DATA PROCESSING AGREEMENT

KNOW ALL MEN BY THESE PRESENTS:

This **Data Processing Agreement** ("Agreement") dated as of the [O] day of [O] in Taguig City, by and between:

> **HC CONSUMER FINANCE PHILIPPINES, INC.** (**"HCPH"** or the **"PIC"**), a corporation duly organized and existing under and by virtue of the laws of the Republic of the Philippines, with principal office address at 15th Floor Ore Central, 9th Avenue corner 31st Street, Bonifacio Global City, Taguig City, represented herein by its Chief Financial Officer, **Jana Pechouckova**;
>
> -and-
>
> **[O]** (**"COMPANY"** or the **"PIP"**), a corporation duly organized and existing under and by virtue of the laws of the Republic of the Philippines, with office address at [O], represented herein by its [O], **[O].**

HCPH and the **COMPANY** may hereinafter be referred to collectively as "**Parties**" or individually as "**Party**".

WITNESSETH: That

WHEREAS, HCPH and the COMPANY executed a [O] dated [O] pertaining to a defined and workable framework upon which the Parties wish to engage and enter into a strategic partnership (the **"Contract"**);

WHEREAS, the Parties acknowledge that Data Subjects have express rights under the Data Privacy Act and its Implementing Rules and Regulations that provide for protection and confidentiality of their Personal Data;

NOW, THEREFORE, for and in consideration of the foregoing premises and mutual covenants herein contained, the Parties hereby agree to bind themselves, as follows:

1. Definitions

The following terms shall have the respective meaning whenever they are used in this Agreement:

A. **Commission** or **NPC** – refers to the National Privacy Commission;

B. **Consent –** refers to any freely given, specific, informed indication of will, whereby the Data Subject agrees to the collection and Processing of his or her Personal Information, Sensitive Personal Information, or privileged information. Consent shall be evidenced by written, electronic or recorded means. It may also be given on behalf of a Data Subject by a lawful representative or an agent specifically authorized by the Data Subject to do so;

C. **Data Processing** – refers to any operation or any set of operations performed upon personal data including, but not limited to, the collection, recording, organization, storage, updating or modification, retrieval, consultation, use, consolidation, blocking, erasure or destruction of data. Processing may be performed through automated

means, or manual processing, if the personal data are contained or are intended to be contained in a filing system. Also see **Processing**;

D. **DPA** – refers to Republic Act 10173, otherwise known as the Data Privacy Act of 2012

E. **Data Protection Officer** or **DPO** – refers to an individual designated by a Party to be accountable for compliance with the DPA, its IRR, and other issuance of the NPC;

F. **Data Subject** – refers to an individual whose Personal Information, Sensitive Personal Information, or privileged information is processed;

G. **IRR** – refers to the implementing rules and regulations of the DPA.

H. **Personal Data** – refers to either of the following:

1. **Personal Information** – refers to any information, whether recorded in material form or not, from which the identity of an individual is apparent or can be reasonably and directly ascertained by the entity holding the information, or when put together with other information would directly and certainly identify an individual; or

2. **Sensitive Personal Information** – refers to Personal Information:

i. About an individual's race, ethnic origin, marital status, age, color and religious, philosophical or political affiliations;
ii. About an individual's health, education, genetic or sexual life of a person, or to any proceeding for any offense committed or alleged to have been committed by such individual, the disposal of such proceedings, or the sentence of any court in such proceedings;
iii. Issued by government agencies peculiar to an individual which includes, but is not limited to, social security numbers, previous or current health records, licenses or its denials, suspension or revocation, and tax returns; and
iv. Specifically established by an executive order or an act of Congress to be kept classified.

I. **Personal Data Breach** – refers to a 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. A Personal Data Breach may be in the nature of:
- an availability breach resulting from loss, accidental or unlawful destruction of Personal Data;
- an integrity breach resulting from alteration of Personal Data; and/or
- a confidentiality breach resulting from the unauthorized disclosure of or access to Personal Data;

J. **Personal Information Controller** or **PIC** – refers to the party who controls the Processing of Personal Data, or instructs another to process Personal Data on its behalf. There is control if the party decides on what information is collected, or the purpose or extent of its Processing;

K. **Personal Information Processor** or **PIP** – refers to any natural or juridical person or any other body to whom a Personal Information Controller may outsource or instruct the processing of Personal Data pertaining to a Data Subject;

L. **Personnel** – shall refer to the employees, officers, agents, or otherwise acting under the authority of the Personal Information Processor or the Personal Information Controller;

M. **Processing** – refers to any operation or any set of operations performed upon Personal Data including, but not limited to, the collection, recording, organization, storage, updating or modification, retrieval, consultation, use, consolidation, blocking, erasure or destruction of data. Processing may be performed through automated means, or manual processing, if the Personal Data are contained or are intended to be contained in a filing system;

N. **Security Incident** – refers to an event or occurrence that affects or tends to affect data protection, or may compromise the availability, integrity and confidentiality of Personal Data. It includes incidents that would result to a Personal Data Breach, if not for safeguards that have been put in place.

2. Purpose

HCPH will share, provide, or disclose to the COMPANY, Personal Data pertaining to its clients, which is in the possession and control of HCPH, for the purpose of [○].

3. Responsibilities of the PIC

The PIC, with regard to the Personal Data in their original possession, is responsible for ensuring that it collects Personal Data lawfully and in accordance with the requirements of the DPA and its IRR.

Prior to collection and sharing, or at the next practicable opportunity, the PIC shall be responsible in apprising the Data Subject with the nature, purpose, and extent of the Processing of his or her Personal Data, including the risks and safeguards involved, the identity of the PIC, his or her rights as a Data Subject, and how these can be exercised.

The PIC warrants that it is compliant with the DPA and its IRR in relation to its Processing of Personal Data. The PIC also warrants that it has in place appropriate administrative, physical, technical, and organizational security measures that protect Personal Data from Security Incidents and Personal Data Breaches.

The PIC shall be responsible for the accuracy and quality of the Personal Data that it collects and shares.

The PIC shall be responsible for addressing any information request, or any complaint filed by a Data Subject and/or any investigation conducted by the Commission. *Provided*, that the Commission shall make a final determination as to who among the Parties is liable for any breach or violation of the DPA, its IRR, or any applicable issuance of the Commission.

a. Responsibilities of the PIP

The PIP shall not share Personal Data obtained from the PIC with any other party without the prior written permission/instruction of the PIC or process Personal Data in any way or for any purpose other than those set out in this Agreement. The PIP shall segregate the Personal Data from its own and its other clients' data.

The PIP shall not sub-contract or engage a third party or another Personal Information Processor to process the Personal Data without the prior knowledge and written agreement of the PIC, and only after the third party has provided all the necessary assurance and guarantees that it has adequate administrative, physical, technical, organizational and procedural security measures to protect the Personal Data.

The PIP shall assist the PIC in ensuring compliance with the DPA, the IRR, other relevant laws, and other issuances of the Commission, taking into account the nature of Processing and the information available to the PIP. The PIP shall immediately inform the PIC if, in its opinion, an instruction infringes the DPA, its IRR, or any other issuance of the Commission.

4. Categories of Personal Data

The categories of Personal Data to be shared by HCPH are as follows:

From HCPH:
[O]
[O]
[O]
From COMPANY:
[O]
[O]
[O]

5. Security

The PIP shall implement strict security measures that ensure the availability, integrity, and confidentiality of Personal Data. The PIP shall implement reasonable and appropriate organizational, physical, technical, administrative, procedural and security measures to protect Personal Data against any Security Breach as prescribed in the DPA, its IRR, and circulars issued by the Commission.

The PIP shall ensure that Personal Data is backed-up on a regular basis and that any back-up is subject to security measures as necessary to protect the availability, integrity and confidentiality of Personal Data.

The PIP undertakes that it will not, at any time, whether during the course of, or after the term of this Agreement, transfer, share, divulge, exploit, and modify any Personal Data to any person.

6. Personnel

Each Party shall take steps to ensure that any person acting under its authority and who has access to Personal Data, does not process them except for purposes of this Agreement or as required by law.

Each Party shall ensure that access to Personal Data is limited only to its Personnel who need access only for purposes of this Agreement.

Each Party shall ensure that its Personnel engaged in the Processing of Personal Data are informed of the confidential nature of the Personal Data and are subject to obligations of confidentiality and such obligations survive the termination of that Personnel's engagement or relationship with each Party.

Each Party shall take reasonable steps to ensure the reliability of any of its Personnel who have access to Personal Data, which shall include ensuring that they all understand the confidential nature of the Personal Data; and have received appropriate training in data

protection prior to their access or Processing of Personal Data, and have signed a written undertaking that they understand and will act in accordance with their responsibilities for confidentiality under this Agreement.

7. Bring Your Own Device (BYOD)

The PIP shall ensure that its Personnel who are allowed to use their personally owned smart phones or devices to process Personal Data for purposes of this Agreement strictly abide by the foregoing obligations. HCPH, in turn, shall respect the privacy of the PIP's Personnel in relation to their personal devices and will only request access to the device to respond to its legitimate interests as a PIC under the DPA such as investigating claims of unauthorized access or disclosure of Personal Data, among others.

The PIP shall ensure that it has adequate policies and procedures in place and any other means it deems necessary to guide its Personnel in ensuring the security and confidentiality of Personal Data processed through their personally-owned devices and to limit the ability of Personnel in transferring data, such as, but not limited to the following: (1) prohibiting Personnel from taking photos, saving back-ups, or transmitting customer Personal Data, (2) requiring strong device passwords, (3) ensuring the adherence of Personnel to acceptable use standards and restrictions on using personally-owned devices in a business environment, (3) prohibiting Personnel from connecting to unsecured networks while working, (4) enforcing appropriate disciplinary actions for its Personnel who fail to abide by the obligations as set forth herein, (5) immediate notification in case the personal device is lost, stolen, or damaged, and (6) ensuring the removal and deletion of apps or customer Personal Data on Personnel devices once said Personnel resigns or gets terminated.

The PIP acknowledges that it assumes full liability for risks including, but not limited to, the partial or complete loss or disclosure of customer Personal Data due to theft, damage, operating system crash, errors, bugs, viruses, malware, and/or other software or hardware failures, or programming errors that are not due to the loan processing application installed by HCPH for purposes of this Agreement and which render the device unusable.

8. Data Subject Access Rights

Data Subjects have a right to see what Personal Data is held about them, and to know why and how it is processed.

The PIC has an obligation to respond to these request or complaints, however, requests made to the PIP should likewise be honored by them. The PIP shall, by appropriate technical and organizational measures and to the extent possible, fulfill the obligation to respond to requests by Data Subjects relative to the exercise of their rights. Inquiries and information requests can be made by submitting a written letter with the following Data Protection Officers (or its equivalent):

HCPH:

Name of DPO : Regine Noelle B. Ignacio-Pariñas
Email : DPO@homecredit.ph
Address : 15th Floor, Ore Central, 9th Avenue cor. 31st Street, Bonifacio Global City, Taguig City

COMPANY:

Name of DPO : [O]
Email : [O]
Address : [O]

The DPO of each Party will be the first port of call for questions about this Agreement, any complaint filed by the Data Subject, and/or investigation by the Commission. If there is a problem such as a potential Personal Data Breach, the relevant DPO must be contacted immediately.

Each Party shall rectify the complaint by any Data Subject within thirty (30) days from receipt of any such complaint. The Data Subject shall be given a response in writing describing how the complaint was rectified and how the situation complained of will be avoided moving forward.

9. Breach Management and Notification

Each Party shall implement policies and procedures for guidance of its Personnel in the event of a Security Incident or a Personal Data Breach, including but not limited to:

A. A procedure for the timely discovery of Security Incidents or Personal Data Breaches, including the identification of person or persons responsible for regular monitoring and evaluation of Security Incidents or Personal Data Breaches;

B. A policy for documentation, regular review, evaluation and updating of the privacy and security policy and practices;

C. Clear reporting lines in the event of a possible Security Incident or Personal Data Breach, including the identification of a person responsible for setting in motion the Security Incident or Personal Data Breach response procedure, and who shall be immediately contacted in the event of a possible or confirmed Security Incident or Personal Data Breach;

D. Conduct of a preliminary assessment for purpose of:
    a. Assessing the nature and scope of the Security Incident and the immediate damage and if the incident is in fact a Personal Data Breach;
    b. Determining the need for notification of law enforcement or external expertise; and
    c. Implementing immediate measures necessary to secure any evidence, contain the Personal Data Breach and restore integrity to the Personal Data;

E. Evaluation of the Security Incident or Personal Data Breach as to its nature, extent and cause, the adequacy of safeguards in place, immediate and long-term damage, impact of the breach, and its potential harm and negative consequences to Personal Data and affected Data Subjects;

F. Procedures for contacting law enforcement in case a Security Incident or Personal Data Breach involves the possible commission of criminal acts;

G. Conduct of investigations that will evaluate fully the Security Incident or Personal Data Breach;

H. Procedures for immediately notifying the PIC when the Security Incident or Personal Data Breach is subject to notification requirement; and

I. Measures and procedures for mitigating the possible harm and negative consequences to the PIC and the affected Data Subjects in the event of a Security Incident or Personal Data Breach. Each Party must be ready to provide assistance to the Data Subjects whose Personal Data may have been affected.

The Parties shall have the manpower, system, facilities, and equipment in place to properly monitor access to Personal Data, and to monitor and identify Security Incidents and Personal Data Breaches.

If a Party becomes aware of any Personal Data Breach by its Personnel, or involving its premises, facilities, system, or equipment, it shall: (a) notify the other Party of the Personal Data Breach; (b) investigate the Personal Data Breach and provide the other Party with information about the Personal Data Breach; and (c) take reasonable steps to mitigate the effects and to minimize any damage resulting from the Personal Data Breach.

The Parties shall cooperate with each other on incident investigation requirements for any Personal Data Breach.

Each Party shall send the written notification via e-mail to their DPO counterpart, of any Personal Data Breach within twenty-four (24) hours from knowledge or discovery thereof.

Upon receipt, confirmation, and knowledge of the Personal Data Breach, the DPO for the PIC shall notify the Commission and the affected Data Subject within seventy-two (72) hours.

The Party who was notified of a Personal Data Breach may require the other Party to provide further details and actions taken on the Personal Data Breach.

10. Duration of this Agreement

Unless extended by mutual written consent of both Parties hereto, this Agreement shall expire either one (1) year from the date hereof or upon the termination of the Contract, whichever occurs last.

This Agreement may be renewed by mutual consent at the option of either Party before its expiration as provided above.

11. Retention of Personal Data

Personal Data should only be processed for as long as is necessary. Processing of Personal Data should be limited accordingly and for a period no longer than the term of this Agreement. Specific justification for processing, specifically retention, of Personal Data beyond said period is required. At the end term of this Agreement or after the expiration of any approved extension, the Personal Data must be deleted, unless otherwise agreed by the Parties in writing.

If Personal Data has been held for longer than one (1) year, an updated version must be obtained as soon as practicable. If a complaint is received about the accuracy of Personal Data which affects the Personal Data and/or Sensitive Personal Information shared with the other Party, an updated replacement Personal Data will be communicated to the other Party. The other Party must replace the out of date data with the revised data.

12. Return or Destruction of Personal Data

Upon expiration or termination of the Contract or this Agreement, whichever comes first, the PIP shall perform the following, within thirty (30) days from date of said expiration or termination:

a. Return all Personal Data of Data Subjects in any recorded form including any other property, information, and documents provided by the PIC;
b. Destroy all copies it made of Personal Data and any other property, information, and documents, if requested by the PIC. For print out or other tangible formats, the document will be shredded. For data in electronic form, the document must be deleted, wiped, overwritten, or otherwise made irretrievable; and
c. Deliver to the PIC a certificate confirming PIP's compliance with the return or destruction obligation under this section, if requested by the PIC.

13. Audits

The PIP shall make available to the PIC all information necessary to demonstrate compliance with the obligations laid down in the DPA, and allow for and contribute to audits, including inspections, conducted by the PIC or another auditor mandated by the latter. In the course of such audit, the PIC may conduct the following measures, but shall not be limited to:

1. Obtain information from the PIP about their Processing operations pertaining to the shared data to verify their compliance with the terms of the Contract or this Agreement.

2. Request the PIP to submit an existing attestation or certificate by an independent professional expert on their compliance to the DPA and applicable data privacy laws and the security requirements therein.

3. Upon reasonable and timely advance notice, during regular business hours, conduct an on-site inspection of the business operations of the PIP or have the same conducted by a qualified third party auditor or assessor, which shall not be an existing independent consultant of the PIP.

4. The PIP shall, after written request by the PIC, and within a reasonable period of time, submit any and all information, documentation, and/or other means of factual proof necessary for the conduct of an audit.

14. Entire Agreement

This Agreement constitutes the entire agreement between the Parties with respect to the subject matter hereof. It excludes and supersedes everything else which has occurred between the Parties whether written or oral, including all other communications with respect to the subject matter hereof.

15. Amendment

This Agreement may not be amended or modified except in writing and consented to by both Parties.

16. Separability Clause

If any provision of this Agreement is illegal or unenforceable, its invalidity shall not affect the other provisions of this Agreement that can be given effect without the invalid provision. If any provision of this Agreement does not comply with any law, ordinance or regulation, such provision to the extent possible shall be interpreted in such a manner to comply with such law, ordinance or regulation, or if such interpretation is not possible, it shall be deemed to satisfy the minimum requirements thereof.

17. Counterparts

This Agreement may be executed in two or more counterpart copies, each of which shall be deemed to be an original, but all of which shall constitute the same agreement.

18. Assignment

Either Party shall not assign or delegate its rights or obligations under this Agreement, in whole or in part, to any third party by operation of law or otherwise, without the prior written consent of the other. Any attempted assignment or delegation that does not comply with this section shall be null and void and of no effect.

19. Non-Waiver of Rights

The failure of a Party to insist upon a strict performance of any of the terms, conditions and covenants hereof, shall not be deemed a relinquishment or waiver of any right/remedy that said Party may have, nor shall it be construed as a waiver of any subsequent breach of the same or other terms, conditions and covenants. Any waiver, extension or forbearance of any of the terms, conditions and covenants of this Agreement by any Party hereto shall be in writing and limited to the particular instance only and shall not in any manner be construed as a waiver, extension, or forbearance of any of the terms, conditions and/or covenants of this Agreement.

20. Legal Capacity of Representatives

Each Party represents and warrants to the other Party that its representative executing this Agreement on its behalf is its duly appointed and acting representative and has the legal capacity required under the applicable law to enter into this Agreement and bind it.

21. Governing Law and Venue

This Agreement shall be governed by and construed in accordance with the laws of the Philippines, without regard to any conflicts of law rules. Exclusive jurisdiction over and venue of any suit arising out of or relating to this Agreement shall be in the courts of Metro Manila, Philippines. The Parties hereby consent and submit to the exclusive jurisdiction and venue of those courts.

IN WITNESS WHEREOF, the Parties have hereunto affixed their signatures on the date and at the place first above-written.

HC CONSUMER FINANCE PHILIPPINES, INC.	**[O]**
By:	By:
JANA PECHOUCKOVA	**[O]**

Signed in the Presence of:

Rejyl Siang	**xx**
Data Protection Officer	xx

ACKNOWLEDGMENT

REPUBLIC OF THE PHILIPPINES)
_____ CITY) S.S.

BEFORE ME, a Notary Public for and in _____ City, personally appeared the following:

Name	**Government ID No.**	**Date/Place Issued**

known to me, and to me known to be the same persons who executed the foregoing instrument entitled “Data Processing Agreement”, and they acknowledged to me that the same is of their free and voluntary act and will, and that of the corporations herein represented.

WITNESS MY HAND AND SEAL on the date and at the place first above-written.

Doc. No. ____;
Page No.____;
Book No.____;
Series of 2021.