EXECUTIVE ORDER NO. 27, SERIES OF 2021

AN ORDER IMPOSING THE POLICIES ON DATA PRIVACY, LOSS OF CONFIDENTIALITY AND PROTECTION OF ELECTRONIC DATA OF THE CITY GOVERNMENT OF SORSOGON

WHEREAS, Article III, Section 7 of the 1987 Philippine Constitution states that "*The right of the people to information on matters of public concern shall be recognized. Access to official records, and to documents, and papers pertaining to official acts, transactions, or decisions, as well as to government research data used as basis for policy development, shall be afforded the citizen, subject to such limitations as may be provided by law*";

WHEREAS, Republic Act No. 10173 otherwise known as the "Data Privacy Act of 2012" declares that "It is the policy of the State to protect the fundamental human right of privacy, of communication while ensuring free flow of information to promote innovation and growth. The State recognizes the vital role of information and communications technology in nation-building and 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";

WHEREAS, the said law applies to the processing of all types of personal information and to any natural and juridical person involved in personal information processing including those personal information controllers and processors who, although not found or established in the Philippines, use equipment that are located in the Philippines, or those who maintain an office, branch or agency in the Philippines;

WHEREAS, the City Government is unyielding in its efforts to be certified under ISO: 9001 2015 in which the maintenance and retention of documented information is of paramount concern;

WHEREAS, to ensure the effective implementation of the Quality Management System (QMS), it is imperative that the LGU impose policies on the protection of data against loss of confidentiality and the establishment of an efficient archive system;

WHEREAS, pertinent data and information must be well protected at all times because it may be legally binding and may constitute the backbone of operations of the local government;

NOW, THEREFORE, I, MA. ESTER E. HAMOR, Mayor of the City of Sorsogon, do hereby order the Strict Implementation of Policies on Data Protection and Establishment of an Archive System in all offices within the City Government of Sorsogon, as follows:

Section 1. DATA PRIVACY. To ensure compliance with Republic Act No. 10173 otherwise known as the Data Privacy Act of 2012, the following mechanisms are established by the LGU, to wit:

1. The designation of Mr. John Jason L. Palma as the Data Protection Officer of the City Government as per Office Order No. 007, Series of 2021 is hereby reiterated with duties and functions enumerated as follows:

    a. Monitor compliance of the City Government with the Data Privacy Act including all pertinent issuances and guidelines of the National Privacy Commission (NPC);
    b. Serve as the contact person of the City Government relative to all matters concerning data privacy and security issues and/or concerns;
    c. Inform, advice and issue recommendations to the management of the City Government in connection with its data processing activities;
    d. Identify and maintain processing activities, measures, projects, programs, or systems and records;
    e. Check for compliance of 3rd party service providers who intends to use the data of the City Government to pertinent Data Sharing Agreement and other contractual obligations;

2. The Data Protection Officer is authorized to affix his signature to the reply and release slip before the same is issued to the client. Any information and data requested for by interested parties shall only be released upon his conformity after verification that such action shall not violate the provisions of Republic Act No. 10173 otherwise known as the "*Data Privacy Act of 2012*";

3. Process for releasing requested information:
    a. Requests for data and/or information must be made in writing addressed to the City Mayor and must comply with the following requisites:
        i. The purpose for the intended use of information if justified and is absolutely necessary;
        ii. The release of information must be on a need-to-know basis only and must comply with the provisions of pertinent laws.
    b. The request must enumerate the data/information requested and shall state intended purpose;
    c. The request shall be forwarded to the office concerned and the Data Protection Officer for processing;
    d. The Data Protection Officer shall verify in close coordination with the head of the office concerned the feasibility of the release of the requested information;
    e. Should the release of such data be a violation of pertinent laws, rules and regulations, the reply and release slip shall be prepared by the office concerned duly noted by the Mayor stating the reasons/s why the information requested cannot be released;
    f. Should the data protection officer give clearance for the release of such information, the office concerned shall prepare pertinent documents as well as the reply and release slip;
    g. The office concerned shall release the information requested to the requesting party and shall have them affix their signature in the receiving copy of the reply and release slip;
    h. A copy of the reply and release slip shall be forwarded to the Data Protection Officer (either in hard or e-copy) for records purposes.

    This section shall apply to those data/information defined under Sections 4, 5 and 6 of the Data Privacy Act of 2012.

Section 2. PROTECTION AGAINST LOSS OF CONFIDENTIALITY. To ensure that no data or information in the possession of the LGU which are of optimum importance in the operations of the City Government, the designated Documented

Information Control Officers (DICOs) of all functional areas shall have additional duties and functions, as follows:

1. The Functional Area DICO shall define the levels of confidentiality of all data and information within the office and shall categorize them into:
    a. Level 1 – those which are for public consumption such as but not limited to forms, demographic data, socio –economic and research and statistical data in general in which no personal details will be given;
    b. Level 2 – those that require clearance from the Data Protection Officer and the Department head before its released i.e., population and survey data, may include personal details subject to the limitations set forth in the Data Privacy Act;
    c. Level 3 – those intended for use for investigation purposes requires clearance from the City Legal Officer and the Local Chief Executive prior to its release.

2. The Functional Area DICO shall likewise be tasked to perform the following duties to wit:
    a. Secure confidential information at all times;
    b. Manage folder access limit employees and clients to the information they need;
    c. Shred confidential documents when they are no longer needed;
    d. Ensure that electronic copies of confidential information are viewed only in secure devices;
    e. Ensure that information is disclosed to other employees only when it is necessary;
    f. Keep confidential documents within the premises of the LGU unless it is necessary to move them upon the direct order of the department head, section chief and/or the Local Chief Executive (LCE);
    g. Ensure that any employee who is separated from employment with the City Government shall return confidential files in their possession.

3. The Confidentiality Policy of the City Government of Sorsogon:

    All confidential information shall be secured at all times and must not be taken outside the Local Government Unit and/or disclosed to others without the conformity of the Data Protection Officer and the Top Management.

    Officials and employees who may have access to confidential activities shall recognize that such proprietary data is valuable and/or easily replicated.

    Thus, all concerned must exercise extraordinary prudence in assuring that these data and information are protected at all times by implementing all legal means necessary to ensure its confidentiality.

4. Confidentiality Measures
    a. Store confidential documents in secure filing cabinets;
    b. Encrypt electronic information and safeguard databases;
    c. Ask employees who request for confidential information to secure clearance from pertinent authorities before the same is released to them;
    d. Require employees who are able to secure clearance to sign a non-disclosure agreement stating, among others, penalties for violation;
    e. Discourage employees to access electronic copies of confidential information via public computers and networks;
    f. Storage of electronics copies of confidential information must include end to end encryption with at rest encryption.

5. Exceptions. Confidential Information may be disclosed for legitimate reasons such as but not limited to the following:

    a. If a regulatory body request for a copy for audit and/or investigation purposes;
    b. If the LGU entails to enter into an agreements that requires disclosing confidential information which must remain within legal boundaries;

    Provided, that such disclosure of confidential information must be properly documented thru the perfection of a non – disclosure agreement and that all required authorizations for its release is complied with.

    Provided further that documentations relative to disclosure of confidential information must bear the signature of the functional area DICO, the Data Protection Officer, the head of the office concerned and the Local Chief Executive to determine its validity.

This section shall apply to hard copies and electronic copies of data and information in the possession of the City Government that are deemed necessary and indispensable for the operations of the LGU.

Section 3. PROTECTION OF ELECTRONIC DATA. To ensure that electronic data used by the City Government at all times, the provisions stated in Sections 1 and 2 hereof are established with additional controls stated below:

1. All Department Heads and Sections Chief are directed to enforce password best practices and prohibit password reuse and sharing;
2. Each department shall likewise enact security policies that shall automatically disapprove the utilization of previously used passwords and impose a mandatory periodic password resets;
3. The Functional Area DICO shall have the following functions relative to Data Protection, as follows:
    a. Classify those information that may be uploaded to the website of the LGU which may be made available for download by the general public;
    b. Ensure that each computer an installed updated Antivirus and that firewalls are activated for devices that are online;
    c. Ensure that all data are save in a hard drive or external drive exclusively for the said purpose;
    d. Establish a System Recovery Point every week;
    e. Conduct a monthly defragmentation and/or disk check.

Section 4. CURRENT POLICIES IN MAINTAINING ICT EQUIPMENT. In the absence of a Department exclusively for the management and maintenance of ICT Equipment, the following guidelines shall govern:

1. It shall be the responsibility of each user to ensure that the device that they are using is of optimum performance;
2. Any problem that may be encountered either in the hardware or software of the device must be reported to a competent technician immediately;
3. Department Heads and Sections Chief are encouraged to include in their respective budget appropriations for the repair and replacement of parts of ICT equipment as well as for updating of software;
4. At present, the City Planning and Development Office (CPDO) is tasked to act as the ICT Section of the City Government in order to respond to the demands to adopt to the era of technological advancement;

5. The CPDO is tasked to spearhead the technical and skills training of the ICT Team to be composed of functional area DICOs on the following subjects:
    a. Minor diagnosis of ICT equipment should there be errors and/or glitches;
    b. Minor repairs;

Section 5. STORAGE AND ARCHIVING POLICY. It shall be the duty of Focal Persons and Functional Area DICOs to ensure that all documents relevant to the operations of their respective offices are stored, recorded and archived properly in accordance with the provisions of the National Archive of the Philippine Act of 2007.

This section shall apply to both hard copies and electronic data stored within the office as well as records of CCTV Cameras over which the provisions of sections 1, 2 and 3 of this order shall apply.

Section 6. CREATION OF AN ICT DEPARTMENT. The CPDO in coordination with pertinent offices is likewise tasked with the formulation of a proposal for the creation and institutionalization of a Department for the Management and Maintenance of ICT equipment and possible infrastructure for the establishment of a centralized archive system.

Section 7. ENFORCEMENT AND TIMELINE. The implementation of the provisions of this Executive Order shall be monitored by the Quality Management Representative assisted by Lead Auditor and the Master Documented Information Control Officer aligned with the standards set forth by ISO:9001 2015 and the provisions of the Local Government Code of 1991.

The completion of the instructions set forth in this Order shall be set on January, 2022 and shall be presented during the first Management Conference for the fiscal year.

Section 8. EFFECTIVITY. This Executive Order shall take effect immediately.

DONE this 4TH day of June, 2021 at Sorsogon City, Philippines.

MA. ESTER E. HAMOR
City Mayor