DATA FORWARDING TERMS AND CONDITIONS

ARTICLE 1. DEFINITIONS

The following terms shall be defined as follows:

1.1. **Applicable Data Protection Law** refers to all privacy and data protection laws and regulations applicable to the Processing of the Forwarded Personal Data, including Philippine Data Protection Law.

1.2. **Commission** refers to the National Privacy Commission of the Philippines or the NPC.

1.3. **Data Portability** refers to the same term as contemplated under Philippine Data Protection Law.

1.4. **Data Protection Officer** refers to the same term as contemplated under Philippine Data Protection Law.

1.5. **Data Forwarding Terms and Conditions** ("**DFTC**") refers to these terms and conditions, including all annexes attached and schedules accomplished pursuant to the same.

1.6. **Data Subject** refers to the same term as contemplated under Philippine Data Protection Law.

1.7. **Forwarded Personal Data** refers to the copies of the Personal Data of Data Subjects that is Ported to the Receiving Party pursuant to the Instruction of Data Subjects, as a result of, or in connection with, this DFTC.

1.8. **GCash** refers to G-Xchange, Inc., one of the Parties in this DFTC.

1.9. **GCash App** shall refer to the application running on mobile devices where Data Subjects can avail themselves of GCash services or make use of the GCash wallet and/or access the Receiving Party's products, services, or platforms.

1.10. **Instruction** refers to the order, command, or direction of Data Subjects to Port their Personal Data to Receiving Party pursuant to their right to Data Portability, prior to using the Receiving Party Products/Services in the GCash App.

1.11. **Main Agreement** refers to the underlying agreement between the Parties to which this DFTC and its annexes and schedules are attached and forms part thereof.

1.12. **Notifiable Personal Data Breach** refers to the same term as contemplated under Philippine Data Protection Law.

1.13. **Party** individually refers to Transmitting Party and Receiving Party, and **Parties** collectively refer to Transmitting Party and Receiving Party.

1.14. **Personal Data** refers to the same term as contemplated under Philippine Data Protection Law.

1.15. **Personal Data Breach** refers to the same term as contemplated under Philippine Data Protection Law.

1.16. **Personal Data Forwarding Request** refers to a continuing arrangement between the Transmitting Party and Receiving Party as necessitated by the Main Agreement, where the Transmitting Party Ports the Forwarded Personal Data to the Receiving Party. The Porting of the Forwarded Personal Data shall be in response to the Instruction of Data Subjects pursuant to their right to Data Portability, arising from their interest to access the Receiving Party Products/Services.

1.17. **Personal Information** refers to the same term as contemplated under Philippine Data Protection Law.

1.18. **Personal Information Controller** ("**PIC**") refers to the same term as contemplated under Philippine Data Protection Law.

1.19. **Personal Information Processor** ("**PIP**") refers to the same term as contemplated under Philippine Data Protection Law.

1.20. **Personnel** shall refer to the directors, employees, agents, consultants, successors, and assigns, or any person otherwise acting under the authority of each of the Parties.

1.21. **Philippine Data Protection Law** collectively refers to the Data Privacy Act of 2012 and its Implementing Rules and Regulations, issuances of the Commission, issuances of the Bangko Sentral ng Pilipinas, and all other applicable laws and regulations relating to privacy and data protection for the time being in force.

1.22. **Point of Porting** refers to the Receiving Party's designated storage or repository that facilitates the Receiving Party's ability to access, retrieve, control, or otherwise engage with the Forwarded Personal Data.

1.23. **Porting** refers to the process of submitting, forwarding, or sending of a copy of the Forwarded Personal Data by the Transmitting Party to the Receiving Party in response to a Personal Data Forwarding Request and Instruction of the Data Subject. The Porting process is initiated when Data Subjects issue an Instruction to Port the Forwarded Personal Data, which may be through an instruction screen or any other means. The Porting process is deemed complete upon the delivery by the Transmitting Party of the Forwarded Personal Data to the Point of Porting.

1.24. **Process/es** or **Processing** refers to the same term as contemplated under Philippine Data Protection Law.

1.25. **Reasonable Belief** refers to a legal standard, as interpreted by the Supreme Court of the Philippines.

1.26. **Receiving Party** refers to the Party who, in accordance with the Main Agreement, receives the Forwarded Personal Data from the Transmitting Party upon the Instruction of Data Subjects.

1.27. **Receiving Party Products/Services** refers to the products, services, or platforms of Receiving Party that operate separately and independently from the GCash App, but may be voluntarily accessed through the GCash App for the convenience and benefit of Data Subjects.

1.28. **Reportable Major Cyber-Related Incident** refers to events which may seriously jeopardize the confidentiality, integrity or availability of critical information, data or systems of Bangko Sentral supervised financial institutions, including their customers and other stakeholders, as contemplated under the relevant Bangko Sentral ng Pilipinas issuances including the Manual of Regulations for Non-Bank Financial Institutions and Circular No. 1019, series of 2018. An incident is considered a Reportable Major Cyber-Related Incident if, after assessing the nature of the incident or attack, the relevant Party has determined that the same:

1.28.1. resulted in an unauthorized access and infiltration into Transmitting Party's internal network (i.e., hacking, advanced persistent threats, presence of malware);

1.28.2. involved a system-level compromise (i.e., attacks on

Transmitting Party's core systems, as opposed to phishing attempts of individual clients);

1.28.3. affected a significant number of customer accounts simultaneously;

1.28.4. involved significant data loss or massive data breach;

1.28.5. indicated spearphishing attacks targeting Transmitting Party's directors, senior executives, officers, or privileged users;

1.28.6. resulted in the unavailability of critical systems/services (e.g., Distributed Denial of Service ("DDoS") attack resulting in service outage);

1.28.7. inflicted material financial losses to Transmitting Party, their customers and other stakeholders; or

1.28.8. has been suspected to be perpetrated by an advanced threat actor.

1.29. **Security Incident** refers to the same term as contemplated under Philippine Data Protection Law.

1.30. **Sensitive Personal Information** refers to the same term as contemplated under Philippine Data Protection Law.

1.31. **Transmitting Party** refers to the Party who, in accordance with the Main Agreement, Ports the Forwarded Personal Data to the Receiving Party upon the Instruction of Data Subjects.

ARTICLE 2. SCHEDULE OF FORWARDED PERSONAL DATA

2.1. To facilitate the Personal Data Forwarding Request between the Parties, the Receiving Party shall provide a *Schedule of Forwarded Personal Data*. The Receiving Party shall provide the Transmitting Party with clear, specific, and documented instructions regarding the Porting of Forwarded Personal Data. These instructions shall be detailed in the Schedule of Forwarded Personal Data and shall include:

2.1.1. The required types of Personal Data and their intended purposes;

2.1.2. The naming conventions and file formats to be used;

2.1.3. The mode of Porting, including the required security measures to safeguard the data during transit (e.g., encryption, secure transfer protocols); and

2.1.4. Any other necessary information to enable the Transmitting Party to process the data in accordance with Applicable Data Protection Law and to facilitate the Data Subject's access to the Receiving Party's Products/Services.

The Transmitting Party shall implement the instructions as specified by the Receiving Party to the extent practicable and reasonable. The Receiving Party acknowledges that responsibility for ensuring the adequacy and effectiveness of such instructions lies solely with the Receiving Party.

2.2. The Forwarded Personal Data shall be limited to the Personal Data instructed by the Data Subjects to be Ported,

which has already been collected, stored, or Processed by the Transmitting Party. In case the Data Subject instructs the Transmitting Party to forward additional Personal Data beyond that already collected, stored, or Processed, or should the Receiving Party request additional Personal Data to enable Data Subjects to avail themselves of the Receiving Party Products/Services, such additional Personal Data shall be deemed as being Processed by the Transmitting Party on behalf of the Receiving Party. In this regard and where applicable, the Parties agree that the Data Processing Terms and Conditions ("**DPTC**") shall govern the Processing of such additional Personal Data, with the Receiving Party acting as the PIC and the Transmitting Party as the PIP. The DPTC, as may be amended periodically, is accessible at https://www.new.gcash.com/data-privacy-agreement/dptc and shall be deemed incorporated into this Agreement.

2.3. Each Schedule of Forwarded Personal Data shall be accomplished using the template appended to this DFTC (the "**Schedule of Forwarded Personal Data**"), which shall be sequentially numbered in the order of its accomplishment. The Parties shall prepare a cover memorandum, in either paper or electronic form, appending the accomplished Schedule of Forwarded Personal Data.

2.4. Should there be a renewal, supplement, or amendment to the Porting, or if there are additional projects, transactions, or services which are not covered by an existing Schedule of Forwarded Personal Data, the Parties shall accomplish a new Schedule of Forwarded Personal Data in accordance with this article. All accomplished schedules shall be annexed to and form an integral part of this DFTC.

ARTICLE 3. RESPONSIBILITIES OF THE PARTIES

3.1. Pursuant to the Personal Data Forwarding Request, the Parties agree, represent, and warrant the following:

3.1.1. The Porting of Forwarded Personal Data shall be made only in accordance with the Instruction of Data Subjects, pursuant to their right to Data Portability. By virtue of the Instruction, the Transmitting Party merely complies with the order of the Data Subject to Port the Forwarded Personal Data to the Receiving Party, and for this purpose, the Transmitting Party acts on behalf of the Data Subject.

3.1.2. The Porting of Forwarded Personal Data is being undertaken to enable the Receiving Party to use or receive the Data Subjects' Personal Data, thereby facilitating their ability to avail themselves of the Receiving Party's Products/Services.

3.1.3. This DFTC does not establish a joint PIC status or responsibility between the Transmitting Party and the Receiving Party.

3.1.4. The Receiving Party shall be the sole PIC of the Forwarded Personal Data from the moment it enters transit, upon reaching the Point of Porting, and for all subsequent Processing activities, continuing through and beyond the completion of the Porting process. The Transmitting Party shall act solely as a facilitator of the data Porting and shall not retain any control over or

responsibility for the Forwarded Personal Data during or after the Porting. The Transmitting Party expressly disclaims any role in determining the purposes or means of Processing the Forwarded Personal Data during transit or any subsequent Processing by the Receiving Party.

3.1.5. They shall abide and comply with the principles of transparency, legitimate purpose, and proportionality under Applicable Data Protection Law in Porting and Processing the Forwarded Personal Data.

3.1.6. This DFTC shall be available for review by the Commission on its own initiative or upon complaint of Data Subjects in accordance with Applicable Data Protection Law. A copy of this DFTC shall also be provided to Data Subjects upon the latter's written request and in accordance with Applicable Data Protection Law.

3.1.7. The Data Protection Officer of the Receiving Party shall be the first port of call for questions about the Forwarded Personal Data during and after transit, any complaint filed by Data Subjects, and/or investigation by the Commission.

3.2. The Transmitting Party, agrees, represents, and warrants the following:

3.2.1. Independently from the Forwarded Personal Data Ported to the Receiving Party, it shall be the PIC of the Personal Data of Data Subjects it has initially collected, stored, or Processed.

3.2.2. It shall Port the Forwarded Personal Data lawfully and in accordance with the requirements of Applicable Data Protection Law.

3.2.3. It shall duly inform Data Subjects of the fact and details of their Instruction and the Porting of the Forwarded Personal Data, including the identity of the Receiving Party as the PIC, through an adequate privacy notice.

3.2.4. It shall apprise Data Subjects of their rights as Data Subjects, and how these rights can be exercised in relation to the Personal Data for which the Transmitting Party is the PIC.

3.2.5. The Transmitting Party shall Port the Forwarded Personal Data on an "as is" basis without warranty of any kind, except that the Forwarded Personal Data has been secured through the Transmitting Party's Know-Your-Customer (KYC) process in accordance with applicable laws. The Transmitting Party expressly disclaims all warranties and conditions, either express or implied, with respect to the Forwarded Personal Data, including all implied warranties, completeness, and fitness for the Receiving Party's particular purpose.

3.3. The Receiving Party, agrees, represents, and warrants the following:

3.3.1. It shall independently verify and confirm the accuracy, completeness, and reliability of the Forwarded Personal Data

for its own purposes. The Transmitting Party is not liable for any errors and omissions in the Forwarded Personal Data, or decisions made by the Receiving Party in light of such data.

3.3.2. The Receiving Party shall ensure that all Forwarded Personal Data is received through secure transfer mechanisms that comply with the Applicable Data Protection Law, including the use of encryption, secure APIs, or other appropriate safeguards to protect the Forwarded Personal Data during transit. The Transmitting Party shall facilitate the use of such mechanisms as reasonably required by the Receiving Party, but assumes no liability for any breach or loss once the Forwarded Personal Data enters transit.

3.3.3. It shall duly inform Data Subjects of the fact and details, including the nature, purpose, and extent, of the Processing of their Forwarded Personal Data, through an adequate privacy notice and/or any other means. The Receiving Party shall ensure that it clearly communicates to Data Subjects that it assumes full responsibility as the PIC for the Forwarded Personal Data from the moment it enters transit. The Transmitting Party shall be identified solely as a facilitator of the Porting process, without further responsibility or control over the Forwarded Personal Data.

3.3.4. It shall employ data minimization so that the Forwarded Personal Data is limited to only those that are necessary for the Receiving Party Products/Services and compatible with this DFTC and the relevant Schedule of Forwarded Personal Data.

3.3.5. It shall address (a) any information request made to it as the PIC, (b) any complaint filed by Data Subjects, or (c) any investigation conducted by the Commission, all in relation to the Forwarded Personal Data and within the context of accessing and using the Receiving Party's Products/Services.

3.3.6. It shall have in place appropriate organizational, technical, and physical security measures to protect the Forwarded Personal Data from the moment it enters transit, upon reaching and including the Point of Porting, and for all subsequent Processing activities.

ARTICLE 4. DATA SUBJECT REQUESTS AND COMPLAINTS

4.1. The Receiving Party shall be responsible for upholding the rights of Data Subjects over the Forwarded Personal Data, under the Applicable Data Protection Law. The Receiving Party shall always ensure the availability of mechanisms by which requests or complaints by Data Subjects may be properly received or resolved which shall, at all times, comply with the requirements provided under Applicable Data Protection Law.

4.2. Any inquiry or request by Data Subjects with respect to the Forwarded Personal Data, including those arising during the data's transit, can be made by submitting a written request to the

Receiving Party's Data Protection Officer.

ARTICLE 5. INCIDENT MANAGEMENT AND BREACH NOTIFICATION

5.1. The Receiving Party shall establish, implement, and maintain policies and procedures to address a Security Incident or Personal Data Breach affecting the Forwarded Personal Data, including ensuring their timely detection, assessment, mitigation, and containment.

5.2. The Receiving Party shall bear sole responsibility and liability for any security incidents and personal data breaches involving the Forwarded Personal Data, commencing from the moment the data enters transit, upon reaching and including the Point of Porting, and extending to all subsequent Processing activities conducted by the Receiving Party.

5.3. To protect the rights and interests of Data Subjects as well as the Transmitting Party, the Receiving Party shall advise the Transmitting Party's Data Protection Officer within seventy-two (72) hours about any of the following events affecting the Forwarded Personal Data:

5.3.1. Upon the Receiving Party's notification of a Notifiable Personal Data Breach; and/or

5.3.2. Where applicable, upon the Receiving Party's reporting of a Reportable Major Cyber-Related Incident.

The information contained in the advice shall include, but not limited to: (a) detailed description of the Notifiable Personal Data Breach and/or Reportable Major Cyber-Related Incident, as well as a copy of the filed notification and/or report; (b) affected Forwarded Personal Data; (c) assessment of impact; (d) measures taken to mitigate; (e) risks and vulnerabilities identified; (f) proposed action to be taken to address the breach and reduce the harm or negative consequences of the breach; (g) other details that will allow the Transmitting Party to assess its corresponding duties, responsibilities, and obligations under the law, if any.

5.4. The Receiving Party shall continue to apprise the Transmitting Party of any additional information related to the Notifiable Personal Data Breach and/or Reportable Major Cyber-Related Incident, which may become available after the initial advice mentioned in Article 5.3. The Receiving Party shall also provide further details and actions taken on the Notifiable Personal Data Breach and/or Reportable Major Cyber-Related Incident, as may be requested by the Transmitting Party. The Receiving Party shall also advise the Transmitting Party of any report, notification, or compliance it submits to any governmental authority in relation to the Notifiable Personal Data Breach and/or Reportable Major Cyber-Related Incident. The Receiving Party shall inform the Transmitting Party of any inquiry, hearing or governmental action taken against it in relation to the Notifiable Personal Data Breach and/or Reportable Major Cyber-Related Incident.

5.5. The Receiving Party shall immediately provide all necessary and relevant information and documentation to enable the Transmitting Party, if necessary, to file a written report with the relevant governmental authorities, or respond to their inquiries as may be required by law.

5.6. If required by law, the Parties shall cooperate and assist each other in any investigation, mitigation, and

remediation that they shall reasonably determine to be necessary, and address the cause of the Notifiable Personal Data Breach and/or Reportable Major Cyber-Related Incident, as well as the possible harm and negative consequences to them and to the affected Data Subjects. Further, they shall undertake immediate action to prevent a repeated occurrence of the same.

5.7. The Parties must maintain strict confidentiality regarding any Notifiable Personal Data Breach and/or Reportable Major Cyber-Related Incident. The Receiving Party is prohibited from discussing such matters with any third party not bound by this DFTC, except where allowed or mandated by law or explicitly authorized in writing by the Transmitting Party.

5.8. The Receiving Party's exposure to a Notifiable Personal Data Breach, a Reportable Major Cyber-Related Incident, or an ongoing investigation by any government authority allows the Transmitting Party to suspend this DFTC. This suspension will be effective immediately upon the Transmitting Party's notification and will remain in place until the Receiving Party submits a certification from an independent professional expert confirming the completion of remediation measures and/or clearance of any liability by the relevant governmental authorities.

5.9. For the avoidance of doubt, nothing in this article shall establish a joint PIC status or responsibility between the Transmitting Party and the Receiving Party. The Receiving Party shall be deemed the sole PIC of the Forwarded Personal Data from the moment it enters transit, upon reaching the Point of Porting, and for all subsequent Processing activities, continuing through and beyond the completion of the Porting process.

ARTICLE 6. PERSONNEL OF PARTIES

6.1. The Receiving Party shall warrant and ensure that all its Personnel, who has access to the Forwarded Personal Data, receives and Processes the same in accordance with this DFTC and Applicable Data Protection Law.

6.2. The Receiving Party shall ensure that its Personnel engaged in the receipt and Processing of the Forwarded Personal Data are informed of and understand the confidential nature of the Forwarded Personal Data, including the operational details of its receipt and Processing, and are subject to obligations of confidentiality. Such obligations of confidentiality shall survive the termination of that Personnel's engagement or relationship with the Receiving Party.

6.3. The Receiving Party shall ensure that only specifically designated Personnel shall Process the Forwarded Personal Data and only for the purpose set out in this DFTC. The Receiving Party shall keep a record of the names of its Personnel who have access to the Forwarded Personal Data and the type of Forwarded Personal Data that was transmitted to them. The Receiving Party shall immediately make such records available to the Transmitting Party upon request.

6.4. The Receiving Party shall implement strict access management and controls to the Forwarded Personal Data and the Point of Porting. The Receiving Party shall ensure the following:

6.4.1. Grant of administrative access and privileges only to specific Personnel necessary for the Processing of the Forwarded

Personal Data. Only the Receiving Party's specifically designated Personnel may process the Forwarded Personal Data in the Point of Porting;

6.4.2. Disabling of any function, applications, and services that are not necessary for the Processing under this DFTC;

6.4.3. If the mode of transmission and access to the Point of Porting requires the issuance of a credential, each credential shall be assigned on an individual basis. Credentials shall not be shared to or used by another Personnel; and

6.4.4. Regular review of access rights and immediate revocation of access when Personnel no longer requires it or has terminated their engagement or relationship with the Receiving Party.

6.5. Failure of the Receiving Party to implement the required controls shall be considered a material breach under this DFTC and shall be a cause for termination under Article 10.3.2.

ARTICLE 7. DISCLOSURE TO THIRD PARTIES

7.1. The Receiving Party assumes all responsibilities and liabilities in connection with, as a result of, its sharing or disclosure of the Forwarded Personal Data to any third party, including its subprocessors.

7.2. The Receiving Party warrants and confirms that it has conducted the appropriate due diligence of its PIPs prior to engagement, and that such PIPs have provided all the necessary assurances and guarantees that they have adequate organizational, technical, and physical security measures to protect the Forwarded Personal Data. These security measures should not be less rigorous than accepted industry practices and applicable standards for information security, privacy, and data protection.

7.3. The Receiving Party shall be fully responsible for the acts or omissions of its PIPs and the PIP's agents, representatives and personnel, which shall be deemed, as far as the Transmitting Party is concerned, to be the acts or omissions of the Receiving Party itself. This responsibility attaches upon the initiation of, throughout, and until the completion of the Forwarding process. If any act or omission by a PIP or its agents, representatives and personnel causes claims or liabilities to be brought against the Transmitting Party, the Transmitting Party shall have the right to seek indemnification from the Receiving Party in accordance with this DFTC.

ARTICLE 8. LIABILITY AND INDEMNIFICATION

8.1. The Receiving Party shall be deemed the sole PIC of, and shall bear exclusive liability and accountability for, the Forwarded Personal Data from the moment it enters transit, upon reaching the Point of Porting, and for all subsequent Processing activities, continuing through and beyond the completion of the Porting process.

8.2. Pursuant to the foregoing, the Receiving Party shall be solely responsible and liable for its acts and omissions and that of its PIPs and Personnel in relation to the Forwarded Personal Data. There shall be no joint and several liability between the Parties.

8.3. The Receiving Party shall indemnify and hold harmless the Transmitting Party and its Personnel, in relation to the Forwarded Personal Data from the

moment it enters transit, against any and all forms of losses, including but not limited to claims, damages, liabilities, fines, sanctions, interests, penalties, and costs. These also encompass charges, expenses, compensation, *ex gratia* payments, costs to protect goodwill, and reasonable legal fees, all calculated on a full indemnity basis for each case, unless otherwise agreed upon by the Parties. This indemnity covers issues arising from complaints of Data Subjects, investigations by the Commission, and demands of other government entities or third parties, attributable to any of the following reasons:

8.3.1. any breach by Receiving Party, its PIPs or Personnel, of obligations under this DFTC, the relevant Schedule of Forwarded Personal Data, or violation of Applicable Data Protection Law;

8.3.2. unauthorized sharing, porting, disclosure, and/or Processing of the Forwarded Personal Data, as well as other illegal acts and omissions of the Receiving Party, its PIPs, or Personnel; and/or

8.3.3. bad faith, negligence, or wilful misconduct by the Receiving Party, its PIPs, or Personnel, in accessing, receiving, sharing, porting, disclosing to third parties, and/or Processing the Forwarded Personal Data.

8.4. The Receiving Party further acknowledges that it has full responsibility and liability over the Point of Porting, regardless of who has ownership, license, and/or custody over it. As such, the Receiving Party warrants and guarantees that it shall indemnify and hold harmless Transmitting Party from and against any and all costs, claims, liabilities, damages, or expenses arising from or related to the Receiving Party's use of the Point of Porting or other related services of the Transmitting Party to enable the Porting. This indemnity includes, without limitation, any claims related to the Porting, migration, loss, destruction, alteration, unauthorized disclosure of, or access to the Forwarded Personal Data.

ARTICLE 9. RETENTION PERIOD

9.1. As the PIC of the Forwarded Personal Data, the Receiving Party shall ensure that it sets the appropriate retention period pursuant to the Applicable Data Protection Law.

9.2. As the PIC, the Receiving Party shall cause the deletion of the Forwarded Personal in the Point of Porting in accordance with its own retention period. As the PIC, the Receiving Party shall bear full responsibility for any Processing of the Forwarded Personal Data done inside the Point of Porting.

ARTICLE 10. TERM, AMENDMENTS, AND TERMINATION

10.1. This DFTC, and its relevant amendments, shall constitute the entire agreement between the Parties with respect to the applicable Schedule of Forwarded Personal Data.

10.2. This DFTC, and its relevant amendments, shall commence on the Effective Date corresponding to the earliest start date among all the completed Schedules of Forwarded Personal Data and will remain in effect until the expiration of the Schedule of Forwarded Personal Data with the latest End Date, unless it is earlier terminated by the Parties. Each Schedule of Forwarded Personal Data within this DFTC is governed by its own Effective Date and End Date, and the expiration of any individual Schedule of Forwarded

Personal Data will terminate all Porting, disclosure and/or Processing activities associated with that particular schedule. However, this termination does not affect the ongoing Porting, disclosure and/or Processing activities under any other active Schedule of Forwarded Personal Data within this DFTC.

10.3. This DFTC or the relevant Schedule of Forwarded Personal Data, may be terminated through any of the following:

10.3.1. By mutual written agreement of the Parties;

10.3.2. By any Party, in case of material breach by the other Party of the terms and provisions of this DFTC ("**Erring Party**").

As used herein a "**material breach**" refers to a Party's failure to perform, or who has made or makes any inaccuracy in, or otherwise breaches any of its obligations, covenants, or representations under this DFTC that serves to defeat its purpose. In such an event, a Party may immediately cause the extrajudicial termination of this DFTC by means of a written notice to the Erring Party, without further liability or obligation to the Erring Party and without prejudice to other remedies available to it under the law;

For the avoidance of doubt, a material breach of the DFTC, shall include, but not be limited to, the violation of any of the provisions on the following:

10.3.2.1. Incident Management and Breach Notification; and

10.3.2.2. Personnel of Parties.

10.3.3. By any Party, for any valid reason and at any time, provided that the relevant Party is given a thirty (30)-calendar day prior written notice;

10.3.4. By any Party after determining, or upon a finding by the Commission, that termination is necessary to preserve and protect the rights of Data Subjects; or

10.3.5. Upon a finding by the Commission that the Porting of the Forwarded Personal Data is: (a) no longer necessary for the specified purposes and its objectives have already been achieved; or (b) that it is detrimental to national security, public interest, or public policy.

10.4. GCash reserves the right to amend this DFTC periodically and at any time. Any Schedule of Forwarded Personal Data executed after the effective date of a new DFTC shall be governed by the terms of that amended DFTC, subject to a maximum applicability period of two (2) years. For previously executed Schedules of Forwarded Personal Data, the Porting of Forwarded Personal Data shall continue to be governed by the version of the DFTC in effect at the time those schedules were executed, unless:

10.4.1. The governing DFTC has been effective for a maximum of two (2) years;

10.4.2. Amended by mutual agreement of the Parties;

10.4.3. Required by changes in applicable laws or regulations; or

10.4.4. Mandated by a governmental authority.

ARTICLE 11. DISPUTE RESOLUTION

11.1. The Parties shall exert good faith efforts to first resolve any dispute, controversy, difference, or claim arising out of or relating to this DFTC, including the existence, validity, interpretation, performance, breach, or termination thereof, or any dispute regarding non-contractual obligations arising out of or relating to it ("**Data Privacy Dispute**") by escalating it to their respective higher levels of management ("**Escalation Notice**").

11.2. If the Data Privacy Dispute continues unresolved for a period of fifteen (15) calendar days from the Escalation Notice, such dispute shall be exclusively referred to and finally resolved by arbitration.

11.2.1. Unless otherwise agreed upon by the Parties in the Main Agreement:

11.2.1.1. the arbitration shall be administered by the Philippine Dispute Resolution Center, Inc. ("**PDRCI**") in accordance with the PDRCI Administered Arbitration Rules ("**Rules**") for the time being in force, which rules are deemed incorporated by reference to this clause;

11.2.1.2. the seat of arbitration shall be Taguig City, Philippines;

11.2.1.3. the tribunal shall consist of one (1) arbitrator;

11.2.1.4. the arbitration proceedings shall be conducted in English; and

11.2.1.5. the law of this arbitration agreement shall be the laws of the Republic of the Philippines.

For the avoidance of doubt, any reference in the Main Agreement and/or its annexures concerning the resort to local courts shall be disregarded. Data Privacy Disputes shall be exclusively referred to and finally resolved by arbitration.

11.2.2. The arbitral tribunal shall maintain the confidentiality of the arbitration and conduct the arbitration in an impartial, practical and expeditious manner, giving each Party sufficient opportunity to present its case.

11.2.3. The Parties undertake to keep confidential all awards and orders in their arbitration as well as all materials in the arbitral proceedings created for the purpose of the arbitration and all other documents produced by another party in the arbitral proceedings not otherwise in the public domain, save to the extent that disclosure is required of a Party by a legal duty, to protect or pursue a legal right or to enforce or challenge an award in legal proceedings before a judicial authority.

11.2.4. Unless otherwise agreed upon by the Parties in the Main Agreement, any notice required

with respect to arbitration should be addressed to the general counsel of each of the Parties, or their designated alternative in their absence, as per the most current information provided in writing by the relevant Party. Notices should be sent to the address of the relevant Party mentioned in the Main Agreement, or any subsequent address provided in writing by the respective Party.

ARTICLE 12. MISCELLANEOUS PROVISIONS

12.1. **Confidentiality.** All matters covered by, and related, necessary, or incidental to this DFTC, including all forms, reports, notifications, and communications between the Parties, as well as company policies, procedures, and instructions shared between them, shall remain strictly confidential, unless otherwise required to be disclosed by applicable law, by agreement of Parties, or in relation to the resolution of disputes between the Parties.

12.2. **Legal Capacity of Representatives.** Each Party represents and warrants to the other that its representatives have accomplished all forms and documents necessary to this DFTC, on its behalf, and that they are duly authorized and have the legal capacity required under applicable law to bind the respective Party.

12.3. **Assignment.** Neither Party may assign this DFTC nor any of their rights or obligations herein without the other Party's written consent.

12.4. **Separability Clause.** If any provision of this DFTC is illegal or unenforceable, its invalidity shall not affect the other provisions of this DFTC that can be given effect without such invalid provision. If any provision of this DFTC 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.

12.5. **Governing Law of this DFTC.** Unless otherwise agreed upon by the Parties in the Main Agreement, this DFTC is to be construed and interpreted in accordance with the laws of the Republic of the Philippines, without reference to its conflict of law principles.

12.6. **Counterparts.** This DFTC may be executed in any number of counterparts, each of which is an original, but all of which together constitute one and the same agreement.

[APPENDICES FOLLOW]

APPENDIX

[FORM OF SCHEDULE OF FORWARDED PERSONAL DATA]

Schedule No. ___

In accordance with the Data Forwarding Terms and Conditions ("**DFTC**") effective on [Date], the latest copy of which is available at https://www.new.gcash.com/data-privacy-agreement/dftc, the Parties hereby affirm and agree to the following terms and conditions outlined in this Schedule of Forwarded Personal Data ("Schedule"):

ARTICLE 1. PROJECT DETAILS

1.1. Name of Project ("Project"): _____.

1.2. Effective Date of Project ("Effective Date"): _____.

1.3. End Date of Project ("End Date"): _____.

ARTICLE 2. PURPOSE AND TYPES OF PERSONAL DATA

2.1. The objective of the Porting of the Forwarded Personal Data is to enable Data Subjects to exercise their right to Data Portability, in relation to their access or use of the following products or services of Receiving Party _____.

Forwarded Personal Data	Type of Personal Data	Purpose	Requested Format, File Naming Convention, and Mode of Porting
[KYC details (including government issued IDs)]	*[Sensitive personal data]*	*[Opening a bank account]*	*[JSON and XML; KYC_File 1, API]*

2.2. The Receiving Party affirms that it shall not sell, lease, license, or otherwise commercially exploit any Forwarded Personal Data received in connection with this Schedule. The Receiving Party further affirms that such data shall not be used, processed, or incorporated, in whole or in part, for the development, training, or enhancement of any artificial intelligence (AI) systems, machine learning models, or similar technologies of the Receiving Party or any third party. Any failure to adhere to this commitment shall constitute a material breach of the DFTC, entitling the Transmitting Party to immediate remedies, including but not limited to injunctive relief and termination of this Agreement.

ARTICLE 3. OPERATIONAL DETAILS

3.1. Below is a brief description of the operational details of the Porting:

[Please provide description of the how the Porting is initiated and what product or service will utilize the Forwarded Personal Data]

ARTICLE 4. DATA PROTECTION OFFICER

	G-Xchange, Inc.		[Insert information]
Name:	John Roy Robert Real, Jr.	Name:	[please insert information]
Email:	privacy@gcash.com	Email:	[please insert information]
Address:	W Global Center 9th Avenue corner 30th Street Bonifacio Global City, Taguig City Metro Manila, Philippines	Address:	[please insert information]

In case of any change in the details of their respective Data Protection Officers set out above, both Parties undertake to notify the other Party in writing at least thirty (30) calendar days before the effectivity of any such change.