## CONTENTS

1. **Aim of the Data Privacy Manual** .......................................................... 4  
2. **Scope of the Data Privacy Manual** ..................................................... 4  
3. **Principles for Processing Personal Data** ........................................... 5  
   3.1 Transparency ................................................................................. 5  
   3.2 Proportionality .............................................................................. 5  
   3.3 Legitimate Purpose ....................................................................... 5  
4. **Policy Statement** ............................................................................. 5  
5. **Office of the Data Protection Officer** ............................................. 6  
   5.1 Data Protection Officer ................................................................. 6  
   5.2 Reporting ..................................................................................... 6  
   5.3 Duties .......................................................................................... 6  
   5.4 Responsibilities ........................................................................... 7  
6. **Collection, Use and Disclosure of Personal Information** ............... 7  
   6.1 Collection of Personal Information ............................................... 7  
   6.2 Collection of Sensitive Personal Information ................................ 8  
   6.3 Receiving Unsolicited Personal Information ................................ 9  
   6.4 Collection of Personal Information for Research Statistics .......... 9  
   6.5 Collection of Personal Data for CCTV Surveillance .................... 9  
   6.6 Use and Disclosure of Personal Information ................................ 10  
   6.7 Use and Disclosure of Government Related Identifiers ............... 10  
7. **Direct Marketing** ........................................................................... 11  
8. **Access to and Correction of Personal Information** .......................... 12  
9. **Maintaining Data Quality** ............................................................... 13  
10. **Storage and Transmission** .............................................................. 13  
11. **Retention** ...................................................................................... 14  
12. **Disposal and Destruction** .............................................................. 15  
13. **Maintaining Data Security** ............................................................. 15  
14. **Inquiries and Complaints** ............................................................... 16  
15. **Data Incident Notification Protocols** .......................................... 16  
16. **Privacy Impact Assessments** ........................................................ 18  
17. **Data Protection Clause in Megaworld’s Standard Contract Terms** .. 20  
18. **Privacy Contract/Agreement for a Supplier Contract** ................... 20  
19. **Consent** ........................................................................................ 21

Republic Act No. 10173, also known as the Data Privacy Act of 2012 (“DPA”), enforces the protection of personal data in information and communication systems between private sectors and 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, Megaworld Corporation (“Megaworld”) is committed in complying with the data privacy laws. It is the policy of Megaworld 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 pursuant to the principles of transparency, legitimate purpose, and proportionality as stated in the DPA.

This Data Privacy Manual (“Manual”) outlines the data protection and security measures adopted by Megaworld to protect data privacy rights and shall serve as a guide in the exercise of rights under the DPA.


This Manual applies to all departments and employees of Megaworld, both onsite and offsite. This Manual extends to all processing of personal data. Anonymized data (e.g. for statistics or studies), and data of legal entities (e.g. corporations or partnerships) are not subject to this Manual.

1 See Definitions of Terms
3. Principles of Processing Personal Data

3.1 Transparency

Processing of personal data shall be known to the data subject, who must be informed about the nature, purpose, method, and extent of processing; the rights of a data subject and how these can be exercised; and the identity and contact details of the Personal Information Controller (“PIC”).

3.2 Proportionality

The processing of information shall be adequate, relevant, suitable, necessary, and not excessive in relation to a declared and specified purpose.

3.3 Legitimate Purpose

The processing of information shall be compatible with a declared and specified purpose, which must not be contrary to law, morals, or public policy.

4. Policy Statement

4.1 All Megaworld employees are responsible for ensuring compliance with this Privacy Manual, and to clarify any of its provision with their immediate leader and that they will not set out to use their own interpretation of such provision.

4.2 Megaworld provides a framework for processing personal data in compliance with local data privacy laws and professional standards, as well as their own internal policies.

4.3 Megaworld’s data privacy policy is based on the following principles:

1. To protect personal data using appropriate physical, technical, and organizational security measures;
2. To process, store, and disclose personal data only for legitimate business purposes;

---

2 Sec. 18, Rule IV, Implementing Rules and Regulations of R.A. No. 10173
3. To contain terms in contracts with third party suppliers to help ensure that company data is managed according to the same standards Megaworld implement across the enterprise;
4. To give additional attention and care to sensitive personal data, and respect local laws and customs;
5. To identify appropriate measures to maintain personal data as accurate, complete, current, adequate, and reliable; and
6. Where applicable, to provide notice to individuals with whom Megaworld engage, advising them of the purpose for which Megaworld is processing their personal information.

5. Office of the Data Protection Officer

5.1 Data Protection Officer

The Data Protection Officer (“DPO”) has been appointed to champion data protection initiatives and be primarily responsible for monitoring Megaworld’s compliance to relevant privacy and protection requirements.

5.2 Reporting

The DPO must have direct reporting responsibilities to Megaworld’s Executive Committee.

5.3 Duties

The DPO, in disposition of his/her duties must perform the following:
1. Inform and advise regarding complaints and/or the exercise by data subjects of their rights;
2. Ascertain the renewal of accreditations or certifications necessary to maintain the required standards in personal data processing;
3. Ensure proper data breach and security incident management by Megaworld, including the preparation and submission to the NPC of reports and other documentation concerning security incidents or data breaches within the prescribed period;
4. Inform and cultivate awareness on privacy and data protection within Megaworld, including all relevant laws, rules and regulations, and issuances of the NPC;

5. Serve as the contact person of Megaworld vis-à-vis data subjects, the NPC, and other authorities in all matters concerning data privacy or security issues or concerns; and

6. Coordinate and seek advice of the NPC regarding matters concerning data privacy and security.

5.4 Responsibilities

The DPO is responsible for:

1. Implementing practices, procedures, and systems relating to the Megaworld’s functions or activities that:
   a. Will ensure that Megaworld complies with applicable privacy laws and privacy principles; and
   b. Will enable Megaworld to deal with enquiries or complaints from individuals about Megaworld’s compliance with applicable privacy laws and privacy principles.

2. Considering requests from individuals for access to, and correction of, personal information;

3. Receiving complaints from individuals regarding an alleged breach/es of privacy of personal data; and

4. Investigating and resolving complaints internally through mediation with the individual.

6. Collection, Use and Disclosure of Personal Information

6.1 Collection of Personal Information

Megaworld employees must not collect personal information unless the information is reasonably necessary for, or directly related to, one or more of the Megaworld’s functions or activities. Megaworld employees may collect
personal information only by lawful and fair means, and not in an intrusive way. Whenever Megaworld employees and contractors collect personal information about an individual, they must take reasonable steps to ensure that the individual is aware of the following:

1. The identity and contact details of Megaworld as the organization collecting and storing the information;
2. The purposes for which the information is collected;
3. The intended recipients or organizations to which Megaworld usually discloses information of that kind;
4. Any law that requires the particular information to be collected;
5. The main consequences (if any) for the individual if all or part of the information is not provided; and

Where it is reasonable and practical to do so, Megaworld employees will collect personal information about an individual only from that individual. If, however, this information is collected from a person other than the individual, Megaworld employees must act reasonably to ensure the individual is or has been made aware of the matters listed above.

For a more detailed discussion, refer to Annex 1 - Privacy Policy for Websites.

6.2 Collection of Sensitive Personal Information

1. Megaworld employees must only collect sensitive information:\n   a. Where the information is reasonably necessary for one or more of Megaworld’s functions or activities, and with the individual’s consent; or
   b. If the collection is required by law.

---

3 See Definition of terms
6.3 Receiving Unsolicited Personal Information

Where Megaworld employees receive unsolicited personal information about an individual they must immediately determine whether they could have collected the information in accordance with Sections 6.1 and 6.2 above. If so, then this policy shall apply to the processing of such information. Otherwise, then they must either destroy or anonymize the information, if they failed to obtain the consent of the individual (lawfully and reasonably).

6.4 Collection of Personal Information for Research and Statistics

Megaworld employees may also collect personal information for research about an individual from a party other than the individual concerned if:

1. The personal data is publicly available; or
2. There is consent from 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.

6.5 Collection of personal data for CCTV Surveillance

Some of Megaworld’s areas, buildings and sites use CCTV systems to monitor their exterior and interior 24 hours a day for security reasons. This data is recorded. The use of CCTV and recording of CCTV data are only carried in accordance with Megaworld-approved guidelines.

Megaworld will take reasonable efforts to alert the individual that the area is under electronic surveillance (e.g., posting of Privacy Notices on conspicuous areas), unless the CCTV’s are conspicuously established in a public place and whenever an individual is entering a private place.

For the Privacy Policy for camera surveillance, refer to Annex 17 - CCTV Surveillance Systems Policy.
6.6 Use and Disclosure of Personal Information

As a general rule, Megaworld employees must not use or disclose personal information about an individual other than for its primary purpose of collection, unless:

1. The individual has consented to the use or disclosure; or
2. The individual would reasonably expect Megaworld to use or disclose non-sensitive information for a secondary purpose and the secondary purpose is related to the primary purpose; or
3. Megaworld has reason to suspect that unlawful activity has been, or may be engaged in, and uses or discloses the personal information as a necessary part of its investigation of the matter or in reporting its concerns to relevant persons or authorities; or
4. The use or disclosure is required or authorized by or under law, rule or regulation; or
5. Megaworld reasonably believes that the use or disclosure is reasonably necessary for a specified purpose by or on behalf of an enforcement or other body; or
6. Megaworld reasonably believes that the use or disclosure is necessary to prevent or lessen a serious and imminent threat to public health or public safety or the life or health of an individual; or
7. Megaworld must only use or disclose personal information in a manner consistent with any privacy notice provided to an individual.

6.7 Use and Disclosure of Government-Related Identifiers

Megaworld employees must not use and/or disclose government related identifiers (e.g., social security numbers, previous or current health records, licenses or its denials, suspension or revocation, and tax returns) unless such use or disclosure is reasonably necessary for Megaworld to verify the identity of the individual for the purpose of Megaworld’s activities and security of its properties and premises, or alternatively, the use or disclosure is required or authorized under law rule or regulation.

Security clearances should be issued to persons exposed to the processing of personal data.
For templates used for issuing security clearance, refer to Annex 16 - Security Clearance Form.

7. Direct Marketing

7.1 Use of personal information for direct marketing purposes is permitted where:
1. The information has been collected from someone other than the individual and Megaworld has either obtained the individual’s consent; or
2. Megaworld has posted a Privacy Notice regarding the use of personal information, in cases where it is impractical for Megaworld to obtain the individual’s consent before that particular use.

The use of sensitive personal information for direct marketing is permitted only when the individual has consented to the use or disclosure of the information for that purpose.

Megaworld has posted a Privacy Policy regarding the use of personal information, including the use for direct marketing, for public awareness.

7.2 When contacting individuals for direct marketing in whatever form, the following conditions must be followed:
1. Megaworld provides a simple means by which the individual may easily request to not receive direct marketing communications from Megaworld;
2. The individual has not made a request to Megaworld to not receive direct marketing communications; and
3. Megaworld will not charge the individual for giving effect to a request to not receive direct marketing communications.
8. Access to and Correction of Personal Information

8.1 As a general rule, the DPO of Megaworld will, on the request by an individual, provide him or her with access to their personal information within a reasonable time after such reasonable request is made, and will consider a request from the individual for correction of that information.

8.2 The DPO of Megaworld may impose a charge upon the individual to cover the cost of locating, retrieving, reviewing, and copying any material requested by the individual.

8.3 The DPO of Megaworld may however choose to not provide an individual with access to such information. This would include cases where:

1. Megaworld reasonably believes that giving access would pose a serious threat to the life, health, or safety of any individual, or to public health or public safety;
2. Providing access would have an unreasonable impact on the privacy and affairs of other individuals;
3. The request for access is frivolous or vexatious, or the information requested is trivial;
4. The information relates to anticipated or existing legal proceedings and would not be discoverable in those proceedings;
5. Providing access would reveal the intentions of Megaworld in relation to negotiations with the individual in such a way as to prejudice those negotiations;
6. Providing access would be unlawful;
7. Denying access is authorized under law, rule or regulation, or a court/tribunal order;
8. Providing access would be likely to prejudice an investigation of possible unlawful activity or affect security, defense or international relations; or
9. Providing access would be likely to prejudice activities which are carried out by Megaworld on behalf of an enforcement or legal body; or
10. Where an individual:
a. Has been refused access to his or her personal information; or
b. Have requested from Megaworld, correction of his personal information and was refused, if already archived and anonymized.

Then in such cases, the DPO of Megaworld will give the individual a notice that sets out the reasons for the refusal.

For the templates used for accessing and correcting their information, refer to:
- Annex 2 - Access Request Form; and
- Annex 3 - Request for Correction and Erasure Form.

For the tracking all the access, correction, and erasure request, use Annex 05 - Request from Data Subjects Log Tracker.

9. Maintaining Data Quality

Megaworld employees will take reasonable steps to make sure that the personal information they collect, use, or disclose is accurate, complete, up to date, and not misleading.

10. Storage and Transmission

10.1 Megaworld shall implement approved security measures to all personal information stored onsite.
10.2 Access to stored personal information shall be limited only to authorized and appropriate Megaworld employees only.
10.3 Megaworld allows outside transmission of information to the effect that encryption is employed to personal information identified as sensitive.
11. Retention

11.1 Personal data shall be retained only for the duration necessary to fulfill the identified lawful business purpose. All personal data of the data subjects shall be retained only for as long as necessary:
1. For the fulfillment of the declared, specified, and legitimate purpose, or when the processing relevant to the purpose has been terminated; or
2. The establishment, exercise, or defense of legal claims; or
3. For legitimate business purposes, which must be consistent with standards followed by the industry; or
4. In some specific cases, as prescribed by law.

11.2 Megaworld shall develop guidelines and procedures for the retention of personal data. These shall address minimum and maximum retention periods, and modes of storage. (Refer to Appendix 1 - Retention Policy.)

11.3 All hard, system, soft, and electronic copies will be disposed appropriately following our disposal and destruction policy. In cases in which we intend to keep the information after retention period, subsequent consent from the data subject must be obtained.

11.4 Personal data collected for other purposes may be processed for historical, statistical, or scientific purposes, and in cases laid down in law may be stored for longer periods, provided that adequate safeguards are guaranteed by said laws authorizing their processing, or consent has been obtained to retain and use for such purposes.

11.5 Personal data shall not be retained in perpetuity in contemplation of a possible future use yet to be determined.
12. Disposal and Destruction

12.1 Guidelines and procedures shall be 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. These shall also address disposal process on each of the following, but not limited to, the types of storage:

1. Files that contain personal data, whether such files are stored on paper, film, optical or magnetic media; and
2. Computer equipment, such as disk servers, desktop computers and mobile phones at end-of-life, especially storage media, provided that the procedure may include the use of degaussers, erasers, and physical destruction devices, among others.

12.2 Upon the expiration of identified lawful business purposes or withdrawal of consent, Megaworld must take reasonable steps to securely destroy or permanently de-identify or anonymize personal information if it is no longer needed. Data may be pseudonymized or anonymized, as deemed appropriate, to prevent unique identification of an individual.

12.3 Disposal should be in a manner that the personal data should be unreadable (for paper) or irretrievable (for digital records).

13. Maintaining Data Security

13.1 Megaworld employees must take reasonable steps to protect the personal information that Megaworld holds from misuse, interference, and loss, and from unauthorized access, modification, or disclosure.

13.2 Megaworld shall ensure that appropriate physical, technical, and organizational security measures are implemented on personal information storage facilities.
13.3 Megaworld employees must not keep personal information longer than is necessary and must take reasonable steps to securely destroy or permanently delete or de-identify personal information if it is no longer needed.

14. Inquiries and Complaints

14.1 Megaworld should receive all inquiries and complaints related to the privacy of the data subject, as well as entertain and institute an investigation in relation thereof.

14.2 Data subjects may inquire or request for information regarding any matter relating to the processing of their personal data under the custody of Megaworld, including the data privacy and security policies implemented to ensure the protection of their personal data. They may write to the DPO and briefly discuss the inquiry, together with their contact details for reference.

For the templates used for inquiries and complaints, refer to **Annex 4 - Inquiry Complaint Form**.

For the tracking all the inquiries and complaints request, use the **Annex 5 - Request from Data Subjects Log Tracker**.

15. Data Incident Notification Protocols

15.1 Data incident notification protocols are established and maintained in order to deal with an incident (e.g. an inadvertent disclosure of data, lost or stolen data, or improper movement of data across national borders) concerning any personal information.

For detailed discussion on the data incident and breach protocols, refer to **Appendix 2** for the guidelines on **Privacy Incident Severity** on this Manual.
15.2 Megaworld employees must immediately notify the Office of the DPO if they become aware of a data incident to enable the appropriate assessment, investigation and remediation measures to be undertaken in a timely manner (including possible notification to the NPC and other relevant bodies). If the incident occurs or is discovered outside normal working hours, this notification should be done as soon as practicable.

For templates used for notifying the incident for investigation, refer to Annex 6 - Security Incident Report Form.

15.3 The DPO of Megaworld shall maintain communications with the Information Systems Management (“ISM”) Group. Incidents identified by the ISM Group affecting Megaworld must be reported to the DPO.

15.4 The DPO shall notify the NPC and affected data subjects within seventy-two (72) hours upon discovery or a reasonable belief that a personal data breach has occurred. If and only if, the following are all present:

1. There is a breach of sensitive personal information or other information that may, under the circumstances, be used to enable identity fraud;
2. The data is reasonably believed to have been acquired by an unauthorized person; and
3. Either the PIC believes that the data breach is likely to give rise to a real risk of serious harm to the affected data subject/s.

For templates used to notifying NPC for breaches, refer to Annex 7 - Data Breach Notification to NPC Template. For notifying the affected data subjects, the DPO of Megaworld may opt to send a formal letter or an email.

15.5 If there is doubt as to whether notification is indeed necessary, the following factors are to be considered:

1. The likelihood of harm or negative consequences on the affected data subjects;
2. How notification, particularly of the data subjects, could reduce the risks arising from the personal data breach reasonably believed to have occurred; and
3. If the data involves:
   a. Information that would likely affect national security, public safety, public order, or public health;
   b. At least one hundred (100) individuals;
   c. Information required by all applicable laws or rules to be confidential; or
   d. The personal data of vulnerable groups.

4. All events must be recorded in an incident reporting template. Refer to Annex 7 - Security Incident Summary Tracker.

5. Initial investigation should be performed as soon as possible within twenty-four (24) hours from the time the personal data breach was reasonably believed to have occurred. Delay may be allowed if the scope of the breach cannot be determined within the 24-hour period. However, the 72-hour period notification to the NPC must be religiously observed.

6. After notifying the NPC, and subject to the advise of the NPC, steps shall be taken to notify the affected data subject/s. The person designated by Megaworld shall notify the data subjects individually through a secure means of communication either through written or electronic mail.

7. The notification may be made on the basis of available information within the 72-hour period if the personal data breach is likely to give rise to a real risk to the rights and freedoms of data subjects.

16. Privacy Impact Assessments

16.1 Privacy Impact Assessment (“PIA”) should be completed when there are events that significantly change in the privacy environment or affect the processing of personal information, consisting the significant events set forth as follows:
   1. New processes or modification to the current process;
   2. New projects;
3. Marketing initiatives; and/or
4. Changes in the IT System Infrastructure.

16.2 For changes in the IT System Infrastructure, the following triggers, at a minimum, should be considered:

<table>
<thead>
<tr>
<th>PIA Trigger</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Digitization of Records</td>
<td>Converting paper-based records to electronic systems</td>
</tr>
<tr>
<td>Anonymous to Non-Anonymous</td>
<td>Operations performed on existing personal information database changes anonymous information into Sensitive Personal Information (SPI) or Personally Identifiable Information (PII).</td>
</tr>
<tr>
<td>Significant System Management Changes</td>
<td>New uses of existing IT systems, including the application of new technologies significantly changes how SPI or PII is managed in the system. For example, when the company employs new relational database technologies or web-based processing to access multiple data stores such additions could create a more open environment and avenues for exposure of data that previously did not exist.</td>
</tr>
<tr>
<td>Significant Merging</td>
<td>The company adopts or alters business processes so that databases holding PII are merged, centralized, matched with other databases or otherwise significantly manipulated. For example, when databases are merged to create one central source of information, such a link may aggregate data in ways that create privacy concerns not previously an issue.</td>
</tr>
<tr>
<td>New User Access Mechanism</td>
<td>User-authentication technology (e.g., password, digital certificate biometric) is newly applied to an electronic information system accessed by users (including Third Party users).</td>
</tr>
<tr>
<td>External Sources</td>
<td>The company systematically incorporates into existing information systems, databases of personally identifiable information purchased or obtained from third parties or public sources. An exception to this</td>
</tr>
</tbody>
</table>
For the templates used for documenting PIAs, refer to:

- Annex 8 - Privacy Impact Assessment Template; and
- Annex 9 - PIA Tracker.

17. Data Protection Clause in Megaworld’s Standard Contract Terms

In light of Megaworld's obligations under applicable data privacy laws, Megaworld’s Standard Contract Terms shall include Data Protection wording to cover instances where the engagement involves collecting and processing personal information which has been provided to Megaworld. All draft contracts that processes PI and SPI must be forwarded to the Office of the DPO for its review and inclusion of Data Privacy Terms applicable for each engagement. All requests for review of contract to the Office of the DPO must first submit a PIA.

Please refer to Annex 8 - Privacy Impact Assessment Template.

18. Privacy Contract/Agreement for a Supplier Contract

In light of Megaworld's obligations under applicable data privacy laws, Megaworld must ensure that appropriate wording is included in a suppliers/service providers contract where a third-party supplier will receive, or have access to any personal information that Megaworld holds.

Please refer to the following templates:

- Annex 10- Data Sharing Agreement with Third Parties Template;
- Annex 11 - Outsourcing Sub-Contracting Agreement Template; and
- Annex 18 - Third Party Tracker.
19. Consent

In light of Megaworld’s obligations under applicable privacy law, Megaworld must ensure that appropriate wording is included in their consent form where Megaworld will receive, or have access to any personal information.

Please refer to Appendix 3 for the Suggested Wording a consent form.

20. Education and Awareness

Megaworld’s directors, officers, and employees must have access to all applicable Data Privacy policies, procedures, guidelines and Privacy Impact Assessment. Regular classroom training or e-learning must be developed for this purpose. Prospectively, subsequent communication of any changes will also be released or communicated via email and/or SMS.

Training materials include the following:
- Salient features of the DPA and its IRR;
- Local Policies/Guidelines on Data Privacy;
- Data Privacy Incident Reporting;
- Breach Reporting;
- Privacy Impact Assessment;
- Violations to the policy.

Any materials used for data privacy education and awareness may be secured from the Office of the DPO, subject to its approval. Please refer to Annex 12 - Data Privacy Awareness Infographics.

21. Compliance Monitoring and Reporting

21.1 Non-compliance with this policy may result in a breach of the Megaworld’s Personal Data Privacy, the Data Privacy Act of 2012 and other applicable laws.
21.2 Megaworld shall maintain the inventories of Personal Data Processing systems. (Refer to Annex 13 - Personal Data Processing Systems Inventory). Significant changes in the Personal Information Processing Systems shall be updated to the NPC within two (2) months after the implementation of the change.

21.3 Megaworld shall perform regular review of its forms, contracts, policies, and procedures pertaining to ensure compliance to Data Privacy.

21.4 Megaworld, as applicable, shall perform regular privacy compliance monitoring, internal assessments and security audits.

21.5 Megaworld shall renew its annual registration and submit its Annual Incident Report to the National Privacy Commission within two (2) months prior to the deadline of 8th of March of the year.

22. Disciplinary Policies

Megaworld’s directors, officers, and employees are committed and expected to maintain high standard of integrity and excellence in all transactions and dealings with our clients, partners and co-employees, to ensure the high quality of our services. In line with this, any alleged non-compliance by an employee with the DPA, the Privacy Policy and/or Privacy Manual and Megaworld’s data privacy principle shall subject an employee to appropriate disciplinary actions, including dismissal and, if warranted, criminal and civil action, the employee’s said act/s being ultra vires (beyond the scope of my authority) and as such not binding upon Megaworld.

Acts that may be considered as non-compliance with the DPA and the Privacy Policy, and the corresponding disciplinary action, are listed under Annex 20 DPA Regulation. Accordingly, the penalties listed in Annex 19 are hereby amended as follows:
<table>
<thead>
<tr>
<th>ACTS</th>
<th>PENALTIES</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Irresponsible Collection or Use of Personal or Sensitive Personal Information, which includes (but not limited) to the following:</td>
<td></td>
</tr>
<tr>
<td>&gt; Irresponsible accessing or processing of Personal or Sensitive Personal Information;</td>
<td></td>
</tr>
<tr>
<td>&gt; Negligently accessing or processing of Personal or Sensitive Personal Information;</td>
<td></td>
</tr>
<tr>
<td>&gt; Improper disposal of Personal or Sensitive Personal Information;</td>
<td></td>
</tr>
<tr>
<td>&gt; Untimely handling of Security Breaches involving Personal Information.</td>
<td>5 days Suspension</td>
</tr>
<tr>
<td>a. without damage to the Company</td>
<td>b. with damage to the Company</td>
</tr>
<tr>
<td>2. Intentional Unauthorized Collection, Access, Processing or Disclosure of Personal and Sensitive Personal Information; or Concealment of Security Breaches Involving Sensitive Personal Information.</td>
<td>Dismissal</td>
</tr>
</tbody>
</table>
23. Exceptions

Any requests for exceptions to this policy should firstly be referred to the DPO. Written approval, if forthcoming from the DPO, should then be forwarded to the person requesting the exception.

24. Supplement and Retroactivity

This Policy shall be in addition or supplement to any existing policies of Megaworld. To the extent permitted by applicable law and not contrary to any existing policies, any rights and powers granted under this policy shall apply to acts and actions occurring or in progress prior to its adoption.

25. Amendments

This policy will be reviewed at least every two (2) years from its issue date or earlier if deemed required by either of the DPO or Compliance Officer for Privacy (“COP”). All policy changes should be drafted by the DPO and approved by Megaworld Senior Management.

26. Effectivity

The provisions of this Privacy Manual are effective this 29th day of March, 2019, or upon publishing on Megaworld’s employees’ portal, until revoked or amended by Megaworld, as supported by a Board Resolution.
27. Annexes

Annex 1 - Privacy Policy for Websites
Annex 2 - Access Request Form
Annex 3 - Request for Correction and Erasure Form
Annex 4 - Inquiry Complaint Form
Annex 5 - Request from Data Subjects Log Tracker
Annex 6 - Security Incident & Breach Notification Form
Annex 7 - Security Incident Summary Tracker
Annex 8 - Privacy Impact Assessment Template
Annex 9 - Privacy Impact Assessment Tracker
Annex 10 - Data Sharing Agreement with Third Parties Template
Annex 11 - Outsourcing Sub-contracting Agreement Template
Annex 12 - Data Privacy Awareness Infographics
Annex 13 - Personal Data Processing Systems Inventory
Annex 14 - Consent Form Template – For Clients
Annex 15 - Consent Form Template – For Employment
Annex 16 - Security Clearance Form
Annex 17 - CCTV Surveillance Systems Policy
Annex 18 - Third Party Tracker
Annex 19 - Megaworld Memo dated 14 June 2018
Appendix 1 – Retention Policy

1. INTRODUCTION

In Section 11.e of the Data Privacy Act of 2012, personal information must be “retained only for as long as necessary for the fulfillment of the purposes for which the data was obtained, or for the establishment, exercise or defense of legal claims, or for legitimate business purpose, or as provided by law”.

All personal information collected by Megaworld shall be retained only for as long as necessary:

a) for the fulfillment of the declared, specified, and legitimate purpose, or when the processing relevant to the purpose has been terminated;
b) or the establishment, exercise or defense of legal claims;
c) for legitimate business purposes, which must be consistent with standards followed by the industry; or
d) in some specific cases, as prescribed by law to hold about the Data Subject. This form is used to confirm your identity and to assist us in locating your personal data.

2. PURPOSE

The purpose of this document is to establish the requirements for records management for the maintenance, identification, indexing, storage, and control of quality of records by:

2.1 Identifying the type of records to be retained, its retention period, where it is stored, and whom is responsible of its retention.
2.2 Specifying the procedures for disposal of records after its retention date
2.3 Providing the guidelines for identification, collection, indexing, filing, storage and maintenance of records

3. SCOPE

This procedure applies to all personal data processed by Megaworld, regardless of the mode of storage, hard, electronic or system copies. However, these guidelines will not apply where the personal data is aggregated, anonymized, or kept in a form which does not permit identification of data subjects, in which case, the data may be kept longer.
4. DEFINITION OF TERMS

Agency Records
Mainly pertain to the information of contractors, such as but not limited to agents, models, drivers and casual employees.

Customer Records
Mainly pertain to filled-out customer information sheets and other attachments collected in connection with the transactions and dealings with Megaworld.

Data Retention
Also referred to as “Records Retention” or simply “retention” in this document and these pertain to the continued storage of Megaworld’s data for compliance or company reasons.

Employee Records
Mainly pertain to 201 files which includes name, employment details, payroll details, vacation authorization, documentation of sick days, continuing education certificates, performance appraisals, medical records, etc.

Other Records
Mainly pertain to customers’ information collected during events, promotions, and sponsorships.

Record
This pertain to a number of related items of information that are handled as a unit.

Retention Period
Identifies the duration of time for which the information should be maintained or "retained", irrespective of format (paper, electronic, or other means). Upon lapse of this period, all copies should be disposed and destroyed using secured technology. Nonetheless, any record may be retained below but not longer than the maximum retention period.

Supplier Records
Mainly pertain to filled-out forms and other attachments of vendors or suppliers that are used in the course of their business transactions with Megaworld.

5. GENERAL REQUIREMENTS

Each unit shall compile and maintain an official listing of existing records in accordance with the records management of Megaworld. This listing is used to facilitate identification, collection, indexing, and filing of the records.

Retention period set for the existing records must conform to existing laws and regulations, wherever applicable. Please see No. 7.0 for the retention period mandated by regulations. The following are factors that may be considered by Megaworld in determining retention periods of personal data records would include:

1. Legal requirements to which Megaworld may be subject to;
2. Applicable prescription periods in existing law (i.e., money claims);
3. Department of Labor and Employment rules;
4. Bureau of Internal Revenue (“BIR”) regulations for bookkeeping requirements; and
5. Industry standards, practice, and other laws and regulations that apply to the sector.

Upon expiration of the retention period enumerated in the different types of records below, all hard (physical) and soft (electronic and other means) copies of personal data records stored in whatever format/container shall be disposed and destroyed through secured means in accordance with the policies and procedures of Megaworld.

6. RETENTION PERIODS

Agency Records

Ten (10) years after completion of existing contract/transaction

Customer Records

Five (5) years after the last transaction (to extent applicable, no balance, claims, pending transactions, etc.)

Employee Records

Ten (10) years after separation from the company

Other Records
Six (6) years after collection of information

Supplier Records

Five (5) years after last order of “clean” suppliers (no balance, claims, pending transactions, etc.)

Note: Personal data collected for other purposes may be processed for historical, statistical or scientific purposes, and in cases laid down in law may be stored for longer periods, provided that adequate safeguards are guaranteed by said laws authorizing their processing.

7. RETENTION PERIOD MANDATED BY REGULATIONS

A. Bureau of Internal Revenue

BIR Revenue Regulation (RR) 17-2013 enforced a 10-year retention and preservation period for books of accounts and other accounting records, reckoned from the date of filing of the corresponding tax returns.

However, under RR 5-2014 (which amended RR 17-2013), taxpayers may now retain hard copies of such records just for the first five (5) years of this prescribed period. Thereafter, the taxpayer may retain only an electronic copy of the hardcopy (paper) of the books of accounts, subsidiary books, and other accounting records in an electronic storage system.

B. Anti-Money Laundering Act (AMLA)

Rule 9 of the Revised Implementing Rules and Regulations of Republic Act No. 9160 (“Anti-Money Laundering Act of 2001”), as amended by Republic Act No. 9194, requires:

“Rule 9.2.a. Record Keeping: Kinds of Records and Period for Retention. - All records of all transactions of covered institutions shall be maintained and safely stored for five (5) years from the dates of transactions. Said records and files shall contain the full and true identity of the owners or holders of the accounts involved in the covered transactions and all other customer identification documents. Covered institutions shall undertake the necessary adequate security measures to ensure the confidentiality of such file. Covered institutions shall prepare and maintain documentation, in accordance with the aforementioned client
identification requirements, on their customer accounts, relationships and transactions such that any account, relationship or transaction can be so reconstructed as to enable the AMLC, and/or the courts to establish an audit trail for money laundering.

“Rule 9.2.b. Existing and New Accounts and New Transactions. - All records of existing and new accounts and of new transactions shall be maintained and safely stored for five (5) years from October 17, 2001 or from the dates of the accounts or transactions, whichever is later.

“Rule 9.2.c. Closed Accounts. - With respect to closed accounts, the records on customer identification, account files and business correspondence shall be preserved and safely stored for at least five (5) years from the dates when they were closed.

“Rule 9.2.d. Retention of Records in Case a Money Laundering Case has been Filed in Court. - If a money laundering case based on any record kept by the covered institution concerned has been filed in court, said file must be retained beyond the period stipulated in the three (3) immediately preceding sub-Rules as the case may be, until it is confirmed that the case has been finally resolved or terminated by the court.

“Rule 9.2.e. Form of Records. - Records shall be retained as originals in such forms as are admissible in court pursuant to existing laws and the applicable rules promulgated by the Supreme Court.”

C. INSURANCE COMMISSION

Title 5, Section 2 of the Insurance Commission’s Circular Letter 32-2006 provides:

“a. All records on the risk profile of each customer and/or beneficial owner and the data obtained through the CDD process, official identification documents, and the account files or business correspondences shall be maintained and stored safely for five (5) years from the dates of transactions.

....

“c. With respect to closed accounts, the records on customer identification, account files and business correspondence, shall be preserved and safely stored for at least five (5) years from the date when they were closed.
“e. Insurance institutions, inclusive of agents or brokers should follow the usual procedure and retain the records of those contracts which have been settled by maturity, claim or cancellation for a period of five (5) years after that settlement.”

D. STATUTE OF LIMITATIONS OF ACTIONS/PRESCRIPTIVE PERIOD

The following statutes of limitations (laws that set the maximum time after an event that legal proceedings based on that event may be initiated) must be taken into consideration when we determine record retention period.

Labor Cases:
Under Article 291 of the Labor Code, all money claims arising from employer-employee relations shall be filed within three (3) years from the time the cause of action accrued. However, if the claim is for illegal dismissal, the prescriptive period is four (4) years as provided in Article 1146 of the Civil Code.

SSS Claim:
Pursuant to Section 22(b), par. 2 of RA 1161, as amended by Section 1 of RA 8282 or the SSS Law, “The right to institute the necessary action against the employer may be commenced within twenty (20) years from the time the delinquency is known (from discovery of the violation) or the assessment is made by the SSS, or from the time the benefit accrues, as the case may be.”
The 20-year prescriptive period applies to administrative and civil actions against an employer for his failure to remit SSS contributions. On the other hand, criminal actions for violations of the SSS law, prescribe in four (4) years.
Retention period for claim records is 10 years under Art 1144 of the Civil Code. Under SSC Resolution Number 10-19279-10, the reckoning point for the 10-year prescriptive period is the initial settlement date of the retirement, disability or death claim.

ECC Claim:
Prescriptive period is three (3) years from any contingency compensable by the Employees’ Compensation Program.
Tax Cases:

The Philippine Tax Code authorizes the examination of internal revenue taxes within three (3) years after the last day prescribed by law for the filing of the return. However, in case of a false or fraudulent return with intent to evade tax or of failure to file a return, the assessment or a proceeding in court for the collection of such tax may be filed without assessment within ten (10) years from the discovery of falsity, fraud or omission. (Section 222[a] NIRC)

Under Section 281 of the NIRC, “All violations of any provision of this Code shall prescribe after five years”.

Claims/Actions under Consumer Act of the Philippines Article 169 of RA 7394 provides that all actions and claims under the said law shall prescribe within 2 years either from (1) the time of the transaction, (2) commission of deceptive or unfair and unconscionable act or practice or (3) discovery of hidden defects. Ad Standards Council ASC Circular No. 2017-001 or the Digital Guidelines for Non-Regulated and Regulated Categories provides that there is no prescriptive period for post-screened ads. Rule V (Procedure on Dispute and Complain), Manual of Procedures provides that there is also no prescriptive period for complaints based on facts (e.g. those that may be directly verified by data, complaints on copy claim that require technical evidence or research). In all other cases, complaints can be filed within sixty (60) calendar days from first airing, posting, publication, or display of subject copy, claim, visual or slogan in a medium.

Civil Actions:

Article 1139 of the Civil Code provides that an action prescribes by the mere lapse of time fixed by law. Here are examples of prescriptive periods: (a) real action over immovables: 30 years; (b) an action upon a written contract, or upon an obligation created by law, or upon a judgment: 10 years; (c) actions for the recovery of movables: 8 years; (d) actions upon an oral contract, or upon a quasi-contract: 6 years; (e) actions for the rescission or annulment of contracts: 4 years; (f) forcible entry and unlawful detainer: 1 year.

Criminal Cases:

Article 90 of the Revised Penal Code provides that crimes punishable by death, reclusion perpetual (life imprisonment) or reclusion temporal (12 years and 1 day to
20 years) (i.e. graft cases) shall prescribe in 20 years; crimes punishable by other afflictive penalties (such as perpetual disqualification and prision mayor – imprisonment from 6 years and 1 day to 12 years) shall prescribe in 15 years; those punishable by a correctional penalty (6 months and 1 day to 6 years) shall prescribe in 10 years; with the exception of those punishable by arresto mayor (1 month and 1 day to 6 months), which shall prescribe in 5 years. The crime of libel or other similar offenses shall prescribe in one year. The crime of oral defamation and slander by deed shall prescribe in six months. Light offenses prescribe in two months.

Section 1 of Act 3326 provides that violations penalized by special acts shall, unless otherwise provided in such acts, prescribe in accordance with the following rules: (a) after a year for offenses punished only by a fine or by imprisonment for not more than one month, or both; (b) after 4 years for those punished by imprisonment for more than one month, but less than two years; (c) after 8 years for those punished by imprisonment for two years or more, but less than six years; and (d) after 12 years for any other offense punished by imprisonment for six years or more, except the crime of treason, which shall prescribe after 20 years. Violations penalized by municipal ordinances shall prescribe after 2 months.
Appendix 2 - Privacy Incident Severity

1. PRIVACY INCIDENT SEVERITY

The severity of privacy incidents is considered during the classification of a privacy incident and is determined by taking into consideration the following factors:

- Volume of records; or
- Sensitivity of records

The method described below explains how to determine the severity of a privacy incident. This severity will ultimately determine the process, tasks, and activities which need to be concluded in order to address the incident, based on the privacy risk that it poses to Megaworld.

1.1 Volume of Records

This refers to the number of data subjects who may be affected by a privacy incident.

Megaworld has defined the following thresholds for volume of records:

<table>
<thead>
<tr>
<th>Level</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Low</td>
<td>Less than 10 data subjects</td>
</tr>
<tr>
<td>Medium</td>
<td>Between 10 and 100 data subjects</td>
</tr>
<tr>
<td>High</td>
<td>100 and above data subjects</td>
</tr>
</tbody>
</table>

1.2 Sensitivity of Records

The possibility that information, if leaked or otherwise misused, would cause damage or harm to the data subject. The following guideline has been adopted at Megaworld to determine sensitivity of records:

<table>
<thead>
<tr>
<th>Level</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Low</td>
<td>No special personal information categories are included.</td>
</tr>
<tr>
<td></td>
<td>Low potential to cause financial loss or physical harm or harm to dignity.</td>
</tr>
<tr>
<td>Medium</td>
<td>No sensitive personal information categories are included.</td>
</tr>
<tr>
<td></td>
<td>There exists some potential (neither low nor high) to cause financial loss or</td>
</tr>
<tr>
<td></td>
<td>physical harm or harm to dignity.</td>
</tr>
<tr>
<td>High</td>
<td>Sensitive personal information categories are involved.</td>
</tr>
<tr>
<td></td>
<td>High potential to cause financial loss or physical harm or harm to dignity.</td>
</tr>
</tbody>
</table>
1.3 Severity Matrix

Taking into consideration both the volume of records and the sensitivity of the records affected by an event or incident, the following matrix is used to determine the overall severity of the incident, with Severity 1 incidents being most serious, to Severity 3 incidents which have the lowest rating:

<table>
<thead>
<tr>
<th>Volume</th>
<th>Severity 1</th>
<th>Severity 1</th>
<th>Severity 1</th>
</tr>
</thead>
<tbody>
<tr>
<td>High (&gt;100)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Medium (10-100)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Low (&lt;10)</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

2. INCIDENT RESPONSE TEAMS

In order to successfully investigate, respond to, and remediate an identified privacy incident, a basic requirement is to establish a cross-functional, multi-disciplinary incident response team.

Based on the severity of an incident, different role players may need to be involved. The sections which follow provide an indication of the role players who would need to be involved in the various severity categories of incident, but the actual role players who will be involved will need to be determined based on the specific nature and circumstances of any incident.

2.1 Severity 1 Response Team

Severity 1 incidents have the highest severity rating and as such need to be addressed more critically and comprehensively than incidents of a lower rating. Consequently, a larger response team involving more role players may be required to address a severity 1 incident.

<table>
<thead>
<tr>
<th>Table 1: Severity 1 Response Team - Role Players</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mandatory role players to be involved in response (kindly check applicability with the company's organizational structure)</td>
</tr>
<tr>
<td>Office of the Data Protection Officer</td>
</tr>
<tr>
<td>Affected Operating Unit / Support Function</td>
</tr>
</tbody>
</table>
Severity 1 incidents are typically of such a nature that a war-room (e.g. a dedicated meeting room / office space) would likely need to be established to act as a central point for investigation, response, and resolution of such an incident. All members of the response team need to convene in the war-room to establish critical next steps for the incident response. The war-room is only concluded once the incident is resolved, or the immediate urgency for resolution has passed and a suitable plan has been established.

### 2.2 Severity 2 Response Team

Severity 2 incidents have a moderate severity rating, and should be treated as important. However, it may not be required that the same level of seniority of Megaworld’s staff be involved in the incident response, and these incidents may not require as large a team to resolve them.

**Table 2: Severity 2 Response Team - Role Players**

<table>
<thead>
<tr>
<th>Mandatory role players to be involved in response</th>
<th>Optional role players (dependent on nature of incident)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Office of the Data Protection Officer</td>
<td>EXECOM representative</td>
</tr>
<tr>
<td>Affected Operating Unit / Support Function</td>
<td>Security Team</td>
</tr>
<tr>
<td>Opportunities and Risk Management Group</td>
<td>MANCOM representative</td>
</tr>
<tr>
<td>Information Systems Management Group</td>
<td>Public Relations and Media Affairs Group</td>
</tr>
</tbody>
</table>
2.3 Severity 3 Response Team

Severity 3 incidents have the lowest severity rating, and thus it may be possible to address these with a smaller response team.

<table>
<thead>
<tr>
<th>Mandatory role players to be involved in response</th>
<th>Optional role players (dependent on nature of incident)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Office of the Data Protection Officer</td>
<td>EXECOM representative</td>
</tr>
<tr>
<td>Affected Operating Unit / Support Function</td>
<td>Security Team</td>
</tr>
<tr>
<td></td>
<td>MANCOM representative</td>
</tr>
<tr>
<td></td>
<td>Public Relations and Media Affairs Group</td>
</tr>
<tr>
<td></td>
<td>Opportunities and Risk Management Department</td>
</tr>
<tr>
<td></td>
<td>Information Systems Management Department</td>
</tr>
</tbody>
</table>
Appendix 3 – Suggested wording for Megaworld Consent Form

“To the extent necessary to process your and/or your principal’s transaction with Megaworld, you hereby authorize Megaworld to (1) obtain personal information from you, and/or from your principal, if applicable, and (2) retain adequate documentation of the file in line based on our retention policy with provision on applicable laws and professional standards after the termination of the Services. I hereby understand and agree with Megaworld’s Privacy Policy and Terms and Condition and give my consent to its processing of my Personal Data under the Data Privacy Act of 2012.”

Alternatively, Megaworld may opt to use a form to fully disclose to the data subjects the purpose, usage, collection, sharing, retention, and disposal of personal information and obtain consent for such processing. Refer to Annex 14 - Consent Form Template for Clients and Annex 15 - Consent Form Template for Employment.
### Appendix 4 – Definition of Terms

The table below defines the terms and definitions used in this policy.

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Access</td>
<td>Refers to an individual’s right to see and know about his or her own personal information that an organization holds.</td>
</tr>
<tr>
<td>Collection</td>
<td>An organization collects personal information if it gathers, acquires or obtains information from any source, by any means, in circumstances where the individual is identified or is reasonably identifiable. It includes, but not limited, information that:</td>
</tr>
<tr>
<td></td>
<td>● is publicly available information about an identifiable individual that an organization comes across;</td>
</tr>
<tr>
<td></td>
<td>● information the organization receives directly from the individual; and</td>
</tr>
<tr>
<td></td>
<td>● Information about an individual an organization receives from somebody else.</td>
</tr>
<tr>
<td>Data Privacy Officer or DPO</td>
<td>Refers to the officer designated by Megaworld to monitor and ensure the implementation of the Data Privacy policies of Megaworld.</td>
</tr>
<tr>
<td>Direct Marketing</td>
<td>Direct marketing includes activities that promote the sale or purchase of products or services or promote charitable fundraising where the individual is approached directly. It includes in-person approaches by mail, e-mail, facsimile and phone. It includes individually targeted approaches by these means where people are encouraged to buy products and services at a distance (e.g., to buy by phone, mail or website) or to donate to a cause by one of these means.</td>
</tr>
<tr>
<td>Megaworld Employees</td>
<td>Refers to individuals who work for and directly employed by Megaworld Corporation, whether full time or part time. These include, the officers, directors, and management who, in the course of their work, have access to personal and sensitive information, but excludes, but not limited to, OJTs, agency workers, volunteers, contractual workers, and other service providers.</td>
</tr>
<tr>
<td>Personal Information</td>
<td>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.</td>
</tr>
<tr>
<td><strong>Primary Purpose</strong></td>
<td>The primary purpose is the dominant or fundamental reason for information being collected in a particular transaction. There can only be one primary purpose of collection for a particular transaction. When an individual gives (and an organization collects) personal information, the individual and the organization almost always do so for a particular purpose, for example, to buy or sell a particular product or to receive a service. This is the primary purpose of collection, even if the organization has some additional purposes in mind. These additional purposes will always be secondary purposes for that transaction, even if the organization tells the person about them, and even if the organization obtains the individual's consent to use or disclose the information for those additional purposes.</td>
</tr>
<tr>
<td><strong>Reasonable</strong></td>
<td>Generally speaking, they relate to decisions or steps to be taken by organizations in particular circumstances (e.g., when collecting, correcting or using and disclosing information) or to expectations of individuals in those circumstances. Determining what is reasonable involves considering the factual circumstances in which a person or organization is acting rather than the individual's or organization's view of what is reasonable or unreasonable.</td>
</tr>
</tbody>
</table>
| **Related Purpose** | A related purpose includes all the purposes that are directly related purposes as well as certain additional ones. Related purposes must have some connection to, and arise in the context of, the primary purpose. Uses or disclosures for a related purpose would include uses or disclosures:  
- giving a person information closely associated with a particular product or service a person receives from an organization; or  
- notifying a person who has received a service or product from an organization in the past of a business change of address. |
| **Required by Law** | Required by law refers to circumstances where a law (other than the Data Privacy Act of 2012) requires an organization to collect, use or disclose or deny access to, personal information. In certain instances, failing to comply with such a legal requirement may be an offence. |
Such a law may specifically require an organization to collect, use, disclose or deny access. It may also be a law that gives another body, such as a government agency, a general information gathering power that includes the power to require an organization to disclose information to it.

| Sensitive Personal Information | Sensitive personal information refers 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 individual, 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 is not limited to, social security numbers, previous or current health records, licenses or it denials, suspension or revocation and tax returns; or
|                               |   ● specifically established by an executive order or an act of Congress to be kept classified. |

| Use | Use of personal information relates to the handling of the personal information within the organization. Examples of uses of information are:
|     |   ● adding information to a database;
|     |   ● forming an opinion based on information collected and noting it on a file; and
|     |   ● including information in a publication. |

| Vulnerable groups | Pertains to group of individuals that are susceptible to be harmed. This includes:
|                  |   ● children or minors
|                  |   ● person with disability
|                  |   ● senior citizen
|                  |   ● pregnant women |