Date: _____

CUSTOMS MEMORANDUM ORDER (CMO)
NO. 16-2021

SUBJECT: PRIVACY MANUAL

Introduction. This Privacy Manual implements the Bureau of Customs' commitment to processing data in accordance with its responsibilities under Republic Act No. 10173, otherwise known as the "*Data Privacy Act of 2012"* (DPA), its implementing rules and regulations, and other relevant policies including issuances of the National Privacy Commission. The Bureau respects and values the data privacy rights of data subjects and makes sure that all personal data collected from them, including the Bureau's clients, and stakeholders, are treated with utmost care and confidentiality.

With this Manual, the Bureau ensures that it collects, shares, stores, transmits, and disposes data fairly, transparently, and with respect towards individual rights. It shall inform data subjects of the Bureau's data protection and security measures and may serve as guide in exercising their rights under the DPA.

Section 1. Scope. This manual refers to all parties (employees, personnel, contractors, clients, importers, exporters, customs brokers, stakeholders, and other interested parties) who provide any amount of personal information to the Bureau of Customs.

Section 2. Objectives.

2.1. To protect the fundamental human right of privacy, of communication while ensuring free flow of information to promote innovation and growth; and

2.2. To ensure that personal information in information and communications systems in the government and in the private sector are secured and protected.

Section 3. Definition of Terms. For purposes of this Manual, the following terms are defined accordingly:

3.1. Bureau – shall refer to the Bureau of Customs.

3.2. Commission – shall refer to the National Privacy Commission created by virtue of Republic Act No. 10173, otherwise known as the "*Data Privacy Act of 2012."*

3.3. Consent of the Data Subject – shall refer to any freely given, specific, informed indication of will, whereby the data subject agrees to the collection and processing of personal information about and/or relating to him or her. Consent shall be evidenced by written, electronic or recorded means. It may also be given on behalf of the data subject by an agent specifically authorized by the data subject to do so.

3.4. Data – shall refer to any information, both personal and sensitive personal information, which is being processed by the Bureau of Customs.

3.5. Data Processing – shall refer to any operation or any set of operations performed upon personal information including, but not limited to, the collection, recording, organization, storage, updating or modification, retrieval, consultation, use, consolidation, blocking, erasure or destruction of data.

3.6. Data Subject – shall refer to an individual whose personal information is being processed by the Bureau.

3.7. Personal Information – shall refer 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.

3.8. Personal Information Controller – shall refer to a person or organization who controls the collection, holding, processing or use of personal information, including a person or organization who instructs another person or organization to collect, hold, process, use, transfer or disclose personal information on his or her behalf, in this case, the Commissioner, the District Collectors, the Head of Groups, the Directors, and the Division Chiefs, with respect to their office. The term excludes:

3.8.1. A person or organization who performs such functions as instructed by another person or organization; and

3.8.2. An individual who collects, holds, processes, or uses personal information in connection with the individual's personal, family or household affairs.

3.9. Personal Information Processor – shall refer to any natural or juridical person qualified to act as such under R.A. 10173 to

whom a personal information controller may outsource the processing of personal data pertaining to a data subject.

3.10. Privacy Impact Assessment – shall refer to the process of understanding the personal data flows in the Bureau. It identifies and provides an assessment of various privacy risks, and proposes measures intended to address them.

3.11. Privileged information – shall refer to any and all forms of data which under the Rules of Court and other pertinent laws constitute privileged communication.

3.12. Sensitive Personal Information – shall refer to personal information:

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

3.12.2. 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 person, the disposal of such proceedings, or the sentence of any court in such proceedings;

3.12.3. Issued by government agencies peculiar to an individual which includes, but not limited to, social security numbers, previous or current health records, licenses or its denials, suspension or revocation, and tax returns; and

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

Section 4. General Policy. As part of the Bureau's operations, there is a need to obtain and process information. This information includes any offline or online data that makes a person identifiable such as names, addresses, usernames and passwords, digital footprints, photographs, government issued identification numbers, financial data, etc.

The Bureau collects this information in a transparent way and only with the full cooperation and knowledge of interested parties. Once this information is available to the Bureau, the policies contained in this manual shall apply.

There must be an agreement of the business process, and the information system and technology platform that are developed and operated to collect, process, store, share, and dispose of in accordance with the data privacy principles as discussed herein.

4.1. Principles of Transparency, Legitimate Purpose, and Proportionality. All processing of personal data within the Bureau should be conducted in compliance with the Principles of Transparency, Legitimate Purpose, and Proportionality as espoused in the Data Privacy Act:

4.1.1. Transparency. The data subject must be aware of the nature, purpose, and extent of the processing of his or her personal data by the Bureau, including risks and safeguards involved, the identity of person 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.

4.1.2. Legitimate Purpose. The processing of personal data by the Bureau shall be compatible with a declared and specified purpose which must not be contrary to law, morals, or public policy.

4.1.3. 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 the Bureau only if the purpose of the processing could not reasonably be fulfilled by other means.

4.2. Principles in Collection, Processing, and Retention. The processing of personal data shall adhere to the following general principles in the collection, processing, and retention of personal data:

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

a. Consent is required prior to the collection and processing of personal data, subject to exemptions provided by the DPA and other applicable laws and regulations. When consent is required, it must be

time-bound in relation to the declared, specified, and legitimate purpose. Consent given may be withdrawn.

b. 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.

c. Purpose should be determined and declared before, or as soon as reasonably practicable, after collection.

d. Only personal data that is necessary and compatible with declared, specified, and legitimate purpose shall be collected.

4.2.2. Personal data shall be processed fairly and lawfully.

a. Processing shall uphold the rights of the data subject, including the right to refuse, withdraw consent, or object. It shall likewise be transparent and allow the data subject sufficient information to know the nature and extent of processing.

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

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

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

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

4.2.3. Processing should ensure data quality.

a. Personal data should be accurate and where necessary for declared, specified and legitimate purpose, kept up to date.

b. Inaccurate or incomplete data must be rectified, supplemented, destroyed or their further processing restricted.

4.2.4. Personal Data shall not be retained longer than necessary.

a. Retention of personal data shall only for as long as necessary:

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

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

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

b. Retention of personal data shall be allowed in cases provided by law.

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

4.2.5. Any authorized further processing shall have adequate safeguards.

a. Personal data originally collected for a declared, specified, or legitimate purpose may be processed further for historical, statistical, or scientific 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.

b. 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.

c. Personal data shall not be retained in perpetuity in contemplation of a possible future use yet to be determined.

4.3. Principles for Data Sharing. Further Processing of Personal Data collected from a party other than the Data Subject shall be allowed under any of the following conditions:

4.3.1. 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 principle of transparency, legitimate purpose and proportionality.

4.3.2. Data Sharing shall be allowed in the private sector if the data subject consents to data sharing, and the following conditions are complied with:

a. Consent for data sharing shall be required even when the data is to be shared with an affiliate or mother company, or similar relationships;

b. Data sharing for commercial purposes, including direct marketing, shall be covered by a data sharing agreement.

i. The data sharing agreement shall establish adequate safeguards for data privacy and security, and uphold rights of data subjects

.

ii. The data sharing agreement shall be subject to review by the Commission, on its own initiative or upon complaint of data subject.

c. The data subject shall be provided with the following information prior to collection or before data is shared:

i. Identity of the personal information controllers or personal information processors that will be given access to the personal data;

ii. Purpose of data sharing;

iii. Categories of personal data concerned;

iv. Intended recipients or categories of recipients of the personal data;

v. Existence of the rights of data subjects, including the right to access and correction, and the right to object;

vi. Other information that would sufficiently notify the data subject of the nature and extent of data sharing and the manner of processing.

d. Further processing of shared data shall adhere to the data privacy principles laid down in the Act, these Rules, and other issuances of the Commission.

4.3.3. Data collected from parties other than the data subject for purpose of research shall be allowed when the personal data is publicly available, or has the consent of the data subject for purpose of research: Provided, that adequate safeguards are in place, and no decision directly affecting the data subject shall be made on the basis of the data collected or processed. The rights of the data subject shall be upheld without compromising research integrity.

4.3.4. 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.

a. Any or all government agencies party to the agreement shall comply with the Act, these Rules, and all other issuances of the Commission, including putting in place adequate safeguards for data privacy and security.

b. The data sharing agreement shall be subject to review of the Commission, on its own initiative or upon complaint of data subject.

Section 5. <u>Processing of Personal Information</u>. The processing of personal information in the Bureau shall be permitted only if not otherwise prohibited by law, and when at least one of the following conditions exists:

5.1. The data subject has given his or her consent;

5.2. The processing of personal information is necessary and is related to the fulfillment of a contract with the data subject or in order to take steps at the request of the data subject prior to entering into a contract;

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

5.4. The processing is necessary to protect vitally important interests of the data subject, including life and health;

5.5. The processing is necessary in order to respond to national emergency, to comply with the requirements of public order and safety, or to fulfill functions of public authority which necessarily includes the processing of personal data for the fulfillment of its mandate; or

5.6. The processing is necessary for the purposes of the legitimate interests pursued by 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.

Section 6. <u>Processing of Sensitive Personal Information</u>.

6.1. The processing of sensitive personal information and privileged information in the Bureau shall be prohibited, except in the following cases:

6.1.1. The data subject has given his or her consent, specific to the purpose prior to the processing, or in the case of privileged information, all parties to the exchange have given their consent prior to processing;

6.1.2. The processing of the same is provided for by existing laws and regulations: Provided, That such regulatory enactments guarantee the protection of the sensitive personal information and the privileged information: Provided, further, That the consent of the data subjects are not required by law or regulation permitting the processing of the sensitive personal information or the privileged information;

6.1.3. 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;

6.1.4. The processing is necessary to achieve the lawful and non-commercial objectives of public organizations and their associations: Provided, That such processing is only confined and related to the bona fide members of these organizations or their associations: Provided, further, That the sensitive personal information are not transferred to third parties: Provided, finally, That consent of the data subject was obtained prior to processing;

6.1.5. The processing is necessary for purposes of medical treatment, is carried out by a medical practitioner or a medical treatment institution, and an adequate level of protection of personal information is ensured; or

6.1.6. The processing concerns such personal information as is 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.

6.2. Responsibility of District Collectors, Head of Groups, Division Chiefs. All sensitive personal information maintained by the Bureau, its ports, groups, and divisions, being Personal Information Controller or Personal Information Processor, shall be secured, as far as practicable, with the use of the most appropriate standard recognized by the information and communications technology industry, and as recommended by the National Privacy Commission. The head of each unit shall be responsible for complying with the security requirements mentioned herein while the NPC through the Data Protection Officer (DPO) shall monitor the compliance and may recommend the necessary action in order to satisfy the minimum standards.

6.3. Access by the Bureau's Personnel to Sensitive Personal Information.

6.3.1. On-site and Online Access. Except as may be allowed through guidelines to be issued by the Commission, 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 office.

6.3.2. Off-site Access. Unless otherwise provided in guidelines to be issued by the Commission, sensitive personal information maintained by the Bureau may not be transported or accessed from a location off the Bureau's property unless a request for such transportation or access is submitted and approved by the head of the agency in accordance with the following guidelines:

a. Deadline for Approval or Disapproval. In the case of any request submitted to the head of an agency, such head of the agency shall approve or disapprove the request within two (2) business days after the date of submission of the request. In case there is no action by the head of the agency, then such request is considered disapproved;

b. Limitation to One thousand (1,000) Records. If a request is approved, the head of the agency shall limit the access to not more than one thousand (1,000) records at a time; and

c. Encryption. Any technology used to store, transport or access sensitive personal information for purposes of off-site access approved under this subsection shall be secured by the use of the most secure encryption standard recognized by the Commission.

Section 7. Subcontracting Data Processing. The Bureau may subcontract the processing of personal information: Provided, That the personal information controller shall be responsible for ensuring that proper safeguards are in place to ensure the confidentiality of the personal information processed, prevent its use for unauthorized purposes, and generally, comply with the requirements of the Data Privacy Act and other laws for processing of personal information. The personal information processor shall comply with all the requirements of the Data Privacy Act and other applicable laws.

In entering into any contract that may involve accessing or requiring sensitive personal information from one thousand (1,000) or more individuals, the Bureau shall require a contractor and its employees to register their personal information processing system with the Commission in accordance with this Act and to comply with the other provisions of this Act including the immediately preceding section, in the same manner as agencies and government employees comply with such requirements.

Section 8. Data Processing Records. Adequate records of the Bureau's Personal Data Processing activities shall be maintained at all times. The Data Protection Officer, with the cooperation and assistance of Personal Information Controllers and Personal Information Processors of the Bureau, shall be responsible for ensuring that these records are kept up to date. These records shall include, at the minimum:

8.1. Information about the purpose of the processing of personal data, including any intended future processing or data sharing;

8.2. A description of all categories of data subjects, personal data, and recipients of such personal data that will be involved in the processing;

8.3. General information about the data flow within the Bureau from the time of collection and retention, including the time limits for disposal or erasure of personal data;

8.4. A general description of the organizational, physical, and technical security measures in place within the Bureau; and

8.5. The name and contact details of the Data Protection Officer, Personal Data Processors, Personal Data Controllers, 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.

Section 9. Extension of Privileged Communication. The Bureau may invoke the principle of privileged communication over privileged information that they lawfully control or process. Subject to existing laws and regulations, any evidence gathered on privileged information is inadmissible.

Section 10. Data Privacy Rights Processes. As provided under the Data Privacy Act, Data Subjects have the following rights in connection with the processing of their personal data: right to be informed, right to object, right to access, right to rectification, right to erasure or blocking, and right to damages. Employees and agents of the Bureau are required to strictly respect and obey the rights of the Data Subjects. The Data Protection Officer, with the assistance of the Human Resources Management Division, and the Public Information and Assistance Division, shall be responsible for monitoring such compliance and developing the appropriate disciplinary measures and mechanism.

10.1. Right to be Informed. The Data Subject has the right to be informed whether Personal Data pertaining to him or her shall be, are being, or have been processed.

The Data Subject shall be notified and furnished with information indicated hereunder before the entry of his or her Personal Data into the records of the Bureau, or at the next practical opportunity:

10.1.1. Description of the Personal Data to be entered into the system;

10.1.2. Purposes for which they are being or will be processed, including processing for direct marketing, profiling or historical, statistical or scientific purpose;

10.1.3. Basis of processing, when processing is not based on the consent of the Data Subject;

10.1.4. Scope and method of the Personal Data Processing;

10.1.5. The recipients or classes of recipients to whom the Personal Data are or may be disclosed or shared;

10.1.6. 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;

10.1.7. The identity and contact details of the Data Protection Officer;

10.1.8. The period for which the Personal Data will be stored; and

10.1.9. The existence of their rights as Data Subjects, including the right to access, correction, and to object to the Processing, as well as the right to lodge a complaint before the National Privacy Commission.

10.2. Right to Object. The Data Subject shall have the right to object to the processing of his or her Personal Data, including manual processing, 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:

10.2.1. The Personal Data is needed pursuant to a subpoena;

10.2.2. The Processing is for obvious purposes, including, when it is necessary for the performance or in relation 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

10.2.3. The Personal Data is being collected and processed to comply with a legal obligation.

10.3. Right to Access. The Data Subject has the right to reasonable access to, upon demand, the following:

10.3.1. Contents of his or her Personal Data that were processed;

10.3.2. Sources from which Personal Data were obtained;

10.3.3. Names and addresses of recipients of the Personal Data;

10.3.4. Manner by which his or her Personal Data were processed;

10.3.5. Reasons for the disclosure of the Personal Data to recipients, if any;

10.3.6. Information on automated processes where the Personal Data will, or is likely to, be made as the sole basis for any decision that significantly affects or will affect the Data Subject;

10.3.7. Date when Personal Data concerning the Data Subject were last accessed and modified; and

10.3.8. The designation, name or identity, and address of the DPO.

10.4. Right to Rectification. The Data Subject has the right to dispute the inaccuracy or rectify the error in his or her Personal Data, and the Bureau shall correct it immediately and accordingly, unless the request is vexatious or otherwise unreasonable. If the

Personal Data has been corrected ,the Bureau shall ensure the accessibility of both the new and the retracted Personal Data and the simultaneous receipt of the new and the retracted Personal Data 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.

10.5. 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 Bureau's filing system.

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

a. The Personal Data is incomplete, outdated, false, or unlawfully obtained;

b. The Personal Data is being used for purpose not authorized by the Data Subject;

c. The Personal Data is no longer necessary for the purposes for which they were collected;

d. The Data Subject withdraws consent or objects to the processing, and there is no other legal ground or overriding legitimate interest for the processing by the Bureau;

e. The Personal Data concerns private information that is prejudicial to Data Subject, unless justified by freedom of speech, of expression, or of the press or otherwise authorized;

f. The Processing is unlawful; or

g. The Data Subject's rights have been violated.

10.5.2. The DPO may notify third parties who have previously received such processed Personal Data that the Data Subject has withdrawn his or her consent to the processing thereof upon reasonable request by the Data Subject.

10.6. Transmissibility of Rights of Data Subjects. The lawful heirs and assigns of the Data Subjects 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 his/her rights.

10.7. Right to Data Portability. Where personal information is processed by the Bureau through electronic means and in a structured and commonly used format, the Data Subject shall have the right to obtain 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 his right shall primarily take into account the right Data Subject to control over his or her Personal Data being processed based on consent or contract, for transactional purpose, or through automated means. The DPO shall regularly monitor and implement the NPC's issuances specifying the electronic format referred to above, as well as technical standards, modalities, procedures and other rules for their transfer.

10.8. Non-applicability of Privacy Rights. The immediately preceding sections are not applicable if the processed personal information are used only for the needs of scientific and statistical research and, on the basis of such, no activities are carried out and no decisions are taken regarding the data subject: Provided, That the personal information shall be held under strict confidentiality and shall be used only for the declared purpose. Likewise, the immediately preceding sections are not applicable to processing of personal information gathered for the purpose of investigations in relation to any criminal, administrative or tax liabilities of a data subject.

10.9. Inquiries and Complaints. Inquiries and complaints of the data subjects in relation to the exercise of their data privacy rights shall be addressed to the Bureau through the Public Information & Assistance Division, personally or by e-mail at *piad@customs.gov.ph,* and shall be resolved by the Bureau in accordance with this Manual, the Data Privacy Act, its IRR, and other applicable laws.

10.10. Fees. The Bureau shall not charge any fee for the exercise of the Data Subject's Data Privacy rights, except in cases wherein a reproduction and copying of documents is involved, a reproduction and copying fee shall be charged which will be the actual amount spent by the Bureau in providing the requested

data to the data subject. The schedule of fees shall be posted by the Bureau.

The Bureau may exempt any Data Subject from payment of such fees, upon request stating the valid reason why he or she shall not pay the fee.

Section 11. Security of Data. As part of the Bureau's commitment to treat personal data of its employees, personnel, contractors, clients, importers, exporters, customs brokers, stakeholders, and other interested parties who share personal information with the Bureau, with utmost care and confidentiality, the Bureau ensures that it gathers, stores, and handles data fairly, transparently and with respect towards individual rights. Hence, it uses the appropriate organizational, physical, and technical security measures in the processing of personal information.

11.1. Data Protection Officer (DPO). In order to effectively and efficiently enforce the Data Privacy Act, adopt generally accepted international principles and standards for personal data protection, and to safeguard the fundamental human right of every individual to privacy while ensuring free flow of information for innovation, growth, and national development, the Bureau shall have a DPO who shall have the following functions:

11.1.1. Monitor the Bureau's compliance with the Data Privacy Act, its Implementing Rules and Regulations, Issuances by the National Privacy Commission and other applicable laws and policies, which may include:

a. Collecting information to identify the processing operations, activities, measures, projects, programs, or systems of the Bureau's Personal Information Controller (PIC) or Personal Information Processor (PIP), and maintain a record thereof;

b. Analyzing and checking 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. Advice the PIC or PIP as regards the necessity of executing a Data Sharing Agreement with third parties, and ensure its compliance with the law;

11.1.2. Ensure the conduct of Privacy Impact Assessments relative to activities, measures, projects, programs, or systems of the PIC or PIP;

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

11.1.4. 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;

11.1.5. Inform and cultivate awareness on privacy and data protection within the Bureau, including all relevant laws, rules and regulations and issuances of the NPC;

11.1.6. 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;

11.1.7. 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 and the PIC or PIP;

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

11.1.9. Perform other duties and tasks that will further the interest of data privacy and security and uphold the rights of the data subjects.

11.2. Organizational Security Measures. The DPO shall assist the Human Resource Management Division (HRMD), in developing and implementing measures to ensure that all the Bureau's staff who have 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 the Bureau and conducting training programs to educate employees and agents on data privacy related concerns.

The DPO shall likewise assist the HRMD, in ensuring that the Bureau shall obtain the employee's informed consent, evidenced by written, electronic or recorded means to:

11.2.1. The processing of his or her personal data for purposes of maintaining the Bureau's records; and

11.2.2. 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 the Bureau. This obligation shall apply even after the employee has left the Bureau for whatever reasons.

11.3. Physical Security Measures. The DPO shall assist the HRMD and the Management Information System and Technology Group (MISTG), in developing and implementing policies and procedures for the Bureau to monitor and limit access to, and activities in, the offices of the Bureau, and/or workstations in the Bureau 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 Bureau 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 workstation, 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.

11.4. Technical Security Measures. The DPO shall assist the MISTG in continuously developing and evaluating the Bureau's security policy with respect to the processing of personal data. The

security policy should include the following minimum requirements:

11.4.1. Safeguards to protect the Bureau'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;

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

11.4.3. Regular monitoring for security breaches, and a process both for identifying and accessing reasonably foreseeable vulnerabilities in the Bureau's computer network and system, and for taking preventive, corrective, and mitigating actions against security incidents that can lead to a personal data breach;

11.4.4. The ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident;

11.4.5. A process for regularly testing, assessing, and evaluating the effectiveness of security measures; and

11.4.6. Encryption of personal data during storage and while in transit, authentication process, and other technical security measures that control and limit access thereto.

11.5. Privacy Operations Manual. All heads of ports, groups, or divisions, who are engaged in the processing of personal information, being PICs or PIPs shall create a Privacy Operations Manual, which shall serve as a guide or handbook for ensuring the compliance of their port, group, or division with the Data Privacy Act, its implementing Rules and Regulations, and other relevant issuances of the Commission. It shall also encapsulate the privacy and data protection protocols observed and carried out within their port, group, or division for specific circumstances (from collection to destruction), directed toward the fulfillment and realization of the rights of the data subjects.

Such Privacy Operations Manual shall be attached to this Privacy Manual which shall form part of it.

11.6. Privacy Notice. In line with the principle of transparency mandated by the DPA, the data subject must be aware of the nature, purpose, and extent of the processing of his or her personal data, including the risks and safeguards involved, the identity of personal information controller, 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.

Thus, in line with the right to information of the data subjects, the personal information controllers and personal information processors of the Bureau shall, before collecting and processing personal information, apprise data subjects by posting Data Privacy Notices inside and/or outside their respective offices, or through the use of electronic and/or digital means of the following:

11.6.1. Description of the personal data to be processed;

11.6.2. Purposes for processing, including direct marketing, profiling, or historical, statistical or scientific purpose;

11.6.3. Basis of processing, when processing is not based on consent;

11.6.4. Scope and method of processing;

11.6.5. Recipient/classes of recipients to whom the personal data are or may be disclosed;

11.6.6. Methods utilized for automated access, if the same is allowed by the data subject, and the extent to which such access is authorized;

11.6.7. Identity and contact details of the PIC or its representative;

11.6.8. Retention period; and

11.6.9. Existence of rights as data subjects, including the right to lodge a complaint before the NPC.

11.7. Privacy Consent. In compliance with the DPA, it is mandatory that consent from the data subject for the purposes of processing his or her personal data shall be acquired before his or her

personal information may be processed by the personal information controller or personal information processor of the Bureau.

Consent of the data subject should be given by a clear affirmative act establishing a freely given, specific, informed and unambiguous indication of will, whereby the data subject agrees to the collection and processing of his or her personal, sensitive personal, or privileged information.

When the processing of personal information is based on consent, the PIC must obtain the consent in relation to the declared purpose for processing. The consent must likewise be evidenced by written, electronic, or recorded means.

11.8. Privacy Impact Assessment. Every Personal Information Controller or Personal Information Processor shall signify its commitment to the conduct of a Privacy Impact Assessment, which includes the following:

11.8.1. Deciding on the need for a Privacy Impact Assessment;
11.8.2. Assigning a person responsible for the whole process;
11.8.3. Providing resources to accomplish the objectives of the Privacy Impact Assessment; and
11.8.4. Issuing a clear directive for its conduct.

In general, a Privacy Impact Assessment should be undertaken for every processing system of a Personal Information Controller or Personal Information Processor that involves personal data. It 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.

A recommendation for the conduct of a Privacy Impact Assessment may also come from the Data Protection Officer of the Bureau.

The Personal Information Controller or Personal Information Processor may forego the conduct of a Privacy Impact Assessment only if it determines that the processing involves minimal risks to the rights and freedoms of individuals, taking into account recommendations from the Data Protection Officer. In making this determination, the Personal Information Controller or Personal Information Processor should consider the size and

sensitivity of the personal data being processed, the duration and extent of processing, the likely impact of the processing to the life of data subject and possible harm in case of a personal data breach.

The conduct of a Privacy Impact Assessment is intended to:

a. Identify, Assess, Evaluate, and Manage the risks represented by the processing of personal data;

b. Assist the Personal Information Controller or Personal Information Processor in preparing the records of its processing activities, and in maintaining its privacy management program;

c. Facilitate compliance by the Personal Information Controller or Personal Information Processor with the Data Privacy Act, its Implementing Rules and Regulations, and other applicable issuances of the NPC, by determining:

i. Its adherence to the principles of transparency, legitimate purpose and proportionality;

ii. Its existing organizational, physical and technical security measures relative to its data processing systems;

iii. The extent by which it upholds the rights of data subjects; and

d. Aid the Personal Information Controller or Personal Information Processor in addressing privacy risks by allowing it to establish a control framework.

The Results of the Privacy Impact Assessment shall be properly documented and reported to management and communicated to internal and external stakeholders of the Bureau. The PIC or PIP can limit the information provided to the public based on its legitimate interests, such as the legal, business operation, or security risks that disclosure may give rise to.

The Privacy Impact Assessment should be evaluated every year. This, however, does not preclude the conduct of a new PIA on the same data processing system, when so required by significant changes required by law or policy, and other similar circumstances.

Section 12. Data Breaches and Security Incidents.

12.1. Data Breach Response Team. The Bureau shall form a Data Breach Response Team which is composed of five (5) members, specifically: One (1) from the Human Resource Management Division, One (1) from the Management Information System and Technology Group, the Data Protection Officer, and two (2) members from the Port/Group/Division concerned where the Data Breach happened, preferably a member with the authority to make immediate decision regarding the critical action, when necessary.

12.2. Data Breach Notification. All employees and personnel of the Bureau involved in the processing of personal information shall regularly monitor their respective offices for signs of possible data breach and security incidents. Any threatened or actual data breach found shall be immediately reported to the Data Breach Response Team.

The Data Breach Response Team, upon receipt of the data breach report, shall immediately make an appropriate assessment, investigation and remediation measures to address the breach.

The Data Breach Response Team, shall also notify the Commission and the Data Subjects affected of such breach within a period of seventy-two (72) hours upon knowledge of or reasonable belief by the PIC or PIP that a personal data breach requiring notification has occurred, as when any of the following circumstances are present:

12.2.1. 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 personal information controller; or

12.2.2. When the PIC or the Commission believes that such unauthorized acquisition is likely to give rise to a real risk of serious harm to any affected data subject.

12.3. Documentation and Reportorial Requirements. All security incidents and personal data breaches shall be documented through written reports, including those not covered by the notification requirements. In the event of a personal data breach, a report shall include the facts surrounding the incident, the effects of such incident, and the remedial action taken by the PIC.

For other security incidents not involving personal data, a report containing aggregated data shall constitute sufficient documentation. Any or all reports shall be made available when requested by the Commission, provided, that a summary of all reports shall be submitted to the Commission annually, comprised of general information including the number of incidents and breach encountered, classified according to their impact on the availability, integrity, or confidentiality of personal data.

Section 13. <u>Administrative Liability</u>.

13.1. Unauthorized Processing of Personal Information and Sensitive Personal Information. Pursuant to Section 25 in relation to Section 36 of the Data Privacy Act, the unauthorized processing of personal information and/or Sensitive Personal Information shall be a ground for Dismissal from Service.

13.2. Accessing Personal Information and Sensitive Personal Information Due to Negligence. Pursuant to Section 26 in relation to Section 36 of the Data Privacy Act, the following acts shall be punishable by:

a. Any person who, due to negligence provided access to personal information without being authorized shall be liable for simple negligence;

b. Any person who, due to negligence provided access to sensitive personal information without being authorized shall be liable for gross negligence.

13.3. Improper Disposal of Personal Information and Sensitive Personal Information. Pursuant to Section 27 in relation to Section 36 of the Data Privacy Act, the improper disposal of personal information and/or Sensitive Personal Information shall be a ground for Dismissal from Service.

13.4. Processing of Personal Information and Sensitive Personal Information for Unauthorized Purposes. Pursuant to Section 28 in relation to Section 36 of the Data Privacy Act, the processing of personal information and/or Sensitive Personal Information for unauthorized purposes shall be a ground for Dismissal from Service.

13.5. Unauthorized Access or Intentional Breach. Pursuant to Section 29 in relation to Section 36 of 1the Data Privacy Act, any person who knowingly and unlawfully, or violating data

confidentiality and security data systems, breaks in any way into any system where personal information and/or sensitive personal Information shall be a ground for Dismissal from Service.

13.6. Concealment of Security Breaches Involving Sensitive Personal Information. Pursuant to Section 30 in relation to Section 36 of the Data Privacy Act, any person who, after having knowledge of a security breach and of the obligation to notify the Commission pursuant to Section 20(f), intentionally or by omission conceals the fact of such security breach shall suffer the penalty of Dismissal from Service.

13.7. Malicious Disclosure. Pursuant to Section 31 in relation to Section 36 of the Data Privacy Act, any person, who, with malice or in bad faith, discloses unwarranted or false information relative to any personal information or personal sensitive information obtained by him or her shall suffer the penalty of Dismissal from Service.

13.8. Unauthorized Disclosure. Pursuant to Section 32 in relation to Section 36 of the Data Privacy Act, any person who discloses to a third-party personal information not covered by the preceding section without the consent of the data subject shall suffer the penalty of Dismissal from Service.

13.9. Combination or Series of Acts. Pursuant to Section 33 in relation to Section 36 of the Data Privacy Act, any combination or series of acts as defined from Sections 13.1 to 13.8 shall suffer the penalty of Dismissal from Service.

13.10. Any Other Acts in Violation of this Privacy Manual. Any other acts in violation or failure to comply with the provisions of this CMO, which was not punishable under the preceding provisions, shall be a ground for the following administrative penalties:

1st Offense – Reprimand

2nd Offense – Suspension of one (1) to thirty (30) days; and

3rd Offense – Dismissal from Service

13.11. Non-prejudice to other penalties. The penalties provided for in this Order shall be without prejudice to other criminal, administrative or civil liability that may arise pursuant to the provisions of applicable law violated.

13.12. Procedure. The Revised Rules on Administrative Cases in the Civil Service shall be applicable in the disposition of cases under this CMO.

Section 14. Periodic Review. Unless otherwise provided, this Privacy Manual shall be reviewed every year, after the evaluation of the Privacy Impact Assessment, and be amended or revised, if necessary.

Section 15. Repealing Clause. This Privacy Manual specifically amends or repeals previously issued CAOs and CMOs which are inconsistent with the provisions herein stated.

Section 16. Separability Clause. If any part of this Privacy Manual is declared unconstitutional or contrary to existing laws, the other parts not so declared shall remain in full force and effect.

Section 17. Effectivity. This Privacy Manual shall take effect immediately.

The Office of the National Administrative Register (ONAR) of the UP Law Center shall be provided three (3) certified copies of this CMO.

REY LEONARDO B. GUERRERO
Commissioner