Annexure: India DPDP Act Supplemental Privacy Provisions

Purpose and Scope

This India DPDP Annexure ("Annexure") supplements the Data Processing and Vendor Security Agreement ("DPVSA") and the Technical and Organizational Measures ("TOMs") for Vendor Security Requirements, as executed between HCLTech and the Vendor.

This Annexure sets out additional obligations specific to the Digital Personal Data Protection Act, 2023, and the Digital Personal Data Protection Rules, 2025 (collectively, "DPDP Act"), applicable to the processing of digital personal data of Data Principals located in India or where the processing is in connection with HCLTech' s India operations.

In the event of any conflict between this Annexure and the DPVSA, the provision that affords greater protection to the Data Principal shall prevail.

Definitions

Unless otherwise defined herein, capitalized terms shall have the meaning ascribed to them in the DPVSA. The following terms are specific to this Annexure and are defined under the DPDP Act:

Consent Manager: A person registered with the Data Protection Board of India who acts as a single point of contact to enable Data Principals to give, manage, review, and withdraw consent (Section 2(g), DPDP Act).

Data Fiduciary: Any person who, alone or in conjunction with other persons, determines the purpose and means of processing personal data (Section 2(i), DPDP Act).

Data Principal: The individual to whom the personal data relates; where such individual is a child, the parent or lawful guardian; and where such individual is a person with disability, the lawful guardian (Section 2(j), DPDP Act).

Data Processor: Any person who processes personal data on behalf of a Data Fiduciary (Section 2(k), DPDP Act).

Data Protection Board of India ("DPBI"): The Board established under Section 18 of the DPDP Act for adjudication of non-compliance.

Digital Personal Data: Means Personal Data in Digital form.

Personal Data: Means any data about an individual who is identifiable by or in relation to such data.

Personal Data Breach: Means any unauthorized processing of personal data or accidental disclosure, acquisition, sharing, use, alteration, destruction or loss of access to personal data, that compromises the confidentiality, integrity or availability of personal data.

Significant Data Fiduciary ("SDF"): A Data Fiduciary or class of Data Fiduciaries notified by the Central Government based on prescribed criteria (Section 10, DPDP Act).

Sub-Processor: Any third party engaged by the Data Processor to carry out processing activities on behalf of the Data Fiduciary.

Roles and Responsibilities

For the purposes of this Annexure:

I. Where HCLTech determines the purpose and means of processing, HCLTech shall be the Data Fiduciary, and the Vendor shall act as a Data Processor.
II. Where HCLTech acts as a Data Processor on behalf of its customers, the Vendor shall act as a sub-processor and shall comply with all obligations applicable to a Data Processor under the DPDP Act and services agreement with HCLTech.
III. Where the Vendor independently determines the purpose and means of processing personal data of Data Principals, the Vendor shall be deemed a Data Fiduciary in its own right and shall independently comply with all obligations under the DPDP Act.

Vendor Obligations

When processing Personal Data for the purposes of this Contract, Vendor shall, including, without limitation:

i. Comply with the Data Processing and Vendor Security Agreement ("DPVSA"), the Technical and Organizational Measures ("TOMs") for Vendor Security Requirements, and the obligations set out in DPDP Annexure. Where the Vendor processes Personal Data on behalf of HCLTech, it acknowledges its role as a Data Processor under the DPDP Act and agrees to implement and maintain the obligations, controls, and requirements set out in the DPDP Annexure and applicable DPDP Rules as a material and non-waivable contractual obligation.
ii. Process Personal Data solely on documented instructions of HCLTech. Any secondary processing, including analytics, profiling, testing, benchmarking, training of artificial intelligence or machine-learning models, or product/service improvement, is strictly prohibited unless expressly authorized in writing by HCLTech.
iii. Apply reasonable and appropriate security safeguards as required under Section 8 of the DPDP Act and Rule 6 of the DPDP Rules, such as securing of Personal Data through encryption, obfuscation, masking or the use of virtual tokens mapped to that personal data.

iv. Implement privacy by design and privacy by default principles in all systems, applications, and processes used for processing Personal Data under this Annexure."

v. Maintain centralized, tamper-evident system logs capturing all access to and processing of Personal Data, retained for not less than twelve (12) months. Such logs shall be made available to HCLTech upon request for audit, investigation, or regulatory purposes.

vi. Provide all necessary cooperation, documentation, and technical details required by HCLTech to conduct data protection impact assessments (DPIAs), risk assessments, or similar evaluations as required under applicable law.

vii. Notify HCLTech without undue delay of any suspected or confirmed Personal Data Breach affecting HCLTech data via an email to Infosecincidents@hcltech.com and the Vendor's primary HCLTech contact, followed up by a detailed incident report with remediation plan within twenty-four (24) hours; enabling HCLTech to meet its own statutory notification obligations under the DPDP Act.

viii. Ensure full transparency of processing activities and shall, upon request, provide detailed information regarding data flows, processing logic, storage locations, and involved systems.

ix. Not engage any sub-processor without HCLTech' s prior written consent and ninety (90) days' advance notice.

x. Shall ensure that each approved Sub-Processor is bound by contractual obligations no less protective than those set out in this Annexure and, where engaged for customer-specific services, complies with all applicable terms, conditions, and obligations committed by HCLTech to its customers, including compliance with the DPDP Act. The Vendor remains fully liable for acts and omissions of its Sub-Processors and shall ensure Sub-Processors notify the Vendor of any Personal Data Breach without undue delay.

xi. Not attempt to re-identify anonymized or pseudonymized Personal Data and shall implement safeguards to prevent such re-identification.

xii. Implement appropriate technical and organizational measures to enable HCLTech to fulfil Data Principal rights under Sections 11–12 of the DPDP Act, including the rights to: (a) access a summary of personal data and processing activities; (b) correction and erasure of inaccurate or misleading data, completion of the incomplete Personal Data; and updating Personal Data; (c) nomination of another individual to exercise rights in the event of death or incapacity; and (d) grievance redressal. The Vendor shall respond to any Data Principal request communicated by HCLTech within seven (7) calendar days or such shorter period as may be prescribed under the DPDP Act and shall not independently respond without HCLTech' s written authorization.

xiii. Not transfer personal data of India-located Data Principals outside India except to countries or territories permitted by the Central Government under Section 16(1) of the DPDP Act and with HCLTech' s prior written authorization. Transfers to restricted or blacklisted territories are prohibited. Where transfers are permitted, the Vendor shall ensure the receiving entity

provides data protection no lower than that under the DPDP Act and shall execute such additional contractual safeguards as HCLTech may require.

xiv. Maintain comprehensive records of all processing activities in a structured and auditable format (categories of data and Data Principals, purposes, cross-border transfer details, retention periods, security measures etc.) and make such records available to HCLTech upon request.

xv. The Vendor shall fully cooperate with HCLTech in responding to any inquiry, investigation, or order from the DPBI relating to processing activities carried out on behalf of HCLTech and shall promptly notify HCLTech of any direct communication from the DPBI. The Vendor shall not engage directly with the DPBI except where required by applicable law, and in such cases shall provide prior notice to HCLTech unless legally prohibited. ,

xvi. Not process personal data of a child (under 18 years) in relation to services provided to HCLTech, without verifiable consent of the parent or lawful guardian and ensure processing does not cause harm to the child. The Vendor shall not undertake tracking, behavioural monitoring, or targeted advertising directed at children, nor process children's data in a manner likely to cause detrimental effect on their well-being. The same protections apply to persons with disabilities who have a lawful guardian. The Vendor shall avail any Central Government exemptions (e.g., age-gating) only upon written confirmation from HCLTech.

xvii. Where HCLTech appoints a Consent Manager in relation to processing activities performed by the Vendor, the Vendor shall cooperate with the Consent Manager, provide necessary information, and, where technically feasible, integrate its systems to support consent record management. The Vendor shall also promptly notify the Consent Manager of any changes to the purpose, scope, or method of processing.

xviii. Securely delete or anonymize all Personal Data (including all copies, backups, and derived data) in accordance with the DPDP Act, promptly upon the earliest of: completion of the specified purpose, withdrawal of consent, termination of the Contract, or written instruction from HCLTech, unless retention is required under applicable law. The Vendor shall, upon request, provide written certification of such deletion, maintain auditable deletion records, ensure equivalent obligations are imposed on all Sub-Processors, and make such records available to HCLTech or the DPBI upon request.

xix. Shall continuously monitor and update its technical and organizational measures to ensure ongoing compliance with applicable data protection laws, including any amendments to the DPDP Act or related rules.

xx. Indemnify and hold harmless HCLTech, its affiliates, officers, and employees from all losses, damages, claims, penalties, fines (including DPBI penalties under Section 33 of the DPDP Act, which may extend up to ₹250 Crore per instance), costs, and expenses arising from: (a) any breach of this Annexure by the Vendor or its sub-processors; (b) non-compliance with the DPDP Act attributable to the Vendor; or (c) personal data breaches

caused by failure to implement reasonable security safeguards. These indemnification obligations survive termination or expiry of this Annexure and the DPVSA.

xxi. HCLTech reserves the right to audit the Vendor and its Sub-Processor's compliance with this Annexure through on-site inspections, document reviews, and third-party audits, consistent with the DPVSA and TOMs. The Vendor shall provide all information and access necessary to demonstrate DPDP Act compliance and shall promptly remediate any non-compliance within agreed timelines.

Governing Law

This Annexure is governed by the laws of India, including the DPDP Act and all rules, regulations, notifications, and circulars issued thereunder. HCLTech reserves the right to amend this Annexure to reflect changes in the DPDP Act or DPBI guidance upon written notice to the Vendor. This Annexure shall be co-terminus with the DPVSA and the underlying Contractual Terms.