Terms & Conditions for Outsourcing Vendors of HDB Financial Services Limited

1. INDEPENDENT SERVICE PROVIDER - PRINCIPAL TO PRINCIPAL

This Agreement is being entered on a principal-to-principal basis and does not create and shall not be deemed to create any employer-employee or a principal-agent relationship between HDBFS and Service Provider and / or its Staff. Service Provider and/or its Staff shall not be entitled to, by act, word, deed or otherwise make any statement on behalf of HDBFS or in any manner bind HDBFS or hold out or represent that Service Provider is representing or acting as an agent of HDBFS.

The Service Provider shall provide the said services hereunder as an independent service provider and nothing contained herein shall be deemed to create any association, partnership, joint venture or relationship of principal and agent or master and servant, or employer and employee between HDBFS and Service Provider and/or the personnel assigned provided/deployed by the Firm or provide either party with the right, power or authority, whether express or implied to create any such duty or obligation on behalf of any of them. Service Provider acknowledges that its rendering of the said services is solely within its control subject to the terms and conditions agreed upon and agrees not to hold itself out to be an employee of HDBFS or any subsidiary or affiliate thereof.

The Service Provider's personnel, employees, agents, etc., have no authority / right to bind HDBFS in any manner. It is also clarified that the personnel employed by Service Provider will be governed by the terms of Service Provider's employment and Service Provider alone shall be responsible and liable in the event of any adverse claims of whatsoever nature made on HDBFS by Service Provider's personnel, employees or agents. This Agreement will bind the successors and permitted assigns of Service Provider and shall inure for the benefit of HDBFS's successors and assigns.

The Service Provider further undertakes to indemnify and hold HDBFS free and harmless from any loss, claim, damage, costs or expenses, including reasonable attorney's fees, to which HDBFS may be subjected, by virtue of any finding related to an employer / employee relationship between the Service Provider and HDBFS in any proceedings initiated by the Service Provider and / or the personnel assigned / provided/ deployed by the Service Provider for rendering of the said services.

2. ACCOUNTABILITY FOR FRAUD AND MALPRACTICE

The Service Provider shall exercise due diligence, care, and integrity in the performance of its obligations under this Agreement.

In the event that any fraud, financial loss, or reputational damage to HDBFS is caused due to wilful negligence, malpractice, or misconduct on the part of the Service Provider, the Service Provider shall be held accountable and liable for all resulting consequences.

The Service Provider agrees to indemnify and hold harmless HBDFS from and against any claims, losses, damages, penalties, or liabilities arising directly or indirectly from such fraudulent or negligent acts of Service Provider.

HDBFS reserves the right to immediately terminate this Agreement with Service Provider without prejudice to any other legal remedies available if the Service Provider is found to be involved in fraudulent or unethical practices.

The Service Provider shall cooperate fully in any investigation undertaken by HDBFS or regulatory authorities in relation to fraudulent activities or misconduct.

This clause shall survive the termination or expiration of this Agreement.

3. CALL RECORDING

Subject to its applicability, the following clause shall apply to Service Providers engaging in Collection Services. All calls made by the Service Provider or its staff / agent / employee / personnel / representatives to the customer (through authorized telecommunication lines) shall be recorded. Such recording will be provided to HDBFS, as and when demanded by HDBFS, for internal check and audit purposes. Further, the Service Provider and its staff / agent / employee / personnel / representatives undertake and agree to follow all the SOPs / Code of Conduct / Policies of HDBFS.

4. CONSIDERATION/REMUNERATION

In consideration of the Service Provider rendering the Services to HDBFS, HDBFS shall pay to Service Provider charges based on applicable scope of services and the Consideration as mentioned in the said Agreement.

HDBFS shall be entitled to set off against / deduct / recover from the aforesaid charges and any other sums payable by HDBFS to the Service Provider at any time in respect of any amount due or claimed to be due to HDBFS or any statutory or regulatory bodies by the Service Provider. The amount, if any net of such set off / deduction / recovery will be paid by HDBFS to the Service Provider.

It is hereby clarified that HDBFS's only obligation is to pay the aforesaid charges to the Service Provider's duly authorized agents, employees, Representatives (all such authorized agents, employees, Representatives of the Service Provider are hereinafter collectively referred as **"Company Staff"**).

Any payment of the charges made to and received by such Authorized agent or the Company Staff shall be considered as a full discharge of HDBFS's obligations for payment of charges hereunder.

The Service Provider shall raise invoice within 15 days of providing the service with required details. HDBFS, on verification will clear the bill and payment will be made within statutory timelines post receipt of complete invoice.

The Service Provider shall submit the Goods and Service Tax (GST) registration number with HDBFS. However, if Service Provider fails to submit the same with HDBFS then HDBFS shall be liable to deduct the GST from bill payment and shall make the balance payment to the Service Provider.

The Service Provider also agrees if HDBFS is not able to claim input credit under Goods and Service Tax due to negligence / mistake / error of Service Provider then HDBFS shall deduct such amount from the future bill payments of the Service Provider and Service Provider shall not dispute the same.

5. ISOLATED / IDENTIFIABLE INFORMATION

The Service provider hereby agrees to ensure that it is able to isolate and clearly identify HDBFS's customer information, documents (in hard copies or soft files), computerized data / information, records and assets to protect the confidentiality of the information.

The Service Provider shall ensure that the data received from HDBFS and the reports or files to be sent to HDBFS shall be maintained during the term of this Agreement.

6. CONFIDENTIALITY

The Service Provider recognises, accepts and agrees that all tangible and intangible information obtained/received/gained/developed or disclosed to or accessed (whether intentionally or inadvertently) by the Service Provider and/or to the Service Provider's Staff (Service Provider shall mean to include its officials, directors, employees, workmen / workers, consultants, retainers, advisors, campaign personnel), including all details, documents, Data, passwords of any nature, business of the HDBFS, Customer information, transaction records, whether proprietary or non-proprietary, financials and/ or operational information, Data, know-how, structure and documentation, Intellectual Property Rights and/or software rights, interest and knowledge, information described as proprietary or designated as confidential information, information disclosed to the Service Provider by any third party which information the Service Provider is obligated (whether by any relevant law or otherwise) to treat as confidential information, and the HDBFS's practices and trade secrets and such other information that the HDBFS may consider confidential, including any information in relation to or of the HDBFS's affiliate, Customers or any third party (all of which are hereinafter collectively referred to as **"Confidential Information")** that the Service Provider and the Service Provider's Staff may be privy to shall be treated as absolutely confidential.

The Service Provider irrevocably agrees, undertakes and ensures that:

(a) The HDBFS does not grant or extend to the Service Provider any right or license of any kind whatsoever which the HDBFS may now have or may hereby obtain with respect to the Confidential Information. In addition to and notwithstanding any other right or obligation arising under this Agreement, the Service Provider shall (and shall ensure that the Service Provider's Staff shall) take all appropriate technical and organisational security measures to ensure that Confidential Information is/are protected against loss, destruction and damage, and against unauthorized or accidental access, processing, erasure, transfer, use, modification, disclosure or other misuse, and that only personnel authorised by the HDBFS have access to Confidential Information.

(b) The Service Provider shall in respect of the Confidential Information:

(i) comply with any request made or direction given by the HDBFS, including in connection with the requirements of any Data Protection Laws;

(ii) not do or permit anything to be done which might jeopardise or contravene the terms of any registration, notification or authorisation under any Data Protection Laws or policies of the HDBFS;

(iii) not access, use, store (beyond the period specified by the HDBFS hereunder) or process any Confidential Information (including any Personal Data) unless it is acting on the express instructions of the HDBFS and only for the purposes of fulfilling its obligations under this Agreement and to comply with instructions the HDBFS from time to time in connection with use of such Confidential Information, and such Data shall be treated as Confidential Information of the HDBFS for the purpose of this Agreement;

(iv) not transfer Confidential Information which has been obtained by or made available to the Service Provider within one country outside that country, or allow persons outside that country to have access to it, without the prior written approval of the HDBFS;

(v) take all reasonable steps to ensure the reliability of the personnel who will have access to any Confidential Information, limit access to those personnel who have a need to know the Confidential Information and ensure that any employee of the HDBFS (or of any of the Service Provider's Staff) requiring access to any Confidential Information gives a written undertaking not to access, use, disclose or retain Confidential Information except in performing their duties of employment and is informed that failure to comply with this undertaking may be a criminal offence and may also lead the Service Provider to take disciplinary action against the Service Provider's Staff; and the Service Provider shall be responsible for any breach of confidentiality contemplated herein by any of its representatives / employees;

(vi) consider all suggestions by the HDBFS to ensure that the level of protection provided for Data is in accordance with this Agreement and to make the changes suggested (at the Service Provider's cost) unless the Service Provider can prove to the HDBFS's reasonable satisfaction that they are not necessary or desirable to ensure ongoing compliance with this Clause;

(vii) take all necessary steps and precautions to protect the Confidential Information against any unauthorized use and / or disclosure in violation of this Agreement and notify the HDBFS in writing immediately upon becoming aware of the occurrence of any unauthorized release/ access/ use/ disclosure of the Confidential Information or any breach of the terms of this Agreement;

(viii) to ensure that each of such Service Provider's Staff to whom the Confidential Information is disclosed, observes strictly the restrictions as to use and disclosure contained herein;

(ix) implement appropriate administrative, technical and physical safeguards to protect the security, confidentiality and integrity of the Confidential Information and such safeguards to be designed to ensure the security and confidentiality of the Confidential Information so as to protect the Confidential Information against any anticipated threats or hazards to the security or integrity of the Confidential Information;

(x) not disclose any Confidential Information of the HDBFS, including information of any business of the HDBFS, internal rates of return etc. to any Customers or to any third party; and

(xi) adopt, maintain, monitor and enforce appropriate security policies as well as Data protection and safeguarding arrangements for the lawful protection of Confidential Information including the Personal Data, sensitive Data etc provided by the HDBFS.

Where applicable, the Service Provider shall be responsible for developing, hosting, managing and maintaining the entire technology platform including the requisite equipment/ software/ infrastructural facilities to provide the Services to the HDBFS in accordance with the terms hereof. In relation thereto, the Service provider shall ensure that the equipment/ software/ infrastructural facilities required by the Service Provider for providing the services, is properly maintained, serviced and operated at all times, including without limitation, identification and rectification of problems/ break-downs and replacement of faulty equipment;

The Service Provider agrees that it will not disclose, transfer, use, lecture upon or publish any of the HDBFS's Confidential Information, including the existence or the terms and conditions of this Agreement, except if such disclosure, use or publication is required in connection with its work on a "need to know" basis or is strictly required by law and only upon obtaining prior permission from the HDBFS or unless the HDBFS expressly authorizes such disclosure, in writing. The Service Provider's obligation to maintain the confidentiality, privacy and security of the Confidential Information remains even after its contract with the HDBFS ends and continues for so long as such Confidential Information remains a secret. The Service Provider recognizes that all information created / accessed / processed by it, shall remain the sole property of the HDBFS and shall be returned to the HDBFS on the expiry of this Agreement.

(a) the Confidential Information will not be used or permitted to be used by the Service Provider or the Service Provider's Staff in any manner even after the expiry / termination of this Agreement.

(b) The Service Provider shall segregate and keep separately all information, documents, properties, assets, monies and records pertaining to the Services, the HDBFS, any of its affiliates and Customers of the HDBFS as also hold the same in trust for the HDBFS and its affiliates and Customers of the HDBFS.

(c) The Service Provider agrees that the HDBFS will suffer irreparable harm if the Service Provider fails to comply with its obligations set forth herein or if the Service Provider breaches any of the terms and conditions set forth herein and the Service Provider shall be completely and solely responsible for any act / deed done to the contrary to the above terms and shall fully indemnify and keep indemnified the HDBFS for any loss / damage that may be caused to or suffered by the HDBFS arising out of or in connection with any wrongful disclosure or misuse of Confidential Information as a result of a breach of this Clause.

The Service Provider acknowledges that any unauthorized access, destruction, alteration, addition or impediment to access or use of that Confidential Information when in transit or stored in any computer, or the publication or communication of any part or document by a person which has come to his knowledge or into his possession or custody by virtue of the performance of this Agreement (other than to a person to whom the Service Provider is authorised to publish or disclose the fact or document) may be a criminal offence. In the event of a breach or threatened breach by the Service Provider of the aforesaid Clause, without prejudice to any other rights or remedies available to the HDBFS hereunder or under Applicable Law, the HDBFS shall be entitled to injunctive relief in addition to monetary damages to restrain the Service Provider from any such breach, threatened or actual.

If the Service Provider is directed by a court or by any governmental or regulatory authority to disclose information or documents relating to the HDBFS including Confidential Information, it shall notify the HDBFS in writing (prior to making any disclosure pursuant to such direction/order/notice), along with a copy of such direction/ order /notice, in sufficient detail immediately upon receipt of such direction/ order / notice in order to permit the HDBFS to make an application for an appropriate protective order and provide such information / documents as may be advised by the HDBFS in writing and keep the HDBFS apprised of any developments in this regard, from time to time.

The Service Provider shall ensure that the HDBFS has a period of at least 3 (three) days to move the appropriate court in appeal to obtain a stay order, if the HDBFS so desires, against any orders of the court / governmental or regulatory authority as mentioned in the foregoing Clause.

Where the introduction, imposition or variation of any law, order or regulation or official directive or any change in the interpretation or application thereof by any competent authority makes it apparent to either party that it is unlawful or impractical without breaching such law, order or regulation or official directive for the party to give effect to its obligations under this Agreement then notwithstanding anything herein to the contrary, the parties concerned at the written request of either of them, shall immediately consult with each other in a spirit of mutual understanding and co-operation to agree on any revision of the terms and conditions of this Agreement reasonably required in view of such circumstances.

The Service Provider agrees to be vigilant and to report all occurrences of breach, violations of security, Data privacy, any Data Compromise Event and any security event that creates a reasonable suspicion of unauthorized access to confidential information or an environment, misappropriation or alteration of any confidential information, or theft, loss of or damage to information assets containing

Confidential Information, immediately to the HDBFS's Information Security Group at informationsecurity@hdbfs.com

The Service Provider further confirms and agrees that it shall

a) comply with the provisions of Applicable Laws in relation to the transactions contemplated under this Agreement including all rules, regulations, guidelines, directions, circulars and notifications of the RBI, labour laws, applicable anti-bribery laws, Information Technology Act, 2000 and the applicable rules thereunder including without limitation the Information Technology (Reasonable security practices and procedures and sensitive Personal Data or information) Rules, 2011, the RBI Guidelines on Managing Risks and Code of Conduct in Outsourcing of Financial Services by HDBFSs (DBOD.NO.BP.40/21.04.158/2006-07 dated November 3, 2006), National Do Not Call Registry, directions/regulations issued by the Telecom Regulatory Authority of India (TRAI) from time to time, and HDBFS's Code of Conduct (including fair practice code) other codes of conduct prescribed by the HDBFS, any law or authority or association, guidelines issued by RBI / other regulators / association, all applicable laws, extant policies and guidelines specified by the HDBFS or any authorities, from time to time as also their own code for collection of dues and shall provide all information and records of the transactions to the HDBFS as and when required by the HDBFS. The Service Provider shall not resort to invasion of privacy, viz. persistently bothering the Customers of the HDBFS at odd hours, violation of "do not call" code, etc.; and

b) promptly disclose any and all breaches in the information security and/ or Data privacy practices, control processes and checks, including but not limited to incidents which, directly or indirectly, have or would have affected the safety and security of the Confidential Information, any equipment downtime or failure, suspicious behaviour incidents or unusual cyber-security incidents (whether they were successful or were attempts which did not fructify), bribery incidents, fraud incidents, suspicious transactions including fraudulent / suspicious currency transactions immediately upon occurrence to the Information Security Group of the HDBFS on informationsecurity@hdbfs.com and also suggest, undertake and assist the HDBFS in implementing remedial/ corrective steps/ suitable servicing of equipment for mitigation of any damage. Notwithstanding the generality of hereunder, the Service Provider shall be liable for all damages arising out of such incidents, breach of security, control processes, checks and other security lapses.

The Service Provider agrees that the HDBFS shall be entitled to notify RBI or any other authority of the details of the Services and/or default in performance of the Services by the Service Provider (including details of any breach of security and leakage of any Confidential Information) and/or that it has entered into material outsourcing or is planning to vary any such outsourcing arrangements.

The Service Provider, providing/performing services on HDBFS's onsite and / or offsite location, hereby confirms that it has read and understood the "Acceptable Usage Policy" as annexed to the Agreement thereto and as the same may be amended by the HDBFS from time to time, and hereby agrees to protect the system and comply with the said policy.

Unless otherwise instructed by the HDBFS in the manner set out in Clause below, the Service Provider shall maintain all Confidential Information, including without limitation, books of accounts, accounting records, documents, information, audit trails, logs for administrative activities in relation to the Services, records relating to the Service Provider's Staff and the records required to be maintained under this Agreement and ensure that the reports to be sent to the HDBFS as also the entire Data management system contents of the Service Provider to the extent they pertain to the HDBFS and the Services provided by the Service Provider to the HDBFS are saved, preserved and maintained as per the directions of the HDBFS and in accordance with Applicable Laws. Notwithstanding the generality of the aforesaid.

The HDBFS may, at any time, whether during the term of this Agreement or thereafter, require the Service Provider to either return or destroy the Confidential Information in the manner set out hereinafter:

a) In case of return of physical Confidential Information, the Service Provider shall return the Confidential Information to the HDBFS within a period of 2 (Two) Business Days from the date of request made by the HDBFS.

b) In case of destruction/ deletion of Confidential Information, the same shall be accomplished by the Service Provider within a period of 5 (Five) Business Days from the date of request made by the HDBFS by destroying or deleting all Confidential Information in its possession by 'purging' or by way of 'physical destruction' in the form of shredding or incineration of all documents and other material in its possession, custody or control in respect of physical documents and irretrievably delete the same if stored on virtual, electronic or magnetic media. For electronic media, Data frequently remains on media after erasure. With respect to such residue Data, additional disposal techniques should be undertaken by the Service Provider, like physical destruction, overwriting Data, degaussing etc., to ensure that the Data contained therein cannot be re-created, accessed or read after the deletion/ disposal.

Pursuant to such return/ destruction/ deletion/ purging of Confidential Information by the Service Provider, the Service Provider shall provide a written declaration to the HDBFS, certifying that all such Confidential Information, documents, material, instructions, manuals, guidelines or other writings (including any copies thereof) and any other property belonging to the HDBFS provided in relation to the provision of the Services or otherwise, that may be in the possession of the Service Provider or any of the Service Provider's Staff, agents or officers, has been returned or destroyed, in the manner specified above, to the HDBFS within 7 (Seven) Business Days from when they were instructed to do so by the HDBFS.

The Confidential Information being shared by the HDBFS (being a listed company) with the Service Provider may be unpublished price sensitive information ("UPSI") relating to HDBFS, and the Service Provider is hereby put to notice to maintain utmost confidentiality of the UPSI in accordance with the SEBI (Prohibition of Insider Trading) Regulations (the "Regulations") as amended from time to time. Further, as per the Regulations, the Service Provider is under obligation not to share this UPSI with any person within its organization, except when warranted for a legitimate purpose and on 'need to know basis'. In case of

any such sharing, the Service Provider is required to obtain details of the person with whom UPSI is shared along with his PAN and date of such sharing. Till such time the relevant UPSI is not disclosed by the HDBFS, in the public domain, there shall be prohibition from trading by the concerned persons including the Service Provider and all concerned persons, in the securities of the HDBFS in accordance with the Regulations and HDBFS's code framed thereunder. Any non-compliance with the above requirements will be viewed very strictly by the HDBFS and may invite action under the Regulations, including reporting to SEBI.
The provisions of this Clause shall survive the expiry or termination and expiry of the tenure this Agreement.

7. DATA SECURITY

The Service Provider shall (and shall ensure that all the Service Provider's Staff) be required to maintain and adhere to such administrative, technical and physical safeguards, and such processes, procedures and checks, to secure the Data which is received from the HDBFS, in any manner whatsoever, in relation to the Services as may be stipulated under Applicable Law and/or industry standards or regulations issued by any governmental authority, which safeguards must be at least equal to or better than (a) the safeguards it currently has in place to protect its own Data; and (b) generally accepted security standards in the financial service industry.

The administrative, technical and physical safeguards, processes, procedures and checks as provided for in this Clause will be designed to:

a. protect the security and confidentiality of the Data in the Service Provider's possession;

b. ensure protection against Data leaks, any anticipated threats or hazards to the security and confidentiality of the Data;

c. protect against unauthorised access to or use or publication or disclosure of the Data or associated records; and

d. ensure the proper and secure disposal of such Data.

Without limiting the generality of the foregoing, the Service Provider shall ensure that all Data, whether in transit, hosted, stored, or held by the Service Provider in the products or in the platform operated by the Service Provider, or on any device owned or in the custody of the Service Provider, including the Service Provider's Staff, or held or retained by the Service Provider (including by any of the Service Provider's Staff), shall be encrypted by 128-bit or higher encryption, at all times until such Data is held by it/ them, pursuant to its/ their obligations under this Agreement.

The Service Provider shall not (and the Service Provider shall ensure that the Service Provider's Staff does not) transmit or disseminate any unencrypted Data over the internet or a wireless network, and not store or retain any Data on any mobile computing device or removable media including inter alia a laptop, desktop computer, USB drive, smart phone, cell phone, backup media or any portable Data device, unless required for the performance of services under this Agreement and pursuant to obtaining necessary permits from the HDBFS's relevant official and then only if the concerned mobile computing device or the removable is protected by 128-bit or higher encryption software approved by the HDBFS. Further, the Service Provider shall ensure that the

Service Provider's Staff shall not connect their personal computers, personal digital assistants, laptops, smart phones, workstations or any such device to the HDBFS's network.

The Service Provider shall undergo periodical cyber assurance activities, including but not limited to vulnerability assessment, integrity assurance, source code review and penetration testing, and also carry out such activities as and when required by the HDBFS, at the cost of the Service Provider. The Service Provider shall provide all periodical reports of such activities to the HDBFS (or as and when requested by the HDBFS).

The Service Provider shall not store and/ or transfer Data which is in the possession of the Service Provider, outside India, or allow persons outside India to have access to the Data, unless required for the provision of the Services and a written permission for the same is obtained from the HDBFS and subject to compliance with Applicable Law. The Service Provider shall, at all times, in providing the Services in terms hereof including, without limitation, when receiving, processing or storing any data, ensure compliance with the provisions of Applicable Law.

The Service Provider shall ensure that the networks used by the Service Provider to access Confidential Information must have security controls that can detect attacks by making use of firewalls, Intrusion Detection/Prevention Systems (IDS/IPS) and other network infrastructure (e.g., routers, load balancers). The Service Provider shall also ensure that their networks have continuous monitoring and all network security related activities (including any Data Compromise Events, security events, errors, or breach) should be recorded and logged.

The Service Provider using business centers to provide the Services shall be responsible for and shall ensure the security and subsequent removal and deletion of any information stored onto such business center's systems, using methods as provided for, in this Agreement.

The Service Provider shall ensure that any deletion/ destruction of electronic or physical Data (or any defective electronic device containing such Data) shall be in the form as prescribed in this Clause of this Agreement.

In environments shared by the Service Provider and the HDBFS, the Service Provider shall ensure the segregation (using physical segregation of network infrastructure or VLAN subnets) of their network, systems and storage to prevent any Data from any unauthorized access of Data.

The Service Provider shall not use the HDBFS's environments or networks for development or testing of any system other than the HDBFS's systems and only for the purposes as prescribed in this Agreement.

Without limiting the generality of the foregoing, the Service Provider shall initiate all measures which a prudent organisation, in a similar situation, would take to secure and defend its systems that contain the Data against "hackers" and others who may seek, without authorisation, to modify, infect or access its

systems or the Data. The Service Provider will periodically test its systems for potential areas where security could be breached.

The Service Provider covenants that it shall take appropriate technical and organisational measures against (a) any unauthorised or unlawful processing or alteration of the Data in the systems of the Service Provider, (b) any resultant loss or destruction of, or damage to, the Data due to unauthorised processing or alterations, and (c) unauthorised or accidental access, processing, erasure, transfer, use, modification, or other misuse of the Data and shall ensure that only authorised personnel bound by adequate confidentiality obligations shall have access to the Data and strictly on a 'need to know' basis.

The Service Provider shall (and shall ensure that its employees, agents and sub-contractors shall) in respect of the Data:

a. comply with any reasonable request made or direction given by any authorised personnel of the HDBFS in connection with the requirements of any Data Protection Laws;

b. not do or permit anything to be done which might jeopardise or contravene the terms of any registration, notification or authorisation under any Data Protection Laws;

c. use the Data or access/ permit the access to the networks or environment of the HDBFS only for the purposes of fulfilling its obligations under this Agreement and to comply with the instructions given by the HDBFS from time to time in connection with use of such Data, and not retain the Data for any longer than is necessary for these purposes;

d. consider and comply with all suggestions by the HDBFS to ensure that the level of protection provided for the Data is in accordance with this Agreement;

e. take all reasonable steps to ensure the reliability of the personnel which will have access to the Data and ensure that the personnel of the Service Provider who access the Data give a written undertaking not to access, use, disclose or retain the Data except in performing their duties of employment and is informed that failure to comply with this undertaking may be a criminal offence and may also lead the HDBFS and/or the Service Provider to take disciplinary action against the employee.

The Service Provider shall ensure that the Data is maintained in such a way that it is protected and is not mixed or mingled with any other Data including any Data of its other customers or clients.

The Service Provider further confirms and agrees that it shall at all times during the subsistence of this Agreement (and any provision hereunder):

a. comply inter alia with the provisions of the Information Technology Act, 2000 and the applicable rules thereunder including without limitation the Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules, 2011;

b. implement secure mail and messaging systems, that include measures inter alia to prevent email spoofing, identical mail domains, protection of attachments, malicious links;

c. comply with all notifications, guidelines, circulars, issued by the RBI as may be required under the Applicable Law;

d. monitor the security practices, control processes and checks in respect of any Data and other confidential information received by the Service Provider, on a regular basis.

The Service Provider shall ensure complete and fool proof security of all Data and shall be responsible and liable therefor at all times, including when:

a. the Data is stored whether permanently or temporarily on the systems of the Service Provider or any of its agents, sub-contractors or representatives;

b. the Data is being transferred to and from the systems of the Service Provider.

During the subsistence or execution of the aforementioned events, the Service Provider shall be solely liable for:

(a) any breach of security, to either the HDBFS or its network resources, including, but not limited to, any unauthorized access to Data, servers, or accounts, circumventing user authentication on any device, sniffing network traffic;

(b) occurrence of a disruption of service to either the HDBFS or other network resources, including, but not limited to, occurrence of events such as ICMP floods, packet spoofing, denial of service, heap or buffer overflows, forged routing information for malicious purposes;

(c) introduction or spread of honeypots, honeynets, or similar technology on the HDBFS's network or the network of the Service Provider which is utilized for dealing with the HDBFS's Data;

(d) Infringement or attempt towards an infringement of any intellectual property of a person or entity, including, but not limited to, illegally downloading, duplicating or transmitting copyrighted pictures, music, video, and software;

(e) exporting or importing software, technical information, encryption software, or technology in violation of international or regional export control laws;

(f) introduction or spread of malicious code, including, but not limited to, viruses, worms, trojan horses, e-mail bombs, spyware, adware, and key loggers; and/ or

(g) compromise, theft, modification and/or corruption of the Data, improper access to, damage to, or loss or theft of any information asset, physical asset made available by the HDBFS to the Service Provider and/or any computer or other media or network on which Confidential Information is accessed or stored;

(Collectively referred to as the **"Data Compromise Events"**), irrespective of whether the Data Compromise Events were the direct or indirect result of any act or omission of the Service Provider.

8. SECURITY AND CONTROL PROCESSES

The Service provider hereby agrees to have sufficient security practices, control process and checks in respect of the job/work/ activity outsourced by HDBFS executed / handled at its premises or in HDBFS's premises on a regular basis.

The Service Provider shall monitor on regular basis and disclose any breaches in the security practices/ processes and controls to HDBFS.

HDBFS has the right to immediately notify the regulators in the event of any breach of security and leakage of confidential customer information / data / records / originating from the Service Provider or the Company Staff / agents / associates of the Service provider.

In these eventualities, HDBFS is liable to its customers for any damages and the Service Provider agrees to indemnify HDBFS for such losses / damages.

9. RIGHT OF HDBFS AND REGULATOR FOR INSPECTION AND AUDIT

The Parties hereby agree and acknowledge that at all points in time during the Term and for a period of ten [10] years from the date of execution of this Agreement and thereafter, the HDBFS as well as RBI shall be entitled to either by itself, or through its internal or external auditors or any external specialists appointed by it in this behalf, to audit, review, monitor and assess the use of any software, data, documentation, records (including copies of any other audit carried out or review reports and findings made with regard to the subject matter of this Agreement), information, books, transactions, security practices, control processes and other necessary information in the nature of operations, financial and business records which the HDBFS or HDBFS' authorised auditors in their absolute discretion deem to be relevant to the ability of Service Provider to fulfil its obligations under this Agreement and compliance by the Service Provider with the terms and conditions of this Agreement including but not limited to the right to conduct audit of any entity/company or sub-contractor utilized by the Service Provider to provide services to HDBFS under this Agreement. The Service Provider forthwith upon being thus required shall permit taking copies of any records, documents, books or other writings of Service Provider by the HDBFS or HDBFS' authorised auditors. Without prejudice to the generality of the foregoing, the HDBFS or HDBFS' authorised auditors shall also have the right to audit, review, monitor and access all details in relation to the Services offered by the Service Provider under this Agreement.

Without prejudice to the right of the HDBFS to require audit as provided for in Clause above, the Service Provider shall regularly provide updates to HDBFS with respect to the Service under this Agreement and shall meet with the officials

designated by the HDBFS to discuss and review the performance of Service Provider at such intervals as may be agreed between the Parties.

The Service Provider shall preserve and maintain all documentation, data and records in relation to the Services as contemplated under this Agreement at all times and shall ensure that the same are in accordance with good industry practices and applicable laws. The Service Provider shall also retain requisite audit trails and logs in relation to the Services and shall make the same accessible to the HDBFS on request.

The Service Provider shall co-operate in good faith with the HDBFS and its employees, personnel and other staff members and with the HDBFS' authorised auditors to correct any practice which is found to be deficient during any audit or monitoring and assessment process. Additionally, the Service Provider shall make available a qualified professional for responding to queries that may arise in the course of such monitoring or assessment process on mutually agreed terms.

Notwithstanding anything to the contrary contained herein, it is hereby agreed between the Parties that any government authority which is entitled to regulate and supervise the activities of the HDBFS, including the Reserve Bank of India and / or any persons authorised by such government authority shall be entitled to require the Service Provider to furnish and submit such data, documentation and records, and / or inspect / cause an inspection to be made of the Service Provider and its operations or books and accounts by one or more of its officers or employees or other persons, or enter upon the premises of the Service Provider and access, inspect, examine, audit and call for all documents, records or transactions and other necessary information given to, stored or processed by the Service Provider (including information maintained in paper and / or electronic formats) in the nature of operations and business records and which the government authority may, in its sole and absolute discretion, deem to be relevant to the provision of the Service and the other terms and conditions, as set forth in the Agreement, with or without provision of prior notice, as the government authority may deem fit and necessary.

In the event that any data, information, documentation or records, which are required by the HDBFS, by the HDBFS' authorised auditors and / or by any such government authority is stored or maintained at any location other than the premises of Service Provider (whether in India or abroad), the Service Provider shall ensure that the HDBFS, the HDBFS' authorised auditors and / or the concerned government authority, as the case may be, has access to such data, information or records to the same extent as if such data, information and records were maintained by Service Provider at its own premises.

The Service Provider shall provide the HDBFS with assistance necessary to meet the HDBFS' statutory, regulatory and system audit requirements and provide access to all information necessary for such audits.
The HDBFS has the right to access, at the HDBFS' discretion, HDBFS' authorised auditor's statement with regard to the audit of the Service Provider for payments made under this Agreement.

10. MONITORING AND ASSESSMENT

The Service Provider shall and undertakes to provide regular updates at such intervals as may be specified by HDBFS with respect to the Services provide in terms of this Agreement.

The Service Provider hereby agrees to ensure that a high standard of care in performing the services in terms of this Agreement and HDBFS has the right to intervene with appropriate measures to meet legal and regulatory obligations.

11. FINANCIAL / OPERATIONAL REVIEW

The Service Provider agrees to provide on annual basis all the required information pertaining to its financial and operational condition to enable HDBFS to assess and analyse the ability of the Service Provider to continue to meet its obligations under this Agreement. The assessment of HDBFS in this regard will be final and binding of the Service Provider.

12. INTELLECTIAL PROPERTY RIGHTS

As a part of this Agreement, HDBFS as well as the Service Provider shall respect each other's intellectual property rights including without limitation, patent, copyright, trade / service mark(s), trade names (s) and logos (hereinafter referred to as **"the intellectual Property Rights**").

The Service Provider agrees not to use or cause to be used the Intellectual Property Rights of HDBFS in any communication to a third party without explicit written permission from HDBFS.

The Service Provider agrees that all the work produced by the Service Provider in terms of the provisions of this Agreement shall be the sole and exclusive property of HDBFS.

In the event of the Service Provider being entitled to be the first owner of any such rights under any law, the Service Provider hereby assigns to HDBFS all copyrights or other intellectual property rights in such an event.

Nothing contained herein shall at any time during the continuation of this Agreement or after the expiry or earlier determination thereof give or be deemed to give or confer upon the Service Provider any right, title or interest or claim is or to be said trademark, copyright, and logos etc. belonging to the HDBFS and shall continue to vest solely and absolutely in favour of HDBFS. The Service Provider further agrees that the name, trademark and or logo of HDBFS shall not be used by the Service Provider or Company Staff, in any sales or marketing publication or advertisement or in any other manner whatsoever without prior written consent of HDBFS in writing.

This clause shall survive the expiry or termination of the Agreement.

13. TAXES

The Service Provider shall be solely liable for the payment of all taxes, duties, fines and penalties by whatever name called as may become due and payable any law, rules or regulations as applicable from time to time in relation to the services hereby agreed to the rendered by the Service Provider

HDBFS shall be entitled to deduct tax at source on payments made to the Service Provider in accordance with the applicable provisions of law. The Service Provider shall be responsible to report any non-receipt of certificate of taxes deducted at source within ninety (90) days of deduction of such taxes at source by HDBFS.

The Service Provider shall extend all the required co-operation in the defense of any claims by any authorities against HDBFS with respect to any taxes and /or duties and payable by, or under the authority of the service provider.

This Para shall be survive the expiry and termination of this Agreement.

14. INSURANCE

The Service Provider shall maintain at its sole expense, throughout the tenure of this Agreement and the extensions thereto, sufficient insurance coverage in respect of all possible threats / losses that may result from the obligations under this Agreement.

It is expressly clarified that the Service Provider shall be solely liable for maintaining sufficient Insurance coverage as mentioned in this clause and HDBFS shall in no circumstances be responsible liable for any risks that may arise due to any failure to comply with clause above.

15. COMPUTERS / SYSTEMS USE

If the rendering of the services requires HDBFS to provide to the Service Provider any documents, HDBFS many provide to the Service Provider the requisite documents, forms, papers, cards and other material to enable the Service Provider to provide the Services.

The Service Provider shall arrange to make the data entry as per the specifications that may be given by HDBFS from time to time. The Service shall provide/furnish to HDBFS the necessary / relevant data and management information reports as may be required by HDBFS time to time.

HDBFS may, as its sole discretion, decide to facilitate connectivity between its computer systems with that of the Service Provider to facilitate transfer of data in electronic form for further processing at both ends.

It is expressly clarified that HDBFS shall not be liable for any loss, damage or hardship caused to the Service Provider due to non -availability of the connectivity between its computer systems and HDBFS's computers for any reasons whatsoever.

16. ASSIGNMENT AND SUB-CONTRACTING

The Service Provider shall perform its obligations under this Agreement and shall not assign, transfer or sub-contract any of its rights and / or obligations under this Agreement except with the prior written permission of HDBFS. However, HDBFS shall be entitled to assign/transfer its rights and benefits under this Agreement to any person.

If such assignment is as a result of operation of any laws, then HDBFS shall have the option on such assignment to forthwith terminate this Agreement and the Service Provider shall be liable to compromise HDBFS for damages suffered by HDBFS for what would otherwise have been the remainder of the agreed tenure of this Agreement.

The Service Provider hereby agrees to obtain prior approval of HDBFS for using sub-contractors for all or part of the work /job / activity outsourced. The Service Provider shall not source or engage services from any sub-contractor blacklisted by HDBFS and shall be fully responsible for the acts and deeds of all his sub-contractors.

The Service Provider shall be fully responsible and liable for the performance and risk management practices of its sub-contractors and third parties engaged in the provision of Services. The Service Provider shall exercise due diligence in selecting, engaging, and managing sub-contractors and third parties to ensure their ability to meet the obligations and standards set out in this Agreement and shall ensure that its sub-contractors and third parties comply with all laws, regulations, industry standards, contractual requirements under this Agreement, and HDBFS' policies, as are required to be adhered to by the Service Provider pursuant to this Agreement.

17. BUSINESS CONTINUITY PLAN

Service Provider hereby confirms that it has developed & established a robust framework or documenting, maintaining & testing Business Continuity & recovery procedures and the same is test periodically and agrees to test the business continuity and recovery plan jointly with HDBFS.

This clause shall survive the expiry or termination of Agreement.

18. ACCESS TO BOOKS, RECORDS & INFORMATION

The Service Provider hereby agrees to provide access to all its books, records and information relevant to the job / work / activity outsourced/entrusted by HDBFS, to it.

19. ACCESS TO REGULATORY AUTHORITIES / EXTERNAL AGENCIES

The Service Provider hereby agrees the right of the Reserve Bank of India to cause an inspection of HDBFS documents, records of transactions, and other necessary information given to, stored or processed by the Service Provider within a reasonable time, books and account by one or more of its officers or employees or other persons.

The Service Provider hereby agrees the right of the Reserve Bank of India to cause an inspection to be made of the Service Provider & its books and account by one or more of its officers or employees or other persons.

In the event of the Service Provider not able to provide access to the necessary information/ records to RBI or the persons authorized by it within a reasonable time, the Service Provider agrees to indemnify and reimburse HDBFS any supervisory fees HDBFS pays to the RBI.

The Service Provider shall comply with the directives given by the RBI from time to time.

20. RIGHT TO CONDUCT AUDIT

The Service Provider hereby agrees the right of HDBFS to conduct audits, on the Service Provider for all or part of the activity outsourced whether by HDBFS's internal auditors or external auditors, or by agents appointed to act on its behalf and to obtain copies of any audit or review reports and findings made on the Service Provider in conjunction with the job/work/activity outsourced or services performed for HDBFS.

21. CUSTOMER RIGHTS AND REDRESSAL

The Service Provider shall ensure that its service arrangements do not affect the rights of the Customers of HDBFS, including but not limited to their ability to seek redressal under relevant laws, regulations, or policies.

HDBFS retains the sole authority to address grievances of Customers of HDBFS, and the Service Provider shall cooperate fully in facilitating the resolution of complaints and disputes.

The Service Provider shall maintain records of all transactions and interactions with Customers of HDBFS as required by applicable laws to support redressal mechanisms.

22. HDBFS OVERSIGHT AND REGULATORY COMPLIANCE

The Service Provider shall not impede or interfere with HDBFS' ability to effectively oversee and manage its outsourced activities.

The Service Provider shall comply with all instructions, policies, and regulatory guidelines prescribed by HDBFS to ensure efficient supervision of outsourced services.

The Service Provider shall not obstruct or hinder the RBI in carrying out its supervisory functions and objectives. The HDBFS shall retain the right to provide full access to regulatory authorities, including the RBI, for audits, inspections, or investigations related to outsourced activities.

23. OWNERSHIP AND CONTROL RESTRICTIONS

The Service Provider, if not a group company of the HDBFS, shall not be owned or controlled directly or indirectly by any director of HDBFS or their relatives, as defined under the Companies Act, 2013.

The Service Provider shall disclose its ownership structure to HDBFS and provide declarations confirming compliance with this requirement.

In the event of any violation of this clause, HDBFS reserves the right to terminate the Agreement with immediate effect and take appropriate legal action.

24. DISCLOSURE OF PRODUCT/SERVICE PROVIDER

HDBFS shall ensure that Customers of HDBFS are clearly informed about the actual entity offering the Product or Service at the time of engagement. This shall be communicated through contractual documents, marketing materials, and direct customer interactions.

Disclosure in Multi-Entity and Cross-Selling scenarios: In cases where multiple group entities are involved or cross-selling occurs, HDBFS shall provide explicit written disclosure to the Customers of HDBFS regarding the legal entity responsible for delivering the Product/ Service.

Prevention of Misrepresentation: HDBFS shall take adequate measures to prevent any form of misrepresentation or ambiguity regarding the identity of the Service Provider. All communications, advertisements, and Agreements shall accurately reflect the details of the offering entity.

HDBFS shall establish processes to educate and inform Customers of HDBFS about the applicable entity offering the Product/ Service, ensuring full transparency in all Customer of HDBFS dealings.

Regulatory and Compliance Adherence: HDBFS shall comply with all applicable laws and regulatory requirements concerning transparency in service offerings, ensuring that Customers of HDBFS are duly informed.

25. BONAFIDE PERFORMANCE

The Service Provider and its staff / agent / employees / personnel / representative will at all times use the best efforts to promote the HDBFS's business and reputation and will comply with HDBFS' instructions on all matters relating to the HDBFS's Business and discharging services more particularly defined in Annexures to this Agreement.

26. RIGHTS OF THIRD PARTIES

It is hereby expressly agreed and confirmed by HDBFS and Service Provider and its staff / agent / employees / personnel / representative that any person who is not a party to this Agreement i.e., any third party will have no right under the Contract (Rights of Third Parties) Act to enforce any of the terms or provisions of this Agreement.

27. DATA RETENTION AND PRESERVATION

The Service Provider shall maintain and securely preserve all books of account, records, documents, reports, files, and data including accounting records, staff-related records, and any information received from or transmitted to HDBFS for a minimum period of eight (8) years from the date of expiry or early termination of this Agreement. This obligation shall apply irrespective of the termination or expiry of this Agreement.

The Service Provider shall ensure that:

i. All data is stored exclusively within India, in compliance with applicable laws.
ii. Records are maintained in a manner that ensures confidentiality, integrity, and availability, including through secure electronic systems.
iii. Logs of all network security activities, including any data compromise events or breaches, are retained as per RBI guidelines.
iv. The Service Provider complies with all applicable provisions under the Companies Act, 2013, Income Tax Act, 1961, and the Reserve Bank of India (Outsourcing of IT Services) Directions, 2023, including but not limited to business continuity, audit readiness, and supervisory access and such other regulation as may be applicable from time to time.

28. ENVIRONMENTAL, SOCIAL AND GOVERNANCE

A. Anti-Bribery and Anti-Corruption

The Service Provider must strictly comply with all anti-bribery and anti-corruption laws (including the Prevention of Corruption Act, 1988) and HDBFS policies on anti-bribery & anti-corruption. The Service Provider, its subcontractors, agents must not offer, promise, or give any financial or other advantage to improperly influence any decision, secure an advantage, or gain business. Any actual or suspected breaches must be reported immediately to HDBFS, and the Service Provider must fully cooperate with HDBFS during audits. Breach of this clause is a material breach resulting in termination of Agreement.

B. Environmental Stewardship Obligations of the Service Provider

The Service Provider is required to operate responsibly by actively minimizing greenhouse gas emissions, waste, and resource consumption. The Service Provider must comply with all applicable environmental laws and maintain an effective Environmental Management System (EMS). Upon request, the Service Provider shall provide annual environmental performance reports (e.g., on carbon footprint, waste, and water usage) and collaborate with HDBFS on sustainable practices.

C. Health & Safety Compliance Clause for Service Providers

The Service Provider must maintain a safe and healthy work environment for its employees and personnel, adhering to all applicable laws (such as the Occupational Safety, Health and Working Conditions Code, 2020). This includes identifying, assessing, and mitigating risks, implementing protocols, and ensuring all personnel receive adequate safety training. All incidents must be reported to HDBFS within 24 hours, investigated, and corrective actions taken. HDBFS retains the right to audit compliance, and non-compliance may lead to corrective action, suspension, or Agreement termination. The Service Provider is responsible for the health and safety compliance of any of its subcontractors.

29. DEFINITIONS

Data Protection Laws shall include all applicable laws or regulations that are currently in force or may into force at a later date, relating to the collection, use, processing, storage, disclosure, transfer of personal information about an individual, including but not limited to the Digital Personal Data Protection Act, 2023 (once implemented), the Information Technology (the Indian Computer Emergency Response Team and Manner of performing functions and duties) Rules, 2013 read with the directions under sub-section (6) of section 70B of the Information Technology Act, 2000 relating to information security practices, procedure, prevention, response and reporting of cyber incidents for safe & trusted internet, and any amendments or replacement thereof, as may be applicable.

Data Principal, for the purposes of this DPA, shall mean the individual to whom the Personal Data relates.

Incident, for the purposes of this DPA, shall mean a cybersecurity incident or cyber incident as defined under Data Protection Laws.

Personal Data, for the purposes of this DPA shall mean any data about an individual who is identifiable by or in relation to such data or is defined as

"personal data" or "personal information" or "sensitive personal data or information" under Data Protection Laws.

Personal Data Breach, for the purposes of this DPA shall mean any unauthorised 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 or is defined as "personal data breach" under Data Protection Laws.

Process or Processing, for the purposes of this DPA shall, in relation to personal data, mean, a wholly or partly automated operation or set of operations performed on digital personal data, and includes operations such as collection, recording, organization, structuring, storage, adaptation, retrieval, use, alignment or combination, indexing, sharing, disclosure by transmission, dissemination or otherwise making available, restriction, erasure or destruction

Processor / Service Provider: For the purposes of these Terms and Conditions, the terms Processor and Service Provider shall have the same meaning and may be used interchangeably. Both refer to any third party engaged by HDB Financial Services Ltd to process personal data on its behalf, in accordance with applicable data protection laws and contractual obligations.

30. DATA PROTECTION

The Service Provider shall, and shall ensure that its affiliates, subsidiaries, agents, and any other persons that it may contract with for the purpose of fulfilling its obligations under this agreement shall:

(a) process personal data only in accordance with HDBFS' instructions and in the manner provided for under this agreement or as may be laid down in a Data Processing Addendum (DPA);

(b) adopt and maintain appropriate security measures and other organizational and technical measures which HDBFS is required to maintain under applicable laws, and (ii) ensure reasonable security safeguards to prevent personal data breaches in accordance with the standards which HDBFS is required to maintain under applicable laws;

(c) not disclose personal data to any third party unless as required under applicable law or as may otherwise be instructed by HDBFS;

(d) providing assistance to HDBFS where the data principals exercise their rights, raise complaints, requests or grievances or in relation to any other matter that enables HDBFS to comply with Data Protection Laws; and

(e) reporting cybersecurity incidents and personal data breaches (as defined under Data Protection Laws) within prescribed time periods.

31. INDEMNITY AND LIMITATION OF LIABILITY

The Service Provider will defend, indemnify and hold HDBFS and its respective officers and directors harmless from and against any claims, demands, proceedings, regulatory actions, liabilities, losses, causes of action, damages, fines, judgments, and settlements, including reimbursement of all reasonable expenses, including legal fees and expenses, arising directly or indirectly from any breach of this agreement or the DPA or any Data Protection Laws by Service Provider, its affiliates, employees, contractors, agents or Sub-processors.

Notwithstanding any other provision to the contrary in the agreement or the DPA, Service Provider's obligations and liability for violation under the Agreement shall not be subject to any limitations and exclusions from liability, if any, that is set forth in the agreement or the DPA.

Definition: For the purposes of this clause, 'Data Protection Laws' (DPA) shall mean all applicable laws in relation to data protection and privacy including the Information Technology Act, 2000; the Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules 2011 and any other rules and regulations framed thereunder, and the Digital Personal Data Protection Act, 2023 and rules issued thereunder, as and when it comes into force.

32. NATURE OF DATA PROCESSING

This DPA governs the Processing (defined below) of Personal Data (defined below) undertaken on behalf of HDBFS by the Processor pursuant to the Agreement and all exhibits, appendices, annexes, attachments, and amendments thereto.

Personal Data, for the purposes of this DPA shall mean any data about an individual who is identifiable by or in relation to such data or is defined as "personal data" or "personal information" or "sensitive personal data or information" under all applicable laws or regulations that are currently in force or may into force at a later date, relating to the collection, use, processing, storage, disclosure, transfer of personal information about an individual, including but not limited to the Digital Personal Data Protection Act, 2023, the Information Technology (the Indian Computer Emergency Response Team and Manner of performing functions and duties) Rules, 2013 read with the directions under sub-section (6) of section 70B of the Information Technology Act, 2000 relating to information security practices, procedure, prevention, response and reporting of cyber incidents for safe & trusted internet, Aadhaar (Targeted Delivery Financial and Other Subsidies, Benefits and Services) Act, 2016 read with its underlying rules, regulations and circulars, from time to time, and any amendments or replacement thereof, as may be applicable (together, Data Protection Laws). Processor will treat all Personal Data received from HDBFS under this DPA as confidential information under the Agreement.

Processing, for the purposes of this DPA shall, in relation to personal data, mean, a wholly or partly automated operation or set of operations performed on digital personal data, and includes operations such as collection, recording, organization, structuring, storage, adaptation, retrieval, use, alignment or combination, indexing, sharing, disclosure by transmission, dissemination or otherwise making available, restriction, erasure or destruction.

The Processing of Personal Data carried out by Processor on behalf of HDBFS and the purposes of such Processing, are described in the Appendix to this DPA, which forms an integral part of the DPA.

33. OBLIGATIONS OF THE DATA PROCESSOR

The Processor shall:

a) Process Personal Data only to the extent necessary for the purposes described in the Appendix to this DPA and not use or Process the Personal Data for any other purpose. The HDBFS may also provide instructions to the

Processor on such Processing from time to time. If the Processor cannot comply with these requirements, it will promptly inform HDBFS, and HDBFS is entitled to immediately terminate this DPA and/or the Principal Agreement, as the case may be, or to take any other reasonable action, including the suspension of Personal Data Processing operations;

b) Where the Processor is collecting or Processing Personal Data directly from individuals on behalf of HDBFS, follow HDBFS's instructions with regard to such Personal Data Processing (including with regard to providing notice and obtaining consent, to the extent applicable);

c) comply with applicable laws including but not limited to Data Protection Laws in relation to the Processing of Personal Data pursuant to the Principal Agreement or this DPA;

d) ensure that its personnel and any Sub-processors (defined below) are legally required in writing to acknowledge and respect the confidentiality of the Personal Data, including after the end of their employment, contract or at the end of their assignment or project, as applicable;

e) if it intends to engage one or more third parties acting on its behalf (Sub-processor) to carry out its obligations under this DPA, or to delegate all or part of the Processing to such Sub-processors, (i) obtain the prior written consent of HDBFS to such subcontracting, upon providing the HDBFS with details of the Processing activities carried out by such Sub-processors, along with the purposes for such Processing and other information as required by the HDBFS; (ii) ensure that such Sub-processors have implemented appropriate security measures (including the measures described under Clause 33 below); and (iii) enter into contractual arrangements with such approved Sub-processors which impose all obligations on the Processor under this DPA on such Sub-processors;

f) permit the HDBFS (or any third party on its behalf) or competent government authority to audit, undertake inspections, or seek information/documentation in relation to verifying the Processor's compliance with obligations under this DPA.

g) remain fully liable for all actions and inactions of any personnel or Sub-processors engaged by it for Processing Personal Data pursuant to this DPA and shall ensure that such personnel and third parties act in compliance with requirements imposed on the HDBFS under Data Protection Laws.

Processor shall inform HDBFS without undue delay if Processor becomes aware of:

- any non-compliance by the Processor or its employees or Sub-processors, as applicable, with this DPA or applicable laws including the Data Protection Laws relating to the terms of this DPA;
- a notice, inquiry, subpoena, investigation or a request for inspection or audit relating to the Processing or any legally binding request for disclosure of Personal Data, from a competent government authority, unless prohibited under applicable law to do so;
- The Processor shall provide all assistance as may be requested by the HDBFS regarding:
- any complaints/ requests from data principals regarding their statutory and legal rights under applicable law including Data

Protection Laws, in connection with their Personal Data Processed as part of this DPA. In the event that a data subject sends such a request directly to the Processor or Sub-processors, the Processor shall pass it on to HDBFS immediately without any delay. The Processor or any of its Sub-processors shall not respond to any such request without HDBFS's prior written authorization;

- the investigation of Personal Data Breaches and the notification to the appropriate regulator or other authorities, as applicable and data principals in respect of such breaches if required under Data Protection Laws;
- the preparation of data protection impact assessments or periodic audits, as required and where applicable, in accordance with Data Protection Laws;
- deletion, retention, erasure, or destruction of Personal Data Processed as part of this DPA including upon HDBFS's instructions and in accordance with Data Protection Laws;
- any notice, inquiry, subpoena, investigation or a request for inspection or audit relating to the Processing or any legally binding request for disclosure of Personal Data, from a competent government authority;
- any other matter and undertake all actions to enable the HDBFS to comply with Data Protection Laws in relation to Personal Data Processed pursuant to this DPA.
- The Processor further agrees to notify the HDBFS of any suspected or actual Personal Data Breach or Incident that may be required to be reported as Personal Data Breach or Incident under Data Protection Laws, in relation to Personal Data Processed by the Processor, or any Sub-processors acting on the Processor's behalf without undue delay and in any event within [2] hours of becoming aware of a Personal Data Breach.
- For the purposes of this DPA, Personal Data Breach shall mean 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.
- For the purposes of this DPA, Incident shall mean a cybersecurity incident or cyber incident as defined under Data Protection Laws.

34. SECURITY

The Processor shall (i) adopt and maintain appropriate security measures and other organizational and technical measures which the HDBFS is required to maintain under Data Protection Laws, and (ii) ensure reasonable security safeguards to prevent Personal Data breaches in accordance with the standards which the HDBFS is required to maintain under Data Protection Laws. The Processor shall and shall ensure that any Sub-processors engaged by it for Processing Personal Data regularly assess and evaluate the effectiveness of the technical, organisational measures and reasonable security safeguards that have adopted by such entities for the Processing of Personal Data pursuant to this DPA.

35. DATA TRANSFERS

The Processor shall transfer Personal Data to other entities, including Sub-processors only in accordance with the instructions provided by the HDBFS if any as well as the requirements imposed on the HDBFS under applicable laws including Data Protection Laws.

36. INDEMNITY AND LIMITATION OF LIABILITY

Processor will defend, indemnify and hold HDBFS, and its' respective officers and directors harmless from and against any claims, demands, proceedings, regulatory actions, liabilities, losses, causes of action, damages, fines, judgments, and settlements, including reimbursement of all reasonable expenses, including legal fees and expenses, arising directly or indirectly from any breach of this DPA, or Data Protection Laws by Processor, its affiliates, personnel, agents or Sub-processors.

Notwithstanding any other provision to the contrary in the Principal Agreement, Processor's obligations and liability for violation of this DPA shall not be subject to any limitations and exclusions from liability, if any, that is set forth in the Principal Agreement.

The parties agree that on the termination of Processing pursuant to the DPA, the Processor and any Sub-processors shall, at the choice of HDBFS, return all the Personal Data and copies of such data to HDBFS or securely erase or destroy them and demonstrate to the satisfaction of HDBFS that it has taken such measures.

In the event Processor or Sub-processors cease operations as a result of this Clause 7, the Processor shall and shall ensure that the Sub-processors shall have a business continuity plan and provide transition related support in the manner required by the HDBFS.

37. TERM AND TERMINATION

This DPA shall remain in effect as long as Processor or Sub-processors Process Personal Data in connection with the terms of the Agreement.

The parties agree that on the termination of Processing pursuant to the DPA, the Processor and any Sub-processors shall, at the choice of HDBFS, return all the Personal Data and copies of such data to HDBFS or securely erase or destroy them and demonstrate to the satisfaction of HDBFS that it has taken such measures.

In the event Processor or Sub-processors cease operations as a result of this Clause 36, the Processor shall and shall ensure that the Sub-processors shall have a business continuity plan and provide transition related support in the manner required by HDBFS.

38. CONFLICT

In the event of any conflict or inconsistency between data protection related terms under the Agreement and this DPA, this DPA would prevail.

39. CONTACT

The Processor shall designate a point of contact to liaise with the HDBFS in relation to the Processor's obligations under this DPA. The Processor shall notify the HDBFS of any change to the point of contact as soon as practicable but no later than [15] days.

Processor Point of Contact:

Name:
Address:
Telephone Number:
Email Address

APPENDIX

DESCRIPITON OF PROCESSING ACTIVITIES

Purpose of Processing	[…]
Types of Personal Data Processed	[…]
Categories of data principals	[…]