REPUBLIC OF THE PHILIPPINES
OFFICE OF THE PRESIDENT
Cagayan Economic Zone Authority

OFFICE OF THE AUDITOR
CEZA
RECEIVED BY:
DATE / TIME: 06-13-22 11:51

MEMORANDUM ORDER NO. 22-021
Series of 2022

SUBJECT: CEZA DATA PRIVACY MANUAL

Republic Act No. 10173 entitled, "An Act Protecting Individual Personal Information in Information and Communications Systems in the Government and the Private Sector" or simply, Data Privacy Act of 2012 (DPA), is the law that gives form to the declared policy of the State to protect the fundamental human right of privacy and communication.

While the State recognizes the vital role of information and communications technology in nation-building, it also acknowledges its inherent obligation to ensure that personal information in information and communications systems in the government and in the private sector are secured and protected.

To this end, in Resolution No. 11-006-21, the CEZA Board of Directors unanimously approved the CEZA Data Privacy Manual in order to implement reasonable and appropriate measures and procedures that guarantee the safety and security of personal data under the control and custody of its departments, divisions, sections, and employees thereby upholding an individual's data privacy rights against natural dangers such as accidental loss or destruction, and human dangers such as unlawful access, fraudulent misuse, unlawful destruction, alteration, and contamination.

In line with the Data Protection Officer's responsibility under Special Order No. 21-099 to ensure compliance with DPA, its IRR, issuances by the NPC, and other applicable laws and policies, the attached CEZA Data Privacy Manual is hereby promulgated.

This Memorandum Order shall take effect immediately through the DMS for internal information and posting in the official website for external information.

SEC. RAUL L. LAMBINO
Administrator and Chief Executive Officer

JUN 10 2022

CEZA
CAGAYAN ECONOMIC ZONE AUTHORITY
20220613-M-03664
Jun 13, 2022 10:16 am

10th floor Greenfield Tower, Mayflower corner Williams Streets,
Greenfield District, Mandaluyong City, Metr Manila, Philippines 1550
Tel. (+632)8291-6704 to 08
Email: info@ceza.gov.ph Website: www.ceza.gov.ph
Cagayan Offices: Centro, Santa Ana, Cagayan 3514 - Tel. (+6378) 395-4832 / 4828
Regional Government Center, Carig Sur,
Tuguegarao City, Cagayan 3500 - Tel. (+6378) 4844 / 4080

BOUNTIFUL CAG

22-097
Republic of the Philippines
Office of the President
CAGAYAN ECONOMIC ZONE AUTHORITY
APPROVED FOR POSTING
Leonardo C. Cruz
Chairman, QMS
06/13/21

CEZA

20220228-M-01242

MEMORANDUM

FOR	:	**ATTY. PERCIVAL P. PERALTA** Attorney V, Legal Division
FROM	:	**RAY-ANN D. QUEREZA-DE ASIS** Legal Researcher
SUBJECT	:	**DATA PRIVACY MANUAL**
DATE	:	**December 9, 2021**

In compliance with Republic Act No. 10173, also known as Data Privacy Act, which aims to protect personal data in information and communications systems, CEZA commits to this mandate and implements this Manual as a reasonable and appropriate measure and procedure that guarantee the safety and security of personal data.

Attached herewith is the Data Privacy Manual duly approved by the CEZA Board of Directors.

DATA PRIVACY MANUAL

REPUBLIC OF THE PHILIPPINES
OFFICE OF THE PRESIDENT
Cagayan Economic Zone Authority

Table of Contents

BACKGROUND

Republic Act No. 10173, otherwise known as the Data Privacy Act of 2012, protects the privacy of individuals while ensuring free flow of information to promote innovation and growth; regulates the collection, recording, organization, storage, updating or modification, retrieval, consultation, use, consolidation, blocking, erasure, or destruction of personal data; and ensures that the Philippines complies with the international standards set for data protection through the National Privacy Commission.

INTRODUCTION

The Cagayan Economic Zone Authority (CEZA) is a government-owned and controlled corporation created by virtue of Republic Act No. 7922, otherwise known as the Cagayan Special Economic Zone Act of 1995, to manage and operate the Cagayan Special Economic Zone and Free Port. CEZA is committed to the highest standards in providing efficient and quality services to all its local and international customers, stakeholders, and other external organizations.

Through the use of Quality Management System, CEZA establishes this privacy manual to implement reasonable and appropriate measures and procedures that guarantee the safety and security of personal data under the control and custody of its departments, divisions, sections, and employees thereby upholding an individual's data privacy rights against natural dangers such as accidental loss or destruction, and human dangers such as unlawful access, fraudulent misuse, unlawful destruction, alteration, and contamination. CEZA respects and values the data privacy of each person, and ensures that all types of personal information collected from individuals, clients, customers, and its employees are processed safely and stored in accordance with the principles of transparency, legitimate purpose, and proportionality.

AIM OF THE DATA PRIVACY MANUAL

Republic Act No. 10173 enforces the protection of personal data in information and communication systems between private sectors and the government. It ensures that personal data are processed according to the general data privacy principles of transparency, legitimate purpose, and proportionality.

It aims to: (1) protect the privacy of individuals while ensuring free flow of information to promote innovation and growth; (2) regulate the collection, recording, organization, storage, updating or modification, retrieval,

consultation, use, consolidation, blocking, erasure or destruction of personal data; and (3) ensure that the Philippines complies with international standards set for data protection through the National Privacy Commission (NPC).

As part of its social responsibility, CEZA is committed to complying with the data privacy laws. It is the policy of CEZA to respect and uphold data privacy rights, and to ensure that all personal data collected from clients, contractors, suppliers, employees, and other third parties, are processed according to the principles of transparency, legitimate purpose, and proportionality as stated in the DPA.

This CEZA Privacy Manual (Manual) is hereby adopted and outlines the data protection and safety measure adopted by CEZA, in compliance with Republic Act No. 10173 or the Data Privacy Act of 2012, its Implementing Rules and Regulations, and other relevant policies, including issuances of the National Privacy Commission.

DEFINITION OF TERMS

For this manual, the following are defined as follows:

a. "Data Subject" refers to an individual whose personal, sensitive personal, or privileged information is processed by CEZA.
b. "Personal Information" refers to any information whether recorded by CEZA in a material form or not, from which the identity of an individual is apparent or can be reasonably and directly ascertained or when put together with other information would directly and certainly identify an individual.
c. Personal Data shall refer to all types of personal information.
d. "Consent of the data subject" refers to any freely given, specific, informed indication of will, whereby the data subject agrees to the collection and processing of his or her personal, sensitive personal, or privileged information.
e. "Processing" refers 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.
f. "Security Incident" refers to an event or occurrence that affects or tends to affect data protection, or may compromise the availability, integrity, and confidentiality of personal data. It includes incidents that would result in a personal data breach, if not safeguards that have been put in place.
g. "Personal Data Breach" or "Data Breach" refers to a breach of security leading to the accidental or unlawful destruction, loss, alteration,

unauthorized disclosure of, or access to, personal data transmitted, stored or otherwise processed.

SCOPES AND LIMITATIONS

This Manual applies to all CEZA departments, divisions and sections, and employees, regardless of the type of employment and contractual arrangement. CEZA Mandaluyong office, Tuguegarao office and Sta. Ana's office must comply with the terms set out in this Manual.

The provisions of this Manual are effective on the date of its promulgation until revoked or amended by the Data Protection Officer.

OFFICE OF THE DATA PRIVACY OFFICER

The Data Protection Officer (DPO) is appointed as a legal requirement, under the Privacy Act of 2021, and to ensure the protection of personal data. It helps improve customer service and enhances responsiveness to growing public awareness and regard for personal data protection.

The DPO is responsible for the supervision and enforcement of this Manual, and the relevant contact details are as follows:

Data Protection Officer
Cagayan Economic Zone Authority
10th floor, Greenfield Tower, Mayflower corner William Street,
Greenfield District, Highway Hills,
Mandaluyong City.

DUTIES OF THE DPO

The DPO, in the disposition of his/her duties, must perform the following:

a. Ensure compliance with DPA, its IRR, issuances by the NPC and other applicable laws and policies;
b. Ascertain that collection of personal data maintains the required standards in personal data processing;
c. Coordinate and cooperate and seek advice to NPC regarding matters concerning data privacy or security issues or concerns;

d. Ensure proper data breach and security incident management, including the preparation and submission to the NPC of reports and other documentation concerning security incidents or data breaches within the prescribed period;
e. Inform and cultivate awareness on privacy and data protection within CEZA, including all relevant laws, rules and regulations, and issuances of the NPC.
f. Serves as the contact person of CEZA vis-à-vis data subject, the NPC, and other authorities in all matters concerning data privacy or security issues or concerns.

CEZA shall conduct mandatory training on data privacy and security as mandated by the Data Privacy Act once a year and will ensure that its personnel who are directly involved in processing personal data shall attend such training.

PROCESSING OF PERSONAL DATA

CEZA, its departments, divisions and sections, and employees process personal data in pursuance of CEZA established procedures:

A. Collection

CEZA shall ensure that the personal information collected from an individual is reasonably necessary, directly related to the activities of CEZA. The personal information of visitors, clients, and customers are limited to the following:

a. Personal details such as full name, gender, affiliations.
b. Contact information such as an address, email address contact number;
c. Applicant information such as academic background and employment background.
d. Medical information collected by the Human Resource and Development for employment purposes.

Personal information is collected in a lawful and fair means, and not in an intrusive way. Whenever personal information is collected by the employees of CEZA, they shall ensure that the individual is aware of the following:

a. Identity of CEZA as the organization collecting and storing the information.
b. Purposes of the information are being collected.
c. Any law, rules, or regulations, if applicable, requires the information to be collected.

d. Consequences for the individual if all or part of the information is provided or not.

The employee attending to the individual will collect such information through the forms that are essential to the services.

The data collected shall be classified as internal or confidential. Data collected as internal are further classified whether it may be publicly available or in confidential nature.

B. Use

As a general rule, CEZA must not use or disclose personal information collected other than for its primary purpose of collection unless the individual consented to the use or disclosure of the information.

Personal information collected shall be used by CEZA for documentation purposes, record keeping, monitoring, reportorial requirements, compliance with legal obligations, and processing of their transaction.

C. Storage, Retention, Destruction.

Personal information collected by CEZA, either by digital/electronic or in physical format shall be kept secured. Information collected and stored in digital/electronic format should be kept in storage devices, limited only to the access of the authorized and appropriate employees. Physical storage of data kept in physical format should be within the premises of CEZA and limited only to the access of the authorized and appropriate employees.

CEZA shall retain personal data collected for a duration necessary to fulfill the identified legitimate purpose or when the processing relevant to the purpose has been terminated.

Guidelines and procedures are developed for the secure disposal and destruction of personal data to prevent further processing, unauthorized access, or disclosure to any other party or public, or prejudice the interests of the data subjects. Upon the expiration of identified purpose, CEZA must take reasonable steps to securely destroy such personal information if it is no longer needed.

All physical copies of personal information under the custody of CEZA personnel that are no longer active and needed are disposed of properly through shredding or any way deemed proper for the safe destruction of the document.

All digital/electronic copies are likewise deleted or any other secured means, from all storage devices, when no longer active or needed.

The processing of personal data shall be in accordance with the parameters and retention periods provided under the Data Privacy Act of 2012, its Implementing Rules, and relevant issuances of the National Privacy Commission, the National Archives of the Philippines Act of 2007, and its implementing Rules and relevant issuances of the National Archives of the Philippines, other CEZA established procedures and laws and regulations that may be connected hereof.

D. Access

As a general rule, the only authorized person shall be allowed to enter or access storage locations, facilities, and devices containing personal data. Other personnel may be granted access upon the approval of the DPO.

The access granted will depend on the classification of the data collected. Data collected internally can be accessed by CEZA personnel who need such data to perform their roles and responsibilities. Data collected that are confidential is highly restricted and may be accessed by certain recognized personnel, only if data is necessary to perform an official task.

Data classified as public are accessible to parties internally and externally of CEZA following some reasonable procedural requirements. No other restrictions are imposed on the access of such data.

E. Disclosure and Sharing

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

SECURITY MEASURES

CEZA implements appropriate security measures to protect all collected personal information of its data subjects against unauthorized access or unauthorized disclosure or destruction. Established procedures outline the proper handling and, securing data collected, as well as the storage. Physical security measures are observed to protect the said information against unauthorized access.

A. Organizational Security Measures.

1. Data Protection Officer and Privacy Focal Persons

The management shall assign a Data Protection Officer which shall exercise the duties and responsibilities as listed herein.

The DPO may promulgate policies, rules, and guidelines related to data privacy, information security, and records management.

In recognition of this Manual, departments. Divisions and sections in the custody of necessary information shall appoint a Privacy Focal Person to support the Data Protection Officer and the implementations of the privacy and security initiatives laid down per office.

The Privacy Focal Person is primarily responsible for the implementation of the initiatives. He/she shall prevent, monitor, mitigate and manage existing and foreseeable security incidents and personal data breaches in their respective units. He/she will report immediately to the DPO privacy issues if necessary.

2. Mandatory Training and Seminars.

CEZA shall ensure to engage personnel primarily involved in the processing of data to attend mandatory training on Records Management and Data Privacy Capacity Building seminar once a year, or as may be necessary to keep abreast the updates on the matter.

The knowledge acquired shall be cascaded to every employee in the forms of training, assemblies, or reading materials available to the employees.

3. Privacy Impact Assessment

The Privacy Focal Person shall conduct Privacy Impact Assessment (PIA) of each department, division, or section relative to the activities involving the processing of personal data.

The PIA includes the assessment of the documents, data processing policies initiated for each department. It also includes the process of understanding the personal data flow, identifying and assessing threats and vulnerabilities, and proposing measures to address privacy risks.

4. Confidentiality

In all actions and decisions involving the processing of personal data, CEZA shall ensure the confidentiality of data not intended for public use.

A non-disclosure agreement shall be signed by an employee in connection with the collection of personal data.

5. **Review of the Privacy Manual.**

The DPO shall ensure that the measures, policies, or procedures set are followed and updated. These measures, policies, or procedures should remain consistent to conform with the current data privacy best practices.

B. Physical Security Measures.

1. Format of data collected.

Personal data collected by CEZA may be in digital/electronic format or paper/physical form.

2. Storage

Personal data in digital/electronic form collected are stored in password-protected computers issued by CEZA. In addition, only CEZA issued Universal Serial Bus (USB), external hard drives, or any other means of storing digital/ electronic data shall be used by authorized CEZA personnel.

Personal data in paper/physical form collected are stored in folders, envelope drawers, or other file storage fixtures within the premises of CEZA. These storages not in use shall be kept secure and locked.

3. Access

Personal data stored in either electronic devices or filing cabinets are accessible only by authorized employees. Other personnel may be granted access upon the approval of the immediate supervisor or the privacy focal person before accessing the said storage.

Any CEZA employee who wishes to see or obtain a photocopy of his/her personal file (CSC 201 File) shall fill up a request form to be approved by the supervisor of the department, division, or section, except for files containing sensitive personal information and privileged personal information which will require the approval of the Data Protection

Officer. The Supervisor shall ensure that the copy to be given to the concerned personnel contains only his/her personal data or file.

4. Monitoring

The inflow and outflow of personal data collected and processed shall be monitored by authorized employees of CEZA through the logbooks or other monitoring procedures best practiced by the department.

The discovery of unauthorized use of personal data shall as soon as possible be reported to the DPO for application of data protection protocols and proper sanction to the person involved thereat.

5. Design of workstations

The machines and workspaces shall be, as much as practicable, be positioned in consideration of privacy and protection of the processing of personal data.

Each department, division, or section shall maintain designated storage which is strictly monitored by the Property Division.

The configuration of the work stations shall be designed to restrict documents or files and screens from the view of those who are not assigned to the concerned work stations.

In recognition of the 5s principle of housekeeping adopted by CEZA, documents about personal data shall be sorted restricting exposure.

6. Duties and responsibilities of data processor

In all actions and decisions involving personal data, CEZA employees shall ensure that the privacy principles of transparency, legitimate purpose, and proportionality are applied.

Personnel in charge of the collecting and processing of data shall always maintain confidentiality and integrity of personal data for its protection. He/she should comply with the measures laid down by CEZA and data privacy regulations.

7. Modes of transfer of Personal data

Transferring of data containing personal information through electronic means shall be used in an encrypted facility.

The use of facsimile technology in transferring personal data is in no case be allowed.

C. Technical Security Measures

1. Monitoring of Security Breaches.

The Management Information Department shall determine and use technologies not falling below industry standards to prevent any attempt to interrupt or disrupt data processing. They shall install/use anti-virus software and encryption in every machine vulnerable to breaches.

The Head of the MID shall regularly read the firewall logs to monitor security breaches and report its status regularly to the DPO.

2. Features of the Security Software

Prior to the installation and use of application software and system software to be used by CEZA, the same shall be reviewed and evaluated by the MID to ensure compatibility of security features.

3. Regular Testing of Security Measures

The MID, in coordination with the DPO, shall review policies, conduct a vulnerability assessment and perform penetration testing within the company on a monthly basis.

4. Encryption

Personal data that are digitally processed are preferably encrypted. Passwords or codes used to access personal data should be sufficient strength to defer password attacks.

BREACH OF SECURITY MEASURES

A. Data Breach Response Team

The Data Breach Response Team (DBRT) is composed of the DPO, the Department Managers of CEZA, or their representatives.

The DBRT shall be responsible for the implementation of the security protocols and compliance with the rules and regulations relevant to the

protection of personal data. They are also responsible for taking immediate action in the event of a security incident or personal data breach, which includes an assessment of the incident or breach that occurred to determine its nature and extent.

B. Measures for the Prevention and Minimization of Security Incidents and Data Breaches

Coordination between privacy focal persons and DPO shall be imposed as needed to identify risks in the processing and monitoring of security breaches.

The DBRT shall conduct PIA annually to identify the possible risk in the processing and monitoring and vulnerability of scanning of computer networks.

CEZA shall conduct an annual review of its policies, guidelines, and procedures, especially those related to data privacy protection.

C. Recovery and restoration Procedure

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

D. Notification Protocol

The privacy focal person who experiences firsthand the risks or breaches shall first report the incident to the DPO for proper investigation or evaluation of the extent of the breach.

The DPO shall then determine the action to respond to the risk and its impending results to mitigate and/or recover the affected data.

In case of an uncontrollable effect, the DPO shall inform the CEZA Administrator and CEO of the breaches and the need to notify the NPC with the affected data subjects within seventy-two hours from the discovery thereof.

When the breaches are controlled and the processing system is stabilized, the DPO shall make a report and recommend plans when encountered with the same incident.

E. Documentation and Reporting of Security Incidents of Personal Data Breach Procedure

The DBRT shall prepare detailed documentation of every security incident and data breach encountered, as well as an annual report to be submitted to the CEZA Administrator and CEO, and the National Privacy Commission.

The report shall contain the following:

1. Personal data involved;
2. Personal Information Controller and contact details;
3. Nature and description of the incident or breach;
4. Date of discovery of the incident or breach;
5. Measures were undertaken to address the breach;

INQUIRIES AND COMPLAINTS

Data subjects may inquire or request information regarding any matter relating to the processing of their personal data under the custody of CEZA, including the data privacy and security policies implemented to ensure the protection of their personal data. Data subjects may write to CEZA at ceza.info.gov.ph and discuss the inquiry, together with their contact details for reference.

Any complaints shall be filed in three (3) copies or sent to ceza.info.gov.ph. The concerned CEZA department, division, or section concerned shall confirm receipt of such to the complainant.

EFFECTIVITY

This Privacy Manual is effective immediately upon approval of the CEZA Board of Directors until revoked, revised, or amended.