JENERICK
INTERNATIONAL MANPOWER INC
POEA-085-LB-081622-R

DATA PRIVACY

Background

Republic Act No. 10173, also known as the Data Privacy Act of 2012 (DPA), aims to protect personal data in information and communications systems both in the government and the private sector.

It ensures that entities or organizations processing personal data establish policies, and implement measures and procedures that guarantee the safety and security of personal data under their control or custody, thereby upholding an individual's data privacy rights. A personal information controller or personal information processor is instructed to implement reasonable and appropriate measures to protect personal data against natural dangers such as accidental loss or destruction, and human dangers such as unlawful access, fraudulent misuse, unlawful destruction, alteration and contamination.

To inform its personnel of such measures, each personal information controller or personal information processor is expected to produce a Privacy Manual. The Manual serves as a guide or handbook for ensuring the compliance of an organization or entity with the DPA, its Implementing Rules and Regulations (IRR), and other relevant issuances of the National Privacy Commission (NPC). It also encapsulates the privacy and data protection protocols that need to be observed and carried out within the organization for specific circumstances (e.g., from collection to destruction), directed toward the fulfillment and realization of the rights of data subjects.

Introduction

This Privacy Manual is hereby adopted in compliance with Republic Act No. 10173 or the Data Privacy Act of 2012 (DPA), its Implementing Rules and Regulations, and other relevant policies, including issuances of the National Privacy Commission. This organization respects and values your data privacy rights, and makes sure that all personal

data collected from you, our clients and customers, are processed in adherence to the general principles of transparency, legitimate purpose, and proportionality.

This Manual shall inform you of our data protection and security measures, and may serve as your guide in exercising your rights under the DPA.

Definition of Terms

Terms used in the Manual must be defined for consistency and uniformity in usage. This portion will make sure of that, and allow users of the Manual to understand the words, statements, and concepts used in the document.

- "Data Subject" – refers to an individual whose personal, sensitive personal or privileged information is processed by the organization. It may refer to officers, employees, consultants, and clients of this organization.
- "Personal Information" – refers to any information whether recorded in a material form or not, from which the identity of an individual is apparent or can be reasonably and directly ascertained by the entity holding the information, or when put together with other information would directly and certainly identify an individual.
- "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.

Scope and Limitations

This section defines the coverage of the Manual. Given that the document is essentially an internal issuance and is meant for the use and application of the organization's staff or personnel, that fact should be emphasized here.

Note that it would be useful to develop a separate Privacy Manual meant for external use or for persons who deal with the organization. Certain information may be omitted from that version, particularly those that relate to internal policies or processes that are relevant only to personnel of the organization.

- All personnel of this organization, regardless of the type of employment or contractual arrangement, must comply with the terms set out in this Privacy Manual.

Processing of Personal Data

A. Collection
    - This company collects the basic contact information of clients and customers, including their full name, address, email address, contact number, together with the position they are applying for abroad. Our staff will be attending to applicants by collecting such information through accomplished order forms.

B. Use
    - Personal data collected shall be used for their application for abroad that will be evaluated by our Foreign Recruitment Agency counterparts

C. Storage, Retention and Destruction
    - This company will ensure that personal data under its custody are protected against any accidental or unlawful destruction, alteration and disclosure as well as against any other unlawful processing. The company will implement appropriate security measures in storing collected personal information, depending on the nature of the information. All information gathered shall not be retained for a period longer than one (1) year. After one (1) year, all hard and soft copies of personal information shall be disposed and destroyed, through secured means.

D. Access
    - Due to the sensitive and confidential nature of the personal data under the custody of the company, only the client and the authorized representative of the company shall be allowed to access such personal data, for any purpose, except for those contrary to law, public policy, public order or morals.

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

Security Measures

A. **Organization Security Measures**

Every personal information controller and personal information processor must also consider the human aspect of data protection. The provisions under this section shall include the following:

1. Data Protection Officer (DPO), or Compliance Officer for Privacy (COP)
    - The designated Data Protection Officer is Ms. Cherry Virtucio, who is concurrently serving as the Human Resource Manager of the organization.

2. Functions of the DPO, COP and/or any other responsible personnel with similar functions
    - The Data Protection Officer shall oversee the compliance of the organization with the DPA, its IRR, and other related policies, including the conduct of a Privacy Impact Assessment, implementation of security measures, security incident and data breach protocol, and the inquiry and complaints procedure.

3. Conduct of trainings or seminars to keep personnel, especially the Data Protection Officer updated vis-à-vis developments in data privacy and security
    - The organization shall sponsor a mandatory training on data privacy and security at least once a year. For personnel directly involved in the processing of personal data, management shall ensure their attendance and participation in relevant trainings and orientations, as often as necessary.

4. Conduct of Privacy Impact Assessment (PIA)
    - The organization shall conduct a Privacy Impact Assessment (PIA) relative to all activities, projects and systems involving the processing of personal data. It may choose to outsource the conduct a PIA to a third party.

5. Recording and documentation of activities carried out by the DPO, or the organization itself, to ensure compliance with the DPA, its IRR and other relevant policies.
    - The organization shall sponsor a mandatory training on data privacy and security at least once a year. For personnel directly involved in the processing of personal data, management shall ensure their attendance and participation in relevant trainings and orientations, as often as necessary.

6. Duty of Confidentiality
    - All employees will be asked to sign a Non-Disclosure Agreement. All employees with access to personal data shall operate and hold personal data under strict confidentiality if the same is not intended for public disclosure.

7. Review of Privacy Manual
    - This Manual shall be reviewed and evaluated annually. Privacy and security policies and practices within the organization shall be updated to remain consistent with current data privacy best practices.

B. **Physical Security Measures**

1. Format of data to be collected
    - Personal data in the custody of the organization may be in digital/electronic format and paper-based/physical format.

2. Storage type and location (e.g. filing cabinets, electronic storage system, personal data room/separate room or part of an existing room)
    - All personal data being processed by the organization shall be stored in a data room, where paper-based documents are kept in locked filing cabinets while the digital/electronic files are stored in computers provided and installed by the company.

3. Access procedure of agency personnel
    - Only authorized personnel shall be allowed inside the data room. For this purpose, they shall each be given a duplicate of the key to the room. Other personnel may be granted access to the room upon filing of an access request form with the Data Protection Officer and the latter's approval thereof.

4. Monitoring and limitation of access to room or facility
    - All personnel authorized to enter and access the data room or facility must fill out and register with the online registration platform of the organization, and a logbook placed at the entrance of the room. They shall indicate the date, time, duration and purpose of each access.

5. Design of office space/work station
    - The computers are positioned with considerable spaces between them to maintain privacy and protect the processing of personal data.

6. Persons involved in processing, and their duties and responsibilities
    - Persons involved in processing shall always maintain confidentiality and integrity of personal data. They are not allowed to bring their own gadgets or storage device of any form when entering the data storage room.

7. Modes of transfer of personal data within the organization, or to third parties
    - Transfers of personal data via electronic mail shall use a secure email facility with encryption of the data, including any or all attachments. Facsimile technology shall not be used for transmitting documents containing personal data.

8. Retention and disposal procedure
    - The organization shall retain the personal data of a client for one (1) year from the data of purchase. Upon expiration of such period, all physical and electronic copies of the personal data shall be destroyed and disposed of using secure technology.

C. **Technical Security Measures**

Each personal information controller and personal information processor must implement technical security measures to make sure that there are appropriate and sufficient safeguards to secure the processing of personal data, particularly the computer network in place, including encryption and authentication processes that control and limit access. They include the following, among others:

1. Monitoring for security breaches
    - The organization shall use an intrusion detection system to monitor security breaches and alert the organization of any attempt to interrupt or disturb the system.

2. Security features of the software/s and application/s used
    - The organization shall first review and evaluate software applications before the installation thereof in computers and devices of the organization to ensure the compatibility of security features with overall operations.

3. Process for regularly testing, assessment and evaluation of effectiveness of security measures
    - The organization shall review security policies, conduct vulnerability assessments and perform penetration testing within the company on regular schedule to be prescribed by the appropriate department or unit.

4. Encryption, authentication process, and other technical security measures that control and limit access to personal data
    - Each personnel with access to personal data shall verify his or her identity using a secure encrypted link and multi-level authentication.

Breach and Security Incidents

Every personal information controller or personal information processor must develop and implement policies and procedures for the management of a personal data breach, including security incidents. This section must adequately describe or outline such policies and procedures, including the following:

1. Creation of a Data Breach Response Team
    - A Data Breach Response Team comprising of five (5) officers shall be responsible for ensuring immediate action in the event of a security incident or personal data breach. The team shall conduct an initial assessment of the incident or breach in order to ascertain the nature and extent thereof. It shall also execute measures to mitigate the adverse effects of the incident or breach.

2. Measures to prevent and minimize occurrence of breach and security incidents
    - The organization shall regularly conduct a Privacy Impact Assessment to identify risks in the processing system and monitor for security breaches and vulnerability scanning of computer networks. Personnel directly involved in the processing of personal data must attend trainings and seminars for capacity building. There must also be a periodic review of policies and procedures being implemented in the organization.

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

4. Notification protocol
    - The Head of the Data Breach Response Team shall inform the management of the need to notify the NPC and the data subjects affected by the incident or breach within the period prescribed by law. Management may decide to delegate the actual notification to the head of the Data Breach Response Team.

5. Documentation and reporting procedure of security incidents or a personal data breach
    - The Data Breach Response Team shall prepare a detailed documentation of every incident or breach encountered, as well as an annual report, to be submitted to management and the NPC, within the prescribed period.

Inquiries and Complaints

Every data subject has the right to reasonable access to his or her personal data being processed by the personal information controller or personal information processor. Other available rights include: (1) right to dispute the inaccuracy or error in the personal data; (2) right to request the suspension, withdrawal, blocking, removal or destruction of personal data; and (3) right to complain and be indemnified for any damages sustained due to inaccurate, incomplete, outdated, false, unlawfully obtained or unauthorized use of personal data. Accordingly, there must be a procedure for inquiries and complaints that will specify the means through which concerns, documents, or forms submitted to the organization shall be received and acted upon. This section shall feature such procedure.

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

  Complaints shall be filed in three (3) printed copies, or sent to info@jenerick.com.ph .The concerned department or unit shall confirm with the complainant its receipt of the complaint.

Effectivity

This section indicates the period of effectivity of the Manual, as well as any other document that the organization may issue, and which has the effect of amending the provisions of the Manual.

- The provisions of this Manual are effective Jan 2022, until revoked or amended by this company, through a Board Resolution.