# DATA REQUEST 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 Requested 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 Protection Officer** refers to the same term as contemplated under Philippine Data Protection Law.

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

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

1.6. **Forwarding** refers to the process of transferring, forwarding, or sending of a copy of the Requested Personal Data by the Transmitting Party to the Requesting Party in response to a Request. The Forwarding process is deemed complete upon the delivery by the Transmitting Party of the Requested Personal Data to the Point of Transfer.

1.7. **GFI** refers to Globe Fintech Innovations, Inc., one of the Parties in this DRTC.

1.8. **Non-Commercial Purpose** refers to the Processing of Personal Data for objectives such as the detection, monitoring, investigation, and analysis of threats, fraud, and crimes. This includes, but is not limited to, activities carried out in compliance with the following laws and regulations:

1.8.1. **Anti-Money Laundering Act (R.A. 9160, as amended)** – among others, for the prevention, detection, and investigation of money laundering and related offenses

1.8.2. **Terrorism Financing Prevention and Suppression Act (R.A. 10168)** – among others, to combat terrorism financing and associated criminal activities.

1.8.3. **Data Privacy Act of 2012 (R.A. 10173)** – among others, for lawful monitoring and investigation of data breaches, unauthorized processing, and other violations.

1.8.4. **Cybercrime Prevention Act of 2012 (R.A. 10175)** – among others, to address cyber-related offenses, including online fraud, hacking, and identity theft.

1.8.5. **Revised Penal Code (Act No. 3815)** – among others, for the investigation of crimes such as fraud, forgery, and related offenses.

1.8.6. **Anti-Trafficking in Persons Act of 2003 (R.A. 9208, as amended by R.A. 10364)** – among others, to monitor and report human trafficking activities, including online exploitation.

1.8.7. **Anti-Violence Against Women and Their Children Act of 2004 (R.A. 9262)** – among others, to detect and address threats and crimes involving violence against women and children.

1.8.8. **Anti-Child Pornography Act of 2009 (R.A. 9775)** – among others, for the monitoring and investigation of crimes involving the exploitation of children.

1.8.9. **National ID System Act (R.A. 11055)** – among others, to safeguard the integrity of personal data in the national ID system and prevent identity fraud.

1.8.10. **Anti-Terrorism Act of 2020 (R.A. 11479)** – among others, to prevent, detect, and suppress terrorism and related financial crimes.

1.8.11. **Anti-Financial Account Scamming Act (AFASA, R.A. 12010)** – among others, to prevent and address scams involving financial accounts and unauthorized access to financial data.

1.8.12. All other applicable laws and regulations.

Such Non-Commercial Purpose also encompasses other similar threats, fraud, and crimes as referred to in relevant rules and regulations issued by governmental agencies or as agreed upon by the Parties. This definition excludes purposes that solely benefit or serve the private interest or advantage of any Party.

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

1.10. **Party** individually refers to Transmitting Party and Requesting Party, and **Parties** collectively refer to Transmitting Party and Requesting Party.

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

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

1.13. **Personal Data Request** refers to a continuing arrangement between the Transmitting Party and Requesting Party, where the Transmitting Party Forwards the Requested Personal Data to the Requesting Party.

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

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

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

1.17. **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.

1.18. **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.

1.19. **Point of Transfer** refers to the Requesting Party's designated storage or repository that facilitates the Requesting Party's ability to retrieve, control, or otherwise engage with the Requested Personal Data.

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

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

1.22. **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:

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

1.22.2. involved a system-level compromise (i.e., attacks on Transmitting Party's core systems, as opposed to phishing attempts of individual clients);

1.22.3. affected a significant number of customer accounts simultaneously;

1.22.4. involved significant data loss or massive data breach;

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

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

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

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

1.23. **Request** refers to the solicitation or request made by the Requesting Party for the Transmitting Party to Forward Personal Data pursuant to a Non-Commercial Purpose.

1.24. **Requested Personal Data** refers to the copies of the Personal Data of Data Subjects Requested by the Requesting Party for a Non-Commercial Purpose, subject to the terms and conditions set forth in this document.

1.25. **Requesting Party** refers to the Party who receives the Requested Personal Data from the Transmitting Party.

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

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

1.28. **Transmitting Party** refers to the Party who Forwards the Requested Personal Data upon the Request of the Requesting Party.

## ARTICLE 2. SCHEDULE OF REQUESTED PERSONAL DATA

2.1. To facilitate the Forwarding of the Requested Personal Data between the Parties, the Requesting Party shall provide a *Schedule of Requested Personal Data*. The Requesting Party shall provide the Transmitting Party with a clear, specific, and documented Request. The Request shall be detailed in the Schedule of Requested Personal Data and shall include:

2.1.1. The specific Non-Commercial Purpose;
2.1.2. The required types of Personal Data and their intended purposes;
2.1.3. The period covered, if applicable;
2.1.4. The naming conventions and file formats to be used;
2.1.5. The designated Point of Transfer;
2.1.6. The mode of Forwarding, including the required security measures to safeguard the data during transit (e.g., encryption, secure transfer protocols); and
2.1.7. Any other necessary information to enable the Transmitting Party to Process the Personal Data in accordance with Applicable Data Protection Law and to facilitate the Non-Commercial Purpose stated by the Requesting Party.

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

2.2. Each Schedule of Requested Personal Data shall be accomplished using the template appended to this DRTC (the "**Schedule of Requested 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 Requested Personal Data.

2.3. Should there be a renewal, supplement, or amendment to the Schedule, or if there are additional Non-Commercial Purpose/s that are not covered by an existing Schedule, the Parties shall accomplish a new Schedule of Requested Personal Data in accordance with this article. All accomplished schedules shall be annexed to and form an integral part of this DRTC.

## ARTICLE 3. RESPONSIBILITIES OF THE PARTIES

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

3.1.1. The Forwarding of Requested Personal Data shall be made only in accordance with the Request of the Requesting Party for the stated Non-Commercial Purpose/s.

3.1.2. This DRTC does not establish a joint PIC status or responsibility between the Transmitting Party and the Requesting Party.

3.1.3. The Receiving Party shall be the sole PIC of the Requested Personal Data from the moment it enters transit, upon reaching the Point of Transfer, and for all subsequent Processing activities, continuing through and beyond the

completion of the Forwarding process. The Transmitting Party shall act solely as a facilitator of the data forwarding and shall not retain any control over or responsibility for the Requested Personal Data during or after the forwarding. The Transmitting Party expressly disclaims any role in determining the purposes or means of Processing the Requested Personal Data during transit or any subsequent Processing by the Requesting Party.

3.1.4. They shall abide and comply with the principles of transparency, legitimate purpose, and proportionality under Applicable Data Protection Law in Forwarding and Processing the Requested Personal Data.

3.1.5. This DRTC 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 DRTC shall also be provided to Data Subjects upon the latter's written request and in accordance with Applicable Data Protection Law.

3.1.6. The Data Protection Officer of the Requesting Party shall be the first port of call for questions about the Requested 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 Requested Personal Data Forwarded to the Requesting Party, the Transmitting Party shall be the PIC of the Personal Data of Data Subjects it has initially collected, stored, or Processed.

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

3.2.3. When applicable, 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.

3.2.4. The Transmitting Party shall Forward the Requested Personal Data on an "as is" basis without warranty of any kind, except that the Requested 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 Requested Personal Data, including all implied warranties, completeness, and fitness for the Requesting Party's particular purpose.

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

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

The Transmitting Party is not liable for any errors and omissions in the Requested Personal Data, or decisions made by the Requesting Party in light of such data.

3.3.2. It shall ensure that all Requested 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 Requested Personal Data during transit. The Transmitting Party shall facilitate the use of such mechanisms as reasonably required by the Requested Party, but assumes no liability for any breach or loss once the data is in transit

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

3.3.4. It shall employ data minimization so that the Requested Personal Data is limited to only those that are necessary for the stated Non-Commercial Purpose and compatible with this DRTC and the relevant Schedule of Requested 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 Requested Personal Data and within the context of the Non Commercial Purpose.

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

3.4. The Transmitting Party reserves the right to charge the Requesting Party reasonable administrative costs in instances where the Request is burdensome or costly. For purposes of this provision, the determination of whether a Request is burdensome or costly shall take into account factors such as the volume and complexity of the Requested Personal Data; the frequency of similar Requests received from the Requesting Party; the technical or operational effort required to process the Request; and any other circumstances that may reasonably affect the effort and cost involved. The Transmitting Party shall inform the Requesting Party in advance of any administrative costs to be charged and provide a detailed explanation of the basis for such costs. The Requesting Party may choose to revise or withdraw the Request upon receipt of such notice.

3.5. Nothing in this DRTC shall be construed to prevent the Transmitting Party from

declining to process a Request that is manifestly unfounded, excessive, or otherwise incompatible with applicable laws or regulations.

## ARTICLE 4. DATA SUBJECT REQUESTS AND COMPLAINTS

4.1. The Requesting Party shall be responsible for upholding the rights of Data Subjects over the Requested Personal Data, under the Applicable Data Protection Law. The Requesting 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 Requested Personal Data, including those arising during the Requested Personal Data's transit, can be made by submitting a written request to the Requesting Party's Data Protection Officer.

## ARTICLE 5. INCIDENT MANAGEMENT AND BREACH NOTIFICATION

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

5.2. The Requesting Party shall bear sole responsibility and liability for any Security Incidents and Personal Data Breaches involving the Requested Personal Data, commencing from the moment the Requested Personal Data enters transit, upon reaching and including the Point of Transfer, and extending to all subsequent Processing activities conducted by the Requesting Party.

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

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

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

The information contained in the advice shall include but not be 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 Requested Personal Data; (c) assessment of impact; (d) measures taken to mitigate the impact of the breach or incident; (e) risks and vulnerabilities identified; (f) proposed action to be taken to address the breach or incident and reduce the harm or negative consequences of the breach or incident; (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 Requesting 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 Requesting 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 Requesting 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 Requesting 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 Requesting 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 Requesting Party is prohibited from discussing such matters with any third party not bound by this DRTC, except where allowed or mandated by law or explicitly authorized in writing by the Transmitting Party.

5.8. The Requesting 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 DRTC. This suspension will be effective immediately upon the Transmitting Party's notification and will remain in place until the Requesting 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 Requesting Party. The Requesting Party shall be deemed the sole PIC of the Requested Personal Data from the moment it enters transit, upon reaching the Point of Transfer, and for all subsequent Processing activities, continuing through and beyond the completion of the Forwarding process.

## ARTICLE 6. PERSONNEL OF PARTIES

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

6.2. The Requesting Party shall ensure that its Personnel engaged in the receipt and Processing of the Requested Personal Data are informed of and understand the confidential nature of the Requested 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 Requesting Party.

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

6.4. The Requesting Party shall implement strict access management and controls to the Requested Personal Data and the Point of Transfer. The Requesting Party shall ensure the following:

6.4.1. Grant of administrative access and privileges only to specific Personnel necessary for the Processing of the Requested Personal Data. Only the Requesting Party's specifically designated Personnel may process the Requested Personal Data in the Point of Transfer;

6.4.2. Disable any function, applications, and services in the Point of Transfer that are not necessary for the Processing under this DRTC;

6.4.3. If the mode of transmission and access to the Point of Transfer 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 Requesting Party.

6.5. Failure of the Requesting Party to implement the required controls shall be considered a material breach under this DRTC and shall be a cause for termination under Article 10.2.2.

## ARTICLE 7. DISCLOSURE TO THIRD PARTIES

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

7.2. The Requesting 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 Requested 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 Requesting 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 Requesting Party in accordance with this DRTC.

## ARTICLE 8. LIABILITY AND INDEMNIFICATION

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

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

8.3. The Requesting Party shall defend, indemnify, and hold harmless the Transmitting Party and its Personnel, in relation to the Requested 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 Requesting Party, its PIPs or Personnel, of obligations under this DRTC, the relevant Schedule of Requested Personal Data, or violation of Applicable Data Protection Law;

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

8.3.3. bad faith, negligence, or wilful misconduct by the Requesting Party, its PIPs, or Personnel, in receiving, sharing, Forwarding, disclosing to third parties, and/or Processing the Requested Personal Data.

8.4. The Requesting Party further acknowledges that it has full responsibility and liability over the Point of Transfer, regardless of who has ownership, license, and/or custody over it. As such, the Requesting 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 Requesting Party's use of the Point of Transfer or other related services of the Transmitting Party to enable the Forwarding. This indemnity includes, without limitation, any claims related to the transfer, migration, loss, destruction, alteration, unauthorized disclosure of, or access to the Requested Personal Data.

## ARTICLE 9. RETENTION PERIOD

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

shall not process and retain the Requested Personal Data longer than necessary.

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

## ARTICLE 10. TERM, AMENDMENTS, AND TERMINATION

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

10.2. This DRTC, and its relevant amendments, shall commence on the Effective Date corresponding to the earliest start date among all the completed Schedules of Requested Personal Data and will remain in effect until the Schedule of Requested Personal Data with the latest End Date, unless it is earlier terminated by the Parties. Each Schedule of Requested Personal Data within this DRTC is governed by its own Effective Date and End Date, and the expiration of any individual Schedule of Requested Personal Data will terminate all Forwarding, disclosure and/or Processing activities associated with that particular schedule. However, this termination does not affect the ongoing Forwarding, disclosure and/or Processing activities under any other active Schedule of Requested Personal Data within this DRTC.

10.3. This DRTC or the relevant Schedule of Requested 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 DRTC ("**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 DRTC that serves to defeat its purpose. In such an event, a Party may immediately cause the extrajudicial termination of this DRTC 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;

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

10.4.1. The governing DRTC 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 DRTC, 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 :

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 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, 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 stated address of the relevant Party, 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 DRTC, 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 DRTC, 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 DRTC nor any of their rights or obligations herein without the other Party's written consent.

12.4. **Separability Clause.** If any provision of this DRTC is illegal or unenforceable, its invalidity shall not affect the other provisions of this DRTC that can be given effect without such invalid provision. If any provision of this DRTC 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 DRTC.** Unless otherwise agreed upon by the Parties, this DRTC 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 DRTC 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 REQUESTED PERSONAL DATA]**

**Schedule No. ___**

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

**ARTICLE 1. DETAILS OF THE REQUEST**

| | | | |
|---|---|---|---|
| 1. | **Details of Authorized Representative of Requesting Party** | **Company:** | |
| | | **Name of Representative:** | |
| | | **Designation:** | |
| | | **Email Address:** | |
| | | **Mobile Number:** | |
| 2. | **Purpose of the Request:**<br><br>*(Note: Kindly provide information as to the necessity of the requested personal data in relation to the incident.)* | | |
| 3. | **Request is for the filing of a complaint or defense of a legal claim**<br><br>(*Note: Check all that apply*) | | Anti-Money Laundering Act (R.A. 9160) |
| | | | Terrorism Financing Prevention and Suppression Act (R.A.10168) |
| | | | Data Privacy Act of 2012 (R.A. 10173) |
| | | | Cybercrime Prevention Act of 2012 (R.A. 10175) |
| | | | Access Devices Regulation Act (R.A. 8484) |
| | | | Revised Penal Code (Act. No. 3815) |
| | | | Anti-Trafficking in Persons Act of 2003 (R.A. 9208, as amended by R.A. 10364) |

| | | | |
|---|---|---|---|
| | | | Anti-Violence Against Women and Their Children Act of 2004 (R.A. 9262) |
| | | | Anti-Child Pornography Act of 2009 (R.A. 9775) |
| | | | Anti-Online Sexual Abuse or Exploitation of Children (OSAEC) and Anti-Child Sexual Abuse or Exploitation Materials (CSAEM) Act (R.A. 11930) |
| | | | National ID System Act (R.A. 11055) |
| | | | Anti-Terrorism Act of 2020 (R.A. 11479) |
| | | | Anti-Financial Account Scamming Act (AFASA, R.A. 12010) |
| | | | Others:<br><br>Please specify:_____. |
| 5. | **Request is for internal investigation purposes only.**<br><br>(*Note: Check all that apply*) | | Detection, monitoring, analysis of threats |
| | | | Detection, monitoring, analysis of attacks |
| | | | Detection, monitoring, analysis of suspicious transactions |
| | | | Detection, monitoring, analysis of scams and phishing |
| | | | Detection, monitoring, analysis of other fraudulent activities |

The Requesting Party expressly warrants and represents that all information, statements, and materials to be provided in connection with its request/s are true, accurate, and complete. The Requesting Party further warrants that the request is made in good faith and is not based on any false, misleading, or fraudulent claims, representations, or omissions. The Requesting Party acknowledges that any breach of this warranty may result in the rejection of the request, termination of any related agreement, and any other remedies available under law or equity.

**ARTICLE 2. REQUESTED PERSONAL DATA**

| Category of Personal Data | Category of Data Subjects | Purpose |
|---|---|---|
| | | |
| | | |

The Requesting Party affirms that it will not sell, lease, license, or otherwise commercially exploit any Requested Personal Data received in connection with this Schedule. The Requesting Party further affirms that such data will 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 Requesting Party or any third party. Any failure to adhere to this commitment shall constitute a material breach of the DRTC, entitling the Transmitting Party to immediate remedies, including but not limited to injunctive relief and termination of this Agreement.

**ARTICLE 3. RETENTION PERIOD**

The Retention Period of the Requested Personal Data under this Schedule shall be for the period indicated below. However, this shall be without prejudice to the retention of Personal Data if the retaining party is required under the law or by court/administrative order to preserve such Personal Data, or if the retention is pursuant to the prosecution or defense of any present claims.

| | |
|---|---|
| **Start Date:** | |
| **End Date:** | |

**ARTICLE 4. REQUESTING PARTY INSTRUCTIONS AND OPERATIONAL DETAILS**

For Requesting Party to provide the information below:

| | |
|---|---|
| **Format of the Requested Personal Data** | ☐ *Written* ☐ *Electronic* ☐ *Recorded* |
| **Period Covered (if applicable)** | *(e.g. date of transaction)* |
| **Naming Conventions** | *(Note: Requesting Party Sample of naming conventions of files formats to be used if format will be Electronic or Recorded)* |
| **Mode of Forwarding** | *(Note: Requesting Party information on mode of Forwarding)* |
| **Designated Point of Transfer** | *(Note: Requesting Party's designated storage or repository that will facilitate the Requesting Party's retrieval, control, or otherwise engage with the Requested Personal Data)* |
| **Required Security Measures to be applied** | *(e.g. encryption, secure transfer protocols, etc.)* |
| **Other Instructions:** | Others:<br><br>Please specify:_____. |
| **Description of the** | *(Please provide a description of the how the Forwarding is initiated and what product or service will utilize the Requested Personal Data)* |

| | |
|---|---|
| **Forwarding** | |

**ARTICLE 5. DATA PROTECTION OFFICER**

| | Globe Fintech Innovations, Inc. | | [Insert Information] |
|---|---|---|---|
| Name: | John Roy Robert Real, Jr. | Name: | [please insert information] |
| Email: | gfi.dataprivacy@mynt.xyz | Email: | [please insert information] |
| Address: | W Global Center<br>9th Avenue corner 30th Street<br>Bonifacio Global City, Taguig City<br>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.