on behalf of the controller), it shall do so by way of a written contract that provides for, in substance, the same data protection obligations as those binding the data importer under these Clauses, including in terms of third-party beneficiary rights for data subjects. The Parties agree that, by complying with this Clause, the data importer fulfils its obligations under Clause 8.8. The data importer shall ensure that the sub-processor complies with the obligations to which the data importer is subject pursuant to these Clauses.

(c) The data importer shall provide, at the data exporter's or controller's request, a copy of such a sub-processor agreement and any subsequent amendments. To the extent necessary to protect business secrets or other confidential information, including personal data, the data importer may redact the text of the agreement prior to sharing a copy.

(d) The data importer shall remain fully responsible to the data exporter for the performance of the sub-processor's obligations under its contract with the data importer. The data importer shall notify the data exporter of any failure by the sub-processor to fulfil its obligations under that contract.

(e) The data importer shall agree a third-party beneficiary clause with the sub-processor whereby – in the event the data importer has factually disappeared, ceased to exist in law or has become insolvent – the data exporter shall have the right to terminate the sub-processor contract and to instruct the sub-processor to erase or return the personal data.

Clause 10

Data subject rights

(a) The data importer shall promptly notify the data exporter and, where appropriate, the controller of any request it has received from a data subject, without responding to that request unless it has been authorised to do so by the controller.

(b) The data importer shall assist, where appropriate in cooperation with the data exporter, the controller in fulfilling its obligations to respond to data subjects' requests for the exercise of their rights under Regulation (EU) 2016/679 or Regulation (EU) 2018/1725, as applicable. In this regard, the Parties shall set out in Annex II the appropriate technical and organisational measures, taking into account the nature of the processing, by which the assistance shall be provided, as well as the scope and the extent of the assistance required.

(c) In fulfilling its obligations under paragraphs (a) and (b), the data importer shall comply with the instructions from the controller, as communicated by the data exporter.

Clause 11

Redress

(a) The data importer shall inform data subjects in a transparent and easily accessible format, through individual notice or on its website, of a contact point authorised to handle complaints. It shall deal promptly with any complaints it receives from a data subject.

(b) In case of a dispute between a data subject and one of the Parties as regards compliance with these Clauses, that Party shall use its best efforts to resolve the issue amicably in a timely fashion. The Parties shall keep each other informed about such disputes and, where appropriate, cooperate in resolving them.

(c) Where the data subject invokes a third-party beneficiary right pursuant to Clause 3, the data importer shall accept the decision of the data subject to:

(i) lodge a complaint with the supervisory authority in the Member State of his/her habitual residence or place of work, or the competent supervisory authority pursuant to Clause 13;

(ii) refer the dispute to the competent courts within the meaning of Clause 18.

(d) The Parties accept that the data subject may be represented by a not-for-profit body, organisation or association under the conditions set out in Article 80(1) of Regulation (EU) 2016/679.

(e) The data importer shall abide by a decision that is binding under the applicable EU or Member State law.

(f) The data importer agrees that the choice made by the data subject will not prejudice his/her substantive and procedural rights to seek remedies in accordance with applicable laws.

Clause 12

Liability

(a) Each Party shall be liable to the other Party/ies for any damages it causes the other Party/ies by any breach of these Clauses.

(b) The data importer shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages the data importer or its sub-processor causes the data subject by breaching the third-party beneficiary rights under these Clauses.

(c) Notwithstanding paragraph (b), the data exporter shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages the data exporter or the data importer (or its sub-processor) causes the data subject by breaching the third-party beneficiary rights under these Clauses. This is without prejudice to the liability of the data exporter and, where the data exporter is a processor acting on behalf of a controller, to the liability of the controller under Regulation (EU) 2016/679 or Regulation (EU) 2018/1725, as applicable.

(d) The Parties agree that if the data exporter is held liable under paragraph (c) for damages caused by the data importer (or its sub-processor), it shall be entitled to claim back from the data importer that part of the compensation corresponding to the data importer's responsibility for the damage.

(e) Where more than one Party is responsible for any damage caused to the data subject as a result of a breach of these Clauses, all responsible Parties shall be jointly and severally liable and the data subject is entitled to bring an action in court against any of these Parties.

(f) The Parties agree that if one Party is held liable under paragraph (e), it shall be entitled to claim back from the other Party/ies that part of the compensation corresponding to its/their responsibility for the damage.

(g) The data importer may not invoke the conduct of a sub-processor to avoid its own liability.

Clause 13

Supervision

(a) Where the data exporter is established in an EU Member State: The supervisory authority with responsibility for ensuring compliance by the data exporter with Regulation (EU) 2016/679 as regards the data transfer, as indicated in Annex I.C, shall act as competent supervisory authority.

Where the data exporter is not established in an EU Member State, but falls within the territorial scope of application of Regulation (EU) 2016/679 in accordance with its Article 3(2) and has appointed a representative pursuant to Article 27(1) of Regulation (EU) 2016/679: The supervisory authority of the Member State in which the representative within the meaning of Article 27(1) of Regulation (EU) 2016/679 is established, as indicated in Annex I.C, shall act as competent supervisory authority.

Where the data exporter is not established in an EU Member State, but falls within the territorial scope of application of Regulation (EU) 2016/679 in accordance with its Article 3(2) without however having to appoint a representative pursuant to Article 27(2) of Regulation (EU) 2016/679: The supervisory authority of one of the Member States in which the data subjects whose personal data is transferred under these Clauses in relation to the offering of goods or services to them, or whose behaviour is monitored, are located, as indicated in Annex I.C, shall act as competent supervisory authority.

(b) The data importer agrees to submit itself to the jurisdiction of and cooperate with the competent supervisory authority in any procedures aimed at ensuring compliance with these Clauses. In particular, the data importer agrees to respond to enquiries, submit to audits and comply with the measures adopted by the supervisory authority, including remedial and compensatory measures. It shall provide the supervisory authority with written confirmation that the necessary actions have been taken.

SECTION III – LOCAL LAWS AND OBLIGATIONS IN CASE OF ACCESS BY PUBLIC AUTHORITIES

Clause 14

Local laws and practices affecting compliance with the Clauses

(a) The Parties warrant that they have no reason to believe that the laws and practices in the third country of destination applicable to the processing of the personal data by the data importer, including any requirements to disclose personal data or measures authorising access by public authorities, prevent the data importer from fulfilling its obligations under these Clauses. This is based on the understanding that laws and practices that respect the essence of the fundamental rights and freedoms and do not exceed what is necessary and proportionate in a democratic society to safeguard one of the objectives listed in Article 23(1) of Regulation (EU) 2016/679, are not in contradiction with these Clauses.

(b) The Parties declare that in providing the warranty in paragraph (a), they have taken due account in particular of the following elements:

(i) the specific circumstances of the transfer, including the length of the processing chain, the number of actors involved and the transmission channels used; intended onward transfers; the type of recipient; the purpose of processing; the categories and format of the transferred personal data; the economic sector in which the transfer occurs; the storage location of the data transferred;

(ii) the laws and practices of the third country of destination– including those requiring the disclosure of data to public authorities or authorising access by such authorities – relevant in light of the specific circumstances of the transfer, and the applicable limitations and safeguards;

(iii)any relevant contractual, technical or organisational safeguards put in place to supplement the safeguards under these Clauses, including measures applied during transmission and to the processing of the personal data in the country of destination.

(c) The data importer warrants that, in carrying out the assessment under paragraph (b), it has made its best efforts to provide the data exporter with relevant information and agrees that it will continue to cooperate with the data exporter in ensuring compliance with these Clauses.

(d) The Parties agree to document the assessment under paragraph (b) and make it available to the competent supervisory authority on request.

(e) The data importer agrees to notify the data exporter promptly if, after having agreed to these Clauses and for the duration of the contract, it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under paragraph (a), including following a change in the laws of the third country or a measure (such as a disclosure request) indicating an application of such laws in practice that is not in line with the requirements in paragraph (a). The data exporter shall forward the notification to the controller.

(f) Following a notification pursuant to paragraph (e), or if the data exporter otherwise has reason to believe that the data importer can no longer fulfil its obligations under these Clauses, the data exporter shall promptly identify appropriate measures (e.g. technical or organisational measures to ensure security and confidentiality) to be adopted by the data exporter and/or data importer to address the situation, if appropriate in consultation with the controller. The data exporter shall suspend the data transfer if it considers that no appropriate safeguards for such transfer can be ensured, or if instructed by the controller or the competent supervisory authority to do so. In this case, the data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses. If the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise. Where the contract is terminated pursuant to this Clause, Clause 16(d) and (e) shall apply.

Clause 15

Obligations of the data importer in case of access by public authorities

15.1 Notification

(a)   The data importer agrees to notify the data exporter and, where possible, the data subject promptly (if necessary with the help of the data exporter) if it:

    (i)   receives a legally binding request from a public authority, including judicial authorities, under the laws of t of destination for the disclosure of personal data transferred pursuant to these Clauses; such notification sł information about the personal data requested, the requesting authority, the legal basis for the reque response provided; or

    (ii)   becomes aware of any direct access by public authorities to personal data transferred pursuant to these accordance with the laws of the country of destination; such notification shall include all information avail importer.

    The data exporter shall forward the notification to the controller.

(b)   If the data importer is prohibited from notifying the data exporter and/or the data subject under the laws of the country of destination, the data importer agrees to use its best efforts to obtain a waiver of the prohibition, with a view to communicating as much information as possible, as soon as possible. The data importer agrees to document its best efforts in order to be able to demonstrate them on request of the data exporter.

(c)   Where permissible under the laws of the country of destination, the data importer agrees to provide the data exporter, at regular intervals for the duration of the contract, with as much relevant information as possible on the requests received (in particular, number of requests, type of data requested, requesting authority/ies, whether requests have been challenged and the outcome of such challenges, etc.). The data exporter shall forward the information to the controller.

(d)   The data importer agrees to preserve the information pursuant to paragraphs (a) to (c) for the duration of the contract and make it available to the competent supervisory authority on request.

(e)   Paragraphs (a) to (c) are without prejudice to the obligation of the data importer pursuant to Clause 14(e) and Clause 16 to inform the data exporter promptly where it is unable to comply with these Clauses.

15.2 Review of legality and data minimisation

(a)   The data importer agrees to review the legality of the request for disclosure, in particular whether it remains within the powers granted to the requesting public authority, and to challenge the request if, after careful assessment, it concludes that there are reasonable grounds to consider that the request is unlawful under the laws of the country of destination, applicable obligations under international law and principles of international comity. The data importer shall, under the same conditions, pursue possibilities of appeal. When challenging a request, the data importer shall seek interim measures with a view to suspending the effects of the request until the competent judicial authority has decided on its merits. It shall not disclose the personal data requested until required to do so under the applicable procedural rules. These requirements are without prejudice to the obligations of the data importer under Clause 14(e).

(b)   The data importer agrees to document its legal assessment and any challenge to the request for disclosure and, to the extent permissible under the laws of the country of destination, make the documentation available to the data exporter. It shall also make it available to the competent supervisory authority on request. The data exporter shall make the assessment available to the controller.

(c)   The data importer agrees to provide the minimum amount of information permissible when responding to a request for disclosure, based on a reasonable interpretation of the request.

SECTION IV – FINAL PROVISIONS

Clause 16

Non-compliance with the Clauses and termination

(a)   The data importer shall promptly inform the data exporter if it is unable to comply with these Clauses, for whatever reason.

(b)   In the event that the data importer is in breach of these Clauses or unable to comply with these Clauses, the data exporter shall suspend the transfer of personal data to the data importer until compliance is again ensured or the contract is terminated. This is without prejudice to Clause 14(f).

(c)   The data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses, where:

   (i)   the data exporter has suspended the transfer of personal data to the data importer pursuant to paragraph (b) and compliance with these Clauses is not restored within a reasonable time and in any event within one month of suspension;

   (ii)   the data importer is in substantial or persistent breach of these Clauses; or

   (iii)   the data importer fails to comply with a binding decision of a competent court or supervisory authority regarding its obligations under these Clauses.

   In these cases, it shall inform the competent supervisory authority and the controller of such non-compliance. Where the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise.

(d)   Personal data that has been transferred prior to the termination of the contract pursuant to paragraph (c) shall at the choice of the data exporter immediately be returned to the data exporter or deleted in its entirety. The same shall apply to any copies of the data. The data importer shall certify the deletion of the data to the data exporter. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit the return or deletion of the transferred personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process the data to the extent and for as long as required under that local law.

(e)   Either Party may revoke its agreement to be bound by these Clauses where (i) the European Commission adopts a decision pursuant to Article 45(3) of Regulation (EU) 2016/679 that covers the transfer of personal data to which these Clauses apply; or (ii) Regulation (EU) 2016/679 becomes part of the legal framework of the country to which the personal data is transferred. This is without prejudice to other obligations applying to the processing in question under Regulation (EU) 2016/679.

Clause 17

Governing law

These Clauses shall be governed by the law of one of the EU Member States, provided such law allows for third-party beneficiary rights. The Parties agree that this shall be the law of France.

Clause 18

Choice of forum and jurisdiction

(a)   Any dispute arising from these Clauses shall be resolved by the courts of an EU Member State.

(b)   The Parties agree that those shall be the courts of France.

(c)   A data subject may also bring legal proceedings against the data exporter and/or data importer before the courts of the Member State in which he/she has his/her habitual residence.

(d)   The Parties agree to submit themselves to the jurisdiction of such courts.

APPENDIX

ANNEX I

A. LIST OF PARTIES

Data exporter(s): [*Identity and contact details of the data exporter(s) and, where applicable, of its/their data protection officer and/or representative in the European Union*]

Name: See Customer's name in the Agreement

Address: See Customer's address in the Agreement

Contact person's name, position and contact details: See Customer's contact person's name, position and contact details in the Agreement

Activities relevant to the data transferred under these Clauses: Same as the Agreement

Signature and date: Same as the Agreement

Role (controller/processor): Processor

Data importer(s): [*Identity and contact details of the data importer(s), including any contact person with responsibility for data protection*]

Name: See HP's name in the Agreement

Address: See HP's address in the Agreement

Contact person's name, position and contact details: Zoe McMahon, DPO, https://www.hp.com/us-en/privacy/ww-privacy-form.html

Activities relevant to the data transferred under these Clauses: Same as the Agreement

Signature and date: Same as the Agreement

Role (controller/processor): Processor

B. DESCRIPTION OF TRANSFER

Categories of data subjects whose personal data is transferred

See Attachment 1

Categories of personal data transferred

See Attachment 1.

Sensitive data transferred (if applicable) and applied restrictions or safeguards that fully take into consideration the nature of the data and the risks involved, such as for instance strict purpose limitation, access restrictions (including access only for staff having followed specialised training), keeping a record of access to the data, restrictions for onward transfers or additional security measures.

See attachment 1.

The frequency of the transfer (e.g. whether the data is transferred on a one-off or continuous basis).

See attachment 1.

Nature of the processing

See Attachment 1.

Purpose(s) of the data transfer and further processing

See attachment 1.

The period for which the personal data will be retained, or, if that is not possible, the criteria used to determine that period

See Agreement and DPA.

For transfers to (sub-) processors, also specify subject matter, nature and duration of the processing

Subject matter: See Agreement 1.

Nature: See Agreement 1.

Duration of the processing: As long as the contract is in effect.

C. COMPETENT SUPERVISORY AUTHORITY

Commission Nationale de l'informatique et des Libertés (CNIL)

TECHNICAL AND ORGANISATIONAL MEASURES INCLUDING TECHNICAL AND ORGANISATIONAL MEASURES TO ENSURE THE SECURITY OF THE DATA

To protect Customer data, HP abides by a robust set of information security controls including policies, practices, procedures, and organizational structures to safeguard 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 HP's technical/organizational security measures 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 is 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 responsible for directing and managing the organization's information security strategy and controls. An Information Security Framework/Management System is put in place to ensure compliance with HP's security policies and controls and 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 periodically and revoked upon personnel departure.

User account creation and deletion procedures, as have been mutually agreed upon, are implemented to grant and revoke access to client systems used during the engagement.

5. Personnel Training

HP employees must complete the Integrity at HP training designed to ensure that employees are familiar with the program, policies, and resources that govern HP's 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 must also complete an annually refreshed

dedicated security awareness training focused on essential security policies and emphasizing the employees' 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.

For applicable suppliers (suppliers that handle/store/transmit HP data and customer owned HP held data or have access to the HP network), HP Cybersecurity performs a risk assessment to verify the existence of an information security program. An adequate program must include physical, technical, and administrative safeguards. This assessment must be done before the supplier has access to HP information.

7. Systems Security

By policy, the 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, including 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 regularly.

8. Physical and Environmental Security

HP facilities are secured using various 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, including 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.

11. 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.

12. 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 their effectiveness. HP currently tests and updates all plans at least yearly and ensures that people with a role in the business continuity plan are trained.

For transfers to (sub-) processors, also describe the specific technical and organisational measures to be taken by the (sub-) processor to be able to provide assistance to the controller and, for transfers from a processor to a sub-processor, to the data exporter

Sub-processors only process: name, business email address, business phone number, business address. The purpose of transferring this data is to complete the contract.

For HP all of the above technical and organizational measures are flowed down to the sub-processors through the partner code of conduct and contract terms. Sub-processors are required to commit to following HP's requirements.

Attachment 4

INTERNATIONAL DATA TRANSFER AGREEMENT (IDTA) (UK)

Part 1: Tables

Table 1: Parties and signatures

Start date	Same as in the Agreement	
The Parties	Exporter (who sends the Restricted Transfer)	Importer (who receives the Restricted Transfer)
Parties' details	Full legal name: See Customer's full legal name in the Agreement Trading name (if different): See Customer's trading name in the Agreement Main address (if a company registered address): See Customer's main address in the Agreement Official registration number (if any) (company number or similar identifier): See Customer's official registration number in the Agreement	Full legal name: See HP's full legal name in the Agreement Trading name (if different): See HP's trading name in the Agreement Main address (if a company registered address): See HP's main address in the Agreement Official registration number (if any) (company number or similar identifier): See HP's official registration number in the Agreement
Key Contact	Full Name (optional): See in the Agreement Job Title: See in the Agreement Contact details including email: See in the Agreement	Full Name (optional): See in the Agreement Job Title: See in the Agreement Contact details including email: See in the Agreement
Importer Data Subject Contact		HP Privacy Office https://www.hp.com/us-en/privacy/ww-privacy-form.html

Signatures confirming each Party agrees to be bound by this IDTA	Signed for and on behalf of the **Exporter** set out above Signed: See in the Agreement Date of signature: See in the Agreement Full name: See in the Agreement Job title: See in the Agreement	Signed for and on behalf of the **Importer** set out above Signed: See in the Agreement Date of signature: See in the Agreement Full name: See in the Agreement Job title: See in the Agreement

Table 2: Transfer Details

UK country's law that governs the IDTA:	☒ England and Wales ☐ Northern Ireland ☐ Scotland
Primary place for legal claims to be made by the Parties	☒ England and Wales ☐ Northern Ireland ☐ Scotland
The status of the Exporter	In relation to the Processing of the Transferred Data: ☒ Exporter is a Controller ☐ Exporter is a Processor or Sub-Processor
The status of the Importer	In relation to the Processing of the Transferred Data: ☐ Importer is a Controller ☒ Importer is the Exporter's Processor or Sub-Processor ☐ Importer is **not** the Exporter's Processor or Sub-Processor (and the Importer has been instructed by a Third Party Controller)
Whether UK GDPR applies to the Importer	☐ UK GDPR applies to the Importer's Processing of the Transferred Data ☒ UK GDPR does not apply to the Importer's Processing of the Transferred Data

Linked Agreement	**If the Importer is the Exporter's Processor or Sub-Processor** – the agreement(s) between the Parties which sets out the Processor's or Sub-Processor's instructions for Processing the Transferred Data:
	Name of agreement: If applicable, see in the Agreement
	Date of agreement: If applicable, see in the Agreement
	Parties to the agreement: If applicable, see in the Agreement
	Reference (if any): If applicable, see in the Agreement
	Other agreements – any agreement(s) between the Parties which set out additional obligations in relation to the Transferred Data, such as a data sharing agreement or service agreement:
	Name of agreement: If applicable, see in the Agreement
	Date of agreement: If applicable, see in the Agreement
	Parties to the agreement: If applicable, see in the Agreement
	Reference (if any If applicable, see in the Agreement **If the Exporter is a Processor or Sub-Processor** – the agreement(s) between the Exporter and the Party(s) which sets out the Exporter's instructions for Processing the Transferred Data:
	Name of agreement: If applicable, see in the Agreement
	Date of agreement: If applicable, see in the Agreement
	Parties to the agreement: If applicable, see in the Agreement
	Reference (if any): If applicable, see in the Agreement
Term	The Importer may Process the Transferred Data for the following time period:
	⊠ the period for which the Linked Agreement is in force
	☐ time period:
	☐ (only if the Importer is a Controller or not the Exporter's Processor or Sub-Processor) no longer than is necessary for the Purpose.
Ending the IDTA before the end of the Term	⊠ the Parties cannot end the IDTA before the end of the Term unless there is a breach of the IDTA or the Parties agree in writing.
	☐ the Parties can end the IDTA before the end of the Term by serving:
	⬜ months' written notice, as set out in Section 29. (How to end this IDTA without there being a breach).

Ending the IDTA when the Approved IDTA changes	Which Parties may end the IDTA as set out in Section 29.2: ☒ Importer ☒ Exporter ☐ neither Party
Can the Importer make further transfers of the Transferred Data?	☒ The Importer MAY transfer on the Transferred Data to another organisation or person (who is a different legal entity) in accordance with Section 16.1 (Transferring on the Transferred Data). ☐ The Importer MAY NOT transfer on the Transferred Data to another organisation or person (who is a different legal entity) in accordance with Section 16.1**Error! Reference source not found.** (Transferring on the T ransferred Data).
Specific restrictions when the Importer may transfer on the Transferred Data	The Importer MAY ONLY forward the Transferred Data in accordance with Section 16.1: ☐ if the Exporter tells it in writing that it may do so. ☐ to: ☐ to the authorised receivers (or the categories of authorised receivers) set out in: ☒ there are no specific restrictions.
Review Dates	☐ No review is needed as this is a one-off transfer and the Importer does not retain any Transferred Data First review date: The Parties must review the Security Requirements at least once: ☐ each ⬚ month(s) ☐ each quarter ☐ each 6 months ☐ each year ☐ each ⬚ year(s) ☒ each time there is a change to the Transferred Data, Purposes, Importer Information, TRA or risk assessment

Table 3: Transferred Data

Transferred Data	The personal data to be sent to the Importer under this IDTA consists of: ☒ The categories of Transferred Data will update automatically if the information is updated in the Linked Agreement referred to. ☐ The categories of Transferred Data will NOT update automatically if the information is updated in the Linked Agreement referred to. The Parties must agree a change under Section 5.3.
Special Categories of Personal Data and criminal convictions and offences	The Transferred Data includes data relating to: ☐ racial or ethnic origin ☐ political opinions ☐ religious or philosophical beliefs ☐ trade union membership ☐ genetic data ☐ biometric data for the purpose of uniquely identifying a natural person ☐ physical or mental health ☐ sex life or sexual orientation ☐ criminal convictions and offences ☒ none of the above ☐ set out in: And: ☒ The categories of special category and criminal records data will update automatically if the information is updated in the Linked Agreement referred to. ☐ The categories of special category and criminal records data will NOT update automatically if the information is updated in the Linked Agreement referred to. The Parties must agree a change under Section 5.3.
Relevant Data Subjects	The Data Subjects of the Transferred Data are: ☒ The categories of Data Subjects will update automatically if the information is updated in the Linked Agreement referred to. ☐ The categories of Data Subjects will not update automatically if the information is updated in the Linked Agreement referred to. The Parties must agree a change under Section 5.3.

Purpose	☐ The Importer may Process the Transferred Data for the following purposes:
	☐ The Importer may Process the Transferred Data for the purposes set out in the Agreement.
	In both cases, any other purposes which are compatible with the purposes set out above.
	☒ The purposes will update automatically if the information is updated in the Linked Agreement referred to.
	☐ The purposes will NOT update automatically if the information is updated in the Linked Agreement referred to. The Parties must agree a change under Section 5.3.

Table 4: Security Requirements

Security of Transmission	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.
Security of Storage	HP's cybersecurity department/organization and HP's legal department maintain a set of documented handling procedures for each information classification type and work along with department in charge of Data Privacy for any pertinent matters. Handling procedures account for: storage, transmission, communication, access, logging, retention, destruction, disposal, incident management, and breach notification. HP Information Technology have a process in place for identifying technical information assets. HP identifies all assets under its responsibility, categorizing the critical assets. A record of information assets and systems that are both HP-owned and externally managed by service providers is maintained. Documented processes for server decommissioning, orphaned and legacy media are also implemented to ensure proper management and disposition of non-removable media.
Security of Processing	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 implements logging mechanisms for system applications and devices. HP has developed robust procedures for the installation, configuration, upgrade,

	testing, and security patching of operational software, including but not limited to email, office productivity suites, and Internet browsers. Internal vulnerability scans are performed both on a quarterly basis and after any significant change.
Organisational security measures	To protect its own as well as Customer Personal Data, 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. Systems with external connections will be protected by hardening and firewalls. Externally facing systems will be placed in a Demilitarized Zone (DMZ) or other similar configuration to protect internal HP systems. Critical network zones are logically isolated. Remote access to devices on the HP internal network, with the exception of the email system, requires the use of HP standard VPN solution. Network Intrusion Detection / Prevention Systems (NIDS/ NIPS) are placed in strategic locations within the network and are monitored and managed 24*7. All devices that have logging capabilities, such as operating systems, databases, applications, firewalls, routers and switches are required to be configured as per HP's logging and auditing standard. HP security policies and standards mandate secure disposal of media.
Technical security minimum requirements	Developers are required to follow the coding standards and testing guidelines defined for the system to comply with application security requirements. Source code is required to be secured in a manner that prevents unauthorized access. Preliminary testing is performed and non-production patch testing is scheduled. Post feedback from the non-production testing, implementation on production environment is scheduled and implemented.
Updates to the Security Requirements	☒ The Security Requirements will update automatically if the information is updated in the Linked Agreement referred to. ☐ The Security Requirements will NOT update automatically if the information is updated in the Linked Agreement referred to. The Parties must agree a change under Section 5.3.

Part 2: Extra Protection Clauses

Extra Protection Clauses:	
(i) Extra technical security protections	
(ii) Extra organisational protections	
(iii) Extra contractual protections	

Part 3: Commercial Clauses

Commercial Clauses	

Part 4: Mandatory Clauses

Mandatory Clauses	Part 4: Mandatory Clauses of the Approved IDTA, being the template IDTA A.1.0 issued by the ICO and laid before Parliament in accordance with s119A of the Data Protection Act 2018 on 2 February 2022, as it is revised under Section 5.4 of those Mandatory Clauses.

Attachment 5

STANDARD CONTRACT CLAUSES (Argentina)

In accordance with the provisions of clause 6.3.1 of the Data Processing Addendum, Customer Personal Data originally collected in the Argentine Republic may be transferred, if required in connection with the services, to third countries.

If the transfer mentioned in the preceding paragraph implies transfer of Customer Personal Data to countries that are not considered as countries that provide adequate levels of protection by applicable Data Protection and Privacy Laws in Argentina, the EU Standard Contractual Clauses included in Attachment 2, with the modifications set forth below, shall be applicable to transfer.

1. Clause 1, items (a), (c) and (e) shall be replaced as follows:

    (a)   *'personal data', sensitive data', 'process/processing', 'controller', 'processor', 'data subject' and 'supervisory authority'* shall have the same meaning as set forth in the Argentine Data Protection Law No. 25.326, its regulatory Decree No. 1558/2001, and their complementary regulations (as amended or replaced from time to time);

    (c) *"the data importer"* means the service provider located outside of Argentina that receives the personal data from the data exporter for the processing in accordance with the terms of this agreement;

    (e)   *'the applicable data protection law'* means the Argentine Data Protection Law No. 25,326 and its supporting regulations (as amended or replaced from time to time).

2. Clause 4, item (f) shall be replaced as follows:

    (f)   that the data subject has been informed or will be informed before, or as soon as possible after, the transfer that its data could be transmitted to a third country not providing adequate protection within the meaning of the Argentine Data Protection Law 25,326 and its supporting regulations (as amended or replaced from time to time).

3. Clause 7, subsection 1, item (b) shall be replaced as follows:

    (b)   to refer the dispute to the judicial and administrative jurisdiction of the Argentine Republic.

4. Clause 9 shall be replaced as follows:

    This agreement shall be governed by the laws of the Argentine Republic, in particular by the Law No. 25,326, its regulations and dispositions issued by the Argentine Data Protection Authority (as amended or replaced from time to time),

In order to ensure that the activities of PI Processor and Overseas Recipient meet the PI protection standards under the Relevant Laws and Regulations of the PRC and specify the PI protection related rights and obligations of PI Processor and Overseas Recipient, the Parties have mutually agreed to enter into this Contract.

PI Processor: see in the Agreement
Address: see in the Agreement
Contact Method: see in the Agreement
Contact Person: see in the Agreement
Title: see in the Agreement

Overseas Recipient: see in the Agreement
Address: see in the Agreement
Contact Method: see in the Agreement
Contact Person: see in the Agreement
Title: see in the Agreement

PI Processor and Overseas Recipient will conduct the outbound transfer of PI in accordance with this Contract, and the Parties have entered into an Agreement as of date stated therein to govern the commercial activities related thereto.

The main body of this Contract is formulated in accordance with the requirements of the Measures on the Standard Contract for Personal Information Cross-Border Transfer, and any other contractual provisions, if any, as agreed between the Parties, can be specified in Annex II, which shall be deemed part of this Contract, if they do not conflict with the main body of this Contract.

Article I – Definitions

In this Contract, unless otherwise provided herein:
1. "PI Processor" refers to an entity or individual in PI processing activities that independently decides the purpose and method of the PI processing activities and transfers PI outside of the PRC.
2. "Overseas Recipient" refers to an entity or individual outside of the PRC that receives the PI from PI Processor.
3. PI Processor or Overseas Recipient are referred to individually as a "Party", and collectively as the "Parties".
4. "PI Subject" refers to a natural person identified by or associated with the PI.
5. "PI" refers to all kinds of information, recorded electronically or otherwise, related to identified or identifiable natural persons, but excluding anonymized information.
6. "Sensitive PI" refers to the PI that, once leaked or illegally used, may damage the personal dignity or endanger the personal or property safety of a natural person, including biometric recognition, religious belief, specific identity, medical health, financial account, personal whereabouts, etc., and the PI of minors under the age of 14.
7. "Regulatory Authority" refers to the cyberspace administration of the PRC at the provincial level or above.
8. "Relevant Laws and Regulations" refer to the PRC Cybersecurity Law, the PRC Data Security Law, the PRC Personal Information Protection Law, the PRC Civil Code, the PRC Civil Procedure Law, the Measures on the Standard Contract for Outbound Transfer of PI, and other PRC laws and regulations.

9. The terms not defined in this Contract have the same meanings as defined under the Relevant Laws and Regulations.

Article 2 – Obligations of PI Processor

PI Processor shall perform the following obligations:

1. process PI in accordance with the Relevant Laws and Regulations, and limit the PI to be transferred abroad to the minimum scope required for the purpose of processing.

2. inform the PI Subject of the name and contact information of Overseas Recipient, the purpose and method of processing, type of PI and retention periods as specified in Annex I – Details of the Outbound Transfer of PI, the methods and procedures for PI Subject to exercise his/her rights, and etc.; in case of an outbound transfer of Sensitive PI, inform the PI Subject of the necessity of the outbound transfer of Sensitive PI and the impact on the rights and interests of the PI Subject; provided in each case that such obligation can be exempted by the laws and administrative regulations.

3. obtain a separate consent of PI Subject if the PI is transferred abroad based on the consent of the individual; or, if the PI of a minor under the age of 14 is involved, obtain a separate consent of the minor's parents or other guardians. The consent shall be in a written form if so required by the laws and administrative regulations.

4. inform PI Subject that PI Processor and Overseas Recipient have agreed that the PI Subject will be a third-party beneficiary under this Contract, and if the PI Subject does not expressly object within 30 days, the PI Subject shall be entitled to the rights of a third-party beneficiary in accordance with this Contract.

5. make reasonable efforts to ensure that Overseas Recipient takes the following technical and managerial measures (comprehensively considering potential PI security risks that may arise from the purpose of PI processing, the type, scale, scope and sensitivity of the PI, the volume and frequency of the PI transfer, the PI transmission, the period of retention by Overseas Recipient, and etc.) to perform its obligations under this Contract: see Annex III.

6. provide copies of the relevant laws and technical standards to Overseas Recipient upon the request of Overseas Recipient.

7. respond to inquiries from the Regulatory Authority about Overseas Recipient's processing activities.

8. conduct a PI protection impact assessment on the proposed transfer of PI to Overseas Recipient in accordance with the Relevant Laws and Regulations. The assessment shall focus on the following matters:

> (1) the legitimacy, justifiability and necessity of the purpose, scope and method of PI processing by PI processor and Overseas Recipient;
>
> (2) the scale, scope, types and sensitivity of the PI to be transferred abroad, and the risks to PI rights and interests that may arise from the cross-border transfer of PI;
>
> (3) the obligations to be undertaken by Overseas Recipient, and whether the management and technical measures and capabilities for performance of the obligations can ensure the security of the PI to be transferred abroad;
>
> (4) the risks of the PI being tampered with, destroyed, leaked, lost or illegally used after its transfer abroad, and whether the channels for safeguarding the PI rights and interests are smooth;
>
> (5) the impact of the PI protection policies and regulations of the country or region where Overseas Recipient is located on the performance of contract; and
>
> (6) other matters that may affect the security of cross-border transfer of PI.

The PI protection impact assessment report shall be kept for at least three years.

9. provide a copy of this Contract to PI Subject upon the request of PI Subject. If trade secrets or confidential business information are involved, the relevant contents of the copy of this Contract can be handled appropriately to the extent not affecting PI Subject's understanding of this Contract.

10. assume the burden of proof on the performance of obligations under this Contract.

11. in accordance with the Relevant Laws and Regulations, provide the Regulatory Authority with all the information under Article 3(11), including all the compliance audit results.

Article 3 - Obligations of Overseas Recipient

Overseas Recipient shall perform the following obligations:

1. process the PI in accordance with Annex I – Details of the Outbound Transfer of PI. If Overseas Recipient processes the PI in a manner that is beyond the purpose and method of PI processing and/or the type of PI as agreed, a separate consent of PI Subject shall be obtained if the PI is transferred abroad based on the consent of the individual; if the PI of a minor under the age of 14 is involved, a separate consent of the minor's parents or other guardians shall be obtained.

2. If entrusted by PI Processor to process PI, process the PI in accordance with the agreement with PI Processor and not process the PI in a manner that is beyond the purpose or method of the PI processing as agreed with PI processor.

3. provide a copy of this Contract to PI Subject upon the request of PI Subject. If trade secrets or confidential business information are involved, the relevant contents of the copy of this Contract can be handled appropriately to the extent not affecting the PI Subject's understanding of this Contract.

4. process the PI in a manner that has the least impact on the rights and interests of PI Subject.

5. ensure that the retention period of PI is the minimum period necessary for achieving the purpose of PI processing. Delete the PI (including all back-up copies) upon expiry of the retention period. Where Overseas Recipient is entrusted by PI Processor to process PI and the entrustment agreement does not take effect, becomes null and void, or is cancelled or terminated, the PI being processed shall be returned to PI Processor or shall be deleted, and a written statement shall be provided to PI Processor. If it is technically difficult to delete the PI, all processing of the PI shall be ceased, other than storing the PI and taking necessary security measures.

6. ensure the security of PI processing in accordance with the following:

   (i) take technical and managerial measures including but not limited to those listed in Article 2(5) of this Contract, and conduct periodic inspections to ensure the security of PI; and

   (ii) ensure that the personnel authorized to process PI perform their confidentiality obligations, and establish access controls based on the minimum authorization principle.

7. In the event that PI is or may be tampered with, destroyed, leaked, lost, illegally used, provided or accessed without authorization, Overseas Recipient shall:

   (i) promptly take appropriate remedial measure to mitigate the adverse impact on PI Subject;

   (ii) immediately notify PI Processor, and report to the Regulatory Authority in accordance with the Relevant Laws and Regulations. The notice shall contain the following contents:

      a. the type of PI being or likely to be tampered with, destroyed, leaked, lost, illegally used, provided or accessed without authorization, the reasons and potential harm of such incident;

      b. the remedial measures that have been taken;

      c. the measures that can be taken by PI Subject to mitigate the harm; and

      d. the contact information of the person or team responsible for handling the relevant incident.

   (iii) where the Relevant Laws and Regulations require a notification to PI Subject, the contents of the notice shall include those under Article 3(7)(ii) above; if Overseas Recipient is entrusted by PI Processor to process PI, the notice shall be sent by PI Processor to PI Subject;

   (iv) record and archive all the circumstances related to the occurrence or likely occurrence of tampering, destruction, leakage, loss, illegal use, unauthorized provision or access, including all remedial measures taken.

8. Overseas Recipient may provide PI to a third party located outside of the PRC only if all of the following requirements are met:

   (i) it is indeed necessary for business purposes;

(ii) unless otherwise provided under the laws and administrative regulations, PI Subject has been informed of the name and contact information of the third party, and the purpose and method of PI processing, the type of PI, retention periods, and the methods and procedures for PI Subject to exercise his/her rights; if Sensitive PI will be transferred to such third party, PI Subject shall also be informed of the necessity for the outbound transfer of Sensitive PI and the impact on the rights and interests of PI Subject;

(iii) if the processing of PI is based on the consent of PI Subject, a separate consent of PI Subject shall be obtained; or, if the PI of a minor under the age of 14 is involved, a separate consent of the minor's parents or other guardians shall be obtained. The consent shall be in a written form if so required by laws and administrative regulations;

(iv) it has entered into a written agreement with the third party to ensure that the processing of PI by the third party meets the standards for protection of PI required by the Relevant Laws and Regulations, and Overseas Recipient will be liable for the infringement of PI Subject's rights due to the provision of PI to such third party;

(v) it will provide a copy of the above-mentioned agreement with the third party to PI Subject upon the request of PI Subject. If trade secrets or confidential business information are involved, the relevant contents of the copy of such agreement can be handled appropriately to the extent not affecting PI Subject's understanding of such agreement.

9. If Overseas Recipient is entrusted by PI Processor to process PI, and Overseas Recipient intends to sub-contract the processing to a third party, Overseas Recipient shall obtain the consent of PI Processor in advance, ensure that the sub-contractor will not process PI in a manner that is beyond the purpose and method of the processing as specified in Annex – Details of the Outbound Transfer of PI, and monitor the PI processing activities of the third party.

10. When making use of PI for automated decision-making, Overseas Recipient shall ensure the transparency of decision-making and fair and impartial results, and shall not carry out unreasonable or differentiated treatment of PI Subject in terms of transaction conditions, such as transaction price. Where automated decision-making is used for information pushing and/or commercial marketing to PI Subject, Overseas Recipient shall also provide PI Subject with options that are not tailored to personal characteristics, or provide a convenient way for PI Subject to opt out.

11. Overseas Recipient shall undertake to provide PI Processor with all necessary information required to comply with the obligations under this Contract, shall allow PI Processor to review the necessary data documents and files, or shall allow PI processor to conduct a compliance audit of the processing activities under this Contract and shall provide facilitation for the compliance audit conducted by the PI Processor.

12. Overseas Recipient shall maintain an objective record of the PI processing activities, keep such records for at least 3 years and provide the relevant records and documents to the Regulatory Authority directly or through PI Processor in accordance with the Relevant Laws and Regulations.

13. Overseas Recipient agrees to accept the supervision and regulation by the Regulatory Authority during the course of its supervision of the implementation of this Contract, including but not limited to responding to inquiries, and cooperating with inspections, by the Regulatory Authority, abiding by the actions taken or decisions made by the Regulatory Authority, and providing written evidence that necessary actions have been taken, etc.

Article 4 – Impact of PI Protection Policies and Regulations in the Overseas Recipient's Country or Region on the Performance of Contract

1. The Parties warrant that they have exercised reasonable care when entering into this Contract and are not aware of PI protection polices and regulations in the Overseas Recipient's country or region (including any requirements on providing PI or authorizing public authorities to access PI) that would impact Overseas Recipient's performance of its obligations under this Contract.

2. The Parties represent that, when making the warranties under Article 4(1), they have conducted an assessment in light of the following circumstances:

> (i) the specific circumstances of the outbound transfer, including the purpose of PI processing, the type, scale, scope and sensitivity of the PI, the volume and frequency of the PI transfer, the PI transmission , the period of retention by Overseas Recipient, the previous experience of Overseas Recipient with respect to similar outbound transfer and processing of PI, whether any PI security incident has occurred to Overseas Recipient and whether such incident was timely and effectively handled, whether Overseas Recipient has received any request to provide PI to the public authorities of the country or region where it is located and how Overseas Recipient responded to such request;
>
> (ii) the PI protection policies and regulations of the country or region where Overseas Recipient is located, including the following factors:
>
>> a. the currently effective PI protection laws, regulations and generally applicable standards of the country or region;
>>
>> b. the regional or global PI protection organizations that the country or region accedes to, and binding international commitments made by the country or region; and
>>
>> c. the mechanisms for PI protection implemented in the country or region, e.g. whether the supervision and enforcement authorities and relevant judicial authorities are capable of protecting PI.
>
> (iii) Overseas Recipient's security management rules and technical capabilities.

3. Overseas Recipient warrants that it has used its best efforts to provide PI Processor with the necessary relevant information for the assessment under Article 4(2).

4. The Parties shall keep a record of the process and results of the assessment carried out under Article 4(2).

5. Where Overseas Recipient is unable to perform this Contract due to any change in the PI protection policies and regulations of the country or region where Overseas Recipient is located (including an amendment to laws in such country or region, or imposition of mandatory measures), Overseas Recipient shall notify PI Processor immediately after becoming aware of such change.

6. If Overseas Recipient is requested by a governmental authority or judicial authority in the country or region where Overseas Recipient is located to provide PI under this Contract, it shall promptly notify PI Processor.

Article 5 – Rights of PI Subject

The Parties agree that PI Subject shall be entitled to the following rights as a third-party beneficiary under this Contract:

1. PI Subject, in accordance with the Relevant Laws and Regulations, has the right to know and the right to make decisions concerning the processing of his/her PI, has the right to restrict or refuse the processing of his/her PI by others, has the right to review, duplicate, correct, supplement or delete his/her PI, and has the right to request others to explain the rules for the processing of his/her PI.

2. When PI Subject requests to exercise the above-mentioned rights regarding his/her PI that has been transferred abroad, PI Subject may request PI Processor or directly request Overseas Recipient to take appropriate measures to realize such rights. If PI Processor is unable to realize those rights, it shall notify Overseas Recipient and request Overseas Recipient to assist.

3. Overseas Recipient shall, in accordance with PI Processor's notice or PI Subject's request, cause the realization of the rights to which PI Subject is entitled s within a reasonable time period and in accordance with the Relevant Laws and Regulations.

Overseas Recipient shall inform PI Subject of the relevant information in a conspicuous, true, accurate and complete manner, and in clear and understandable language.

4. If Overseas Recipient refuses PI Subject's request, it shall inform PI Subject of the reasons for the refusal, and how PI Subject can raise complaints to the Regulatory Authority and seek judicial remedies.

5. PI Subject is a third-party beneficiary to this Contract, and has the right to claim against one or both of PI Processor and Overseas Recipient in accordance with this Contract and require them to perform the following clauses under this Contract relating to the rights of PI Subject:

      (i) Article 2, except for Articles 2(5), 2(6), 2(7) and 2(11);
      (ii) Article 3, except for Articles 3(7)(ii) and 3(7)(iv),3(9),3(11),3(12) and 3(13);
      (iii) Article 4, except for Articles 4(5) and 4(6);
      (iv) Article 5;
      (v) Article 6;
      (vi) Article 8(2) and 8(3); and
      (vii) Article 9(5).

The provisions agreed above shall not affect the rights and interests of PI Subject under the PRC Personal Information Protection Law.

Article 6 - Remedies

1. Overseas Recipient shall identify a contact person who is authorized to respond to inquiries or complaints concerning the processing of PI, and shall promptly handle such inquiries or complaints raised by PI Subject. Overseas Recipient shall notify PI Processor of the contact information of such contact person and shall, by separate notice or announcement on its website in an easy-to-understand manner, inform PI Subject of the contact information of such contact person. [The specific language shall be:] Contact person and contact information (office phone number or email address).

2. If a dispute arises between a Party and PI Subject with respect to the performance of this Contract, such Party shall notify the other Party and the Parties shall cooperate to resolve the dispute.

3. If the dispute cannot be resolved through friendly corporation and PI Subject exercises the rights as a third-party beneficiary in accordance with Article 5, Overseas Recipient shall accept that PI Subject may choose from of the following:

      (i) making a complaint to the Regulatory Authority,
      (ii) bringing a lawsuit to the court specified under Article 6(5).

4. The Parties agree that when PI Subject exercises the rights as a third-party beneficiary with respect to a dispute under this Contract, if PI Subject chooses to apply the Relevant Laws and Regulations of the PRC, such choice shall prevail.

5. The Parties agree that when PI Subject exercises the rights as a third-party beneficiary with respect to a dispute under this Contract, PI Subject may file a lawsuit with a competent court in accordance with the PRC Civil Procedure Law.

6. The Parties agrees that the choices made by PI Subject to safeguard his/her rights is without prejudice to PI Subject's rights to seek remedies in accordance with other laws and regulations.

Article 7 - Termination of the Contract

1. If Overseas Recipient breaches the obligations under this Contract or Overseas Recipient is unable to perform this Contract due to a change in the PI protection policies and regulations of the country or region where Overseas Recipient is located (including an amendment to laws in such country or region, or imposition of mandatory measures), PI Processor may suspend the provision of PI to Overseas Recipient until the breach is rectified or the Contract is terminated.

2. Under any one of the following circumstances, PI Processor shall be entitled to terminate this Contract and notify the Regulatory Authority where necessary:

      (i) PI Processor has suspended the provision of PI to Overseas Recipient in accordance with Article 7(1) for more than one month;
      (ii) Overseas Recipient's compliance with this Contract will violate the laws and regulations of its own country or region;

(iii) Overseas Recipient seriously or continuously breaches the obligations under this Contract;
(iv) Overseas Recipient or PI Processor has been determined to have breached this Contract pursuant to a final decision of a competent court or the regulatory body supervising Overseas Recipient; or Overseas Recipient may also terminate this Contract in case of sub-paragraph (i), (ii) or (iv) of above.

3. This Contract may be terminated upon mutual agreement by the Parties, provided that such termination shall not exempt the Parties from the obligations of protecting PI during the processing of the PI.

4. If the Contract is terminated, Overseas Recipient shall promptly return or delete the PI (including all back-up copies) received hereunder and provide PI Processor with a written statement. If it is technically difficult to delete the PI, other than storing and taking necessary security protection measures, all processing of the PI shall be ceased.

Article 8 – Liability for Breach of the Contract

1. Each Party shall be liable for any damages as a result of its breach of this Contract suffered by the other Party.

2. Each Party shall bear civil liabilities to PI Subject if its breach of this Contract infringes on the rights of PI Subject, without prejudice to the administrative, criminal or other legal liabilities that shall be assumed by PI Processor under the Relevant Laws and Regulations.

3. If the Parties shall assume joint and several liabilities in accordance with the law, PI Subject shall have the right to request each Party or both of the Parties to assume liabilities. When the liability assumed by one Party exceeds the liability such Party shall be assumed, such Party shall have the right to claim against the other Party accordingly.

Article 9 – Miscellaneous

1. If this Contract conflicts with any other legal documents between the Parties, this Contract shall prevail.

2. The formation, validity, performance and interpretation of this Contract and any dispute between the Parties arising from this Contract shall be governed by the Relevant Laws and Regulations.

3. All notices shall be promptly transmitted or sent by e-mails, cable, telex, facsimile (a confirmation copy shall be sent by airmail), or registered airmails to [address of the Parties respectively] or such other addresses designated by a written notice). The notice under this Contract sent by registered airmail shall be deemed to have been received [*] days after its postmark-date, and [*] working days after it is sent via e-mail, cable, telex or facsimile.

4. For any dispute arising from this Contract between the Parties, and any claim by either Party against the other for recovery of payment for the infringement on PI Subject, the Parties shall resolve such dispute or claim through negotiation; if such negotiation fails, either Party may adopt any of the following methods to resolve the dispute (check the box for the chosen arbitration institution if the Parties choose arbitration):
    (i) Arbitration. The dispute shall be submitted to:
        • China International Economic and Trade Arbitration Commission
        • China Maritime Arbitration Commission
        • Beijing Arbitration Commission (Beijing International Arbitration Center)
        • Shanghai International Arbitration Center
        • Other arbitration institutions that are members of the Convention on the Recognition and Enforcement of Foreign Arbitral Awards
    The arbitration shall be conducted in [venue] in accordance with its arbitration rules then in force.
    (ii) Litigation. The dispute shall be submitted to a competent PRC people's court in accordance with law.

5. This Contract shall be interpreted in accordance with the Relevant Laws and Regulations and shall not be interpreted in a manner inconsistent with the rights and obligations set forth in the Relevant Laws and Regulations.

6. This Contract shall be executed in [*] originals, and each Party shall hold [*] original(s) respectively, and all of which shall have equal legal effect. This contract is signed in [*].

PI Processor: see in Agreement
Date: see in Agreement

Overseas Recipient: see in Agreement
Date: see in Agreement

Details of the cross-border transfer of personal information under this Contract are agreed upon as follows:

1. Purpose of processing:

2. Method of processing:

3. The scale of PI to be transferred abroad:

4. Type of PI to be transferred abroad see the types in the Information Security Technologies – PI Security Specifications (GB/T 35273) and relevant standards):

5. Type of Sensitive PI to be transferred abroad (if applicable, see the types in the Information Security Technologies - PI Security Specifications of GB/T 35273 and relevant standards):

JTN Note: GB/T 35273 lists the following information as Sensitive PI (not exhaustive):
- *Personal Asset Information: Bank accounts, identification information (password), information on deposit (including amount of deposit, payment and saving records, etc.), real estate information, credit loan information, creditability information, transaction and consumption record, daily accounts, etc.; and virtual currency, virtual transaction, video game tokens and other virtual asset information.*
- *Personal Health Biotic Information: Records generating from an individual's medical treatment due to illness and etc., e.g. name of the disease, medical records, doctor's notices, [physical] examination report, record of surgery and anesthesia, caring service record, medicine record, information of allergy re food and medicine, fertility information, disease history, status of medical treatment, family disease history, current disease status, History of infection, etc.*
- *Personal Identification Biotic Information: Individual's gene, fingerprint, voiceprint, handprint, auricle, iris, facial identifiable features, etc.*
- *Personal Identification Information: ID card, certificate of military officers, passport, driving license, work permit, social security card, residence permit, etc.*
- *Other Information: Sexual orientation, marriage history, religious belief, unpublished criminal record, communication record and contents, address books, friend lists, group lists, whereabouts, webpage history, accommodation record, accurate location information, etc.*

6. The Overseas Recipient transfers PI only to the following third parties outside the People's Republic of China (if applicable):

7. Method of transfer:

8. Retention period after the cross-border transfer:

9. Storage location after the outbound transfer:

10. Other matters (to be filled in as appropriate):

Annex II
Other Terms Agreed Upon By the Parties (If necessary)

Annex III

Technical and organizational measures

1. Organization

HP has an Information Security Organization responsible for directing and managing the organization's information security strategy and controls. An Information Security Framework/Management System is put in place to ensure compliance with HP's security policies and controls and 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.

2. Asset Management

HP has a process in place for identifying technical information assets, and through this process, HP identifiesall 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.

3. 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 periodically and revoked upon personnel departure.

User account creation and deletion procedures, as have been mutually agreed upon, are implemented to grant and revoke access to client systems used during the engagement.

4. Personnel Training

HP employees must complete the Integrity at HP training designed to ensure that employees are familiar with the program, policies, and resources that govern HP's 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 must also complete an annually refreshed dedicated security awareness training focused on essential security policies and emphasizing the employees' responsibilities related to incident management, data privacy, and information security.

5. Third Parties and Subcontractors

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

For applicable suppliers (suppliers that handle/store/transmit HP data and customer owned HP held data or have access to the HP network), HP Cybersecurity performs a risk assessment to verify the existence of an information security program. An adequate program must include physical, technical, and administrative safeguards. This assessment must be done before the supplier has access to HP information.

6. Systems Security

By policy, the 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, including 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 regularly.

7. Physical and Environmental Security

HP facilities are secured using various 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.

8. Operations Management

HP has defined a minimum set of hardening requirements for technology infrastructure, including 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.

9. 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.

10. 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.

12. 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 documentedplanning processes.

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