

## **Data Processing Addendum to HCLTech Customer Terms – Software as a Service**

This Data Processing Addendum (hereinafter 'DPA') sets out the terms and conditions for the Processing of Personal Data by HCL Technologies Limited and/or its Affiliates (hereinafter 'HCLTech') in their capacity as Processor. This DPA is incorporated by reference into the HCLTech Customer Terms – Software-as-a-Service (hereinafter referred to as 'Contractual Terms').

The Parties agree that this DPA governs the Processing of Personal Data pursuant to the provision of Services provided by HCLTech under the Contractual Terms. The Parties shall, at all times, comply with their respective obligations under applicable Data Protection Law(s) and Regulation(s).

### **1. Definitions and Interpretations**

In this DPA, 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 DPA will have the meanings provided in the Contractual Terms that Parties have entered into or as per the Data Protection Law(s) and Regulation(s) governing this DPA.

Where applicable, the terms, "Service Provider" and "Sell" will have the same meaning as in the California Privacy Rights Act of 2020 (CPRA). The following terms are understood and construed to have the same meaning in this DPA: "Controller" and "Business," "Processor" and "Service Provider," and "Personal Data" and "Personal Information."

#### **Controller:**

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.

#### **Customer:**

The natural or legal person, public authority, agency or other body to which HCLTech provides Services under the Contractual Terms.

#### **Customer's Personal Data:**

For the purposes of this DPA, Customer's Personal Data means any personal data which may be supplied by Customer and/or its Affiliates to HCLTech under the Contractual Terms and/or which HCLTech (and/or any of its Sub-Processors) generates, collects, stores, transmits or otherwise processes on behalf of Customer and/or its Affiliates.

#### **Data Protection Law(s) and Regulation(s):**

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 Rights 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”); (e) the Argentina’s Personal Data Protection Act, Act No. 25.326 of 2000, (f) the Mexico’s Federal Law on Protection of Personal Data Held by Private Parties (‘FLPPDPP’); (g) the Quebec’s An Act to modernize legislative provisions as regards the protection of personal information (Law 25) together with any amending or replacement legislation; and (h) 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:**

The identified or identifiable natural person to whom the Personal Data relates as stipulated in the applicable Data Protection Laws.

**Data Transfer Impact Assessment (TIA):**

The assessment where, under Data Protection Laws, HCLTech shall assess and provide necessary information to enable the Customer or HCLTech, such as in performing i. 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 ii. the privacy assessment as required under Quebec Law 25 for transfer of Personal Data outside of the province of Quebec and iii. the appropriate TIA as required under Data Protection Laws.

**EU/EEA:**

European Union/European Economic Area respectively.

**GDPR:**

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).

**Party/Parties:**

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:**

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.

**Personal Data Breach:**

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.

**Personal Data Incident:**

Any potential breach of Personal Data, or possession, use, knowledge, destruction, loss, alteration, disclosure or theft of, or unauthorized access to Customer confidential Information, including Personal Data, in violation of this DPA or applicable law, or standard which may or may not result in loss of Customer Personal Data and/or adverse effects and disruption of Services pursuant to the Processing of said Personal Data.

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

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:**

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

**Restricted Transfer:**

- (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 Laws), a transfer of Personal Data originating from the

Data Subject's habitual place of residence to countries that do not offer adequate protection or which is not subject to adequacy regulations per such laws.

**Services:**

The Processing activities and other procedures carried-out by HCLTech or HCLTech's Processors/Sub-Processors pursuant to the Contractual Terms executed between HCLTech and Customer or as otherwise instructed or directed by Customer.

**Standard Contractual Clauses" or "SCC":**

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 of their respective jurisdictions.

**Sub-Processor:**

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

**Supervisory Authority:**

An independent public authority which is established by an EU Member State pursuant to the GDPR or an authority established under Data Protection Laws.

**UK GDPR:**

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 DPA, 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.

**2. Authority**

The Customer warrants that it has all necessary rights to provide the Personal Data to HCLTech for the Processing to be performed in relation to the Services, and that one or more lawful bases set forth in Data Protection Laws support the lawfulness of the Processing. To the extent required by Data Protection Laws, the Customer is responsible for ensuring that all necessary privacy notices are provided to Data Subjects, and unless another legal basis set forth in respective Data Protection Laws support the lawfulness of the Processing, that any necessary Data Subject consents to the Processing are obtained, and for ensuring that a record of such consents is maintained. Should such consent be revoked by a Data Subject, the Customer is responsible for communicating the fact of such revocation to HCLTech, and

HCLTech remains responsible for implementing Customer's instruction with respect to the Processing of that Personal Data.

### **3. Processing Terms**

- 3.1. The subject-matter, nature, and purpose of Processing to be undertaken by HCLTech and the type of Personal Data and categories of Data Subjects involved are specified in Schedule I (Details of Personal Data and Processing) to this DPA.
- 3.2. The Parties agree that Customer is the Controller of Personal Data and HCLTech is the Processor of such data.
- 3.3. The Parties agree that Customer is a Business and HCLTech is its Service Provider in relation to this DPA and Personal Data that is Processed in the course of HCLTech' provision of the Services set forth in the DPA.
- 3.4. Permitted Processing
  - a. HCLTech shall only Process Personal Data on behalf of HCLTech's Customer in accordance with this DPA including the agreed Contractual Terms, Data Protection Laws and any other approved written instructions that HCLTech may receive from the Customer.
  - b. If HCLTech cannot comply with such instructions, meet its legal obligations under Data Protection Laws and/or the terms of the DPA for whatever reason, it agrees to inform the Customer of its inability to comply, in which case the Customer is entitled to suspend the Processing.
  - c. HCLTech shall only disclose Personal Data to its employees on a need-to-know basis, for the performance of HCLTech's obligations under this DPA. Any such employees shall be bound by confidentiality obligations no less restrictive than those contained in this DPA and the Contractual Terms.
  - d. HCLTech may not disclose Personal Data to any other third party without the prior written consent of the Customer. Under no circumstances may HCLTech sell, share, rent or lease Personal Data to any third parties or otherwise Process the Customer's Personal Data for its own Purposes.
  - e. Processing by HCLTech shall only take place for the duration specified either in the Contractual Terms (s) between the Parties or Schedule I to this DPA, as applicable.
  - f. Customer shall ensure that Customer's Personal Data is accurate and up to date. Customer shall inform HCLTech without delay if the Customer becomes aware that the Customer's Personal Data that HCLTech is Processing is inaccurate or has become outdated.
  - g. Subject to applicable laws and regulations, HCLTech on receiving any lawful access request by way of order of a court or subpoena, or by a law enforcement agency, shall inform Customer of any such request when legally permissible.

- h. HCLTech understands the restrictions set forth in Section 1798.140(ag) of the CPRA and will comply with them.
- i. If Customer uses the Service to Process any categories of data not expressly covered by this DPA, Customer acts at its own risk.

#### 4. HCLTech as controller

Customer authorizes HCLTech and its Affiliates to store and use Customer's business contact information wherever it does business, in connection with Customer's use of HCLTech Programs and related services or Support, or in furtherance of HCLTech's business relationship with Customer. Any such personal data used by HCLTech as a controller will be processed under the terms of the HCLTech online privacy statement found here: <https://www.hcltech.com/privacy-statement>.

#### 5. Security of Processing

- a. HCLTech in accordance with the written instructions of the Customer 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 well as the risk of varying likelihood and severity for the rights and freedoms of natural persons(including protection against unauthorized or unlawful Processing and against accidental or unlawful destruction, loss or alteration or damage, unauthorized disclosure of, or access to, Personal Data), including those measures set forth in the Schedule A I, as may be amended from time to time.

#### 6. Engaging Sub-Processors

- a. The Customer agrees that HCLTech may use its Affiliates and other Sub-Processors, listed in Schedule I, to fulfil its contractual obligations under this DPA or to provide Services on its behalf, provided that HCLTech complies with the provisions of the Section 3 specified above. HCL remains responsible for its Sub-Processors' compliance with the obligations of this Agreement.
- b. The Customer gives a general consent for HCLTech to engage new or replace existing Sub-Processors provided that HCLTech gives prior notice of any new Sub-Processor appointments.
- c. The Customer is allowed to object for good cause within 15 days of the date by which the notification was sent to the Customer. If there is no written objection received within the 15 days period, the consent to the engagement of new Sub-Processor shall be deemed to have been given.
- d. If the Customer objects to the sub-processing and it is not possible for HCLTech to commission another Sub-Processor at short notice on reasonable terms, the HCLTech has the right to adjust the agreed fees/charges for the higher costs arising from the alternative sub-processing or to terminate whole or part of Contractual Terms.

- e. HCLTech shall 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 DPA.

## **7. Assistance to Customer**

- a. Upon the Customer's reasonable request, HCLTech shall assist Customer, at Customer's cost, in ensuring compliance with the obligations pursuant to Articles 32 to 36 of the GDPR taking into account the nature of the processing and the information available to HCLTech.
- b. HCLTech shall notify the Customer without undue delay if it or any of its Sub-Processors pursuant to this DPA receive a request from a Data Subject for which Customer is the Controller, under any Data Protection Law in respect to Customer's Personal Data Processed pursuant to this DPA. The Customer will be solely responsible for responding to any such Data Subject Requests or communications involving Customer's Personal Data.

## **8. Personal Data Breach Handling Requirements**

HCLTech shall notify the Customer without undue delay after it becomes aware of a Personal Data Breach impacting Customer's Personal Data. HCLTech shall provide timely information relating to the Personal Data Breach as it becomes known or reasonably requested by the Customer. At Customer's request, HCLTech will promptly provide reasonable assistance as necessary to enable Customer to notify relevant Personal Data Breach to competent authorities and/or affected Data Subjects, when applicable.

## **9. Deletion or return of Personal Data**

Upon the Customer's written request, or upon fulfilment of all purposes agreed in the context of the Services whereby no further Processing is required, HCLTech shall, at the discretion of the Customer, either delete, destroy or return all Personal Data to the Customer and destroy or return any existing copies unless HCLTech has an obligation to retain data as per the applicable laws and regulations.

HCLTech shall notify all third parties supporting its own Processing of the Personal Data of the termination of the fulfilment of all purposes agreed and shall ensure that all such third parties shall either destroy the Personal Data or return the Personal Data to the Customer, at the discretion of the Customer.

## **10. Audit rights**

Customer agrees that its right to audit HCLTech may be fulfilled by HCLTech responding to Customer's written request with reasonable information and independent attestations, reports or extracts solely related to the provision of Services under the relevant Contractual Terms and necessary to determine HCLTech compliance with this DPA. To the extent it is not possible to satisfy an audit obligation mandated by Data Protection Laws through such manner, the Customer, has the right to onsite audit. The Customer shall incur all audit related expenses (incl. HCLTech's expenses). The Customer shall provide at least thirty (30) days notification before conducting an audit unless such audit is required due to a Data Breach

involving HCLTech. HCLTech and Customer shall mutually agree upon the timing, scope, and duration of the audit before it commences. The scope of the audit must be defined in advance and limited to the systems and data dedicated to the HCLTech Services to Customer.

Customer may request a written audit information or audit HCLTech no more than once every 12 months. Customer's audits shall be subject to the terms of an applicable non-disclosure agreement and not prejudice other confidential information (including Personal Data and/or Content) of HCLTech, its Affiliates or its other customers. Any third-party auditors engaged by the Customer, should not be competitors to HCLTech.

## 11. Personal Data Transfers

11.1. Customer declares being fully aware and acknowledges that HCLTech operates as a global company with locations across the world. In order to provide Customer with the service level continuity targeted by Customer and to optimize both organization and management of the quality of its products and services, HCLTech reserves itself the right to have Personal Data processed by other HCLTech affiliates or by sub-processors listed Schedule A III and that may be located in a different region than where the original processing took place, which Customer accepts.

11.2. Data originating in the EEA or Switzerland: The parties agree that in the case of any authorized processing of Personal Data originating from the EEA or Switzerland being carried out in a country outside the EEA or Switzerland, either directly or via an onward transfer, where the EU Commission have reached an adequacy decision, this decision shall be used to safeguard the applicable Restricted Transfers, and where no EU Commission adequacy decision exists, the unedited 2021 EU SCCs, which shall be deemed executed upon execution of this DPA, shall apply as follows with respect of such processing:

- a In relation to Personal Data that HCLTech processes where Customer is the Controller, the EU SCCs shall apply as follows:
  - i. Module Two (Controller to Processor) will apply;
  - ii. in Clause 7, the optional docking clause will apply;
  - iii. in Clause 9, Option 2 will apply, and the time period for prior notice of Sub Processor changes shall be as set as thirty (30) days;
  - iv. in Clause 11, the optional language will not apply;
  - v. in Clause 17, Option 1 will apply, and where the law of the EU Member State in which the data exporter is established does not allow for third-party beneficiary rights, the EU SCCs will be governed by Irish Law;
  - vi. in Clause 18(b), disputes shall be resolved before the courts of Ireland;
  - vii. Annex I B of the EU SCCs shall be deemed complete with the information set out in Schedule A I
  - viii. Annex II of the EU SCCs shall be deemed completed with the information set out in Schedule A II; and
  - ix. Annex III of the EU SCCs shall be deemed completed with the information set out in Schedule A III

- b. In relation to Customer Personal Data that HCLTech processes where Customer's client is the Controller and Customer is the Processor; the EU SCCs shall apply as follows:
  - i. Module Three (Processor to Processor) will apply; 10
  - ii. in Clause 7, the optional docking clause will apply;
  - iii. in Clause 9, Option 2 will apply, and the time period for prior notice of Sub processor changes shall be as set as thirty (30) days;
  - iv. in Clause 11, the optional language will not apply;
  - v. in Clause 17, Option 1 will apply, and where the law of the EU Member State in which the data exporter is established does not allow for third-party beneficiary rights, the EU SCCs will be governed by Irish law;
  - vi. in Clause 18(b), disputes shall be resolved before the courts of Ireland;
  - vii. Annex I B of the EU SCCs shall be deemed complete with the information set out in Schedule A I
  - viii. Annex II of the EU SCCs shall be deemed completed with the information set out in Schedule A II; and
  - ix. Annex III of the EU SCCs shall be deemed completed with the information set out in Schedule A III
- 11.3. Personal Data originating in the UK: The parties agree that in the case of any authorized processing of Personal Data originating from the UK being carried out in a country outside the UK, either directly or via an onward transfer, parties hereby enter into the EU SCCs (as set out above), and these shall be read in accordance with, and deemed amended by, the provisions of "Part 2: Mandatory Clauses" of the UK International Data Transfer Addendum to the EU Commission Standard Contractual Clauses ("IDTA") (<https://ico.org.uk/media/fororganisations/documents/4019483/international-data-transfer-addendum.pdf>) as follows
  - a. Part 1: Tables shall be deemed complete with the information set out in Schedule A I and II;
  - b. In Table 4: Ending this Addendum when the Approved Addendum Changes" parties agree that either party may end the Addendum as set out in Section 12.6.
- 11.3.1. The Parties shall comply with the requirements of applicable Data Protection Law, including but not limited to the Personal Information Protection Law (PIPL) of China, the California Consumer Privacy Act (CCPA) including any amendments, and any other relevant data protection regulations, concerning restricted transfers of Personal Data. Each Party agrees to: a) Ensure that Personal Data transferred across borders is handled in compliance with applicable legal requirements, including obtaining necessary consents where required, b) Implement appropriate safeguards to protect Personal Data, such as SCCs, government-approved certifications, or other legally valid mechanisms. This obligation shall extend to all Personal Data shared or processed under this DPA and continue for the duration of the data processing activities.
- 11.3.2. To the extent that the Controller or the Processor are relying on a specific statutory mechanism to normalize Restricted Data Transfer that is subsequently modified, revoked, or held in a court

of competent jurisdiction to be invalid, the Controller and the Processor agree to cooperate in good faith to promptly terminate the transfer or to pursue a suitable alternate mechanism that can lawfully support the transfer.

## **12. General Terms**

### **12.1. Order of precedence**

- a. Subject to section 11.2.a., with regard to the subject matter of this DPA, in the event of inconsistencies between the provisions of this DPA 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 DPA, the provisions of this DPA shall prevail.

### **12.2. Changes in Data Protection Laws**

- a. HCLTech may by written notice to Customer propose any other variations to this DPA which HCLTech reasonably considers to be necessary to address requirements of any Data Protection Laws.
- b. HCLTech shall not require the consent or approval of the Customer to amend this DPA pursuant to this section 11 or otherwise.
- c. Should any provision of this DPA be invalid or unenforceable, then the remainder of this DPA 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.

### **12.3. Limitation of Liability**

- a. Parties agree that the maximum aggregate liability of HCL Tech and its affiliates to Data Controller and its affiliates for breaches of its obligations hereunder pertaining to personal data (including violation of data privacy laws) shall be limited and subject to the liability cap provided in the Contractual Terms. For clarity, nothing herein shall limit either party's liability to data subjects, to the extent such limitation is not allowed under applicable law.

### **12.4. Variation**

- a. Any amendment or variation to this DPA shall be in writing and signed by duly authorized representatives of each of the Parties.

**12.5. Commencement, duration, and survival**

- a. This DPA 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 DPA 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 Process Personal Data of the other Party.

**12.6. Termination of this DPA**

- a. Each Party may terminate this DPA immediately by giving the other Party written notice to that effect in the following circumstances:
  - i. the other Party has materially breached Data Protection Laws in connection with either this DPA 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 30 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 DPA.

**12.7. Effects of termination**

- a. Any provision of this DPA that expressly or by implication should come into or continue in force on or after termination of this DPA will remain in full force and effect.
- b. The termination of this DPA will be without prejudice to any other rights or remedies of any Party under this DPA 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.
- c. Upon termination of this DPA for any reason HCLTech shall immediately stop Processing the Personal Data and take action specified in the Section 8 above.

## Schedule A

### Details of Personal Data and Processing

#### I. DESCRIPTION OF TRANSFER/PROCESSING

##### Categories of Data Subjects whose Personal Data is transferred/Processed

Any data subject that is identified in the Contractual Terms

Fraud Risk Management (FRM) as a Service

Any data subject whose Personal Data is stored by the Customer on the business applications (including metadata), IT and network infrastructure including Call Detail Record Data and Subscribers Data .

Device Entitlement Gateway (DEG) as a Service

Any data subject whose Personal Data is stored by the Customer on the business applications (including metadata), IT and network infrastructure including Device Identification Data, Electronic Communications Metadata, Authentication Data.

##### Categories of Personal Data transferred/Processed

Any Personal Data categories that are identified in the Contractual Terms

Fraud Risk Management (FRM) as a Service

The type of personal data processed will depend on the data the Customer has stored on the HCLTech FRM platform and it includes the following personal data:

1. Call Detail Record Data (IMSI, MSISDN, Device ID, IMEI, EID, ICCID, etc.)
2. Subscribers Data (Customer's subscribers demographic and payment data such as: user's name, address, contact phone number/email, bank accounts/credit cards, etc.)

Device Entitlement Gateway (DEG) as a Service

The type of personal data processed will depend on the data the Customer has stored on the business applications (including metadata), IT and network infrastructure and it includes following personal data: • IMSI, MSISDN, Device ID (IMEI, EID, ICCID) • IP address, Cookie.

##### Nature and Purpose of the Processing/Transfer

As defined in Contractual Terms

Fraud Risk Management (FRM) as a Service

As part of services consisting of (i) making available HCLTech FRM platform, and (ii) providing software maintenance support and professional services, HCLTech may have access to Customer Personal Data stored in HCLTech FRM platform.

### Device Entitlement Gateway (DEG) as a Service

As part of providing software maintenance support and professional services, HCLTECH may have access to data stored in the HCLTECH DEG Platform (including metadata). This data may include Customer Personal Data

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

HCLTech shall process Customer Personal Data for the duration of the applicable Contractual Terms.

### Fraud Risk Management (FRM) as a Service

All the personal data will be stored on the FRM platform for max 12 months.

### Device Entitlement Gateway (DEG) as a Service

All the personal data will be stored on the DEG platform for max 6 months.

## II. TECHNICAL AND ORGANISATIONAL MEASURES INCLUDING TECHNICAL AND ORGANISATIONAL MEASURES TO ENSURE THE SECURITY OF THE DATA

### Identity and Access Control

HCLTech as an organization shall ensure:

- A documented access control policy is in place and is reviewed at least annually.
- User roles with their entitlements and access rights are defined and documented.
- Access to IT (Information Technology) infrastructure components are granted based on least privilege principle and are managed through robust identity management tools such as enterprise Active Directory solution or similar.
- Individual's access to systems, network resources and other IT resources is formally approved and controlled through unique User IDs and individual passwords.
- Policy and associated system configurations make certain that:
  - Users are required to change their password upon initial sign-on
  - Passwords meet the requirement set by the policy based on industry standard, including but not limited to length, expiry, complexity, password history, failed attempts, account lockout duration, password age, and change on first logon etc.
  - Generic and shared IDs are not used unless a formal justification is in place and is approved by senior management along with a mechanism to track the usage of such IDs and ensure it is possible to trace the actions performed using those IDs to the individual.

- Secure mechanisms are used to deliver user passwords
- Validate user identities before initiating password resets
- Privileged access to resources is restricted to defined user roles and access to such roles are approved by authorized personnel or resource owners.
- Privilege user accounts are managed by PAM and configured to use multifactor authentication.
- Periodic access reviews are carried out and any identified exceptions are addressed promptly, the periodic access reviews must be documented and logged. Privileges that are no longer required are revoked immediately.
- Systems that do not support active directory authentication or are required to be built standalone are configured to enforce strong authentication which is no less than the configuration defined in central password and access control policies.
- Standard processes for user onboarding and deboarding are in place including keeping records of relevant approvals.
- Reconciliation of all user IDs (Including but not limited to, domain, applications, network devices, IT systems, middleware, databases etc.) is performed quarterly or as per industry standard and corrective actions to mitigate any identified exceptions are taken promptly.
- All systems, applications, network devices and IT infrastructure components are configured to use secure log-on procedures via approved identity and access management mechanism.
- Access to critical IT infrastructure, systems, network devices and applications such as remote access and access to critical servers, network devices etc. is protected using multifactor authentication mechanism.
- Solutions to prevent unauthorized changes to critical system files are implemented.
- Use of administrative credentials is restricted to limited circumstances such as troubleshooting purposes and users perform their day-to-day operations with least privileged credentials.
- Segregation of duties is maintained while creating/amending user IDs and assigning privileges.
- Vendor-supplied default credentials are changed before systems, applications, network devices or other IT infrastructure devices are put in production.
- All non-console administrative access is encrypted using industry approved encryption algorithms and unsecure protocols such as telnet/ftp are prohibited for non-console administrative access.
- Third party vendor access to network and systems is strictly controlled and should be based on need to know and based on a formal approval process.
- Systems and applications are configured for idle session time out to prevent unauthorized access.

## Asset Management

Asset labelling, information classification policy and supporting procedures/guidelines are maintained. All assets are labelled as per labeling instructions and information is classified and protected as per the classification levels.

- Asset inventories are maintained, capturing all required details such as asset owner details, contact information, location etc.
- Asset management procedures and configuration controls to manage the availability of critical assets and the configurations of critical network and information systems are established and maintained
- Records of Information Technology assets (Hardware, OS, applications & database etc.) are maintained and reviewed periodically to keep the list accurate and up to date.
- Policies and procedures for controlling mobile devices used to store, transmit or process business information are in place. Ensure adequate protection is in place before granting mobile devices access to business information and resources.
- Acceptable usage policy and asset management guidelines for handling assets are maintained and communicated to all applicable employees and contractors.
- Processes are in place to validate and ensure allocated assets to an employee/contractor are returned without undue delay to the corresponding asset management team upon termination/separation of employment, contract, or agreement.
- Use of removable mass storage devices is prohibited by default and any exceptions are recorded and formally approved with proper business justification.
- Documented procedures are in place for safeguarding information assets, identification of assets due for disposal and for secure disposal of such assets.
- Use of unlicensed/ unapproved software is prohibited and processes are in place to identify any violations and take necessary actions to address such violations.

## IT Operations

HCLTech as an organization shall ensure:

- Procedures for the operation of critical networks and information systems by personnel which include but is not limited to the following are established and maintained:
  - Formal approval to access the IT assets/technology.
  - Robust authentication mechanism for use of all technologies such as VPN, Windows logon etc.
  - Review of privilege entitlements
  - Network locations are identified for critical technologies based on business continuity requirements
  - Processes to ensure only company approved software are used
  - Data retention requirements are identified, documented, and complied with
  - Standard operating procedures (SOP's) and configuration standards are defined for all systems, applications, tools, and technologies.

Change management processes are established to ensure changes to IT systems, applications, databases, and network components etc. are logged, reviewed, tested, and formally approved by authorized personnel before changes are implemented. The change management plan includes the rollback of changes if the proposed changes have a negative impact. Records of all changes are maintained, and File Integrity monitoring checks are in place for systems and network components handling sensitive and confidential information. and Processes are in place to monitor the available capacity of systems and applications to identify resource requirements for the IT environment.

Backup policy and supporting procedures are clearly documented. Data backups are taken periodically using a secure and reliable mechanism. Backup restoration processes are documented, and restoration of data is tested at defined frequency and corresponding evidence is maintained. A copy of critical data backup files is kept in secure offsite location(s). Backup policy and supporting procedures are clearly documented. Data backups are taken periodically using a secure and reliable mechanism. Backup restoration processes are documented, and restoration of data is tested at defined frequency and corresponding evidence is maintained. A copy of critical data backup files is kept in secure offsite location(s). information in backup media or storage appliance is encrypted using strong encryption algorithm.

- Logs for failed backups (if any) are monitored by backup admin and corresponding corrective action is performed and documented.
- Hardening baselines for all its IT infrastructure components are defined and documented. The Operating Systems, databases, applications, and network devices etc. are configured as per respective hardening baselines before introducing them to the production environment.
- Systems and network components are configured to use authorized Network Time Protocol (NTP) source for time synchronization.
- Processes are in place for proactive and preventive maintenance of all critical systems, applications, network devices and end user machines at regular interval.
- Firewall and router rule set reviews are conducted on a quarterly basis or as per industry standard and any unnecessary or unauthorized rule sets are removed immediately.
- Controls are in place to maintain the integrity of information and software.
- Controls are in place for redundancy in IT Infrastructure such as redundancy of LAN, WAN, servers, workstation, and IT Infrastructure etc. to ensure continuity of operations.
- Controls to facilitate secure internet browsing for end users e.g., through web proxy, web content filter etc., are in place.

## Human Resource Security

HCLTech as an organization shall ensure:

- Policy and procedures for background checks are established and maintained.
- Appropriate background checks are performed on personnel (employees, contractors, and third-party users) before they are onboarded and to the extent legally permitted for their duties and responsibilities.
- A program for training and awareness is implemented to make sure all personnel have sufficient and up-to-date information security knowledge.
- HCLTech employees undergo information security and data privacy training and assessment at the time of joining and at least annually thereafter.
- Training and awareness program is reviewed and updated periodically, taking into account changes in business requirements, legislation, and based on past incidents.
- An appropriate process for managing changes in personnel or changes in their roles and responsibilities and to educate new personnel on the policies and procedures is in place.

- Following changes in personnel, access rights, badges, equipment, et cetera are revoked if no longer necessary or permitted.
- A disciplinary process for employees who violate security policies is established and maintained either standalone or as part of a broader process that covers security breaches caused due to violations by personnel.
- Personnel are held accountable for violating security policies, for example via employment contracts, third party contracts, etc.

## Information Security & Governance

HCLTech as an organization shall ensure:

- HCLTech has an established security standard framework for information and cyber security governance which covers the following components:
  - Information and Cyber Security policies and procedures which are reviewed (at least annually), approved and communicated
  - An information security strategy
  - Governance and risk management processes which address information and cyber security risks
  - Legal and regulatory requirements regarding Information and Cyber Security
- Appropriate roles and responsibilities for Information and Cyber Security are defined and implemented.
- A Chief Information Security Officer (or equivalent) is appointed who holds a senior position within the organization and has responsibility for the enterprises' information security program.
- A committee or equivalent body (e.g., information security steering committee) is established which coordinates information security activities across the organization and is chaired by a suitably senior member of staff and meets on a regular basis.
  - Information security objectives and associated activities to ensure commitment towards Information security management systems (ISMS) are identified and documented and an Information security management system is established which is aligned to meet the information security objectives of the organization. Processes and/or tools are in place to identify events that cause interruptions to organizations key business purpose. Critical systems are protected against Denial of Service (DoS) and Distributed Denial of Service (DDoS) attacks. A formal risk management framework approved by Sr. Management is in place for: Identifying both internal and external threats Sensitivity of information / data in scope Assessing potential business impacts
  - Assessing Threats, vulnerabilities, and corresponding risks
- All risks and threats identified as part of the risk assessment are prioritized and addressed to mitigate the risks in a timely manner.
- Notify appropriate leadership immediately if unable to remediate or reduce any material risk that could have an impact on data processing activities

## **Network Security**

HCLTech as an organization shall ensure:

- The HCLTech network is designed using “defense in depth” principles to ensure information and cyber security breaches are minimized by ensuring appropriate controls such as network segmentations are in place.
- External connections to the network are routed through a firewall, verified, and approved prior to the connections being established.
- Design and implementation of the network is reviewed at least annually.
- All wireless access to the network is subject to authentication, authorization, segmentation, and encryption protocols. Mechanisms are in place to detect and respond to presence of rogue wireless access points/unauthorized connection to wireless network.
- Communications between network devices and workstations used for management of such devices are secure.
- Non-console administrator access is over an industry approved encrypted channel.
- Strong architectural design with effective identity management and operating system configuration are used.
- Services, applications, and ports that are not in use are disabled.
- Appropriate measures are in place for intrusion detection and/or prevention for critical network segments.
- Guest accounts are disabled or removed, and all default and vendor supplied passwords are changed before network devices are commissioned in the production environment.
- Network is configured to meet all applicable legal and regulatory requirements
- Implement controls to prevent/minimize unauthorized individuals from gaining access to the Vendor Network.
- Any remote access to vendor and client network must be approved and must be over an encrypted Virtual Private Network (VPN) connection configured with Multifactor authentication.

## **Cryptography**

HCLTech as an organization shall ensure:

- Policy and supporting procedures for cryptographic controls required to comply with all applicable legal, regulatory, and business requirements are established.
- Use of only secure and industry approved encryption algorithms and key strengths which ensure adequate protection of data is permitted.
- Passwords are always encrypted when stored and during transit.
- Key Management procedures for secure key generation, ownership, distribution, archival, storage, and revocation to protect keys throughout the life cycle are established and maintained.

Cryptographic solutions based on industry best practices to enable secure encryption and in line with applicable laws and regulations are implemented to make sure confidential information is protected and access to sensitive data is restricted e.g., encryption of data during transit and while at rest.

**Data Security**

HCLTech as an organization shall ensure:

- Systems, applications, and networks components that process, store, and transmit HCLTech or HCLTech Customer's data are protected against data leakage using a combination of tools such as centrally administered data leakage prevention tool, log and file integrity monitoring and auditing tool etc. to prevent unauthorized disclosure of confidential Information. Data leakage prevention events are reviewed by the central Security Operations Centre (SOC) team and tracked to closure as per defined policies and processes.
- Full disk encryption is configured for workstations. Documented data classification policy is in place and data is classified based on its criticality and sensitivity using the data classification solution. Central data restriction controls for sharing outside HCLTech are applied basis data criticality.

**Information Communication**

HCLTech as an organization shall ensure:

- Controls e.g., Web Content filtering software are in place to prevent access to websites hosting malicious content. Security controls are in place to prevent misuse of email system and ensure all email communications are over an encrypted channel. Anti-phishing and Anti-Spam filters along with other configurations such as Spoof protection etc. to prevent email bound threats are enabled on the email gateway.
- Access to all systems and applications is over an authenticated and secure channel, and client server communication of applications and web portals is over an encrypted channel.

**Software Development**

HCLTech as an organization shall ensure:

- Systems and applications are developed as per HCLTech's Secure Software Development guidelines. Software code is protected from unauthorized modification and is securely stored and subject to Quality Assurance and peer reviews.
- Applications are thoroughly tested for security and functionality related issues before deploying them in the production environment.
- Production and non-production environments are segregated appropriately.
- Business critical live data is masked and sanitized before being used for testing. Any exception, approval from data owners.
- Segregation of duties between production and non-production developments is maintained.

**Application security**

HCLTech as an organization shall ensure:

- Application security assessments are performed for all newly developed applications and any existing applications that are going through a significant change to identify any known security vulnerabilities.
- All security vulnerabilities as per severity are actioned upon prior to deployment of application in the production environment.
- Strong authentication mechanisms are used, and periodic access rights reviews for application users are being performed as per role granted to application users.
- Application developers are trained in secure coding techniques and such training/awareness is conducted periodically.
- Secure code review processes are in place to identify and correct any code that may lead to security vulnerability.

**Patch Management**

HCLTech as an organization shall ensure:

- Security patches are applied to systems, Networks, applications, and databases etc. are applied regularly in accordance to the patch management policy. Patches are obtained from respective OEMs directly for proprietary systems.
- Patches are reviewed for applicability and tested before deployment of the patches to production systems and are controlled by change management process.
- Appropriate mitigations are in place, where applicable, if a system cannot be patched. For other cases, risk assessment is done, recorded and accepted by management as per Risk Acceptance process.

**Malware Protection**

HCLTech as an organization shall ensure:

- HCLTech has deployed endpoint protection (malware and advanced malware protection) solutions on endpoints for protection.
- Regular updates against Malwares on regular basis are pushed to ensure systems are protected against latest threats.
- Malware protection software is configured to run scheduled and on demand scans and to isolate/delete any malicious files or software.
- Prohibit ability for end users to disable endpoint protection software.

### Vulnerability Management

HCLTech as an organization shall ensure:

- Established policies, processes, and procedures for vulnerability and penetration testing are in place.
- Internal and external vulnerability scans and penetration testing are conducted on HCLTech assets regularly as per defined vulnerability management policy.
- Reported vulnerabilities are remediated withing defined SLA as per vulnerability severity.
- Any non-remediated vulnerability is recorded and tracked till closure.
- HCLTech has subscribed to leading industry threat intel services for Zero day vulnerability alerts. Such vulnerabilities are remediated immediately as per the defined Zero Day vulnerability management process.

### Logging and monitoring

HCLTech as an organization shall ensure:

- There is an established and consistent audit and log management process in place.
- Critical systems including applications are set to log key events (including those of privileged access and user activity) and retain such for a minimum period of 1 year or as per applicable regulatory requirements.
  - Logs as per the Log management policy are enabled and monitored.
- Audit logs are collected and correlated from multiple sources and stored securely and are tamper-proof to enable the reconstruction of such events.
- Incident alert thresholds are configured to determine the impact of any events and ensure such events are responded to in a timely manner as per the criticality of the alarm.

### Incident management

HCLTech as an organization shall ensure:

- Documented incident management policy and associated procedures are in place for management of security incidents.
- Responsibilities and practices for ensuring a quick, effective, and structured response to information security and privacy incidents are defined and established.
- Employees and contractors are educated in what qualifies as a security incident and where and how to report any such potential or confirmed security incidents.
- HCLTech has SIEM solution for detection correlation of security logs and 24X7 SOC service to monitor security events and create incidents as per defined process.
- Employees responsible for analyzing and responding to incidents are qualified in the subject matter and are periodically trained on how to effectively respond to incidents.
- Repository of all reported incidents is maintained along with the actions taken to mitigate the impact of the incident and lessons learnt.

### Compliance

HCLTech as an organization shall ensure:

- Processes are in place to identify, record, and track all applicable legal, regulatory, and contractual requirements for the organization.
- Periodic assessments are performed to validate compliance with legal, regulatory, and contractual obligations. Records are maintained for such assessments and identified gaps are mitigated without undue delay. 24
- Policies, procedures, and guidelines are reviewed at least annually and updated as per the legal, regulatory, and contractual requirements.
- Key Performance Indicators for critical functions such as IT, Information Security and Data Privacy etc. are defined, formally documented, periodically assessed, and reported to Senior management.

### **Physical and Environmental Security**

HCLTech as an organization shall ensure:

- Policy and associated procedures for physical security measures and environmental controls based on industry standard implementation of physical and environmental controls are implemented.
- All critical facilities and locations which house the important IT systems, applications, and personnel (e.g., data centers, operational facilities) are physically protected against accidents, attacks, and unauthorized access etc.
- Security controls such as electronic access controls, identity verification, security guards, visitor management and 24x7 CCTV monitoring etc. are in place to protect the buildings against unauthorized access.
- CCTV recordings are retained for a minimum of 30 days or as per applicable legal and regulatory requirements.
- Access to facilities is restricted and only granted for specific and authorized purposes and is subject to regular reviews.
- All visitors are escorted while inside the premises and the entry and exit times are logged and monitored. Visitors are issued Visitor IDs which are required to always be worn while inside the premise. ID/Access cards or keys issued to visitors should be collected at the time of their departure from the premises.
- All critical facilities and locations are physically protected against loss of power to prevent any interruption in service. Critical facilities are protected by uninterruptible power supply (UPS) or generators to support operation in case of a prolonged power loss. Periodic maintenance of all critical equipment like Generators/UPS/smoke detectors/fire extinguishers/fire suppression systems, access control systems is performed, and records of such maintenance are maintained. All critical facilities and IT system locations are housed in secure buildings that have been built using fire-proof materials and are equipped with fire alarms, smoke detectors, temperature sensors, flood detection sensors, fire extinguisher systems etc. to protect against fire, the weather, flooding, and other natural hazards. Mechanisms for secure disposal of data in hard and soft copy format are defined and implemented. Cross cut shredders are used for disposing off paper documents, and use (where appropriate) methodologies such as sanitization, Degaussing and physical destruction for shredding of electronic media. A clear desk policy is in place to ensure secure disposal of Post It notes, keeping written notes in a safe place, and ensuring that any removable media is not left lying around. Effectiveness of physical and environmental controls are evaluated at least annually.

Privacy and Data Protection In the capacity of a controller while processing employee's data and/or while processing client's data as a part of a business engagement in the capacity of a processor, HCLTech shall ensure:

- Compliance with all applicable data protection laws.
- An established privacy management framework is in place which covers the following components:
  - Privacy policies, statements, notices, and procedures which are reviewed (at least annually), approved and communicated
  - Privacy Governance and risk management processes which address personal data risks
  - Legal and regulatory requirements regarding data privacy
- Up-to-date records of processing activities for all personal data processing activities performed on HCLTech's business engagements are maintained.
- Appropriate roles and responsibilities for Data Privacy are defined and implemented.
- A Data Privacy Officer (or equivalent) is appointed who holds a senior position within the organization and has responsibility for Data Privacy Program.
- A committee or equivalent body which coordinates Data Privacy Compliance activity across the organization is in place and is chaired by a senior member of staff and meets on a regular basis.
- A dedicated Data Privacy function with suitable and defined roles and responsibilities is in place.
- In particular implement administrative, physical and technical safeguards to protect HCLTech's or its customer's information that are as per industry accepted practices (such as ISO/IEC 27001:2013 – Information Security Management Systems – Requirements and ISO-IEC 27002:2013 – Code of Practice for International Security Management, The Control Objectives for Information and related Technology (COBIT) standards [or] other applicable industry standards for information security), and ensure that all such safeguards, including the manner in which the information is collected, accessed, used, stored processed, disposed of and disclosed, comply with applicable data protection and privacy laws.
- If the processing involves sensitive 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 or any other data types considered sensitive personal data with regards to applicable data protection law, HCLTech shall apply specific restrictions and additional safeguards to protect sensitive personal data e.g., by implementing encryption, pseudonymization techniques etc.
- Access to personal data and associated application and systems is restricted to authorized individuals on a need to know and least privilege basis. The access rights of employees supporting the processing activities are promptly removed upon termination of their employment or their separation from HCLTech engagement or when their roles have changed. In addition, periodic access rights reviews are performed to identify and correct unnecessary permissions timely to prevent misuse.
- All persons authorized to process the Personal Data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality in relation to such Personal Data.
- HCLTech shall ensure that it informs the data subjects of the purposes for collecting and/or processing personal data. HCLTech will only process personal data using an appropriate lawful basis.

- HCLTech shall ensure that the lawful basis along with the purpose of collecting data is communicated to the individual at the time of collecting personal data through a Privacy Notice that is drafted in clear and easy to understand language.
- HCLTech shall ensure that the personal data is only stored/possessed for only as long as it is necessary for the purpose for which the data was originally processed/collected unless retention of the data is necessitated by any contractual, business or regulatory requirement. HCLTech shall ensure to have a policy that sets retention periods wherever possible to comply with contractual, business and regulatory requirements. 26
- HCLTech shall have a documented DSAR handling guidelines/procedure document that outlines the process for responding to Data Subject rights' requests under the applicable Data Protection laws.
- When acting as a Data Controller, HCLTech must respond to the Data subject request without undue delay. The request must be fulfilled within the applicable timeframe (as per the relevant data protection law) post HCLTech receiving a validated request. This timeframe can be extended only where the request is particularly complex or consists of a large dataset as per the applicable law.
- When acting as a Data processor, HCLTech must inform the client/customer as soon as a request is received unless HCLTech has agreed to action such request as per the client contract.
- HCLTech shall define and document processes of handling privacy incidents and security breaches concerning personal data possessed at HCLTech, and as a part of it:
  1. Have a documented response plan, including but not limited to record, handle, assess, notify and manage personal data breaches
  2. Develop procedures to classify severity of a breach and responsibilities of each stakeholder involved in the handling and response of incidents/breaches.

### **Contracting Measures**

HCLTech shall ensure:

- It appoints a processor under a binding written contract which states that the processor:
  - 1) Shall only process personal data in accordance with the controller's written instructions
  - 2) Must ensure the security of the personal data.
- HCLTech should ensure that vendor due diligence is performed before onboarding the third-party vendor and periodic assessments are carried out post onboarding the vendor
- HCLTech should ensure that there are relevant privacy clauses agreed in the contract with the vendor which covers the Vendor Security and Privacy Requirements/TOMs agreed with the vendor
- HCLTech shall ensure as a processor that contractual agreements are executed for all clients/customers and HCLTech processes personal data only as per client's written instructions or as agreed in the contract

### **Cloud Security Measures**

- HCLTech ensures that HCLTech's cloud environment and SaaS applications are subject to appropriate controls equivalent to the latest version of the Cloud Security Alliance, Cloud Controls Matrix (CCM) or ISO27017.

- Security measures are implemented across all aspects of the services, such that it safeguards confidentiality, availability, and integrity by minimizing opportunities of unauthorized individuals (e.g., other cloud customers) from gaining access to HCLTech information and the services utilized by HCLTech.

### **Business Continuity Management**

HCLTech as an organization shall ensure:

- A formal Business Continuity Management (BCM) Policy, plan and associated procedures capturing business continuity objectives are established, reviewed, and approved at least annually.
- A BCM testing framework is developed and implemented to validate effectiveness of the business continuity strategies implemented.
- A formal BCM training and awareness program is implemented.
- Business Impact analysis (BIA) & Risk assessments (RA) are performed at least annually or following a significant change.
- A crisis management plan (including pandemic preparedness) is established to ensure appropriate responses to emergency situations by enabling the protection of employees, visitors, the environment, assets, and business operations.

Testing of the effectiveness of Business Continuity Management System is performed on an annual basis and records of such testing are maintained.

### **III. LIST OF SUB-PROCESSORS**

The Customer has authorised the use of the following Sub-Processors:

1. HCLTech Limited 806 Siddharth, 96 Nehru Place, New Delhi-110019 India
2. Amazon Web Services, Inc. (AWS) Cloud hosting, United States