JUNE 2021 | VOL. NO. 27

NMM | NAGUE MALIC MAGNAWA & ASSOCIATES
Customs Brokers

COMPLIANCE BEYOND BORDERS

# CUSTOMS GAZETTE

## Updates on Customs-Related Matters

**Disclaimer**

THIS IS NOT A LEGAL DOCUMENT AND MAY NOT BE USED AS SUCH. IT IS AN ADVISORY AND INFORMATION TOOL ONLY.

# In Brief

# In Brief

**Tariff Commission Circulars/Advance Rulings (TCC/AR)** - AOCG MEMO NO. 221-2021 (page 48)

**Tariff Commission Circulars/Advance Rulings (TCC/AR)** - AOCG MEMO NO. 222-2021 (page 49)

**Acceptance and System of Verification of Scanned Copies of Compassionate Special Permits (CSPs) Issied by the Food and Drug Administration (FDA)** - AOCG MEMO NO. 234-2021 (page 50)

**Implementation of Executive Order No. 134 Entitled "Further Modifying the Rates of Import Duty on Fresh, Chilled or Frozen Meat of Swine under Section 1611 of Republic Act No. 10863, Otherwise Known as the "Customs Modernization and Tariff Act," Repealing Executive Order No. 128 (S. 2021) for the Purpose** - AOCG MEMO NO. 235-2021 (page 51)

# CMO NO. 16-2021

**Issue Date: May 7, 2021**

## *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.

## *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.

## *Objectives*

- To protect the fundamental human right of privacy, of communication while ensuring free flow of information to promote innovation and growth; and
- To ensure that personal information in information and communications systems in the government and in the private sector are secured and protected.

## *Definition of Terms*

**Bureau** — shall refer to the Bureau of Customs.

**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. "

**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.

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

**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.

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

**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.

**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:

- A person or organization who performs such functions as instructed by another person or organization; and
- An individual who collects, holds, processes, or uses personal information in connection with the individual's personal, family or household affairs.

**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.

**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.

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

**Sensitive Personal Information** — shall refer to personal information:

- About an individual's race, ethnic, origin, marital status, age, color, and religious, philosophical or political affiliations;
- 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;
- 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
- Specifically established by an executive order or an act of Congress to be kept classified.

## *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.

- **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:
  - **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.
  - **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.
  - **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.

- **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:
  - Collection must be for a declared, specified, and legitimate purpose.
    - 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.
    - 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.
    - Purpose should be determined and declared before, or as soon as reasonably practicable, after collection.
    - Only personal data that is necessary and compatible with declared, specified, and legitimate purpose shall be collected.
  - Personal data shall be processed fairly and lawfully.
    - 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.
    - Information provided to a data subject must always be in clear and plain language to ensure that they are easy to understand and access.
    - Processing must be in a manner compatible with declared, specified, and legitimate purpose.
    - Processed personal data should be adequate, relevant, and limited to what is necessary in relation to the purposes for which they are processed.
    - Processing shall be undertaken in a manner that ensures appropriate privacy and security safeguards.
  - Processing should ensure data quality.
    - Personal data should be accurate and where necessary for declared, specified and legitimate purpose, kept up to date.
    - Inaccurate or incomplete data must be rectified, supplemented, destroyed or their further processing restricted.

- Personal Data shall not be retained longer than necessary.
  - Retention of personal data shall only for as long as necessary:
    - for the fulfillment of the declared, specified, and legitimate purpose, or when the processing relevant to the purpose has been terminated;
    - for the establishment, exercise or defense of legal claims; or
    - for legitimate business purposes, which must be consistent with standards followed by the applicable industry or approved by appropriate government agency.
  - Retention of personal data shall be allowed in cases provided by law.
  - Personal data shall be disposed or discarded in a secure manner that would prevent further processing, unauthorized access, or disclosure to any other patty or the public, or prejudice the interests of the data subjects.
- Any authorized further processing shall have adequate safeguards.
  - 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.
  - 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.
  - Personal data shall not be retained in perpetuity in contemplation of a possible future use yet to be determined.

- **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:
  - 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.

- Data Sharing shall be allowed in the private sector if the data subject consents to data sharing, and the following conditions are complied with:
  - Consent for data sharing shall be required even when the data is to be shared with an affiliate or mother company, or similar relationships;
  - Data sharing for commercial purposes, including direct marketing, shall be covered by a data sharing agreement.
    - The data sharing agreement shall establish adequate safeguards for data privacy and security, and uphold rights of data subjects.
    - The data sharing agreement shall be subject to review by the Commission, on its own initiative or upon complaint of data subject.
  - The data subject shall be provided with the following information prior to collection or before data is shared:
    - Identity of the personal information controllers or personal information processors that will be given access to the personal data;
    - Purpose of data sharing;
    - Categories of personal data concerned;
    - Intended recipients or categories of recipients of the personal data;
    - Existence of the rights of data subjects, including the right to access and correction, and the right to object;
    - Other information that would sufficiently notify the data subject of the nature and extent of data sharing and the manner of processing.
  - 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.
- 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.
- 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.

- Any or all government agencies patty 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.
- The data sharing agreement shall be subject to review of the Commission, on its own initiative or upon complaint of data subject.

## *Processing of Personal Information*

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:

- The data subject has given his or her consent;
- 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;
- The processing is necessary for compliance with a legal obligation to which the personal information controller is subject;
- The processing is necessary to protect vitally important interests of the data subject, including life and health;
- 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
- 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.

## *Processing of Sensitive Personal Information*

- The processing of sensitive personal information and privileged information in the Bureau shall be prohibited, except in the following cases:The data subject has given his or her consent;
  - 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;

- 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;
- 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;
- 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;
- 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
- 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.

- **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.

- **Access by the Bureau's Personnel to Sensitive Personal Information.**
  - **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.
  - **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:
    - **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;
    - **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
    - **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.

## *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.

## *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:

- Information about the purpose of the processing of personal data, including any intended future processing or data sharing;
- A description of all categories of data subjects, personal data, and recipients of such personal data that will be involved in the processing;
- 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;
- A general description of the organizational, physical, and technical security measures in place within the Bureau; and
- 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.

## *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.

## *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.

- **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:
  - Description of the Personal Data to be entered into the system;
  - Purposes for which they are being or will be processed, including processing for direct marketing, profiling or historical, statistical or scientific purpose;
  - Basis of processing, when processing is not based on the consent of the Data Subject;
  - Scope and method of the Personal Data Processing;
  - The recipients or classes of recipients to whom the Personal Data are or may be disclosed or shared;
  - 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;
  - The identity and contact details of the Data Protection Officer;
  - The period for which the Personal Data will be stored; and
  - 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.

- **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:
  - The Personal Data is needed pursuant to a subpoena;
  - 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
  - The Personal Data is being collected and processed to comply with a legal obligation.
- **Right to Access.** The Data Subject has the right to reasonable access to, upon demand, the following:
  - Contents of his or her Personal Data that were processed;
  - Sources from which Personal Data were obtained;
  - Names and addresses of recipients of the Personal Data;
  - Manner by which his or her Personal Data were processed;
  - Reasons for the disclosure of the Personal Data to recipients, if any;
  - 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;
  - Date when Personal Data concerning the Data Subject were last accessed and modified; and
  - The designation, name or identity, and address of the DPO.
- **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.

- **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.
  - This right may be exercised upon discovery and substantial proof of any of the following:
    - The Personal Data is incomplete, outdated, false, or unlawfully obtained;
    - The Personal Data is being used for purpose not authorized by the Data Subject;
    - The Personal Data is no longer necessary for the purposes for which they were collected;
    - 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;
    - 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;
    - The Processing is unlawful; or
    - The Data Subject's rights have been violated.
  - 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.
- **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.
- **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.

- **Non-applicability of Privacy Rights.** The immediately preceding sections are not applicable if the processed personal information is 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.
- **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.
- **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.

## *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.

- **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:
  - 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:
    - 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;
    - Analyzing and checking the compliance of processing activities, including the issuance of security clearances to and compliance by third-party service providers;
    - Inform, advise, and issue recommendations to the PIC or PIP;
    - Ascertain renewal of accreditations or certifications necessary to maintain the required standards in personal data processing; and
    - 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;
  - Ensure the conduct of Privacy Impact Assessments relative to activities, measures, projects, programs, or systems of the PIC or PIP;
  - 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);
  - 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;
  - Inform and cultivate awareness on privacy and data protection within the Bureau, including all relevant laws, rules and regulations and issuances of the NPC;
  - 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;

- Serve as the contact person of the PIC or PIP vis-å-vis data subjects, the NPC and other authorities in all matters concerning data privacy or security issues or concerns and the PIC or PIP;
- Cooperate, coordinate and seek advice of the NPC regarding matters concerning data privacy and security; and
- Perform other duties and tasks that will further the interest of data privacy and security and uphold the rights of the data subjects.

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

- **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:
  - 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;
  - The ability to ensure and maintain the confidentiality, integrity, availability, and resilience of the Bureau's data processing systems and services;
  - 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;
  - The ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident;
  - A process for regularly testing, assessing, and evaluating the effectiveness of security measures; and
  - Encryption of personal data during storage and while in transit, authentication process, and other technical security measures that control and limit access thereto.
- **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.

- **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:
  - Description of the personal data to be processed;
  - Purposes for processing, including direct marketing, profiling, or historical, statistical or scientific purpose;
  - Basis of processing, when processing is not based on consent;
  - Scope and method of processing;
  - Recipient/classes of recipients to whom the personal data are or may be disclosed;
  - Methods utilized for automated access, if the same is allowed by the data subject, and the extent to which such access is authorized;
  - Identity and contact details of the PIC or its representative;
  - Retention period; and
  - Existence of rights as data subjects, including the right to lodge a complaint before the NPC.
- **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.

- **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:
  - Deciding on the need for a Privacy Impact Assessment;
  - Assigning a person responsible for the whole process;
  - Providing resources to accomplish the objectives of the Privacy Impact Assessment; and
  - 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:

- Identify, Assess, Evaluate, and Manage the risks represented by the processing of personal data;
- Assist the Personal Information Controller or Personal Information Processor in preparing the records of its processing activities, and in maintaining its privacy management program;

- 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:
  - Its adherence to the principles of transparency, legitimate purpose and proportionality;
  - Its existing organizational, physical and technical security measures relative to its data processing systems;
  - The extent by which it upholds the rights of data subjects; and
  - 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.

## *Data Breaches and Security Incidents*

- **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.
- **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:

- 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
- 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.

- **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.

## *Administrative Liability*

- **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.

- **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:
  - Any person who, due to negligence provided access to personal information without being authorized shall be liable for simple negligence;
  - Any person who, due to negligence provided access to sensitive personal information without being authorized shall be liable for gross negligence.
- **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.
- **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.
- **Unauthorized Access or Intentional Breach.** Pursuant to Section 29 in relation to Section 36 of the 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.
- **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.
- **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.
- **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.

- **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 the Unauthorized Processing of Personal Information and Sensitive Personal Information section to the Unauthorized Disclosure section shall suffer the penalty of Dismissal from Service.
- **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
- **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.
- **Procedure.** The Revised Rules on Administrative Cases in the Civil Service shall be applicable in the disposition of cases under this CMO.

## *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.

## *Repealing Clause*

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.

## *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.

## *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.

# CMO NO. 17-2021

**Issue Date:** May 18, 2021

## *Objectives*

- To implement the Automated Bonds Management System (ABMS) for General Warehousing Bonds (GWB) in all Customs Ports.
- To provide detailed instruction to declarants, brokers, importers, accredited Value-Added Service Providers (VASPs), surety companies and Bureau personnel on the Customs processes to be observed under the ABMS for GWB.
- To effectively monitor the status of bonds from its posting up to its cancellation and expedite the settlement or collection of due and demandable bonds.

## *Scope*

This Order shall apply to all Warehousing Bond Accounts opened under the Electronic to Mobile (E2M) Customs System in all Collection Districts, including sub-ports and other Bureau offices.

## *Administrative Provisions*

- The ABMS is a bureau-wide system for processing bond transactions established pursuant to CMO No. 14-2012. It monitors and ages bond balances and flags those that have expired.
- Warehousing bond accounts shall be covered under the ABMS.
- For purposes of this Order, only CBW operators registered with the Client Profile Registration System (CPRS) shall be allowed to avail of the ABMS in the E2M Customs System.
- Approved bond policies filed on the current year will expire on the 31st day of December of the calendar year.
- The GWB shall be exclusively used to secure the duties and taxes reflected in the Warehousing Single Administrative Document (WSAD). The current practice of charging against the GWB the amount of duties and taxes due on shipments for transit to CBWs shall be discontinued. Instead, the CBW operator must open a bond account for the transit of the goods from the Port of Discharge to the CBW.

## *Operational Provisions*

- **Creation of a Bond Account.**
  - The CBW operator shall create a bond account by submitting the bond policy electronically to the Bureau through its accredited VASP. For uniformity, the CBW Operator shall only encode the numeric character of the policy number (without spaces).
  - The E2M Customs System shall automatically send the following feedback or status:
    - STORED — which means the electronic submission of the bond policy has been successfully lodged; or
    - Reject the electronic lodgement, specifying therein the reasons why the electronic submission of the bond policy has failed.
  - Once the bond policy has been stored in the E2M Customs System, the applicant shall submit the hard copy of the bond policy, together with the supporting documents, to the Bonds Division of the Port having jurisdiction over the Customs Bonded Warehouse through the port's Customer Care Portal System (CCPS).
  - The Bonds Examiner receives the original bond policy and the supporting documents, retrieves the filed bond record in the ABMS and verifies the bond information against the details in the hard copy of the original bond policy.

    They shall likewise check for the following:
    - Authenticity, validity and completeness of the submitted bonds and the supporting documents;
    - Information entered by the importer against the original bond policy and supporting documents; and
    - Accreditation of the surety company with the Bureau.
  - Bonds Examiner tags the bond application in the ABMS as follows:
    - "EXAMINED" — which means the application shall be submitted to the Division Chief for approval; or
    - "EXAMINED FAILED" — which means the application is rejected. The original bond policy, together with supporting documents shall be returned to the importer or his authorized representative. The reasons for the failed examination shall be stated.

      However, if the discrepancy or error is only on the details in the ABMS, the Bonds examiner need not return the original bond together with supporting

documents to the applicant. The CBW operator shall rectify by relodgement of correct information to the VASP system.

- If the application passes the examination by the Bonds Examiner, the original bond, together with supporting documents, is then forwarded to the Chief, Bonds Division.
- The Bonds Division Chief shall review the findings of the bonds examiner then tags the application as follows:
  - "APPROVED" — which means the bonds application is approved; or
  - "REJECTED" - which means the application is rejected. The original bond policy, together with supporting documents shall be returned to the importer or his authorized representative. The reasons for the rejection shall be stated.

    However, if the discrepancy or error is only on the details in the ABMS, the Chief, Bonds Division need not return the original bond together with supporting documents to the applicant. The CBW operator shall rectify by re-lodgement of correct information to the VASP system.
- Approved bonds automatically generate the following in the ABMS:
  - Bond Account containing the Account Holder and Account Information;
  - §Account Policies containing Policy Details; and
  - Bond Charging/Cancellation History in ledger form.
- A CBW operator can add more bond policies to his account by following the same procedure during the first bond application. The ABMS automatically adds up the approved new policies to the existing bond account and consequently increase the value of the bond.

- **Bonds Charging**
  - Upon lodgement of the goods declaration for warehousing, the Warehousing Entry System (WES) sends request to the ABMS to charge against a particular bond account.
  - Upon assessment, the ABMS checks for the sufficiency of the bond.
    - If the bond is insufficient, a bond error message is displayed in the E2M Customs System to the principal appraiser and the assessment cannot proceed.

      The Principal appraiser shall notify the CBW operator through the CCPS that the bond is insufficient to cover the assessed duties and taxes, with request to post additional security.

The CBW operator shall apply and post a new bond sufficient to cover the computed duties and taxes.
    - If the bond is sufficient, the WES debits the amount charged to the available bond balance. The SAD Assessment Notice is the notification that the assessed duties and taxes is charged against the bond.
  - If the goods declaration is cancelled, the ABMS cancels the amount charged and reverts to the previous bond balance.
- **Bond Cancellation**
  - The Chief, Bonds Division may cancel an approved bond if upon further review, there are still errors or discrepancies on the details in the ABMS and the hard copy of the bond policy, provided that the same has not been charged against goods declaration; or
  - Upon liquidation of the warehousing goods declaration, cancellation of bonds shall be covered by a separate Raw Materials Liquidation system (RMLS).

## *Repealing Clause*

All orders, memoranda, circulars and issuances inconsistent herewith are hereby repealed and/or deemed modified accordingly.

## *Separability Clause*

If any part or provision of this Order is later declared invalid or illegal, the remaining portion shall remain valid and enforceable.

## *Effectivity*

This Order shall take effect five (5) days after publication in a newspaper of general circulation.

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

# CMO NO. 18-2021

**Date Issued**: May 19, 2021

## *Objectives*

This Order is issued to provide an alternative mode of payment of duties, taxes and other charges for all goods declarations lodged through the E2M.

## *Coverage*

The following goods declaration shall be covered by this Order:

- Consumption (Formal);
- Transit;
- Warehousing;
- Export;
- Informal Entry; and
- Transshipment

## *General Provisions*

- Any accredited importer or exporter is given an option to open prepayment accounts from which payments of duties, taxes and other charges may be made as an alternative to the PASS5 system required to be used by all E2M users.
- Importer or exporter may open and maintain one or more prepayment accounts in any Collection District from which he/she will specify where payment should be made on a per-transaction basis.

  The prepayment account can be used to make payments in any Collection District regardless of where it was opened.
- The following stakeholders can open prepayment accounts for their respective goods declaration:

| Type of Entry | Stakeholders |
|---|---|
| Consumption Formal | Accredited Importer |
| Transit (including shipments from local ports to free zones) | Accredited Importer |
| Warehousing | Accredited Importer |
| Export | Accredited Exporter |
| Informal Entry | Small Value Importer and Air Express Cargo Operators |

## *Procedure for Opening a Prepayment Account*

- An accredited importer or exporter shall download and fill out a Prepayment Registration Form (PRF) (Annex A).
- A ticket shall be opened in the Customer Care Portal System (CCPS) where the electronic Portable Document Format (PDF) of the PRF shall be submitted to the following:
  - Chief, Collection Division - if in the main port of a collection district; or
  - Cashier - if in a sub-port.
- The scanned copy of the PRF may be submitted online or through Flash Drive (USB). Only PDF file type shall be accepted and each document should be submitted as a separate file. The resolution of the electronic documents shall be at least 600dpi. The file name format shall be as follows:
  - PREPAYMENT.PREPAYMENT REGISTRATION FORM
  - PREPAYMENT.CERTIFICATE OF REGISTRATION IN THE CPRS AS IMPORTER/EXPORTER/DECLARANT

    The same template shall be applied in case there are other documents to be submitted.
- Upon receipt of the filled out PRF, the chief of the Collection Division or cashier, as the case may be, shall:
  - Download and print a copy of the PRF;
  - Assign a prepayment account reference number;
  - Create the prepayment account in the E2M Customs Prepayment System;
  - Sign the filled out PRF, with the Account Reference Number filled out; and
  - Upload the signed PRF in the CCPS.
- The accredited importer or exporter shall download the signed PRF. He/she shall present the same to the inhouse bank (Landbank) and make a deposit of any amount into the prepayment account.
- Upon deposit, the inhouse bank (Landbank) shall issue a Bureau of Customs Official Receipt (BCOR) evidencing deposit into the prepayment account.

## *Utilization of Prepayment Account*

- Upon lodgement of goods declaration, the declarant shall fill out the prepayment account number in SAD Box 48 to indicate the utilization of prepayment account as a mode of payment. The Bank Reference Number in SAD Box 28 shall not be filled out.
- In case where the amount deposited in the prepayment account is insufficient to pay duties, taxes and other charges, the assessment of the goods declaration cannot be completed in the E2M System. Thus, the Customs Operations Officer V (principal appraiser) shall forward the notice of assessment through the CCPS in accordance with the template provided under Annex B.
- Once the account has been replenished, the declarant shall notify the principal appraiser through the CCPS after which the processing of the goods declaration in the E2M shall continue.

## *Transferring Funds between Prepayment Accounts*

Funds in any prepayment account cannot be withdrawn. However, they can be transferred from one prepayment account to another prepayment account which is also under the same holder's name.

## *Checking Balance in a Prepayment Account*

Any importer or exporter can check the balance in his prepayment account by inquiring at the Management Information System and Technology Group (MISTG)-Site Team through the CCPS or any other secured BOC prepayment online query by providing the prepayment account number and transaction dates or period covered.

## *Monitoring System*

The MISTG shall create a Monitoring System indicating the real time collection and utilization of the prepayment account. The Monitoring System shall be accessible to the Ports concerned, which shall likewise bear the responsibility of ensuring the accurate recording of the prepayment transactions.

## *Payment Reconciliation*

For purposes of payment reconciliation, the Monitoring System shall likewise be accessible to the Revenue Accounting Division of the Bureau.

## *Repealing Clause*

CMO No. 27-2014 and all orders, memoranda, circulars and issuances inconsistent herewith are hereby repealed and/or deemed modified accordingly.

## *Separability Clause*

If any part of this Order is declared unconstitutional or contrary to existing law, the other parts not so declared shall remail in full force and effect.

## *Effectivity Clause*

This Order shall take effect on May 25, 2021. The Office of National Administrative Register (ONAR) of the UP Law Center shall be provided three (3) certified copies of this Order.

**ANNEX A**

**PRE-PAYMENT REGISTRATION FORM**

**Port of** _____

| | | |
|---|---|---|
| **Type of Account:** ☐ **Importer** ☐ **Exporter** | | |
| **Tax Identification Number (TIN):** | **Account No:** | |
| **Company Name:** | | |
| **Office Address:** | | |
| **Contact Person:** | **Position:** | |
| **Email Address:** | **Tel No/ Mobile No.** | |
| **Submitted by:** | **Account Registered by :** | |
| ***(Signature Over Printed Name)*** | ***(Chief, Collection Division)*** | |

**ANNEX B**

Date _____

Consignee Name
Address

**Notice of Assessment with Insufficient Prepayment Account Balance**

This is to inform you that your goods declaration reference no. _____ for your shipment covered by BL No. _____ with a completed assessment of _____ could not be processed due to insufficient balance in your prepayment account. The computed duties, taxes and other charges are as follows:

| | **Amount Assessed** |
|---|---|
| Customs Duty | |
| Value Added Tax | |
| Others (IPF+CSF+CDS+IRS) | |
| Special Duty | |
| Surcharge | |
| TOTAL | |

We strongly advise you to replenish your prepayment account to proceed with the clearance of your shipment pursuant to Customs Memorandum Order No. _____.

Please be informed that failure to pay the assessed duties, taxes and other charges within fifteen (15) days from receipt hereof shall be a ground for instituting abandonment proceedings against your shipment without prejudice to the application of Section 104 and 1425 of the Customs Modernization and Tariff Act (CMTA).

_____
Principal Appraiser

# CMC NO. 102-2021

**Issue Date:** May 18, 2021

In view of the effectivity of **Executive Order No. 134 (series of 2021)** on "Further Modifying the Rates of Import Duty on Fresh, Chilled or Frozen Meat of Swine under Section 1611 of Republic Act No. 10863, otherwise known as the "Customs Modernization And Tariff Act," Repealing Executive Order No. 128 (s. 2021)" on **18 May 2021**, all concerned are informed that all articles specifically listed in Annex A of EO 134 (s. 2021), which are entered into or withdrawn from warehouses in the Philippines for consumption, shall be levied the temporary MFN rates of duty as prescribed therein.

EO 128 (s. 2021) is hereby repealed. All other issuances, administrative rules and regulations, or parts thereof, which are inconsistent with EO 134 (s. 2021) are likewise repealed and modified accordingly.

EO 134 (s. 2021) shall be effective for a period of one (1) year.

Thus, the Bureau of Customs' Electronic to Mobile (E2M) System is hereto required to reflect the temporary MFN rates of duty pursuant to the said EO.

All District and Sub-port Collectors, and all others concerned are hereby directed to confirm the dissemination of this Order throughout their offices within five (5) days from receipt thereof for records purposes.

This Order shall take effect immediately.

# MISTG MEMO

**Issue Date:** May 19, 2021

In line with the forthcoming implementation of the CMO on the Revised Rules and Regulations on the Opening and Utilization of Prepayment Accounts which repeals CMO No. 27-2014 on the Establishment of Prepaid accounts, Importers and Exporters are given an option to settle their payments of duties, taxes, and other charges in the E2M Prepayment System, aside from the PASS5 system. They may open and maintain their Prepaid accounts with the Land Bank of the Philippines (LBP).

Brokers are no longer allowed to open Prepaid Accounts or make a deposit under their existing Prepaid accounts starting 24 May 2021. Only Importers and Exporters are given an option to do so. For Brokers with existing Prepaid accounts, the funds on the said accounts cannot be withdrawn but can still consume their remaining balance in their accounts while we are on transition stage.

This becomes effective once the CMO is approved and signed by the Commissioner. We will provide you a copy of the signed memorandum for your reference.

For your information and guidance.

# OCOM MEMO NO. 73-2021

**Issue Date:** May 3, 2021

In line with the Bureau's mandate to strengthen its efforts against smuggling and other customs fraud and to closely monitor the entry of meat, poultry, fish and other agricultural products, you are hereby directed to:

- strictly monitor and examine all importation of such shipments verifying the authenticity of the required import clearances, permits, certificates, licenses and other documentary requirements, subject to existing rules and regulations governing importation of agricultural products prior to release from Customs' custody;
- coordinate and endorse all importation of the said products to the Department of Agriculture (DA) and its attached Bureaus-Bureau of Animal Industry (BAI), Bureau of Fisheries and Aquatic Resources (BFAR) and National Meat Inspection Service (NMIS) for the conduct of First Border Inspection; and
- submit consolidated weekly reports to the Port Operations Service, AOCG on all importation of meat, poultry, fish, and other agricultural products in addition to the daily report being submitted to the AOCG, together with a list of such shipments which are either subject to seizure being imported without the required Sanitary and Phytosanitary Import Clearance (SPSIC) or subject to a higher tariff rate in the absence of the required Minimum Access Volume Import Certificate (MAVIC). The report must follow the prescribed format (Annex "A") and must be submitted electronically thru pdc.aocg@customs.gov.ph and pocd@customs.gov.ph not later than Monday of the following week starting May 3 to 9, 2021. Anent thereto, monthly report shall be submitted not later than the first working day of the following month.

For strict compliance.

# OCOM MEMO NO. 75-2021

**Issue Date:** May 3, 2021

Pursuant to the legal opinion of the Office of the Solicitor General on the matter of RA 4653 in relation to importation inside the Freeport Zones, the Bureau will abide by the principle of stare decisis in the application of RA 4653 to importation of used clothing inside the Freeport Zones as instructed by the OSG.

The doctrine of stare decisis directs the adherence to judicial precedents and pursuant to the Supreme Court Resolution in Bureau of Customs vs. Interlink Recyclers Philippines, Freeport Zones being treated as separate customs territory shall be excluded from the prohibition provided under RA 4653, unless the goods are brought into domestic commerce.

For strict compliance.

# OCOM MEMO NO. 77-2021

**Issue Date:** May 11, 2021

- Reference:
  - Customs Memorandum Order (CMO) No. 09-2017 on "STRENGTHENING THE LEGAL SERVICE BY CONSOLIDATING ITS FUNCTIONS UNDER E.O. 724 AND OTHER PERTINENT LAWS, RULES AND REGULATIONS AND CREATING UNITS UNDER THAT SERVICE TO INTENSIFY ITS ROLE IN THE ANTISMUGGLING EFFORTS OF THE BUREAU OF CUSTOMS".
- Relative to the above subject, pertinent provisions of CMO No. 09-2017 are hereunder reproduced as a reminder:

  **"V. OPERATIONAL PROVISIONS**

  **A. Seizure/Forfeiture/Administrative Cases**

  xxx xxx xxx

  ii. All District Collectors/Port Collectors shall, within forty-eight (48) hours from their issuance of a Warrant of Seizure and Detention (WSD), furnish a copy thereof, including its supporting documents, to the Legal Service for the immediate and effective prosecution of seizure cases. Furthermore, in order for the Legal Service to monitor all existing cases in all the Ports, and to take appropriate steps to protect the interest of the government, all District Collectors are required to submit a status report of all pending cases in their respective jurisdiction to the Deputy Commissioner, RCMG, copy furnished the Director, Legal Service, within thirty (30) days from the effectivity of this Order.

  iii. All apprehending units shall be required to submit within forty-eight (48) hours from the issuance the WSD, their Apprehension Report/Officer-on-Case Report together with the supporting copies of Import Entry, Inward Foreign Manifest (IFM), Bill of Lading, Commercial Invoice, and other pertinent documents, to the Director, Legal Service for immediate prosecution of the seizure/forfeiture cases against the apprehended articles and for the initiation of appropriate criminal case against all personalities involved therein."
- For strict and immediate compliance.

# OCOM MEMO NO. 82-2021

**Issue Date:** May 21, 2021

In compliance with the No-Contact Policy and the streamlining of customs policies and procedures, the Public Information and Assistance Division through the Customer Care Center has created a matrix containing all help topics, issues, and concerns raised through portal as well as the offices involved in providing resolution.

All offices are hereby directed to submit their respective turnaround time. In addition, all offices are directed to reply and resolve portal issues based on the turnaround time submitted.

All offices are hereby mandated to appoint BOC-CARES Compliance Focal person who will be the main point of contact for BOC Compliance Team.

All information to be submitted shall be sent to BOC-CARES Senior Compliance Officer Patrick Junior Salantes via email patrickjunior.salantes@customs.gov.ph using the following format:

| HELP TOPIC | OFFICE | TURN AROUND TIME |
|---|---|---|
| | | |

Attached is t
offices for your reference.

For strict compliance.

**BUREAU OF CUSTOMS**
**CUSTOMER CARE PORTAL SYSTEM I** HELP TOPIC

*as of August 2020

| HELP TOPIC | CONCERNED OFFICE |
|---|---|
| AMO Document Submission– Broker – New | AMO |
| AMO Document Submission– Importer – New | AMO |
| AMO Document Submission – Importer – Non-Regular Importer (Once a Year) | AMO |
| AMO Document Submission– Importer – Renewal | AMO |
| AMO Document Submission– Issuance of COA-COR | AMO |
| AMO Accreditation | AMO |
| AMO Accreditation/Issuance of COA/COR | AMO |
| AMO Document Submission | AMO |
| AMO Other Inquiries | AMO |
| Shipment-Alert Concerns | AMT |
| Advance Ruling System | AOCG |
| Customs Bonded Warehouse (CBW) – Renewal of Operator | AOCG |
| Discharge Port Survey | AOCG |
| Balikbayan Box Inquiries | BOC Cares |
| BB File for Deconsolidators ONLY | BOC CARES |
| Feedback | BOC CARES |
| General Inquiry | BOC CARES |
| Package Claim | BOC Cares |
| Report a Problem | BOC CARES |
| Report a Problem (Access Issue) | BOC CARES |
| Automated Bonds Management | Bonds Division |
| Task Force – CAIDTF | CAIDTF |
| Duty Drawback | CIIS |
| AMO Document Submission– Broker – Renewal | CIIS – Port Concerned |
| Order of Payment – Miscellaneous Fees | Collection Division |
| Deferred Payment | Collection Service |
| Appointment | Concerned Office |
| CY/CFS and PEZA | Deputy Collector for Operations |
| Office of the DepColl Operations | Deputy Collector for Operations |
| Operations - Amendment of BL | Deputy Collector for Operations |
| Operations- Copy of Entry Documents | Deputy Collector for Operations |
| Operations - Direct Validation | Deputy Collector for Operations |
| Operations - Extension for Period to File Goods Declaration | Deputy Collector for Operations |
| Operations – Lifting of Abandonment | Deputy Collector for Operations |
| Operations – Others | Deputy Collector for Operations |
| Operations – Request for Dummy BL | Deputy Collector for Operations |
| Operations - Request for Permit to Transfer to CY-CFS | Deputy Collector for Operations |
| Operations - Request for Stripping | Deputy Collector for Operations |
| Advance Ruling System/Origin | ECD |
| TRADENET/E-Certification of Origin | ECD |
| TRADENET/Product Evaluation List | ECD |
| Registered Exporter System (REX) | ECD - AOCG |
| Clearance – Motor Vehicle (EMVMCO) | EMVMCO |
| Task Force – EPCD | EPCD |
| Application for Rapid Pass | ESS |
| Certificate of Origin (CO) | Export Division |

| | |
|---|---|
| Goods Declaration – Export | Export Division |
| Goods Declaration – Consumption | FED |
| PRU Verification | FED |
| Shipment – Examination Schedule | FED |
| Certificate of Payment | FED – Sec 05 |
| Order of Payment – Additional Duties and Taxes | FED/IED |
| Procurement and Other General Services Matters | GSD |
| Employee Retirement | HRMD |
| Recruitment – Hiring and Promotion | HRMD |
| Advance Ruling System/Valuation | IAS |
| Clearance - Value Verification | IAS |
| Goods Declaration – Informal | IED |
| Shipment – Spotcheck and Inspection | Inspection Unit |
| Cancellation Slip | LBD |
| Order of Payment – Demand Letter | LBD |
| Clearance – Legal Matters | Legal Service |
| MISTG Concerns | MISTG |
| MISTG – Data Request | MISTG |
| MISTG – e2m issues and other concerns | MISTG |
| MISTG – Manual Payment | MISTG |
| MISTG – NSW issues | MISTG |
| TRADENET/Application for User Account | MISTG |
| TRADENET/Technical Issues and Concerns | MISTG |
| Office of the Commissioner | OCOM |
| Shipment – Manual Release | ODC |
| Goods Declaration – Transshipment | Operations |
| Order of Payment – PCAG matters | PCAG |
| Bunkering Permit – POM | PID |
| Gate pass (Release/Validation) | PID |
| Notice of Arrival | PID |
| Operations – Boarding Pass | PID |
| Pier and Inspection Division | PID |
| Bunkering Permit – Other Ports | POCD |
| AMO Document Submission – Importer – Small Value Importer (SVI) | Port Concerned |
| AMO Document Submission– Other Government Agencies (OGAS) | Port Concerned |
| Auction | Port Concerned |
| LPSR Validation | Port Concerned |
| Order of Payment – Paymaya (Renewal) | RAD |
| VAT Refund | RAD |
| SGL Accreditation Concerns | SGL Committee – AOCG |
| Tax Exempt | TED |
| Certificate of Identification (CI) Validation | WAD |
| Goods Declaration – Warehousing | Warehouse Offices |
| X-ray Inspection Project | XIP |

# OCOM MEMO NO. 83-2021

**Issue Date:** May 19, 2021

- **Reference:**
  - Customs Memorandum Order (CMO) No. 16-2021 on "PRIVACY MANUAL"
- Relative to the above subject, pertinent provisions of CMO 16-2021 are hereunder reproduced as a reminder:

  "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."
- For strict and immediate compliance.

# OCOM MEMO NO. 85-2021

**Issue Date:** May 27, 2021

In the exigency of service and for the seamless transition to implement the changes introduced by Customs Memorandum Order No. 18-2021 on the "Revised Rules and Regulations on the Opening and Utilization of Prepayment Accounts," all customs brokers with depleted accounts may utilize their existing Prepayment or Prepaid Account and deposit funds therein until **15 June 2021**.

In this regard, all Chiefs of the Collection Division or equivalent units and all offices concerned are directed to inform all customs brokers who will avail of the period extension, that it is incumbent upon them to deposit only the funds necessary to cover their transactions until 15 June 2021. Otherwise, the remaining balance after the period of extension may no longer be utilized and may be subject to refund in accordance with the existing provisions under the Customs Modernization and Tariff Act and other related rules and regulations.

All Chiefs of the Collection Division or equivalent units are likewise enjoined to expedite the approval of the Prepayment Registration Form and the creation of the prepayment account to prevent any delays in the customs clearance of shipments.

For your guidance.

# AOCG MEMO NO. 219-2021

**Issue Date:** May 4, 2021

Pursuant to the provisions of Section 1603 (D of the Customs Modernization and Tariff Act (Republic Act 10863) and Section 4.9 of Commission Order No. 2017-1 (Procedure on Application for an Advance Ruling on Tariff Classification related to Importation of Goods), the Tariff Commission furnished copies of the Advance Ruling (AR) on Tariff Classification with Tariff Classification Circulars (TCC/AR) issued on 27 April 2021 and the same having been reviewed and summarized as follows:

| TCC NO. | DESCRIPTION OF ARTICLES | 2017 AHTN CODE | 2020 RATES OF DUTY |
|---|---|---|---|
| 21-039 | "SONY SOUND BAR, MODEL: HT-G700" | 8518.29.90 | MFN - 3% Ad Valorem<br>ACFTA - Zero* |
| 21-040 | "SONY HOME THEATRE SYSTEM, MODEL: HT-S20R" | 8518.29.90 | MFN - 3% Ad Valorem<br>ACFTA - Zero* |
| 21-041 | "SHRIMP PROTEIN POWDER" | 2309.90.20 | MFN - Zero*<br>ATIGA - Zero* |
| 21-052 | "CHOLINE CHLORIDE" | 2309.90.20 | MFN - Zero* |
| ***Subject to submission of their corresponding CERTIFICATE OF ORIGIN (CO).*** | | | |

# AOCG MEMO NO. 220-2021

**Issue Date:** May 4, 2021

Pursuant to the provisions of Section 1603 (f) of the Customs Modernization and Tariff Act (Republic Act 10863) and Section 4.9 of Commission Order No. 2017-1 (Procedure on Application for an Advance Ruling on Tariff Classification related to Importation of Goods), the Tariff Commission furnished copies of the Advance Ruling (AR) on Tariff Classification with Tariff Classification Circulars (TCC/AR) issued on 15 April 2021 and the same having been reviewed and summarized as follows:

| TCC NO. | DESCRIPTION OF ARTICLES | 2017 AHTN CODE | 2020 RATES OF DUTY |
|---|---|---|---|
| 21-048 | "HUCOG® 5,000 HP (HUMAN CHORIONIC GONADOTROPHIN)" | 3004.39.00 | MFN - 1% Ad Valorem<br>AIFTA -Zero* |
| 21-053 | "HUMOG-150 (HIGHLY PURIFIED MENOTROPHIN)" | 3004.39.00 | MFN - 1% Ad Valorem<br>AIFTA - Zero* |
| 21-054 | "HUMOG-75 (HIGHLY PURIFIED MENOTROPHIN)" | 3004.39.00 | MFN - 1% Ad Valorem<br>AIFTA - Zero* |
| ***Subject to submission of their corresponding CERTIFICATE OF ORIGIN (CO).*** | | | |

# AOCG MEMO NO. 221-2021

**Issue Date:** May 4, 2021

Pursuant to the provisions of Section 1603 (f) of the Customs Modernization and Tariff Act (Republic Act 10863) and Section 4.9 of Commission Order No. 2017-1 (Procedure on Application for an Advance Ruling on Tariff Classification related to Importation of Goods), the Tariff Commission furnished copies of the Advance Ruling (AR) on Tariff Classification with Tariff Classification Circulars (TCC/AR) issued on 21 April 2021 and the same having been reviewed and summarized as follows:

| TCC NO. | DESCRIPTION OF ARTICLES | 2017 AHTN CODE | 2020 RATES OF DUTY |
|---|---|---|---|
| 21-029A | "EASY OPEN END OR LID" | 8309.90.99 | MFN - 10% Ad Valorem<br>ATIGA - Zero* |
| 21-050 | "ACTIM® PARTUS" | 3002.15.00 | MFN - 1% Ad Valorem |
| 21-051 | "ACTIM® PROM" | 3002.15.00 | MFN - 1% Ad Valorem |
| 21-058 | "FISHERMAN'S FRIEND LEMON & MENTHOL FLAVOUR LOZENGES SUGAR FREE" | 2106.90.99 | MFN - 7% Ad Valorem<br>ATIGA - Zero* |
| ***Subject to submission of their corresponding CERTIFICATE OF ORIGIN (CO).*** | | | |

# AOCG MEMO NO. 222-2021

**Issue Date:** May 4, 2021

Pursuant to the provisions of Section 1603 (f) of the Customs Modernization and Tariff Act (Republic Act 10863) and Section 4.9 of Commission Order No. 2017-1 (Procedure on Application for an Advance Ruling on Tariff Classification related to Importation of Goods), the Tariff Commission furnished copies of the Advance Ruling (AR) on Tariff Classification with Tariff Classification Circulars (TCC/AR) issued on 26 April 2021 and the same having been reviewed and summarized as follows:

| TCC NO. | DESCRIPTION OF ARTICLES | 2017 AHTN CODE | 2020 RATES OF DUTY |
|---|---|---|---|
| 21-042 | "VELO NICOTINE POUCH (POLAR MINT, MEDIUM STRENGTH)" | 3824.99.99 | MFN - 3% Ad Valorem |
| 21-056 | "EUXYL® PE 9010" | 3808.99.90 | MFN - 3% Ad Valorem |
| 21-062 | "CONDALAB ANAEROBIC AGAR" | 3821.00.10 | MFN - 3% Ad Valorem |
| ***Subject to submission of their corresponding CERTIFICATE OF ORIGIN (CO).*** | | | |

# AOCG MEMO NO. 234-2021

**Issue Date:** May 11, 2021

This has reference to the Compassionate Special Permits (CSPs) being issued by the FDA Director General to specialized institutions and specialty societies to avail of unregistered or investigational drug products through licensed establishments for certain kind/type of patients, with a specific volume and period of use.

Due to the urgency of the CSP applications and to address the limitations posed by the COVID-19 pandemic, please be informed that scanned copies of approved CSPs are emailed in advance to the clients to facilitate the process of the importation of drugs that are urgently needed to save lives or prevent deterioration of patient condition.

In view thereof, you are hereby directed to:

- ·accept the scanned copies of CSP and utilize the verification system to expedite the importation of urgently needed drugs. Verification of such can be done through clinicalresearch@fda.gov.ph; and
- submit a weekly report on IMPORTATION OF DRUGS WITH CSI's. said report shall be submitted through pocd@customs.gov.ph not later than Monday of the following week starting May 10 to 16, 2021.

For compliance.

# AOCG MEMO NO. 235-2021

**Issue Date:** May 19, 2021

In compliance with Executive Order No. 134 dated 15 May 2021, please be informed that the rates mentioned in the said order has already been updated in the E2M System effective May 19, 2021.

For information.

**ABOUT US**

Nague Malic Magnawa & Associates Customs Brokers (NMM) is a general professional partnership of customs brokers duly registered by the Securities and Exchange Commission and the Bureau of Customs. As the first general professional partnership of customs brokers registered with SEC and BOC, it complies with RA 9280, or the Customs Brokers Act of 2004. It has offices in Metro Manila and Cebu, and brokers in Clark, Subic, Davao, Cagayan de Oro, Batangas, and other major ports and special economic zones in the Philippines.

To learn more about the company, please visit our website at:

**http://www.nmmcustomsbrokers.com/**

If you have questions or comments, you may send them to:

**Atty. Ferdinand Nague**
Managing Partner
rnague@nmm.ph



Digital copies of this Gazette may be viewed and downloaded from:

**http://nmmcustomsbrokers.com/?q=content/nmm-customs-gazette**