Data Privacy Manual

MUFG Bank, Ltd.

Manila Branch

As of August 2023

MUFG Bank Ltd. Manila Branch
Data Privacy Manual

Table of Contents

.

I. Background

Republic Act No. 10173, also known as the Data Privacy Act of 2012 (DPA), aims to protect personal data in information and communications systems both in the government and the private sector.

It ensures that entities or organizations processing personal data establish policies, and implement measures and procedures that guarantee the safety and security of personal data under their control or custody, thereby upholding an individual's data privacy rights. A personal information controller or personal information processor is instructed to implement reasonable and appropriate measures to protect personal data against natural dangers such as accidental loss or destruction, and human dangers such as unlawful access, fraudulent misuse, unlawful destruction, alteration and contamination.

To inform its personnel of such measures, each personal information controller or personal information processor is expected to produce a Privacy Manual. This Manual serves as a guide or handbook for ensuring the compliance of MUFG with the DPA, its Implementing Rules and Regulations (IRR), and other relevant issuances of the NPC. It also encapsulates the privacy and data protection protocols that need to be observed and carried out within MUFG for specific circumstances (e.g., from collection to destruction), directed toward the fulfillment and realization of the rights of data subjects.

II. Introduction

This Privacy Manual is hereby adopted in compliance with Republic Act No. 10173 or the Data Privacy Act of 2012 (DPA), its Implementing Rules and Regulations, and other relevant policies, including issuances of the National Privacy Commission. MUFG respects and values your data privacy rights, and makes sure that all personal data collected from you, our clients and customers, are processed in adherence to the general principles of transparency, legitimate purpose, and proportionality.

This Manual shall inform describe MUFG's data protection and security measures, and may serve as data subjects guide in exercising their rights under the DPA.

In addition this Manual also makes reference and provides guidance (for the benefit of customers from the European Union) on compliance to the European Union's General Data Protection Regulation.

III. DEFINITION OF TERMS

Data Privacy Act or DPA refers to Republic Act No. 10173 or the Data Privacy Act of 2012 and its implementing rules and regulations.

Data Subject refers to an individual whose Personal Information, Sensitive Personal Information, or Privileged Information is processed. It may refer to authorized signatories of MUFG customers, officers, employees, consultants, and clients of MUFG.

GDPR refers to the European Union's General Data Protection Regulation

MUFG refers to **MUFG BANK LTD. Manila Branch**.

NPC refers to the **National Privacy Commission.**

Personal Data collectively refers to Personal Information, Sensitive Personal Information, and Privileged Information.

Personal Information refers to any information, whether recorded in a 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.

Processing refers to any operation or 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.

Privacy Impact Assessment refers to a process undertaken and used to evaluate and manage the impact on privacy of a particular project, program, process or measure.

Privileged Information refers to any and all forms of Personal Data, which, under the Rules of Court and other pertinent laws constitute privileged communication.

Security Incident is 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.

Sensitive Personal Information refers to Personal Data:

1. About an individual's race, ethnic origin, marital status, age, color, and religious, philosophical or political affiliations;

2. About an individual's health, education, genetic or sexual life, 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;

3. 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

4. Specifically established by an executive order or an act of Congress to be kept classified.

IV. Scope and Limitations

All personnel of MUFG, regardless of the type of employment or contractual arrangement, must comply with the terms set out in this Privacy Manual.

The relevant portions of procedures issued by the Global Compliance Division related to GDPR shall be suppletorily applicable and implemented by MUFG.

V. Processing of Personal Data

A. Collection (e.g. type of data collected, mode of collection, person collecting information, etc.)

- MUFG collects the basic contact information of clients and customers, including the personal information of individual representatives' full name, address, email address, contact number, etc. The Relationship Managers, Account Assistants and Transactors attending to customers will collect such information through accomplished bank forms. MUFG's HRD likewise collects personal information and sensitive personal information from employment applicants and new employees.

B. Use

- Personal data collected shall be used by MUFG from data subjects for Know Your Customer (KYC) compliance, credit documentation purposes, for Know Your Employee requirements, etc.

C. Storage, Retention and Destruction (e.g. means of storage, security measures, form of information stored, retention period, disposal procedure, etc.)

- MUFG will ensure that personal data under its custody are protected against any accidental or unlawful destruction, alteration and disclosure as well as against any other unlawful processing. MUFG will implement appropriate security measures in storing collected personal information, depending on the nature of the information. All information gathered shall not be retained for a period longer than MUFG's approved retention period for personal information. After the expiration of the approved retention period, all hard and soft copies of personal information shall be disposed and destroyed, through secured means.

D. Access (e.g. personnel authorized to access personal data, purpose of access, mode of access, request for amendment of personal data, etc.)

- Due to the sensitive and confidential nature of the personal data under the custody of MUFG, only the client and their authorized representative shall be allowed to access such personal data, for any purpose, except for those contrary to law, public policy, public order or morals.
- Employees shall be allowed to access their personal data at reasonable times of the day and upon submission of a prior written request to MUFG's Human Resources Department ("HRD").

E. Disclosure and Sharing (e.g. individuals to whom personal data is shared, disclosure of policy and processes, outsourcing and subcontracting, etc.)

- All employees and personnel of MUFG shall maintain the confidentiality and secrecy of all personal data that come to their knowledge and possession, even after resignation, termination of contract, or other contractual relations. Personal data under the custody of MUFG shall be disclosed only pursuant to a lawful purpose, and to authorized recipients of such data.

VI. Security Measures

MUFG shall implement reasonable and appropriate physical, technical and organizational measures for the protection of personal data. Security measures aim to maintain the availability, integrity and confidentiality of personal data and protect them against natural dangers such as accidental loss or destruction, and human dangers such as unlawful access, fraudulent misuse, unlawful destruction, alteration and contamination. In this section, you give a general description of those measures.

A. TECHNICAL SECURITY MEASURES

The DPO, with the cooperation and assistance of Systems Office for Asia – Philippines ("ASO-PH"), shall continuously develop and evaluate MUFG's security policy with respect to the Processing of Personal Data. The security policy should include the following minimum requirements:

a. safeguards to protect MUFG's computer network and systems against accidental, unlawful, or unauthorized usage, any interference which will affect data integrity or hinder the functioning or availability of the system, and unauthorized access;

b. the ability to ensure and maintain the confidentiality, integrity, availability, and resilience of MUFG's data processing systems and services;

c. regular monitoring for security breaches, and a process both for identifying and accessing reasonably foreseeable vulnerabilities in MUFG's computer network and system, and for taking preventive, corrective, and mitigating actions against security incidents that can lead to a Personal Data breach;

d. the ability to restore the availability and access to Personal Data in a timely manner in the event of a physical or technical incident;

e. a process for regularly testing, assessing, and evaluating the effectiveness of security measures; and

f. encryption of Personal Data during storage and while in transit, authentication process, and other technical security measures that control and limit access thereto.

B. ORGANIZATIONAL SECURITY MEASURES

1. Data Protection Officer

A Data Protection Officer ("DPO") shall be appointed by MUFG. The functions and responsibilities of the DPO shall particularly include, among others:

a) monitor MUFG's compliance with the DPA, its IRR, issuances by the NPC and other applicable laws and policies. For this purpose, the DPO may:

    1. collect information to identify the processing operations, activities, measures, projects, programs, or systems of MUFG, and maintain a record thereof;
    2. analyze and check the compliance of processing activities, including the issuance of security clearances to and compliance by third-party service providers;
    3. inform, advise, and issue recommendations to MUFG;
    4. ascertain renewal of accreditations or certifications necessary to maintain the required standards in personal data processing; and
    5. advice MUFG as regards the necessity of executing a Data Sharing Agreement with third parties, and ensure its compliance with the law;

b) ensure the conduct of Privacy Impact Assessments relative to activities, measures, projects, programs, or systems of MUFG;
c) advice MUFG regarding complaints and/or the exercise by data subjects of their rights (e.g., requests for information, clarifications, rectification or deletion of personal data);

d) ensure proper data breach and security incident management by MUFG, including the latter's preparation and submission to the NPC of reports and other documentation concerning security incidents or data breaches within the prescribed period;
e) inform and cultivate awareness on privacy and data protection within MUFG, including all relevant laws, rules and regulations and issuances of the NPC;
f) advocate for the development, review and/or revision of policies, guidelines, projects and/or programs of MUFG relating to privacy and data protection, by adopting a privacy by design approach;
g) serve as the contact person of MUFG vis-à-vis data subjects, the NPC and other authorities in all matters concerning data privacy or security issues or concerns and the PIC or PIP;
h) cooperate, coordinate and seek advice of the NPC regarding matters concerning data privacy and security; and
i) perform other duties and tasks that may be assigned by MUFG that will further the interest of data privacy and security and uphold the rights of the data subjects.

2. Compliance Officer for Privacy

A Compliance Officer for Privacy ("COP") shall likewise be appointed by MUFG. Except for items (a) to (c), a COP shall perform all other functions of a DPO, specifically for MUFG's Global Services Operations Center. Where appropriate, the COP shall act as the deputy and assist the DPO in the performance of the latter's functions.

3. Data Privacy Principles

All Processing of Personal Data within MUFG should be conducted in compliance with the following data privacy principles as espoused in the Data Privacy Act:

a. ***Transparency.*** The Data Subject must be aware of the nature, purpose, and extent of the Processing of his or her Personal Data by MUFG, including the risks and safeguards involved, the identity of persons and entities involved in Processing his or her Personal Data, his or her rights as a Data Subject, and how these can be exercised. Any information and communication relating to the Processing of Personal Data should be easy to access and understand, using clear and plain language.

b. ***Legitimate purpose.*** The Processing of Personal Data by MUFG shall be compatible with a declared and specified purpose which must not be contrary to law, morals, or public policy.

c. ***Proportionality.*** The Processing of Personal Data shall be adequate, relevant, suitable, necessary, and not excessive in relation to a declared and specified purpose. Personal Data shall be processed by MUFG only if the purpose of the Processing could not reasonably be fulfilled by other means.

.

4. Data Processing Records

Adequate records of the MUFG's Personal Data Processing activities shall be maintained at all times. The DPO, with the cooperation and assistance of all the concerned business and service units involved in the Processing of Personal Data, shall be responsible for ensuring that these records are kept up-to-date. These records shall include, at the minimum:

1. information about the purpose of the Processing of Personal Data, including any intended future Processing or data sharing;

2. a description of all categories of Data Subjects, Personal Data, and recipients of such Personal Data that will be involved in the Processing;

3. general information about the data flow within MUFG, from the time of collection and retention, including the time limits for disposal or erasure of Personal Data;

4. a general description of the organizational, physical, and technical security measures in place within MUFG; and

5. the name and contact details of the DPO, Personal Data processors, as well as any other staff members accountable for ensuring compliance with the applicable laws and regulations for the protection of data privacy and security.

5. Management of Personal Data at HRD

The DPO, with the cooperation of MUFG's HRD shall develop and implement measures to ensure that all MUFG's staff that has access to Personal Data will strictly process such data in compliance with the requirements of the Data Privacy Act and other applicable laws and regulations. These measures may include drafting new or updated relevant policies of MUFG and conducting training programs to educate employees and agents on data privacy related concerns.

The DPO, with the assistance of HRD, shall ensure that MUFG shall obtain the employee's informed consent, evidenced by written, electronic or recorded means, to:

1. The Processing of his or her Personal Data, for purposes of maintaining MUFG's records; and

2. A continuing obligation of confidentiality on the employee's part in connection with the Personal Data that he or she may encounter during the

period of employment with MUFG. This obligation shall apply even after the employee has left MUFG for whatever reasons.

6. Data Collection Procedures

The DPO, with the assistance of the MUFG's HRD and all other departments of MUFG responsible for the Processing of Personal Data, shall document MUFG's Personal Data Processing procedures. The DPO shall ensure that such procedures are updated and that the consent of the Data Subjects (when required by the DPA or other applicable laws or regulations) is properly obtained and evidenced by written, electronic or recorded means.

Such procedures shall also be regularly monitored, modified, and updated to ensure that the rights of the Data Subjects are respected, and that Processing thereof is done fully in accordance with the DPA and other applicable laws and regulations.

7. Data Retention Schedule

Subject to applicable requirements of the DPA and other relevant laws and regulations, Personal Data shall not be retained by MUFG for a period longer than necessary and/or proportionate to the purposes for which such data was collected. The DPO, with the assistance of MUFG's HRD and all other departments of MUFG responsible for the Processing of Personal Data, shall be responsible for developing measures to determine the applicable data retention schedules, and procedures to allow for the withdrawal of previously given consent of the Data Subject, as well as to safeguard the destruction and disposal of such Personal Data in accordance with the DPA, MUFG's Information Security Standard Procedure (ISSP) and other applicable laws and regulations.

C. PHYSICAL SECURITY MEASURES

The DPO, with the assistance of HRD and ASO-PH shall develop and implement policies and procedures for MUFG to monitor and limit access to, and activities in, the offices of HRD, as well as any other departments and/or workstations in MUFG where Personal Data is processed, including guidelines that specify the proper use of, and access to, electronic media.

The design and layout of the office spaces and work stations of the abovementioned departments, including the physical arrangement of furniture and equipment, shall be periodically evaluated and readjusted in order to provide privacy to anyone Processing Personal Data, taking into consideration the environment and accessibility to unauthorized persons.

The duties, responsibilities, and schedules of individuals involved in the Processing of Personal Data shall be clearly defined to ensure that only the individuals actually performing official duties shall be in the room or work station, at any

given time. Further, the rooms and workstations used in the Processing of Personal Data shall, as far as practicable, be secured against natural disasters, power disturbances, external access, and other similar threats.

VII. Personal Data Breach and Security Incidents

A. Data Breach Notification

All employees and agents of MUFG involved in the Processing of Personal Data are tasked with regularly monitoring for signs of a possible data breach or Security Incident. In the event that such signs are discovered, the employee or agent shall immediately report the facts and circumstances to the DPO within twenty-four (24) hours from his or her discovery for verification as to whether or not a breach requiring notification under the Data Privacy Act has occurred as well as for the determination of the relevant circumstances surrounding the reported breach and/or Security Incident.

The DPO shall notify the NPC and the affected Data Subjects pursuant to requirements and procedures prescribed by the DPA. The notification to the NPC and the affected Data Subjects shall at least describe the nature of the breach, the Personal Data possibly involved, and the measures taken by MUFG to address the breach.

The notification shall also include measures taken to reduce the harm or negative consequences of the breach and the name and contact details of the DPO. The form and procedure for notification shall conform to the regulations and circulars issued by the NPC, as may be updated from time to time.

1. Creation of a Data Breach Response Team
   - A Data Breach Response Team led by the Data Protection Officer and the Compliance Officer for Privacy shall be responsible for ensuring immediate action in the event of a security incident or personal data breach. The team shall conduct an initial assessment of the incident or breach in order to ascertain the nature and extent thereof. It shall also execute measures to mitigate the adverse effects of the incident or breach.

2. Measures to prevent and minimize occurrence of breach and security incidents
   - MUFG shall regularly conduct a Privacy Impact Assessment to identify risks in the processing system and monitor for security breaches and vulnerability scanning of computer networks. Personnel directly involved in the processing of personal data must attend trainings and seminars for capacity building. There must also be a periodic review of policies and procedures being implemented in MUFG.

3. Notification procedure

- The Head of the Data Breach Response Team shall inform the Management of the need to notify the NPC and the data subjects affected by the incident or breach within the period prescribed by law. Management may decide to delegate the actual notification to the head of the Data Breach Response Team.

B. Breach Reports

All Security Incidents and Personal Data breaches shall be documented through written reports, including those not covered by the notification requirements. In the case of Personal Data breaches, a report shall include the facts surrounding an incident, the effects of such incident, and the remedial actions taken by MUFG. In other security incidents not involving Personal Data, a report containing aggregated data shall constitute sufficient documentation. These reports shall be made available when requested by the NPC. A general summary of the reports shall be submitted by the DPO to the NPC annually.

VIII. Inquiries and Complaints

MUFG employees may inquire or request for information regarding any matter relating to the processing of their personal data under the custody of MUFG, including the data privacy and security policies implemented to ensure the protection of their personal data. They may write to MUFG's DPO at dpo@ph.mufg.jp and briefly discuss the inquiry, together with their contact details for reference.

MUFG's customer complaints regarding Data Privacy concerns shall be filed in three (3) printed copies, or sent to dpo@ph.mufg.jp. The concerned department or unit shall confirm with the complainant its receipt of the complaint.

Every data subject has the right to reasonable access to his or her personal data being processed by the personal information controller or personal information processor. Other available rights include:

(1) right to dispute the inaccuracy or error in the personal data;

(2) right to request the suspension, withdrawal, blocking, removal or destruction of personal data; and

(3) right to complain and be indemnified for any damages sustained due to inaccurate, incomplete, outdated, false, unlawfully obtained or unauthorized use of personal data. Accordingly, there must be a procedure for inquiries and complaints that will specify the means through which concerns, documents, or forms submitted to the organization shall be received and acted upon. This section shall feature such procedure.

.

IX. Outsourcing and Subcontracting Agreements

Any Personal Data Processing conducted by an external agent or entity (third party service provider) on behalf of MUFG should be evidenced by a valid written contract with MUFG. Such contract should expressly set out the subject matter and duration of the Processing, the nature and purpose of the Processing, the type of Personal Data and categories of Data Subjects, the obligations and rights of MUFG Company, and the geographic location of the Processing under the contract.

The contract and the subcontracting contract shall include express stipulations requiring the external agent or entity (including the subcontractor) to:

A. process the Personal Data only upon the documented instructions of MUFG, including transfers of Personal Data to another country or an international organization, unless such transfer is required by law;

B. ensure that an obligation of confidentiality is imposed on persons and employees authorized by the external agent/entity and subcontractor to process the Personal Data;

C. implement appropriate security measures;

D. comply with the Data Privacy Act and other issuances of the NPC, and other applicable laws, in addition to the obligations provided in the contract, or other legal act with the external party;

E. not engage another processor without prior instruction from MUFG: Provided, that any such arrangement shall ensure that the same obligations for data protection under the contract or legal act are implemented, taking into account the nature of the Processing;

F. assist MUFG, 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;

G. assist MUFG in ensuring compliance with the Data Privacy Act and other issuances of the NPC, taking into account the nature of Processing and the information available to the external party who acts as a Personal Information Processor as defined under the Data Privacy Act;

H. at the choice of MUFG, delete or return all Personal Data to it after the end of the provision of services relating to the Processing: Provided, that this includes deleting existing copies unless storage is authorized by the Data Privacy Act or other applicable laws or regulations;

I. make available to MUFG all information necessary to demonstrate compliance with the obligations laid down in the Data Privacy Act, and allow for and contribute to audits, including inspections, conducted by MUFG or another auditor mandated by the latter; and

J. immediately inform MUFG if, in its opinion, an instruction violates the Data Privacy Act or any other issuance of the NPC.

X. Amendment of Registration Information

Changes in any of the following information shall require the amendment of MUFG's registration with the NPC:

1. Changes in the organization
    a. Bank name
    b. Address
    c. Contact number
2. Change of CH
    a. Name
    b. Email address
    c. Contact number
3. Change of Data Protection Officer
    a. Name
    b. Email address
    c. Telephone number
    d. Mobile number

Scan-Email the following documents to NPC at dporegistration@privacy.gov.ph:

1. Amendment Cover Letter[1] signed by DPO; and
2. Notarized DPO Registration Form[2] with supporting documents.

The DPO Registration Form must be filled-out digitally (this can be done with Adobe Reader or MS Edge). HANDWRITTEN FORMS WILL NOT BE ACCEPTED. Do not leave any blank fields, state N/A if the field is not applicable. The email address and Philippine cellphone number provided will be treated as the official contact channels. Select "Bank" and "Commercial Bank" as the applicable sectors on Pages 2 to 4 of the form.

XI. Effectivity

The provisions of this Manual are effective this 1st day of October, 2018, until revoked or amended by MUFG Bank Ltd, through a Management Resolution.

[1] https://www.privacy.gov.ph/wp-content/files/attachments/nwsltr/AmendmentDPOForm_CoverLetterTemplatev2.pdf

[2] https://www.privacy.gov.ph/wp-content/files/attachments/nwsltr/NPCformOrg_01-2019.pdf