Data Processing and Vendor Security Agreement

This Data Processing and Vendor Security Agreement (hereinafter 'DPVSA') sets out the terms and conditions for the Processing of Personal Data by the Vendor on behalf of HCL Technologies Limited and/or its Affiliates (hereinafter 'HCL'). This DPVSA is incorporated by reference into the Master Vendor Agreement and/or Purchase Order Terms and any other HCL Agreements that the parties may have entered into for the procurement and provision of Services from the Vendor to HCL (hereinafter referred to as 'Contractual Terms').

The parties also agree that, unless a separate Data Processing Agreement exists, this DPVSA governs the processing of Personal Data pursuant to the provision of Services to HCL.

1. Definitions

In this Agreement, the following terms shall have the meanings set out below and cognate terms shall be construed accordingly. Capitalized terms used but not defined in this Agreement will have the meanings provided in the relevant Contractual Terms that Parties have entered into.

Aggregated Personal Data means:

Any Personal Data that relates to multiple Data Subjects that fall into the same group or category, from which individual Data Subject identities have been removed, that is not linked or reasonably linkable to any Data Subject or household, including via a device.

Agreement means:

This DPVSA as agreed between the Parties consisting of the Processing details, and the Processing conditions.

The California Privacy Right Act of 2020" or "CPRA" means:

Assembly Bill 375 of the California House of Representatives, an act to add Title 1.81.5 (commencing with Section 1798.100) to Part 4 of Division 3 of the Civil Code, relating to privacy and approved by the California Governor on June 28, 2018, as amended November 3, 2020, by initiative Proposition 24. Effective December 16, 2020, and operative January 1, 2023.

Confidential Information means:

Any information which is identified as confidential or proprietary, or of a confidential nature including trade secrets, personal data, information of a commercial value, financial and charging information, content of this Agreement, Customer identities and information which relates to either Party or its customer or sub-processor. Personal Data shall remain confidential in all circumstances.

Controller means:

The natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the Processing of Personal Data; where the purposes and means of such Processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law.

Customer means:

The natural or legal person, public authority, agency or other body to which HCL provides services.

Data Protection Law(s) and Regulation(s) means:

Any and all applicable data protection, security or privacy-related laws, statutes, directives or regulations (hereinafter "Data Protection Laws"), including but not limited to: (a) the General Data Protection Regulation ("GDPR") together with any amending or replacement legislation, any EU Member State or United Kingdom laws and regulations promulgated thereunder; (b) the California Privacy Right Act of 2020 ("CPRA") together with any amending or replacement legislation; (c) the Brazil's General Data Protection Law ("LGPD") together with any amending or replacement legislation; (d) the China's Personal Information Protection Law ("PIPL") together with any amending or replacement legislation; and
e) all other applicable laws and regulations in any relevant jurisdiction relating to Personal Data and privacy, and as each may be amended, extended or re-enacted from time to time.

Data Subject means:

The identified or identifiable natural person to whom the Personal Data relates.

Data Transfer Impact Assessment (TIA) means:

The assessment where Vendor shall assess and provide necessary information to enable the Customer or HCL in performing the risk assessment as required by The Court of Justice of the European Union in its judgment in the case of the Data Protection Commissioner Ireland v Facebook Ireland Ltd., Maximillian Schrems, known as 'Schrems II' in July 2020. These Transfer Impact Assessments typically consider the sufficiency of foreign protections on a case-by-case basis when data is transferred using Standard Contractual Clauses, binding corporate rules or other EU-approved data transfer mechanisms

De-identified Personal Data means:

Any Personal Data that cannot reasonably identify, relate to, describe, be capable of being associated with, or be linked, directly or indirectly, to a particular Data Subject.

EU/EEA means:

European Union/European Economic Area respectively.

GDPR means:

The regulation (EU) 2016/679 of the European Parliament and of the Council of the 27th of April 2016 on the protection of natural persons with regard to the Processing of Personal Data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).

HCL Information means:

Information and data received or accessed by the Vendor and governed as part of this Agreement, including any Personal Data, as well as any new data created by the Vendor on behalf of HCL from the said information and data (including aggregated or anonymized data).

Party/Parties means:

An individual or business who enters into a binding agreement with another contracting **party/parties**, thus accepting the obligations, responsibilities, and benefits specified within the agreement

Personal Data means:

Any information that relates to an identified or identifiable natural person, an identifiable natural person is one who can be identified (a) either directly or indirectly, in particular by reference to an identifier such as name, an identification number, location data, an online identifier, or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person. For the purposes of this Agreement this can include current, past or potential employees or customers of HCL and any employees or end users of our customers, and (b) covered by Data Protection Laws, including but not limited to the following: (i) a first name and last name; (ii) a home or other physical address, including street name and name of city or town; (iii) an email address or other name, that reveals an individual's email address; (iv) a telephone number; (v) a Social Security number; (vi) credit or debit card information; (vii) checking account information, account number and check number; (viii) a driver's license, military or state identification number; (ix) a persistent identifier, such as a customer number held in a "cookie" or processor serial number, that is combined with other available data that identifies an individual; (x) human resources information, such as benefits plan information, member number, salary information, performance history, health history, and similar information; (xi) financial or transactional information; (xii) employee ID number; (xiii) government passport number or alien registration number, or (xiv) any other information that is identifiable to or identifies an individual, whether combined with any of (i) through (xiv) above.

Personal Data Breach means:

Each breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Personal Data transmitted, stored or otherwise processed, by the Processor.

Process, Processed, Processing and/or Processing Operation means:

Any operation or set of operations performed on Personal Data or sets of Personal Data, whether or not by automated means. Processing includes the collection, recording, organization, structuring, alteration, use, access, disclosure, copying, transfer, storage, retention, deletion, combination, restriction, adaptation, retrieval, consultation, destruction, disposal, sale, sharing or other use of Personal Data.

Processor means:

Natural or legal person, public authority, agency, or other body which processes Personal Data on behalf of the Controller. Processor can include Vendor or a Sub processor, or HCL if it is providing services to or acting on behalf of a HCL Customer.

Restricted Transfer means:

(i) Where the GDPR applies, a transfer of Personal Data originating from the EEA to a country outside of the EEA which is not subject to an adequacy determination by the European Commission; (ii) where the UK GDPR applies, a transfer of Personal Data originating from the United Kingdom to any other country which is not subject to adequacy regulations adopted pursuant to Section 17A of the United Kingdom Data Protection Act 2018; (iii) where the Swiss Data Protection Act applies, a transfer of Personal Data originating from Switzerland to a country outside of Switzerland which is not included on the list of adequate jurisdictions published by the Swiss Federal Data Protection and Information Commissioner; and (iv) with regards to any other Data Protection Law(s) and Regulation(s), a transfer of Personal Data originating from the respective country to a country which is not subject to adequacy regulations per such laws.

Security Incident means:

An actual, potential, or attempted security breach or Personal Data Breach, or possession, use, knowledge, destruction, loss, alteration, disclosure or theft of, or unauthorized access to HCL Confidential Information, including Personal Data and/or Customer Data, in violation of this Agreement or applicable law, or the Parties' security policies , or standard which may or may not result in loss of HCL Information, Personal Data, and/or Customer Data and/or adverse effects and disruption of service.

Services means:

The data processing activities and other procedures carried-out by the Vendor for HCL and/or Information in terms of this Agreement or as otherwise instructed or directed by HCL.

Standard Contractual Clauses" or "SCC" means:

The European Commission's Standard Contractual Clauses for the transfer of Personal Data from the European Union to Processor established in third countries or any other applicable Personal Data transfer mechanisms published by the relevant Supervisory Authorities and/or regulatory bodies.

Sub-processor means:

Any person (including any third party and any Vendor Affiliate, but excluding an employee of Vendor appointed by or on behalf of Vendor or any Vendor Affiliate to Process Personal Data on behalf of any Customer group member in connection with the Contractual Terms(s) executed between the Parties.

Supervisory Authority means:

An independent public authority which is established by an EU Member State pursuant to the GDPR or an authority established under applicable privacy and data protection laws.

UK GDPR means

The GDPR as transposed into the national law of the United Kingdom through the operation of section 3 of the European Union (Withdrawal) Act 2018. In this Agreement, in circumstances where and solely to the extent that the UK GDPR applies, references to the GDPR and its provisions shall be construed as references to the UK GDPR and its corresponding provisions, references to European Union or Member State law shall be construed as references to UK law and references to the European Commission shall be construed as references to the UK Government or Information Commissioner Office.

Vendor means:

Anyone who provides goods or services to HCL or its Customer(s) as contemplated in this Agreement or any Contractual Terms as agreed between the Parties that involves the Processing of Personal Data.

2. Authority

Before any Vendor or its Affiliate processes any Personal Data on behalf of HCL, Vendor accepts that it has the authority to enter into this Agreement as agent for and on behalf of the Vendor and/or its Affiliates.

3. Processing Terms

3.1 Roles and Responsibilities

For the purposes of this Agreement:

i. HCL may be a Controller for the Personal Data it collects or processes for its own Purposes and Vendor will be a Processor
ii. HCL may be a Processor/Sub-Processor acting on behalf of its Customers, and Vendor will be a Sub-Processor;
iii. If applicable, Vendor agrees it is a "Service Provider" as defined in CPRA Section 1798.140(v).

3.2 Details of Personal Data Processing

The subject-matter, nature, and purpose of Processing to be undertaken by Vendor and the type of Personal Data and categories of Data Subjects involved are specified in Schedule A to this Agreement.

3.3 Permitted Processing

a. Vendor shall only process Personal Data on behalf of HCL in accordance with this Agreement including the agreed Contractual Terms, and any other written instructions it may receive from HCL.
b. If Vendor cannot comply with such instructions, meet its legal obligations under Data Protection Laws and/or the terms of the Agreement for whatever reason, it agrees to inform HCL promptly of its inability to comply, in which case HCL is entitled to suspend the Processing. In no circumstances shall the Vendor be entitled toprocess the Personal Data for its own purposes. Vendor certifies that it understands and will comply with these restrictions.
c. The Vendor shall only disclose Personal Data to its employees on a need-to-know basis, for the performance of the Vendor's obligations under this Agreement. Any such employees shall be bound by confidentiality obligations no less restrictive than those contained in this Agreement and the Contractual Terms.
d. The Vendor may not disclose Personal Data to any other third party without the prior written consent of HCL. Under no circumstances may Vendor sell, share, rent or lease Personal Data to any third parties.
e. In the event the Contractual Terms or this Agreement permits or instructs Vendor to Process De-identified and/or Aggregated Personal Data, Vendor will do so only with Personal Data that has been De-identified and/or Aggregated. For deidentified Personal Data, Vendor shall

implement the following measures at a minimum: (1) technical safeguards that prohibit reidentification of the Data Subject to whom the Personal Data may pertain; (2) business processes that specifically prohibit reidentification of the Personal Data; and (3) business processes to prevent inadvertent release of de-identified information. Vendor represents and warrants that it will make no attempt to reidentify de-identified or aggregated Personal Data.

f. If the Vendor is permitted under the Contractual Terms to collect Personal Data directly from Data Subjects, Vendor shall do so under the following restrictions:
    i. Vendor shall collect only Personal Data needed to perform its obligations under the Contractual Terms and this Agreement;
    ii. Vendor shall inform the Data Subjects about the purposes for collecting such Personal Data, how to contact the Vendor with any inquiries or complaints, the types of third parties to which the Vendor discloses the Personal Data, and the choices and the means the Vendor offers Data Subject for limiting the use and disclosure of Personal Data, including the opportunity to choose (opt out) whether their Personal Data may be disclosed to a third party;
    iii. The Vendor shall provide such notice in clear and plain language when Data Subjects are first asked to provide Personal Data to the Vendor, or as soon thereafter as is practicable, but in any event before the Vendor uses the Personal Data for Processing and/or discloses the Personal Data to a third party;
    iv. The Vendor shall afford Data Subjects a readily available and affordable means by which to exercise the option of choosing whether their Personal Data may be disclosed to a third party; and
    v. Vendor represents and warrants that it shall not invade the privacy of Data Subjects by seeking to obtain sensitive, personal information such as medical or health conditions, racial or ethnic origin, political opinions, religious or philosophical beliefs or trade union membership unless permitted by the Contractual Terms or this Agreement.
g. Processing by the Vendor shall only take place for the duration specified either in the Contractual Terms (s) between the Parties or Schedule A to this Agreement, as applicable.
h. Vendor shall ensure that Personal Data is accurate and up to date. Vendor shall inform HCL without delay if the Vendor becomes aware that the Personal Data it is Processing is inaccurate or has become outdated.
i. Vendor will assist HCL, taking into account the nature of the Processing, by implementing appropriate technical and organizational measures, insofar as this is possible, for the fulfilment of HCL and/or Customer's obligation to respond to and to fulfil requests from Data Subjects exercising their rights.
j. The Vendor shall appoint or establish a single point of contact to handle and respond to all privacy and data protection queries of HCL, confirm compliance with all privacy and Data Protection Laws, rules, regulations, orders, conventions, and ordinances applicable to HCL and the Vendor, and to confirm that data processing policies and procedures required to be followed and adhered to by the Vendor under the Agreement have been implemented and maintained
k. Subject to applicable laws and regulations, the Vendor on receiving any lawful access request to HCL Information by way of order of a court or subpoena, or by a law enforcement agency, shall inform HCL of any such request within two (2) working days of receiving such request.

Further, subject to applicable laws and regulations, the Vendor will liaise with HCL before responding to such requests. The Vendor shall act as HCL's representative during all privacy related proceedings or enquiries received from the government regulator(s) in connection with HCL Information being processed by the Vendor. The Vendor, wherever necessary, will notify the regulator of the nature of its data processing and will, at all times, ensure compliance with all privacy and data protection laws applicable to HCL under the Agreement and the agreed Contractual Terms.

l. The Vendor shall make available to HCL all information necessary to demonstrate compliance with the obligations that are set out in these Clauses and stem directly from Regulation (EU) 2016/679 and/or Regulation (EU) 2018/1725 and/or other Data Protection Laws.

m. If the CPRA is applicable to the transfer of Personal Data, then Vendor is prohibited from the sale or sharing (as defined in the CPRA) of Personal Data it receives from HCL. For purposes of this section, Vendor understands and certifies that it understands its contractual restrictions under the CPRA as amended and shall comply with them.

n. HCL retains the rights to (a) take reasonable and appropriate steps to ensure that Vendor uses the Personal Data transferred in a manner consistent with the business's legal obligations; and (b) take reasonable and appropriate steps to stop and remediate unauthorized use of Personal Data.

o. Vendor is prohibited from combining Personal Data it receives pursuant to a written contract with the Personal Data it receives from another person or collects from its own interaction with consumers, except as permitted by regulations promulgated by the relevant Privacy Protection Agencies.

4. Information Security

a. Vendor shall ensure a level of security appropriate to the risk, taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of Processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, provided, however, that such measures shall at a minimum include the specific technical, administrative, physical and organizational measures identified in the Agreement and in Schedule A of this Agreement, including but not limited to:

   i. The measures described in the provisions of the Agreement containing specific data security obligations;

   ii. The encryption, pseudonymization, or anonymization of data, as appropriate, including when specified by HCL;

   iii. The ability to restore the availability and access to Personal Data in a timely manner in the event of a physical or technical incident;

   iv. A process for regularly testing, assessing and evaluating the effectiveness of technical and organizational measures for ensuring the security of the data processing; and

   v. The Technical and Organizational Measures (TOMs) available at https://www.hcltech.com/HCL-vendor-privacy-and-information-security-

requirements#standard-privacy-security-terms

5. Engaging Sub-processors

Vendor shall not engage or replace a sub-processor for the performance of Vendor's Processing of Personal Data under this Agreement, without obtaining a specific or general written approval from HCL in advance and in each case Vendor will:

a. Provide Ninety (90) days prior written notice of the appointment of any new sub-processor or change in sub-processor, including full details of the Processing to be undertaken by the sub-processor.
b. Carry out adequate due diligence to ensure that the sub-processor is capable of providing the level of protection of Personal Data required by this Agreement;
c. Ensure that the arrangement with the sub-processor is governed by a written contract including terms which offer at least the same level of protection of Personal Data as those set out in this Agreement.
d. If that arrangement involves a restricted transfer as per the relevant data protection laws, ensure that the Standard Contractual Clauses or equivalent legal mechanism for cross-border data transfer are at all relevant times incorporated into the agreement with the sub-processor.
e. Provide to HCL for review such copies of the agreements with sub-processors (which may be redacted to remove confidential commercial information not relevant to the requirements of this Agreement) as HCL may request from time to time.

6. Data Subject Rights

a. Taking into account the nature of the Processing, Vendor shall assist HCL by implementing appropriate technical and organizational measures, insofar as this is possible, for the fulfilment of HCL's obligations, to respond to requests for the exercise of Data Subject rights under the Data Protection Laws.
b. Vendor shall promptly and no later than two (2) days of receiving such request notify HCL if it or any of its Sub-Processors pursuant to this Agreement receive a request from a Data Subject under any Data Protection Law in respect to Personal Data processed pursuant to this Agreement; and
c. Vendor shall ensure that it and any of its Sub-Processors pursuant to this Agreement do not respond to that request except on the documented instructions of HCL or as required by Data Protection Laws to which the Vendor and/or the Sub-Processor is subject, in which case Vendor shall to the extent permitted by Data Protection Laws inform HCL of that legal requirement before the Vendor or its Sub-Processor responds to the request.
d. Where HCL is of the opinion that in order to honour a modification / withdrawal of consent (for Processing Personal Data) or a request for access, change, correction or choice modification, some action(s) would be required to be taken by the Vendor, HCL will communicate the said modification / withdrawal of consent or the request for access, change, correction or choice modification to the Vendor without delay, and through an appropriate system, to ensure timely completion of the required action(s) by the Vendor. Vendor agrees to take all the actions as may be required to honour modification / withdrawal of consent or to respond to any request for access, change, correction, or choice modification to Personal Data, made by or through HCL, or made pursuant to procedures established by HCL, in a manner which will result in completion of the action in a period (inclusive of any time required by Vendor's subsequent sub-processors) no longer than: (1) twenty (20) days; or (2) such period that may be imposed on HCL as a matter of Applicable Law; whichever is shorter.

7. Security Incident Handling Requirements

a. As soon as possible, but in no event more than 12 hours from discovery of a Security Incident the Vendor must:
   i. ensure the security of Processing;
   ii. provide notifications to HCL of any Security Incident and/or any breach of the technical and/or organizational measures taken with sufficient information to allow HCL to meet any obligations to report or inform Supervisory Authority and if applicable Data Subjects, of the Security Incident under the Data Protection Laws;
   iii. assist with the assessment of impact on rights and freedoms of data subjects affected by the Security Incident; and
   iv. assist with any prior consultations that HCL has with any supervisory authority; and provide formal written communication including actions taken to mitigate, if it was possible to do so.

b. Vendor shall co-operate with HCL and take such reasonable commercial steps as are directed by HCL to assist in the investigation, mitigation, and remediation of each such Security Incident.

8. Data Protection Impact Assessment and Prior Consultation

Vendor shall provide reasonable assistance to HCL with any data protection impact assessments, and prior consultations with Supervisory Authorities or other competent data privacy authorities, which HCL reasonably considers to be required of HCL by article 35 or 36 of the GDPR or equivalent provisions of any other Data Protection Laws, in each case solely in relation to Processing of Personal Data under this Agreement.

9. Deletion or return of Personal Data

a. Except as otherwise provided in this Agreement, upon expiration or termination of this Agreement, or at any time upon HCL's request, Vendor or Vendor's sub-processors immediately return and/or destroy all originals and copies of HCL Data in any media in which data is stored on Vendor or Vendor sub-processors' systems, including, without limitation, recordings, electronic or hard copy format, in accordance with the requirements of this Agreement and applicable laws and regulations

b. Vendor shall promptly upon HCL's request and instructions and/or after the termination of this Agreement and/or at the end of Processing of the Personal Data by Vendor:
   i. return a complete copy of all HCL Personal Data to HCL by secure file transfer in standard and non-proprietary format; and
   ii. return, destroy or dispose all information processed by Vendor or any Sub-Processor, after the relevant timeframe in a secure manner using industry standard data wiping

process . Upon termination of this Agreement and/or at the end of Processing of the Personal Data by Vendor, Vendor shall confirm, within 30 days of termination of the contract about the return of all information assets to HCL or about securely wiping off all information processed under this Agreement. Any sensitive HCL information or its customer' shall be destroyed in such a manner that it cannot be retrieved or restored.

10. Audit rights

a. Vendor and any Sub-Processors shall make available to HCL, upon request, all information necessary to demonstrate compliance with this Agreement at reasonable intervals, and shall allow for and contribute to audits, including inspections, by any Customer or an auditor mandated by HCL or Customer in relation to the Processing of Personal Data by the Vendor. Audits may also include inspections at the premises or physical facilities of the Vendor. The Parties shall make the information referred to in this Clause, including the results of any audits, available to the competent supervisory authority/ies upon request
b. HCL, before undertaking an audit shall notify the Vendor reasonably in advance or as per timelines agreed by Parties in Contractual Terms of any audit or inspection to be conducted and shall make (and ensure that each of its mandated auditors makes) reasonable endeavours to avoid causing (or, if it cannot avoid, to minimize) any damage, injury or disruption to the Vendors' premises, equipment, personnel and business while its personnel are on those premises in the course of such an audit or inspection.

11. Personal Data Transfers

a. Vendor shall not process Personal Data outside the country in which it is received by Vendor or its permitted Sub-Processors, without HCL's prior written authorization. Vendor acknowledges that any such transfers of Personal Data may be subject to Data Protection Laws and may require Vendor to enter into an appropriate data transfer agreement or additional terms with HCL prior to any data transfer.
b. The Parties or their affiliates shall take all necessary measures as are necessary to ensure such Processing or transfer is in compliance with applicable Data Protection Law(s) and Regulation(s) (including such measures as may be communicated by HCL to Vendor). Without prejudice to the foregoing, the parties agree that when a transfer of Personal Data byHCL (as data exporter) to Vendor (as data importer) under this Agreement is a Restricted Transfer, the Vendor shall be bound by the Standard Contractual Clauses prescribed by the European Commission or any relevant Data Protection Authority. For the purposes of this Agreement, the Standard Contractual Clauses are available on https://www.hcltech.com/HCL- vendor-privacy-and-information-security-requirements#standard-contractual-clauses
c. For any other Restricted Transfer, the parties shall abide by any relevant cross-border data transfer requirements as necessary and/or mandated by HCL.

d. In the event that (i) applicable Data Protection Law(s) and Regulation(s) and/or a competent supervisory authority no longer permits the transfer of Personal Data to Vendor pursuant to the Standard Contractual Clauses, and (ii) no other approved mechanism is in place to permit the transfer to Vendor in accordance with Data Protection Law(s) and Regulation(s), at HCL's discretion, HCL may terminate the Agreement or require Vendor to comply with alternate or successor data transfer mechanisms.

12. Data Transfer Impact Assessment and Supplementary Measures

Where the applicable Data Protection Laws require a Data Transfer Impact Assessment, Vendor will:

a. support HCL in ensuring compliance with Data Protection Laws for the transfer of Personal Data of data subjects located in the EEA to third countries by completing and providing an impact assessment. The Parties agree to keep the Data Transfer Impact Assessment updated and the Vendor agrees to make it available to HCL and/or competent Supervisory Authority upon request. If further guidance about the use of the Standard Contractual Clauses and accompanying supplementary measures become available, the Parties shall agree to execute any required amendments pursuant to this Agreement.
b. warrant that it has 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 Vendor or its sub-processors, including any requirements to disclose Personal Data or measures authorizing access by public authorities, prevent the Vendor from fulfilling its obligations under this Agreement and the Standard Contractual Clauses.
c. warrant that it has not obtained access requests from public authorities, interpreted in the widest sense, for the provision of Personal Data processed by the Vendor, and to the best of its knowledge, it is not aware of any surveillance or monitoring activities exercised by public authorities for the purpose of obtaining information on individuals under the Vendor's control.
d. warrant that i) it has not created any "backdoors" or similar programming that could be used to access the system and/or Personal Data, ii) nor does the applicable Data Protection Laws require to maintain such back doors to facilitate access to Personal Data or to hand over an encryption key, and, iii) it has not and will not change its business processes in a way which facilitates unauthorized access to its systems and/or the Personal Data
e. promptly notify HCL if Vendor becomes aware of any laws or change in law, or government policies that affects the Data Transfer Impact Assessment, in particular if any such law or government policies prevents Vendor from complying with its warranties and obligations in this Agreement. Upon such notification by Vendor, Vendor will propose any amendments which are required to the Data Transfer Impact Assessment and HCL is entitled to suspend the transfer of data until a new Data Transfer Impact Assessment is completed and the measures described therein are implemented by Vendor.

f. In the case of a transfer of Personal Data to a third country not providing an adequate level of protection, the following provisions will apply to the Parties in addition to the Standard Contractual Clauses:
    i. Vendor shall ensure that the appropriate technical and organizational measures it implements and maintains, as required by Security of processing clause of the Standard Contractual Clauses, address the risks associated with the transfer of Personal Data to a third country. Vendor shall implement any further additional safeguards required by the Data Transfer Impact Assessment.
    ii. Vendor will challenge at its own expenses any access requests when received from public authorities with all reasonable means. If necessary, it will approach adequate legal counsel to assist in the legal proceedings. The Vendor should, if legally possible, pursue obtaining interim measures which suspend the access to the Personal Data. It will inform HCL of the status of such legal proceedings on a daily basis;
    iii. The Vendor represents and warrants that it will promptly notify HCL and, where possible and in cooperation with HCL, also the data subjects about any legally binding request for disclosure of or actual or documented access attempt by public authorities to Personal Data, unless prohibited by applicable law.

13. Complaint and Supervisory Authority Cooperation

a. The Vendor shall fully cooperate and make available to HCL on its demand all information that is necessary to demonstrate compliance with the GDPR and Data Protection Law obligations and obligations under this Agreement.
b. The Vendor shall immediately notify HCL, but not later than 24 hours, if any complaint, allegation, or request relating to the Vendor's Processing of the Personal Data Impacts Vendor's Processing activities. The Vendor shall provide all such cooperation and assistance as HCL may reasonably require in relation to any such complaint, allegation, or request.
c. If required, the Vendor shall co-operate with the competent supervisory authority.

14. General Terms

14.1 Order of precedence

a. Nothing in this Agreement increases or reduces Vendor's or any Vendor Affiliate's liability to HCL under the Contractual Terms in relation to the protection of Personal Data or permits Vendor or any Vendor Affiliate to Process (or permit the Processing of) Personal Data in a manner which is prohibited by the Contractual Terms.
b. Subject to section 14.2.a., with regard to the subject matter of this Agreement, in the event of inconsistencies between the provisions of this Agreement and any other agreements between the Parties, including the Contractual Terms and including (except where explicitly agreed otherwise in writing, signed on behalf of the Parties) agreements entered into or purported to be entered into after the date of this Agreement, the provisions of this Agreement shall prevail.

c. Nothing in this Agreement directly or indirectly contradicts the Standard Contractual Clauses, and in the event of a conflict, the Standard Contractual Clauses will prevail over any term of this Agreement.

14.2 Changes in Data Protection Laws, etc.

a. HCL may by written notice to Vendor from time to time propose any other variations to this Agreement which HCL reasonably considers to be necessary to address the requirements of any Data Protection Law.

b. HCL shall not require the consent or approval of Vendor or any Vendor Affiliate to amend this Agreement pursuant to this section 14 or otherwise.

c. Should any provision of this Agreement be invalid or unenforceable, then the remainder of this Agreement shall remain valid and in force. The invalid or unenforceable provision shall be either:
    i. Amended as necessary to ensure its validity and enforceability, while preserving the Parties' intentions as closely as possible or, if this is not possible,
    ii. Construed in a manner as if the invalid or unenforceable part had never been contained therein.

14.3 Variation

Any amendment or variation to this Agreement shall be in writing and signed by duly authorised representatives of each of the Parties.

14.4 Commencement, duration, and survival

a. This agreement shall commence on the same date the Contractual Terms or any contractual agreement signed between the Parties commences and shall be co-terminus with those Contractual Terms .
b. The obligations set forth in this Agreement shall survive the expiration or termination (for whatever reason) of the Contractual Terms signed between the Parties for as long as one of the Parties processes Personal Data of the other Party.

14.5 Termination of this Agreement

a. Each Party may terminate this Agreement immediately by giving the other Party written notice to that effect in the following circumstances:
    i. the other Party has breached Data Protection Laws in connection with either this Agreement or the Personal Data provided by (or on behalf of) the terminating Party and such breach is either not capable of remedy or is not remedied within 10 days of written notice from the terminating Party;

ii. the terminating Party considers that the other Party is not Processing the Personal Data provided by (or on behalf of) such terminating Party in accordance with this Agreement

iii. Any provision of this Agreement that expressly or by implication should come into or continue in force on or after termination of this Agreement will remain in full force and effect.

iv. The termination of this Agreement will be without prejudice to any other rights or remedies of any Party under this Agreement or at law and shall not affect any claims or rights which a Party may have against the other which have accrued prior to such termination.

14.6 Effects of termination

Upon termination of this Agreement for any reason vendor shall immediately stop Processing the Personal Data and take action specified in the Section 9 above.