REPUBLIC OF THE PHILIPPINES
DEPARTMENT OF FINANCE
BUREAU OF INTERNAL REVENUE
Quezon City

January 6, 2020

REVENUE MEMORANDUM ORDER No. 1-2020

SUBJECT : DATA PRIVACY MANUAL OF THE BUREAU OF INTERNAL REVENUE

TO : All Internal Revenue Officials and Employees and Others Concerned

---

Section 270 of the National Internal Revenue Code of 1997 (NIRC), as amended, provides that tax return information from taxpayers, be it individual or corporate, shall be held in strict confidence by the Bureau and shall not be divulged to third persons or to the public in general unless divulgence is allowed under the exceptions provided for therein.

The effectivity of Republic Act No. 10173 (RA 10173) or the Data Privacy Act of 2012 has extended and expanded the Bureau's mandate to secure such personal, sensitive personal information, privilege information as well as business information of individual taxpayers that have already been collected, or will still be collected, in the course of the performance of its official functions. The Act also requires that such information should be collected, processed and secured in adherence to the general data privacy principles of transparency, legitimate purpose and proportionality.

Relative hereto, the BIR Data Privacy Manual (Annex A) is hereby promulgated in order to prescribe the policies and guidelines for personal data protection and security in compliance with the Data Privacy Act of 2012 and inform users hereof of the rights of the data subjects. Henceforth, to ensure faithful compliance and observance of the BIR Data Privacy Manual, everyone is directed to read and be familiar with its provisions.

All concerned are hereby enjoined to be guided accordingly and give this Order as wide a publicity as possible.

This Order shall take effect immediately.

(Original Signed)
CAESAR R. DULAY
Commissioner of Internal Revenue

DATA PRIVACY MANUAL FOR BUREAU OF INTERNAL REVENUE

I. INTRODUCTION

The Bureau of Internal Revenue (BIR) is the premiere revenue collecting agency of the government. Its mandate is to raise revenue through collection of taxes and fees imposed by law to fund the socio-economic programs of the government for the benefit of the more than 100 million Filipinos here and abroad.

The mandate of the Bureau follows the State's policy contained in the Tax Reform For Acceleration and Inclusion (TRAIN) Law, to rationalize internal revenue tax system and tax administration. Attainment of this mandate would require a well-organized, failsafe and reliable profile of taxpayers, both natural and juridical.

The main source of the Bureau's collection comes from about 60 million taxpayers from all walks of life, more than 80% of which are individual taxpayers. All these taxpayers are readily identified individually upon their registration with the BIR and through periodic filing of tax returns wherein information obtained about their person and their earnings, business income and other sources of gain are reported.

Information from taxpayers, be it personal or corporate, are held in strict confidence by the Bureau and are strictly prohibited to be divulged to third persons, or to the public in general. Section 270 of the National Internal Revenue Code of 1997 (NIRC), as amended, imposes penalties upon each act or omission in violation thereof.

The effectivity of Republic Act No. 10173 (RA 10173) or the Data Privacy Act of 2012 has extended and expanded the Bureau's mandate to secure such personal, sensitive personal information, privilege information as well as business information of individual taxpayers that have already been collected, or will still be collected, in the course of the performance of its official functions. The Act also requires that such information are collected, processed and secured in adherence to the general principles of transparency, legitimate purpose and proportionality.

This Data Privacy Manual, prepared and circularized, specifically lays out the processes and procedures mandated by law in compliance with the requirements of the data privacy management and security.

II. DEFINITION OF TERMS

For consistency and uniformity in usage, the following terms are herein defined:

a. **"Act"** or **"DPA"** – refers to Republic Act No. 10173, also known as the Data Privacy Act of 2012;

b. **"Bureau"** refers to the Bureau of Internal Revenue;

c. "**Compliance Officer for Privacy" or "COP"** refers to an individual or individuals who shall perform some of the functions of a Data Protection Officer (DPO);

d. "**Conflict of Interest"** refers to a scenario wherein a DPO is charged with performing tasks, duties and responsibilities that may be opposed to or could affect his performance as DPO. This includes, *inter alia*, holding a position within the Personal Information Controller or Personal Information Processor that leads him to determine the purposes and the means of the processing of personal data;

e. **"Consent of the data subject"** refers to any freely given, specific, informed indication of will, whereby the data subject agrees to the collection and processing of his or her personal, sensitive personal, or privilege information. Consent shall be evidenced by written, electronic or recorded means. It may also be given on behalf of a data subject by a lawful representative or an agent specifically authorized by the data subject to do so;

f. **"Data subject"** refers to an individual whose personal, sensitive personal, or privileged information is processed; For purposes of this Manual, it refers to taxpayers, job applicants, current and past personnel parties to contracts, contractual and job order workers and other sources of personal information;

g. **"Data processing systems"** refers to the structure and procedure by which personal data is collected and further processed in an information and communications system or relevant filing system, including the purpose and the intended output of the processing;

h. **"Data sharing"** is the disclosure or transfer to a third party of personal data under the custody of a personal information controller or personal information processor. In the case data sharing made by the latter, such disclosure or transfer must have been upon the instructions of the personal information controller concerned. The term excludes outsourcing, or the disclosure or transfer of personal data by a personal information controller to a personal information processor;

i. **"Filing system"** refers to any set of information relating to natural or juridical persons to the extent that, although the information is not processed by equipment operating automatically in response to instructions given for that purpose, the set is structured either by reference to individuals or by reference to criteria relating to individuals, in such a way that specific information relating to a particular individual is readily accessible;

j. **"Information and communications system"** refers to a system for generating, sending, receiving, sorting, or otherwise processing electronic data messages or electronic documents, and includes the computer system or other similar device by which data is recorded, transmitted, or stored, and any procedure related to the recording, transmission, or storage or electronic data, electronic message, or electronic document;

k. **"Personal data**" refers to all types of personal information;

l. **"Personal data breach**" refers to a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored or otherwise processed;

m. **"Personal Data Sheet" or "PDS**" refers to the form prepared by the BIR officials and employees containing their personal information which is prepared and filed annually and on specified occasions such as upon hiring, promotion, transfer and other changes in employment status;

n. **"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;

o. **"Personal information controller" or "PIC**" refers to a natural or juridical person, or any other body who controls the processing of personal data, or instructs another to process personal data on its behalf.

There is control if the natural or juridical person or any other body decides on what information is collected, or the purpose or extent of its processing.

For purposes of this Manual, the Commissioner of Internal Revenue shall be automatically designated as the PIC.

p. **"Personal information processor" or "PIP"** refers to any natural or juridical person or any other body to whom a PIC may outsource or instruct the processing of personal data pertaining to a data subject;

q. **"Privacy by Design"** is an approach to the development and implementation of projects, programs, and processes that integrates into the latter's design or structure safeguards and are necessary to protect and promote privacy, such as appropriate organizational, technical and policy measures;

r. **"Privacy Impact Assessment"** is a process undertaken and used to evaluate and manage the impact on privacy of a particular project, program, process or measure;

s. **"Privileged information"** refers to any and all forms of data, which, under the rules of Court and other pertinent laws constitute privileged communication;

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

u. **"Profiling"** refers to any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyze or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behavior, location or movements;

v. **"Public authority"** refers to any government entity created by the Constitution or law, and vested with law enforcement or regulatory authority and functions;

w. **"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 have resulted to a personal data breach, if not for safeguards that have been put in place; and

x. **"Sensitive personal information**" refers to personal information:

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 of a person, or to any proceeding for any offense committed or alleged to have been committed by such individual, the disposal of such proceedings, or the sentence of any court in such proceedings;

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.

III. SCOPE AND LIMITATIONS

This Data Privacy Manual specifies the processing, security measures and assurance of security and confidentiality of personal data or information obtained in the performance of the Bureau's official functions mandated by law and inform users hereof of the rights of the data subjects.

All personnel of the BIR, therefore, regardless of the type of employment or contractual arrangements, must comply with the terms set out in this Data Privacy Manual.

IV. BIR DATA PRIVACY COMMITTEE

The Bureau shall constitute the Data Privacy Committee composed of the following groups/teams:

1. Executive Sponsors:
   Commissioner of the Internal Revenue
   Deputy Commissioner – Operations Group (OG)
   Deputy Commissioner – Resource Management Group (RMG)
   Deputy Commissioner – Legal Group (LG)
   Deputy Commissioner – Information Systems Group (ISG)

2. Data Protection Officer (DPO) – Deputy Commissioner – ISG

3. Compliance Officers on Privacy (COP) - a). National Office designate
   b). Regional Directors (Regional Offices)

   Assistant Compliance Officers (ACOP) - a). National Office designate
   b). Revenue District Officers (District offices)

4. Data Privacy Teams

   4.1. Privacy Impact Assessment (PIA) Team
   a. Existing Programs, Systems, Processes Group
   b. New Programs, Systems, Processes Group

   4.2 Privacy Management Program and Privacy Manual Team

   4.3 Incident Management Team

   4.4 Data Security and Physical Security Team

   4.5 Third Parties and Contracts Team

   4.6 Manage HR Team

The Commissioner, in his capacity as the Personal Information Controller (PIC) shall designate duly qualified personnel of the Bureau as lead and members of the teams and shall set forth their roles and responsibilities.

A. DATA PROTECTION OFFICER

The Data Protection Officer (DPO) shall be designated by the PIC or PIP who shall be accountable for ensuring the compliance by the PIC or PIP with the DPA, its IRR, issuances by the National Privacy Commission (NPC), and other applicable laws and regulations relating to privacy and data protection.

1. General Qualifications

The DPO shall possess specialized knowledge and demonstrate reliability necessary for the performance of his or her duties and responsibilities. As such, the DPO should have expertise in relevant privacy or data protection policies and practices. He/she should have sufficient understanding of the processing operations being carried out by the PIC or PIP, including the latter's information systems, data security and/or protection needs.

2. Position of the DPO or Compliance Officer on Privacy (COP)

The DPO or COP to be assigned by the PIC or PIP may be a career or appointive position. In the event that the position of DPO or COP is left vacant, the PIC or the PIP will provide for the appointment, reappointment or hiring of his or her replacement within a reasonable period of time. The PIC or PIP may also require the incumbent DPO or COP to occupy such position in a holdover capacity until the appointment or hiring of a new DPO or COP, in accordance with the PIC or PIP's internal policies and the provisions of the appropriate contract

The DPO or COP must be independent in the performance of his or her functions, and should be accorded a significant degree of autonomy by the PIC or PIP. In his or her capacity as DPO or COP, an individual may perform or be assigned to perform other tasks or assume other functions that do not give rise to any conflict of interest.

3. Duties and Responsibilities of the DPO and COP

3.1. The DPO shall:

3.1.1 Monitor the Bureau's compliance with the DPA, its IRR, issuances by the NPC and other applicable laws and policies. For this purpose, he or she may:

a. Collect information to identify the processing operations, activities, measures, projects, programs, or systems of the Bureau and/or its PIP, and maintain a record thereof;

b. Analyze and check the compliance of processing activities, including the issuance of security clearances to and compliance by third-party service providers;

c. Inform, advise, and issue recommendations to the PIC or PIP;

d. Ascertain renewal of accreditations or certifications necessary to maintain the required standards in personal data processing; and

e. Advise the PIC or PIP as regards the necessity of executing a Data Sharing Agreement with third parties, and ensure their compliance with the law.

3.1.2 Ensure the conduct of Privacy Impact Assessments relative to activities, measures, projects, programs, or systems of the Bureau or its PIP;

3.1.3 Advise the PIC or PIP regarding complaints and /or the exercise of data subjects of their rights (e.g., requests for information, clarifications, rectification or deletion of personal data);

3.1.4 Ensure proper data breach and security incident management by the PIC or PIP, 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;

3.1.5 Inform and cultivate awareness on privacy and data protection within the organization of the PIC or PIP, including all relevant laws, rules and regulations and issuances of the NPC;

3.1.6 Advocate for the development, review and/or revision of policies, guidelines, projects and/or programs of the PIC or PIP relating to privacy and data protection, by adopting a privacy by design approach;

3.1.7 Serve as the contact person of the PIC or PIP vis-à-vis data subjects, the NPC and other authorities in all matters concerning data privacy or security issues or concerns;

3.1.8 Cooperate, coordinate and seek advice of the NPC regarding matters concerning data privacy and security; and

3.1.9 Perform other duties and tasks that may be assigned by the PIC or PIP that will further the interest of data privacy and security and uphold the rights of the data subjects.

3.2. The Compliance Officers On Privacy (COP) and Assistant COPs shall:

3.2.1 Assume all of the above functions of the DPO, except for items a) to c) of the Duties and Responsibilities of the DPO, in their respective jurisdictions;

3.2.2 Cooperate, coordinate and seek advice from the DPO regarding matters concerning data privacy and security; and

3.2.3 Where appropriate, COPs shall assist the DPO in the performance of the latter's functions.

The DPO or COP must have due regard for the risks associated with the processing operations of the Bureau and/or its PIP, taking into account the nature, scope, context and purposes of processing. Accordingly, he or she must prioritize his or her activities and focus his or her efforts on issues that present higher data protection risks.

4. Protection of the DPO and COP

To strengthen the autonomy of the DPO or COP and to ensure the independent nature of his or her role in the organization, a PIC or PIP should not directly or indirectly penalize or dismiss the DPO or COP for performing his or her tasks. It is not necessary that the penalty is actually imposed or meted out. A mere threat is sufficient if it has the effect of impeding or preventing the DPO or COP from performing his or her tasks. However, nothing shall preclude the legitimate application of labor, administrative, civil or criminal laws against the DPO or COP, based on just or authorized grounds.

5. Weight of Opinion

The opinion of the DPO or COP must be given due weight. In case of disagreement, and should the PIC or PIP choose not to follow the advice of the DPO or COP, it is recommended, as good practice, to document the reasons therefor.

B. DATA PRIVACY TEAMS

The Data Privacy Teams shall have the following duties and responsibilities:

1. Privacy Impact Assessment (PIA) Team

1.1 Existing Programs, Systems and Processes

1.1.1 Conduct Privacy Impact Assessment (PIA)

a. Identify the "potential risk" of existing personal or sensitive personal information on the Bureau's systems;

b. Classify personal data by type (e.g. sensitive, confidential, public); and

c. Maintain flow charts for key data flows (e.g. between systems, between processes.

1.1.2 Submit PIA to DPO;

1.1.3 Monitor all phases of the PIA undertakings;

1.1.4 Record and maintain all documentations;

1.1.5 Organize and make all necessary arrangements for the Data Privacy meetings/presentations; and

1.1.6 Recommend actions/safeguards to ensure privacy/data protection on existing programs systems and processes.

1.2 New Programs, Systems and Processes

1.2.1 Monitor organizational practices to identify new processes or material changes to existing processes and ensure the implementation or Privacy by Design principles;

1.2.2 Conduct PIAs for new programs, systems and processes;

1.2.3 Maintain PIA guidelines and templates; and

1.2.4 Maintain a procedure to address data protection issues identified during PIAs.

2. Privacy Management Programs and Privacy Manual Team

2.1 Establish and formulate policies/procedures/manuals for personal data handling and collection and use of sensitive personal data;

2.2 Translate the DPA into a policy based on the Bureau's operations, types of personal data handled and the lifecycle of the personal data;

2.3 Develop processes for consent, withdrawal handling, data access request, complaints handling;

2.4 Establish and develop Privacy Notice that details the Bureau's personal data handling policies;

2.5 Obtain approval notices;

2.6 Conduct research on developments in law;

2.7 Maintain subscription to compliance reporting service/law firm updates to stay informed on new developments;

2.8 Attend/participate in privacy conferences, or think-tank events;

2.9 Record/report the tracking of new Rule Sources or amendments to Rule Sources;

2.10 Seek legal opinions regarding recent developments in laws; and

2.11 Review or participate in studies related to best practices in data privacy management.

3. Incident Management Team

3.1 Develop processes and procedures for incident and breach management;

3.2 Create an Incident and Data Breach Response Team to:

3.2.1 Ensure immediate action in the event of a security incident or personal data breach;

3.2.2 Conduct an initial assessment of the incident or breach in order to ascertain the nature and extent thereof; and

3.2.3 Execute measures to mitigate the adverse effects of the incident or breach.

3.3 Ensure procedure for recovery and restoration of personal data;

3.4 Ensure notification protocol wherein the head of the Incident and Data Breach Response Team shall inform the DPO of the need to notify the NPC and the data subjects affected by the incident or breach within the period prescribed by law; and

3.5 Ensure submission of detailed documentation of every incident or breach encountered, as well as an annual report, to be submitted to the DPO.

4. Data Security and Physical Security Team

4.1 Ensure that security measures are in place to maintain the availability, integrity and confidentiality of personal data;

4.2 Ensure that technical security measures are in place to make sure that there are appropriate and sufficient safeguards to secure the processing or personal data, particularly the computer network in place, including encryption and authentication processes that control and limit access;

4.3 Ensure use of an intrusion detection system to monitor security breaches and alert the Bureau of any attempt to interrupt or disturb the system;

4.4 Ensure that personnel with access to personal data shall verify his or her identity using a secure encrypted link and multi-level authentication;

4.5 Ensure that software applications are reviewed and evaluated before the installation in computers and devices;

4.6 Ensure conduct of vulnerability assessments and penetration testing within the Bureau on regular schedule; and

4.7 Ensure that personal data are protected against natural dangers such as accidental loss or destruction, and human dangers such as unlawful access, fraudulent misuse, unlawful destruction, alteration and contamination.

5. Third Party and Contracts Team

5.1 Maintain contracts and agreements with third-parties and affiliates consistent with the data privacy policy, legal requirements, and operations risk tolerance;

5.2 Maintain data privacy requirements for third parties (e.g. vendors, processors, and affiliates);

5.3 Maintain procedures to execute contracts or agreements with all processors;

5.4 Maintain a vendor data privacy risk assessment process;

5.5 Conduct due diligence around the data privacy and security posture of potential vendors/processors;

5.6 Maintain procedures to address instances of non-compliance with contracts and agreements;

5.7 Conduct ongoing due diligence around the data privacy and security posture of vendors/processors based on a risk assessment; and

5.8 Review long-term contracts for new or evolving data protection risks.

6. Manage HR Team

6.1 Conduct data privacy training needs analysis by position/job responsibilities;

6.2 Maintain a core training program for all employees;

6.3 Conduct training for newly appointed employees upon assignment to privacy-sensitive positions;

6.4 Conduct regular refresher training to reflect new developments;

6.5 Integrate data privacy into other training programs such as HR, security training etc.; and

6.6 Ensure that employees shall operate and hold personal data under strict confidentiality even after leaving public service, transferring to another position, or upon terminating their employment or contractual relations.

V. PROCESSING OF PERSONAL DATA

A. RECORDS OF PROCESSING ACTIVITIES

The Bureau shall maintain records that sufficiently describe its data processing system, and identify the duties and responsibilities of those individuals who will have access to personal data.

Records should include:

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 the organization, from the time of collection, processing, 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; and

5. The name and contact details of the personal information controller and where applicable, the joint controller, its representative, and the compliance officer or Data Protection Officer, or any other individual or individuals accountable for ensuring compliance with the applicable laws and regulations for the protection of data privacy and security.

The Bureau shall register its processing systems with NPC in accordance and in compliance with NPC issuances.

B. SOURCES OF PERSONAL DATA

The BIR requires certain persons to declare personal information as part of, and in compliance with, its official duties and functions and for certain undertakings with the public to form part of its files. The following constitutes the main sources of such information, including personal and sensitive information:

1. Taxpayers in general;

2. Job applicants seeking employment with this Bureau;

3. Current and past personnel and officials of this Bureau;

4. Parties entering into business contracts with the BIR;

5. Foreigners who are potential income earners or have business transactions in the Philippines who are required to register;

6. Contractual employees/Job Order workers; and

7. Personal information gathered by way of sharing of information

C. MODES OF DATA COLLECTION:

1. From Taxpayers:

   1.1 Registration by taxpayers and use of BIR online services;

   1.2 Filing of tax returns, business financial statements and other information certifications and information returns either on line or in hard copy;

   1.3 Contracts and agreements;

   1.4 Periodic examination of accounting books and records of business transactions;

   1.5 Access/gathering of information thru third party information programs;

1.6 Sharing of information with other government agencies;

1.7 Surveillance procedures; and

1.8 Arrest and seizures pursuant to Sec. 15, NIRC of 1997, as amended.

2. From Employees:

2.1 Interview of job applicants; and

2.2 Submission of Personal Data Sheet (PDS) and other related documents

D. COLLECTION OF PERSONAL INFORMATION

To ensure that the rights of the data subjects are fully protected, the BIR shall enforce the following policies and principles on personal data collection and management:

1. Collection must be for a declared, specified and legitimate purpose.

2. Data subject's consent must be obtained before collecting and processing the information subject to exemptions provided by the Act and other applicable laws and regulations. When consent is required, it must be time-bound in relation to the declared, specified and legitimate purpose;

3. The data subject must be provided specific information regarding the purpose and extent of processing including where applicable, the automated processing of his or her personal data for profiling or processing for direct marketing and data sharing;

4. Purpose should be determined and declared before, or as soon as reasonably practicable the data shall be collected; and

5. Personal information collected must be reasonably necessary or directly related to the Bureau's functions or purposes. Personal information shall not be collected in anticipation for future use ("just in case" it is needed).

Ideally, the purpose of such collection of information should be stated in the Personal Data Sheet and other requisite forms and the consent of the data subject shall be obtained through the forms, which must be filled out and signed by the data subject. However, since the Bureau's current PDS and other requisite forms do not yet contain said privacy statement/s, data subjects shall be required to sign a written document that includes a provision or a variation of the following privacy statements:

"All information shall be used by the BIR for legitimate purposes specifically for_____ and shall be processed by authorized personnel in accordance with the data privacy policies of the BIR."

"I hereby allow/authorize the BIR to use, collect and process the information for legitimate purposes specifically for _____, and allow authorized personnel to process the information."

E. USE OF PERSONAL INFORMATION

Personal data collected shall be used by the Bureau only for legitimate purposes and solely for evaluation, reportage and documentation purposes. The Bureau shall ensure that there is no manipulation of personal data and that the same shall not be used against any individual, unless required in the performance of its official functions and responsibilities.

Authorized revenue officials are allowed to access, use and process said personal data for legitimate purposes or that which is stated in the privacy statement contained in the documents signed by the personnel, job applicants and taxpayers, provided the following circumstances are present:

1. The employee, applicant or taxpayer has consented to the use or disclosure of said personal data, and

2. The employee, applicant or taxpayer would reasonably expect the Bureau through its authorized personnel to use or process personal information only for legitimate purposes.

   Examples are: Tax information of data subjects, such as business addresses, TIN, gross and taxable incomes, etc., shall be used only for legitimate purposes such as profiling of a taxpayer.

F. PROCESSING OF PERSONAL DATA

The following general principles shall govern the processing of personal data:

1. Personal data shall be processed fairly and lawfully. For processing to be lawful, any of the following conditions must be complied with:

   1.1 The data subject must have given his or her consent prior to the collection, or as soon as practicable and reasonable;

   1.2 The processing involves the personal information of a data subject who is a party to a contractual agreement, in order to fulfill obligations under the contract or to take steps at the request of the data subject prior to entering the said agreement;

   1.3 The processing is necessary for compliance with a legal obligation to which the personal information controller is subject;

   1.4 The processing is necessary to protect vitally important interests of the data subject, including his or her life and health;

   1.5 The processing of personal information is necessary to respond to national emergency or to comply with the requirements of public order and safety, as prescribed by law;

   1.6 The processing of personal information is necessary for the fulfillment of the constitutional or statutory mandate of a public authority; or

   1.7 The processing is necessary to pursue the legitimate interests of the personal information controller, or by a third party or parties to whom the data is disclosed, except where such interests are overridden by fundamental rights

and freedoms of the data subject, which require protection under the Philippine Constitution.

2. Processing shall uphold the rights of the data subject. It shall likewise be transparent, and allow the data subject sufficient information to know the nature and extent to processing;

3. Information provided to a data subject must always be in clear and plain language to ensure that they are easy to understand;

4. Processing must be in a manner compatible with declared, specified and legitimate purpose;

5. Processed personal data should be adequate, relevant, and limited to what is necessary in relation to the purpose for which they are processed;

6. Processing shall be undertaken in a manner that ensures appropriate privacy and security safeguards; and

7. Processing should ensure data quality. Inaccurate or incomplete data should be rectified, supplemented, destroyed or their further processing restricted.

G. VERIFICATION OF INFORMATION

Authorized Bureau personnel shall take reasonable steps to ensure that the collected personal data of personnel are up-to-date, complete, relevant and not misleading.

The Personnel Division shall conduct verification of employee information and background checks. The Revenue District Office, through its Client Support Section, is responsible for taxpayer record updates and modification of taxpayer information, correction, or update of information.

Employees may update their personal information through filling up of appropriate forms managed by the Personnel Division. For taxpayers, they may write or directly go to the concerned Revenue District Office to update their information.

In case of erroneous or false information, the employees or taxpayers may correct, rectify, block or erase such information using the same process.

H. STORAGE, RETENTION AND DESTRUCTION OF PERSONAL DATA

The Bureau shall ensure that personal data under its custody are protected against any accidental or unlawful destruction, alteration and disclosure. It shall implement appropriate security measures in storing collected personal information, depending on the nature of the information. The following policies/guidelines shall be observed:

1. Personal data shall not be retained longer than necessary

   1.1. for the fulfillment of the declared, specified, and legitimate purpose or when the processing relevant to the purpose has been terminated;

   1.2. for the establishment, exercise or defense of legal claims; or

   1.3. for legitimate business purposes, which must be consistent with standards followed by the applicable or approved by appropriate government agency.

2. Personal data originally collected for a declared, specified, or legitimate purpose may be processed further for historical, or statistical purposes, and, in cases laid down in law, may be stored for longer periods, subject to implementation of the appropriate organizational, physical and technical security measures required by the Act in order to safeguard the rights and freedoms of the data subject;

3. Personal data which is aggregated or kept in a form which does not permit identification of data subjects may be kept longer than necessary for the declared, specified, and legitimate purpose;

4. Personal data shall not be retained in perpetuity in contemplation of a possible future use yet to be determined. The Bureau shall retain personal data in its custody following the storage and retention period as provided in Revenue Memorandum Circular (RMC) No. 73-2008; and

5. Personal data shall be disposed or discarded in a secure manner that would prevent further processing, unauthorized access, or disclosure to any other party of the public, or prejudice the interests of the data subjects.

   The Bureau shall ensure that personal data shall be disposed of properly in a way that the same be unreadable (for paper) or irretrievable (for digital records). It shall include in its procedure the use of degaussers, erasers and physical destruction of devices to secure the disposal of computer equipment, disk servers, desktop computers and mobile phones at end-of-life.

I. CONFIDENTIALITY/DISCLOSURE OF INFORMATION

There shall be capacity building, orientation or training programs for all Bureau employees, agents or representatives, regarding privacy or security policies.

All employees and personnel of the Bureau and its agents or representatives shall maintain the confidentiality and secrecy of all personal data that come to their knowledge and possession, even after their resignation, termination of contract, or other contractual relations.

Personal data under the custody of the BIR shall be disclosed only pursuant to a lawful purpose, and only to authorized recipients of such data.

1. Sensitive personal information

Sensitive personal information may not be disclosed or processed, except in any of the following cases:

1.1 Consent is given by data subject, prior to the processing of the sensitive personal information or privileged information, which shall be undertaken pursuant to a declared, specified, and legitimate purpose of the Bureau;

1.2 The processing is necessary to protect the life and health of the data subject or another person, and the data subject is not legally or physically able to express his or her consent prior to the processing;

1.3 The processing is necessary to achieve the lawful and noncommercial objectives of the Bureau, provided that the processing is confined and related

to the bona fide employees of the Bureau; the sensitive personal information is not transferred to third parties; and consent of the data subject was obtained prior to processing;

1.4 The processing is necessary for the purpose of medical treatment: *Provided*, that it is carried out by a medical practitioner or a medical treatment institution, and an adequate level of protection of personal data is ensured; and

1.5 The processing concerns sensitive personal information or privileged information necessary for the protection of lawful rights and interests of natural or legal persons in court proceedings, or the establishment, exercise, or defense of legal claims, or when provided to government or public authority pursuant to a constitutional or statutory mandate.

2. Government-Related Use and Disclosures

Personal information is allowed to be used and disclosed to government agencies to satisfy reportorial requirements in line with their constitutionally or legislatively mandated functions pursuant to existing education or labor laws or when the use of pursuant to lawful order of a court or tribunal.

J. DATA SHARING

The Bureau shall enter into Data Sharing Agreements prior to any actual transfer of personal data or a copy from one party to another, such transfer shall comply with security requirements imposed by law.

1. Data sharing shall be allowed when it is expressly authorized by law: Provided, that there are adequate safeguards for data privacy and security, and processing adheres to principles of transparency, legitimate purpose and proportionality;

2. Data sharing between government agencies for the purpose of a public function or provision of a public service shall be covered by a data sharing agreement; and

3. The data sharing agreement shall be subject to review of NPC, on its own initiative or upon complaint of data subject.

K. NON-APPLICABILITY OF THE ACT TO CERTAIN PERSONAL INFORMATION

The Act and its Rules shall not apply to the following specified information, only to the minimum extent of collection, access, use, disclosure or other processing necessary to the purpose, function, or activity concerned:

1. Information processed for purpose of allowing public access to information that fall within matter of public concern, pertaining to:

    1.1 Information about any individual who is or was an officer or employee of the government that relates to his or her position or functions, including:

        1.1.1 The fact that the individual is or was an officer or employee of the government;

        1.1.2 The title, office address, and office telephone number of the individual;

1.1.3 The classification, salary range, and responsibilities of the position held by the individual; and

1.1.4 The name of the individual on a document he or she prepared in the course of his or her employment with the government.

1.2 Information about an individual who is or was performing a service under contract for a government institution, but only in so far as it relates to such service, including the name of the individual and the terms of his or her contract;

1.3 Information relating to a benefit of a financial nature conferred on an individual upon the discretion of the government, such as the granting or a license or permit, including the name of the individual and the exact nature of the benefit: Provided, that they do not include benefits given in the course of an ordinary transaction or as a matter of right;

2. Personal information processed for journalistic, artistic or literary purpose, in order to uphold freedom of speech, of expression, or of the press, subject to requirements of other applicable law or regulations;

3. Personal information that will be processed for research purposes, intended for a public benefit, subject to the requirements of applicable laws, regulations, or ethical standards;
4. Information necessary in order to carry out the functions of public authority, in accordance with a constitutionally or statutorily mandated function pertaining to law enforcement or regulatory function, including the performance of the functions of the independent, central monetary authority, subject to restrictions provided by law. Nothing in this privacy manual, however, shall be construed as having superior application over Republic Act No. 1405, otherwise known as the Secrecy of Bank Deposit Act; Republic Act No. 6426, otherwise known as the Foreign Currency Deposit Act; and Republic Act No. 9510, otherwise known as the Credit Information System Act (CISA); and

5. Personal Information originally collected from residents of foreign jurisdictions in accordance with the laws of those foreign jurisdictions, including any applicable data privacy laws, which is being processed in the Philippines. The burden of proving the law of the foreign jurisdiction falls on the person or body seeking exemption. In the absence of proof, the applicable law shall be presumed to be the Act and its Rules.

Provided that the non-applicability of the Act and of its Rules do not extend to the PIC or its PIP, who remain subject to the requirements of implementing security measures for personal data protection; Provided further, that the processing of the information provided in the preceding paragraphs shall be exempted from the requirements of the Act only to the minimum extent necessary to achieve the specific purpose, function, or activity.

VI. SECURITY MEASURES

The Bureau shall establish and implement reasonable and appropriate physical, technical, and organizational measures to ensure privacy and data protection. These security measures aim to regulate the collection, recording, organization, storage, updating or modification, retrieval, use, blocking an erasure or destruction of personal data, maintain the confidentiality, integrity and, availability of personal data and protect personal information and sensitive personal information (personal data) against natural dangers, such as accidental loss or destruction, and human dangers, such as unlawful access, unlawful divulgence, fraudulent issue, unlawful destruction, alteration, and contamination.

A. PHYSICAL SECURITY MEASURES

1. Format of Data

Personal data in the custody of the Bureau may be in digital/ electronic format and/ or paper-based/ physical format.

Officials/ employees are responsible for providing reasonable security for all information, documents and property entrusted to them.

2. Storage Type and Location

All personal data being collected and processed by the Bureau shall be stored in a secured facility, whether virtual or physical. Papers or physical documents bearing personal data shall be stored in locked filing cabinets/ room, access keys to which shall be entrusted only to authorized personnel. Digital or electronic documents containing personal data shall be stored in computers, portable disks, and other devices, provided either the document or the device where it is stored is protected by passwords or passcodes. Computers, portable disks and other devices used by the Bureau and its PIP/s in processing personal data shall be encrypted with the most appropriate encryption standard but which should not be lower than AES 250 encryption.

3. Access and Security Clearances

Only authorized personnel issued with security clearance by the Commissioner of Internal Revenue and PIP/s may access the personal data stored by the Bureau. The clearance shall be issued to personnel whose performance of official functions directly depends on such access or cannot otherwise be performed without such access.

4. Monitoring of Access

Access of personal data by all authorized personnel and employees whose request to access personal data were approved shall be monitored by the COP/ACOP concerned, or the Chief of Office concerned. All those who enter and access the storage/archive room of the Bureau must fill out and register in the logbook, which shall indicate the date, time, duration, and purpose of each access.

Access to the Bureau's data centers shall be restricted to personnel who have the appropriate security clearance.

Access to records and procedures shall be reviewed by DPO and COP regularly.

5. Design of Office Space and/ or Work Station

All offices specially those rendering front line services shall arrange their computers and tables with considerable spaces between them and a countertop positioned to prevent entry of visitors and/ or taxpayers to maintain the privacy and protect the processing of personal data. Posting of the appropriate signage “Restricted Area”, “No Entry”, “Unauthorized Person Not Allowed”, “Deposit your Firearm/s, Camera and/ or Mobile Phone with Camera at the Assigned Lobby Guard/s”, etc., and installation of CCTVs at strategic locations are essential to minimize risk of personal data breach and other security incident/s.

6. Use of Gadgets and Storage Devices

Confidentiality shall be observed and maintained at every stage of the data processing systems. Employees, whether authorized personnel or not, shall not be allowed to bring, connect and/ or use their own gadgets or storage devices of any form when processing personal data. Only prescribed devices properly configured to the Bureau’s security standards are authorized to access personal data.

7. Modes of Transfer of Personal Data within the Bureau or to Other Parties

Transfer of personal data *via* electronic mail shall use a secure email facility with encryption of the data, including any or all attachments. The Bureau shall ensure that the uses of portable media such as disk or USB drive to store or transfer Personal Data is encrypted. Personal data stored in paper files or any physical media shall be transmitted only thru registered mail or, where appropriate, authorized parcel post service. As much as possible, facsimile technology shall not be used to transmitting documents containing personal data.

B. TECHNICAL SECURITY MEASURES

1. Prevention and Monitoring for Security Breaches

The Bureau shall:

a. Use an intrusion detection and protection system to monitor security breaches and to be alert of any attempt to interrupt or disturb its information and communication system/s;

b. Use data leakage prevention software to establish rules for accessing sensitive information, keeping unauthorized users from sharing data maliciously;

c. Conduct security testing/vulnerability test to identify the weaknesses of a system in terms of data breaches or any other external attacks;

d. Protect the information systems from known vulnerabilities by applying the latest security patches recommended by the product vendors or implementing other compensating security measures. Prior to security patches, proper risk evaluation and testing should be conducted to minimize the undesirable effects to the information systems;

e. Perform at least once every two years, a security risk assessment for information systems and production applications shall be. A security risk assessment shall also be performed before production, and prior to major enhancements and changes associated with these systems or applications;

f. Perform periodic audit on information systems to ensure the compliance of IT security policies and effective implementation of security measures. The selection of auditors and conduct of audits shall ensure objectivity and impartiality of the audit process;

g. Maintain the integrity of an application with appropriate security measures such as version control mechanism and separation of environments for development, system testing, acceptance testing, and live operation. Change control procedures for requesting and approving program/system changes shall be documented;

h. Ensure observation and compliance by external service providers with BIR IT security policy provided in BIR Security Manual. BIR offices utilizing external services or facilities shall identify and assess the risks to the BIR data and business operations;

i. Document and implement security measures, service levels and management requirements of external services or facilities commensurate with the data classification and business requirements. The security responsibilities of external service providers shall be defined and agreed;

j. Monitor and review with external service providers to ensure that operations by external service providers are documented and managed properly. Confidentiality and non-disclosure agreements shall be properly managed, and reviewed when changes occur that affect the security requirement; and

k. Reserve audit and compliance monitoring rights to ensure external service providers have implemented sufficient controls on BIR information systems, facilities and data. Alternatively, the external service providers shall provide security audit report periodically to prove the measures put in place are satisfactory.

2. Security Features of the Software/s and Application/s Used

a. The Bureau shall procure and install effective and reliable antivirus software for all devices where personal data are stored, including laptops/tablets that regularly access the Internet. The Head of offices shall ensure that the antivirus software is updated and a system check is done periodically;

b. To ensure compatibility and data security, software applications shall be reviewed and evaluated by authorized technical personnel before utilization of computers and devices;

c. The Bureau shall use web application firewall to protect servers and databases from malicious online attacks; and

d. All systems shall be protected by both a host-based and a network-based firewall that allows only those connections necessary to fulfill the business of that system.

3. Regular Testing, Assessment and Evaluation of Security Measures

The Bureau shall:

a. Conduct periodic penetration testing of the firewall appliance from outside BIR premises and from within to conduct vulnerability assessment of the same;

b. Conduct regular monitoring to ensure that the comprehensive information security program is operating in a manner reasonably calculated to prevent unauthorized access to or unauthorized use of personal information and upgrading information security as necessary to limit risk;

c. Review scope of security measures at least annually or whenever there is material change in business practices that may reasonably implicate the security or integrity of records containing personal information; and

d. Document responsive actions taken in connection with any incident involving a breach of security, and mandatory post-incident review of events and action taken, if any, to make changes in business practices relating to protection of personal information.

4. Encryption, Authentication Process, and Other Technical Security Measures

4.1 Encryption – Proper encryption security controls shall be employed to protect sensitive data and data communication over wireless communications with connection to BIR internal network.

4.2 Authentication – Each personnel with access to personal data shall verify his/her identity using a secure encrypted link and multi-level authentication. Passwords or passcodes used to access data should be sufficient strength to deter password attacks. A password policy shall be strictly enforced.

5. Other Technical Security Measures -

The Bureau shall use other technical security measures to keep its software security tools up-to-date.

C. ORGANIZATIONAL SECURITY MEASURES

1. Contracts with Personal Information Processors (PIP)

The PIC through appropriate contractual agreements, shall ensure that its PIP, where applicable, shall also implement the security measures required by the Act and its Rules. It shall only engage those PIP that provide sufficient guarantees to implement appropriate security measures specified in the Act and its Rules, and ensure the protection of the rights of the data subject.

2. Privacy Impact Assessment (PIA)

A PIA should be undertaken for every processing system of the Bureau or its PIP that involves personal data. It may also be carried out vis-à-vis the entire organization with the involvement or participation of the different process owners and stakeholders.

A PIA should be conducted for both new and existing systems, programs, projects, procedures, measures, or technology products that involve or impact processing

personal data. For new processing systems, it should be undertaken prior to their adoption, use or implementation. Changes in the governing law or regulations, or those adopted within the organization or its industry may likewise require the conduct of a PIA, particularly if such changes affect personal data processing.

A PIC may require a PIP or a service provider to conduct a PIA. For this purpose, the report prepared by the PIP of the service or product provider may be considered by the PIC in determining whether the former is able to provide a comparable level of protection to the processing of personal data.

3. Control framework

A control framework is a comprehensive set of measures intended to address the risks identified in the privacy impact assessment. It includes organizational, physical and technical measures that maintain the availability, integrity and confidentiality of personal data and protect the latter against natural dangers such as accidental loss or destruction, and human dangers such as unlawful access, fraudulent misuse, unlawful destruction, alteration and contamination.

It includes nature of the personal data to be protected, risks represented by the processing, the size of the organization and complexity of its operations, current data privacy best practices and costs of security implementation

4. Privacy by Design

The Bureau shall consider data privacy in the design of its processing systems considering the following:

4.1 Purpose specification – seeks to ensure the maximum degree of privacy by ensuring that personal data are automatically protected in ICT systems and business practices;

4.2 Collection limitation – the collection of personal information must be fair, lawful and limited to that which is necessary for the specified purpose.

4.3 Data minimization –

a. the collection of personally identifiable information should be kept to a strict minimum;

b. by the design or programs, ICT, and systems should begin with non-identifiable interactions and transactions, as the default; and

c. whenever possible, identifiability, observability and linkability of personal information should be minimized.

4.4 Use, Retention and disclosure limitation – The use, retention and disclosure of personal information shall be limited to the purposes for which the individual has consented (unless required by law). Personal information shall be retained only as long as necessary to fulfill the stated purposes, and then securely destroyed.

D. SECURITY OF SENSITIVE PERSONAL INFORMATION IN GOVERNMENT

All sensitive personal information maintained by the Bureau shall be secured with the use of the most appropriate standard recognized by the information and communications technology industry, subject to the Rules and other issuances of NPC. The PIC and PIP shall be responsible for complying with the security requirements herein mentioned.

1. Access by the Bureau Personnel to Sensitive Personal Information

1.1 On-site and Online Access

1.1.1 No employee of the Bureau shall have access to sensitive personal information on government property or through online facilities unless the employee has received a security clearance from the head of the source agency. The source agency is the government agency which originally collected the personal data.

1.1.2 A source agency shall strictly regulate access to sensitive personal information under its custody or control, particularly when it allows online access. An employee of the government shall be granted a security clearance when the performance of the employee's official functions or the provision of a public service directly depends on and cannot otherwise be performed unless access to the personal data is allowed.

1.1.3 The online access allowed shall be subject to the following conditions:

a. An information technology governance framework has been designed and implemented;

b. Sufficient organizational, physical and technical security measures have been established;

c. The agency is capable of protecting sensitive personal information in accordance with data privacy practices and standards recognized by the information and communication technology industry; and

d. The employee of the government is only given on-line access to sensitive personal information necessary for the performance of official functions or the provision of a public service.

2. Off-site access

2.1 Sensitive personal information maintained by the Bureau may not be transported or accessed from a location off or outside of government property, whether by its agent or employee, unless the head of agency has ensure the implementation of privacy policies and appropriate security measures. A request for such transportation or access shall be submitted to and approved by the head of agency. The request must include proper accountability mechanisms in the processing of data.

2.2 The Commissioner or his representative shall approve request for off-site access in accordance with the following guidelines:

2.2.1 Deadline for Approval or Disapproval. The head of agency shall approve or disapprove the request within two (2) business days after the date of

submission of the request. Where no action is taken by the head of agency, the request is considered disapproved;

2.2.2 Limitation to One thousand (1,000) Records. Where a request is approved, the head of agency shall limit the access to not more than one thousand (1,000) records at a time, subject to the next succeeding paragraph; and

2.2.3 Use of Encryption. Any technology used to store, transport or access sensitive personal information for purposes of off-site access, shall be secured by the use of the most secure encryption standard recognized by the NPC.

3. Applicability to Government Contractors

In entering into any contract with a private service provider that may involve accessing or requiring sensitive personal information from the one thousand (1,000) or more individuals, the Bureau shall require such service provider and its employees to register their personal data processing system with NPC. The service provider, as PIP, shall comply with the other provisions of the Act and its Rules, similar to a government agency and its employees.

VII. DATA BREACH AND SECURITY INCIDENTS

Policies and procedures for the management of a personal data breach and security indents shall be developed and implemented.

1. Creation of an Incident and Data Breach Response Team

An Incident and Data Breach Response Team (IDBRT) shall be established by the Bureau which shall be responsible for ensuring immediate action in the event of a security incident or personal data breach to minimize impact and restore operations as quickly as possible. The team shall conduct an assessment of the incident or breach in order to ascertain the nature and extent thereof, recommend appropriate courses of action and prepare/submit the necessary communications and documentations.

2. Measures to prevent and minimize occurrence of breach incidents

The Bureau 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 or personal data must attend trainings and seminars for capacity building. There must be a periodic review of policies and procedures being implemented in the Bureau.

3. Procedure for recovery and restoration of personal data

The Bureau shall always maintain a backup file for all personal data under its custody. In the event of a security incident or data breach, it shall always compare the backup with the affected file to determine the presence of any inconsistencies or alterations resulting from the incident or breach.

4. Notification protocol

The leader of the Incident and Data Breach Response Team shall inform the DPO of the need to notify the NPC and the data subjects affected by the incident or breach within

the period prescribed by law. The Bureau may decide to delegate the actual notification to the leader of the Incident and Data Breach Response Team.

5. Documentation and reporting procedures of security incidents or a personal data breach

The Incident and Data Breach Response Team shall prepare a detailed documentation of every incident or breach encountered, as well as an annual report, to be submitted to the Bureau and the NPC, within the prescribed period.

a. NPC and the affected data subjects shall be notified by the personal information controller within seventy-two (72) hours upon knowledge of, or when there in reasonable belief by the PIC or PIP that, a personal data breach requiring notification has occurred;

b. Notification of personal data breach shall be required when sensitive personal information or any other information that may, under the circumstances, be used to enable identity fraud are reasonably believed to have been acquired by an unauthorized person, and the PIC believes that such unauthorized acquisition is likely to give rise to a real risk of serious harm to any affected data subject; and

c. Depending on the nature of the incident, or if there is delay or failure to notify, the NPC may investigate the circumstances surrounding the personal data breach. Investigations may include on-site examination of systems and procedures.

5.1 Contents of Notification

The notification shall at least describe the nature of the breach, the personal data possibly involved, and the measures taken to reduce the harm or negative consequences of the breach, the representatives of the personal information controller, including their contact details, from whom the data subject can obtain additional information about the breach, and any assistance to be provided to the affected data subjects.

5.2 Delay in Notification

Notification may be delayed only to the extent necessary to determine the scope of the breach, to prevent further disclosures, or to restore reasonable integrity to the information and communications system. The notification by the PIC may be dispensed with by the NPC when such notification would not be in the public interest, or in the interest of the affected data subject. The notification may be postponed where it may hinder the progress of a criminal investigation related to a serious breach.

5.3 Breach Report

5.3.1 The PIC shall notify the NPC by submitting a report, whether written or electronic, containing the required contest of notification. The report shall also include the name of a designated representative of the PIC, and contact details; and

5.3.2 All security incidents and personal data breaches shall be documented by the Incident and Data Breach Response Team 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 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 to the NPC annually.

5.4 Procedure for Notification

The procedure for breach notification shall be in accordance with the Act, its Rules, and any other issuance of the NPC.

VIII. RIGHTS OF THE DATA SUBJECT

1. Right to be Informed

1.1 The data subject has a right to be informed whether personal data pertaining to him or her shall be, are being, or have been processed, including the existence of automated decision-making and profiling.

1.2 The data subject shall be notified and furnished with information indicated hereunder before the entry of his or her personal data into the processing system of the personal information controller, or at the next practical opportunity:

1.2.1 Description of the personal data to be entered into the system;

1.2.2 Purpose for which they are being or will be processed, including processing for profiling or historical or statistical purposes;

1.2.3 Basis for processing, when processing is not based on the consent of the data subject;

1.2.4 Scope and method of the personal data processing;

1.2.5 The recipient or classes of recipients to whom the personal data are or may be disclosed;

1.2.6 Methods utilized for automated access, if the same is allowed by the data subject, and the extent to which such access is authorized, including meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject;

1.2.7 The identity and contact details of the personal data controller or its representative;

1.2.8 The period for which the information will be stored; and

1.2.9 The existence of their rights as data subjects, including the right to access, correction, and object to the processing, as well as the right to lodge a complaint before the Commission.

2. Right to Object

The data subject shall have the right to object to the processing of his or her personal data, including processing for automated processing or profiling. The data subject shall also be notified and given an opportunity to withhold consent to the processing in case of changes or any amendment to the information supplied or declared to the data subject in the preceding paragraph.

When a data subject objects or withholds consent, the Bureau shall no longer process the personal data, unless:

2.1 The personal data is needed pursuant to a subpoena;

2.2 The collection and processing are for obvious purposes, including, when it is necessary for the performance of or in relating to a contract or service to which the data subject is a party, or when necessary or desirable in the context of an employer-employee relationship between the Bureau and the data subject; or

2.3 The information is being collected and processed as a result of a legal obligation, and in the performance of the Bureau's official functions.

3. Right to Access

The data subject has the right to reasonable access to upon demand, the following:

3.1 Contents of his or her personal data that were processed;

3.2 Sources from which personal data were obtained;

3.3 Names and addresses of recipients of the personal data;

3.4 Manner by which such data were processed;

3.5 Reasons for the disclosure of the personal data to recipients, if any;

3.6 Information on automated processes where the data will, or is likely to be made as the sole basis for any decision that significantly affects or will affect that data subject;

3.7 Data when his or her personal data concerning the data subject were latest accessed and modified; and

3.8 The designation, name or identity, and address of the personal information controller.

4. Right to Rectification

The data subject has the right to dispute the inaccuracy or error in the personal data and have the personal information controller correct it immediately and accordingly, unless the request is vexatious or otherwise unreasonable. If the personal data has been corrected, the personal information controller shall ensure the accessibility of both the new and the retracted information and the simultaneous receipt of the new and the retracted information by the intended recipients thereof: Provided, that recipients or third parties who have previously received such processed personal data

shall be informed of its inaccuracy and its rectification, upon reasonable request of the data subject.

5. Right to Erasure or Blocking

The data subject shall have the right to suspend, withdraw or order the blocking, removal or destruction of his or her personal data from the personal information controller's filing system.

5.1 This right may be exercised upon discovery and substantial proof of any of the following:

5.1.1 The personal data is incomplete, outdated, false or unlawfully obtained;

5.1.2 The personal data is being used for purpose not authorized by the data subject;

5.1.3 The personal data is no longer necessary for the purposes for which they were collected;

5.1.4 The data subject withdraws consent or object to the processing and there is no other legal ground or overriding legitimate interest for the processing;

5.1.5 The personal data concerns private information that is prejudicial to the data subject, unless justified by freedom of speech, or expression, or of the press or otherwise authorized;

5.1.6 The processing is unlawful; and

5.1.7 The personal information controller or personal information processor violated the rights of the data subject.

5.2 The personal information controller may notify third parties who have previously received such processed personal information.

6. Right to Damages

The data subject shall be indemnified for any damages sustained due to such inaccurate, incomplete outdated, false, unlawfully obtained or unauthorized use of personal data, taking into account any violation of his or her rights and freedom as data subject.

7. Transmissibility of Rights of the Data Subject

The lawful heirs and assigns of the data subject may invoke the rights of the data subject to which he or she is an heir or an assignee, at any time after the death of the data subject, or when the data subject is incapacitated or incapable of exercising the rights as enumerated in the immediately preceding section.

8. Right of Data Portability

Where his or her data is processed by electronic means and in a structured and commonly used format, the data subject shall have the right to obtain from the personal information controller a copy of such data in an electronic or structured format that is commonly used and allows for further use by the data subject. The

exercise of this right shall primarily take into account the right of data subject to have control over his or her personal data being processed based on consent of contract, for commercial purpose, or through automated means. The NPC may specify the electronic format referred to above, as well as the technical standards, modalities, procedures and other rules for their transfer.

9. Limitation of Rights

The immediate preceding sections shall not be applicable if the processed personal data are used for the purpose of investigations in relation to any criminal, administrative or tax liabilities of a data subject. Any limitations on the rights of the data subject shall only be to the minimum extent necessary to achieve the purpose of said research or investigation. Provided, that the personal data shall be held under strict confidentiality and shall be used only for the declared purpose.

IX. INQUIRIES AND COMPLAINTS

Data subjects may inquire or request for information from the Bureau regarding any matter relating to the above rights and to the processing of their personal data under the custody of the Bureau, including the data privacy and security policies implemented to ensure the protection of their personal data.

Any request or inquiry relative to the foregoing shall be made in writing, briefly and clearly discussing the concern or inquiry, and indicating the full name and contact details of the data subject for reference. Written inquiries and/or requests shall be sent to the Data Protection Officer (DPO) or emailed at bir_dpo@bir.gov.ph. The DPO shall acknowledge receipt of such letter and take the necessary action on the same.

Any violation of the Bureau's data privacy policies, data privacy rights, or any breach, loss or unauthorized access or disclosure of personal information in the possession or under the custody of the Bureau may also be reported to the DPO. The report/complaint shall be made in writing and sent to the same contact details above.

The DPO shall verify the allegations in the complaint and shall conduct an investigation in cases of serious security breach as provided under the Act and its Implementing Rules and Regulations.

The DPO may recommend actions for the violation/s committed, particularly when such is serious or causes or has the potential to cause material damage to the Bureau or any of its clients or employees. Such recommendation shall be submitted to the Commissioner for approval. The Decision of the Commissioner may be appealed by the affected parties within 15 days from receipt of the Decision.

A. Handling of Complaints:

1. COP shall report periodically to DPO.

2. Complaints shall be received by/filed with the COP who shall conduct a local verification/investigation of the complaint. COP shall be assisted by Chief, DPD, Chief, Legal Division, Chief, Regional Investigation Division and a representative from the concerned RDO. Resolution shall be made in 10 days from filing of complaint.

3. If complaint cannot be resolved in the regional level, the complaint shall be forwarded to the DPO. A National Office committee composed of a

ACIR/HREA from the ISG, Chief, Legal Division and the Head of the NO Incident and Data Breach Response Team shall assist the DPO.

4. All investigations or verifications conducted by the NO or Regional COP shall be formally documented and filed with the NPC, if necessary.

5. DPO shall recommend changes in procedures/policies through local memorandum/issuances and/or RMO/RMCs to enhance, correct, revise existing procedures.

6. Persons/personnel liable shall be heard and investigated and shall be imposed statutory penalties. Civil, criminal, administrative cases shall likewise be recommended for filing, depending on the gravity of the offense.

B. Inquiries

Data subjects may make their inquiries with the Regional Director who shall assign the same to the concerned ACOP.

X. EFFECTIVITY –

This Data Privacy Manual shall be effective immediately.