ANCHOR LAND

PRIVACY MANUAL

Table of Contents

Table of Contents

Background

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

Further, it (1) protects the privacy of individuals while ensuring free flow of information to promote innovation and growth; (2) regulates the collection, recording, organization, storage, updating or modification, retrieval, consultation, use, consolidation, blocking, erasure or destruction of personal data; and (3) ensures that the Philippines complies with international standards set for data protection through National Privacy Commission (NPC).

Section 1. Introduction

Anchor Land Holdings, Inc. ("ALHI" or "Company") hereby adopts its own Privacy Manual, which encapsulates the privacy and data protection protocols of the Company, in compliance with the Republic Act No. 10173 or the Data Privacy Act of 2012 (DPA), its Implementing Rules and Regulations (IRR), and other relevant policies, including issuances of the National Privacy Commission.

The Company respects and values data privacy rights, and makes sure that all personal data collected from our clients, customers, employees, partners and

stakeholders are processed in adherence to the general principles of transparency, legitimate purpose, and proportionality.

This Privacy Manual is intended to inform clients, customers, employees, partners and stakeholders of the Company's data protection and security measures, and may serve as guide in exercising the rights of the data subjects under the DPA.

Section 2. Definition of Terms

The following terms shall have their corresponding meanings as provided below:

DPA	refers to Republic Act No. 10173, also known as the Data Privacy Act of 2012
Commission	refers to the National Privacy Commission
Consent of the data subject	refers to any freely given, specific, informed indication of will, whereby the data subject agrees to the collection and processing of his or her personal, sensitive personal, or privileged information. Consent shall be evidenced by written, electronic or recorded means. It may also be given on behalf of a data subject by a lawful representative or an agent specifically authorized by the data subject to do so
Data subject	refers to an individual whose personal, sensitive personal or privileged information is processed. It may refer to officers, employees, consultants, and clients of this Company
Data processing systems	refers to the structure and procedure by which personal data is collected and further processed in an information and communications system or relevant filing system, including the purpose and intended output of the processing
Data sharing	the disclosure or transfer to a third party of personal data under the custody of a personal information controller or personal information processor. In the case of the latter,

	such disclosure or transfer must have been upon the instructions of the personal information controller concerned. The term excludes outsourcing, or the disclosure or transfer of personal data by a personal information controller to a personal information processor
Direct marketing	refers to communication by whatever means of any advertising or marketing material which is directed to particular individuals
Filing system	refers to any set of information relating to natural or juridical persons to the extent that, although the information is not processed by equipment operating automatically in response to instructions given for that purpose, the set is structured, either by reference to individuals or by reference to criteria relating to individuals, in such a way that specific information relating to a particular individual is readily accessible
Information and communications system	refers to a system for generating, sending, receiving, storing, or otherwise processing electronic data messages or electronic documents, and includes the computer system or other similar device by which data is recorded, transmitted, or stored, and any procedure related to the recording, transmission, or storage of electronic data, electronic message, or electronic document
Personal data	refers to all types of personal information
Personal data breach	refers to a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored, or otherwise processed
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
Personal information controller	refers to a natural or juridical person, or any other body who controls the processing of personal data, or instructs another to process personal data on its behalf. The term excludes: 1. A natural or juridical person, or any other body, who performs such functions as instructed by another person or organization; or 2. A natural person who processes personal data in connection with his or her personal, family, or household affairs. There is control if the natural or juridical person or any other body decides on what information is collected, or the purpose or extent of its processing
Personal information processor	refers to any natural or juridical person or any other body to whom a personal information controller may outsource or instruct the processing of personal data pertaining to a data subject
Processing	refers to any operation or any set of operations performed upon personal data including, but not limited to, the collection, recording, organization, storage, updating or modification, retrieval, consultation, use, consolidation, blocking, erasure or destruction of data. Processing may be performed through automated means, or manual processing, if the personal data are contained or are intended to be contained in a filing system
Profiling	refers to any form of automated processing of personal

	data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyze or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behavior, location or movements
Privileged information	refers to any and all forms of data, which, under the Rules of Court and other pertinent laws constitute privileged communication
Security incident	an event or occurrence that affects or tends to affect data protection, or may compromise the availability, integrity and confidentiality of personal data. It includes incidents that would result to a personal data breach, if not for safeguards that have been put in place
Sensitive personal information	refers to personal information: 1. About an individual's race, ethnic origin, marital status, age, color, and religious, philosophical or political affiliations; 2. 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; 3. 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 its denials, suspension or revocation, and tax returns; and 4. Specifically established by an executive order or an act of Congress to be kept classified.
Process owner	refers to the office that owns, administers, and/or manages a data processing system, or is the principal

custodian of a particular personal data under the control or custody of the Company. It excludes offices or units of service providers.

Section 3. Scopes and Limitations

3.1. This Manual encapsulates the privacy and data protection protocols that need to be observed and carried out within the Company.

3.2. This is applicable to all employees of the Company, regardless of the type of employment or contractual arrangement, and to the extent practicable, agents, brokers, suppliers, contractors, lessors, tenants, customers, and business partners who may receive personal information from the Company, have access to personal data collected or processed by or on behalf of the Company, or who provide information to the Company.

3.3. This Manual covers all personal data collected and processed by the Company subject to compliance with the requirements of the DPA, its IRR, and other issuances of the NPC.

3.4. This Manual also covers the personal data disclosed, shared or transferred by the Company as disclosing party to authorized third parties and that third parties shared, disclosed or transferred with the Company.

Section 4. Data Privacy Principles

The processing of personal data shall be allowed, subject to compliance with the requirements of the DPA, its IRR and other laws allowing disclosure of information to the public, and adherence to the principles of transparency, legitimate purpose and proportionality.

4.1. General Data Privacy Principles

Transparency The data subject must be aware of the nature, purpose, and extent of the processing of his or her personal data, including the

risks and safeguards involved, the identity of personal information controller, his or her rights as a data subject, and how these can be exercised. Any information and communication relating to the processing of personal data should be easy to access and understand, using clear and plain language.

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.
Proportionality	The processing of information shall be adequate, relevant, suitable, necessary, and not excessive in relation to a declared and specified purpose. Personal data shall be processed only if the purpose of the processing could not reasonably be fulfilled by other means.

4.2. General Principles in Collection, Processing and Retention of Data

4.2.1 Data Collection must be for a declared, specified, and legitimate purpose

a. Consent is required prior to the collection and processing of personal data, subject to exemptions provided by the Act and other applicable laws and regulations. When consent is required, it must be time-bound in relation to the declared, specified and legitimate purpose. Consent given may be withdrawn.

b. The data subject must be provided specific information regarding the purpose and extent of processing, including, where applicable, the automated processing of his or her personal data for profiling, or processing for direct marketing, and data sharing.

c. Purpose should be determined and declared before, or as soon as reasonably practicable, after collection of personal data.

d. Only personal data that is necessary and compatible with declared, specified, and legitimate purpose shall be collected.

4.2.2 Data Collection shall be processed fairly and lawfully

a. Processing of data shall uphold the rights of the data subject, including the right to refuse, withdraw consent, or object. It shall likewise be transparent, and allow the data subject sufficient information to know the nature and extent of processing.

b. Information provided to a data subject must always be in clear and plain language to ensure that they are easy to understand and access.

c. Processing of data must be in a manner compatible with a declared, specified, and legitimate purpose.

d. Processed of personal data should be adequate, relevant, and limited to what is necessary in relation to the purposes for which they are processed.

e. Processing of data shall be undertaken in a manner that ensures appropriate privacy and security safeguards.

4.2.3 Data Processing should ensure data quality

a. Personal data should be accurate and where necessary for a declared, specified and legitimate purpose, kept up to date.

b. Inaccurate or incomplete data must be rectified, supplemented, destroyed or their further processing restricted.

4.2.4 Personal data shall not be retained longer than necessary

a. Retention of personal data shall only be for as long as necessary:

(a) for the fulfillment of the declared, specified, and legitimate purpose;

(b) for the establishment, exercise or defense of legal claims; or

(c) for legitimate business purposes, which must be consistent with standards followed by the applicable industry or approved by appropriate government agency.

b. Retention of personal data shall be allowed in cases provided by law.

c. Personal data shall be disposed or discarded in a secure manner that would prevent further processing, unauthorized access, or disclosure to any other party or the public, or prejudice the interests of the data subjects.

4.2.5 Any authorized further processing shall have adequate safeguards

a. Personal data originally collected for a declared, specified, or legitimate purpose may be processed further for historical, statistical, or scientific purposes, and, in cases laid down in law, may be stored for longer periods, subject to implementation of the appropriate organizational, physical, and technical security measures required by the Act in order to safeguard the rights and freedoms of the data subject.

b. Personal data which is aggregated or kept in a form which does not permit identification of data subjects may be kept longer than necessary for the declared, specified, and legitimate purpose.

c. Personal data shall not be retained in perpetuity in contemplation of a possible future use yet to be determined.

4.3. General principles for Data Sharing

4.3.1 Data sharing shall be allowed when it is expressly authorized by law, provided that there are adequate safeguards for data privacy and security, and processing adheres to principle of transparency, legitimate purpose and proportionality.

4.3.2 Data Sharing shall be allowed in the private sector if the data subject consents to data sharing, and the following conditions are complied with:

a. Consent for data sharing shall be required even when the data is to be shared with an affiliate or mother company, or similar relationships.
b.
c. Data sharing for commercial purposes, including direct marketing, be covered by a data sharing agreement.

    (1) The data sharing agreement shall establish adequate safeguards for data privacy and security, and uphold rights of data subjects.

    (2) The data sharing agreement shall be subject to review by the Commission on its own initiative or upon complaint of data subject.

d. The data subject shall be provided with the following information prior to collection or before data is shared:

    (1) Identity of the personal information controllers or personal information processors that will be given access to the personal data;

    (2) Purpose of data sharing;

    (3) Categories of personal data concerned;

    (4) Intended recipients or categories of recipients of the personal data;

    (5) Existence of the rights of data subjects, including the right to access and correction, and the right to object; and

    (6) Other information that would sufficiently notify the data subject of the nature and extent of data sharing and the manner of processing.

e. Further processing of shared data shall adhere to the data privacy principles laid down in the Act, these Rules, and other issuances of the Commission.

4.3.3 Data collected from parties other than the data subject for purpose of research shall be allowed

When the personal data is publicly available, or has the consent of the data subject for purpose of research, data collection shall be allowed; provided that adequate safeguards are in place, and no decision directly affecting the data subject shall be made

on the basis of the data collected or processed. The rights of the data subject shall be upheld without compromising research integrity.

Section 5. Processing of Personal Data

5.1. Collection of personal information (PI)

a. In circumstances where consent is needed, the Company will not collect personal information unless the data subject has given his or her consent prior to the collection or as soon as practicable and reasonable. The consent given is time-bound in relation to the declared, specified and legitimate purpose.

b. Personal information is collected where a data subject is a party to a contractual agreement, and the collection is necessary in order to fulfil obligations under a contract.

c. Personal Information is collected when it is necessary for compliance with a legal obligation to which the personal information controller is subject.

d. Personal Information is collected when it is necessary to protect vitally important interest of the data subject, including life and health.

e. Personal Information is collected when it is necessary to respond to national emergency, to comply with the requirements of public order and safety, or to fulfil functions of public authority.

f. Personal Information is collected when it is reasonably necessary for, or directly related to, one or more of the Company's legitimate business purposes, activities, or functions.

g. The Company will collect personal information about an individual only from the individual alone, except when circumstances warrants that such information be collected from a third party. Nevertheless, the Company will act reasonably to ensure that the individual is or has been made aware of the matter through its Privacy Policy.

5.2. Collection of sensitive personal information (SPI)

a. The Company will not collect sensitive personal information, except in any of the following cases:

   (a) When the data subject has given his or her consent prior to the processing of SPI; or

(b) When the processing of SPI is provided for by existing laws and regulations, and such other lawful criteria for processing SPI as provided by the DPA and other relevant laws.

b. Should collection of sensitive personal information of an individual be necessary, the Company will take reasonable steps to ensure that the individual is aware of the matter through its Privacy Policy.

5.3. Privacy Notice

Whenever the Company collects personal data about an individual, reasonable steps will be employed to ensure that the individual is aware of the following:

(a) What information is collected
(b) The purpose for which the information is collected
(c) The intended recipients or parties to which the Company usually discloses such information
(d) The security measures employed to protect information
(e) The retention and disposal of information
(f) The rights of the data subjects
(g) The identity and contact details of the Company as the organization collecting and storing the information

5.4. Use

The Company, its management and employees shall use the personal data collected only for its declared, specified, and legitimate purpose. However, in the event where the information will be used for a purpose other than those previously declared and specified, the Company shall reasonably act to ensure that the data subject is informed and his or her consent is obtained prior to processing.

5.4.1 Direct Marketing

Personal Information. Use of personal information for direct marketing is permitted where the information has been collected from the data subject and the processing is necessary for the legitimate interests pursued by the Company.

Sensitive Personal Information. Use of sensitive personal information for direct marketing is permitted only when the data subject has consented to the use or disclosure of the information for that purpose.

In each direct marketing communication with the data subject, the Company shall prominently display a notice, that he or she may express a wish to "unsubscribe" or "opt-out" or not to receive any further direct marketing communications. The Company will not charge the data subject for giving effect to a request not to receive direct marketing communications.

5.5. Access and Correction

5.5.1 As a general rule, the DPO shall, at the request of the data subject, provide the data subject with access to his/her personal data within a reasonable time after such request is made and will consider a request from the data subject for correction of that information.

5.5.2 The Company may impose a minimal charge upon the data subject to cover the cost of locating, retrieving, reviewing, and copying any material requested by the data subject.

5.5.3 Nevertheless, the Company may choose not to provide a data subject with access to in cases where:

1. The Company 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 data subjects;
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 the Company in relation to negotiations with the data subjects 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 the Company on behalf of an enforcement or legal body.

In such cases, the DPO of the Company will give the individual a notice that sets out the reasons for the refusal.

5.6. Data Sharing to Third Parties

Personal data shall be disclosed to third parties only for identified lawful business purposes and after obtaining appropriate consent from the data subjects, unless a law or regulation allows or requires otherwise. The Company shall ensure that data sharing shall have adequate safeguards for data privacy and security, and processing adhere to principles of transparency, legitimate purpose and proportionality.

Third parties collecting, storing or processing personal data on behalf of the Company shall:

1. Execute a Data Sharing Agreement to protect personal data consistent with this Manual, Privacy Policy and Notices, and other security measures as prescribed by law.
2. Sign non-disclosure agreements or confidentiality agreements which include privacy clauses in the contracts.
3. Establish procedures to meet the terms of their agreement with the Company to protect personal data in their custody or control.

5.7. Storage, Retention and Destruction

Storage. The Company will ensure that personal data under its custody is 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.

Retention. All information gathered shall be retained in accordance with the retention limit set by our industry standards. The personal data shall be retained only for as long as necessary:

1. For the fulfilment of the purposes for which the data was obtained;
2. For the establishment, exercise, or defense of legal claims;
3. For legitimate business purposes; or
4. In some specific cases, as provided by law.

Destruction. Thereafter, all hard and soft copies of personal information shall be disposed and destroyed, through secured means.

Section 6. Security Measures

Security measures aim to maintain the *availability*, *integrity* and *confidentiality* of personal data and protect them against natural dangers such as accidental loss or destruction, and human dangers such as unlawful access, fraudulent misuse, unlawful destruction, alteration and contamination.

The Company shall implement reasonable and appropriate physical, technical and organizational measures for the protection of personal data under its custody or control.

The Process Owner/s, with the assistance of the DPO and Security Incident Response Team, shall monitor and implement the Company's compliance with Security Measures herein specified:

6.1. Organizational Security Measures

Organizational Security Measures pertains to the human aspect of data protection, and shall include the following

6.1.1 Data Protection Officer (DPO), or Compliance Officer for Privacy (COP).

The Company shall designate an individual who shall function as DPO. The DPO shall be accountable for ensuring the compliance by the Company with the DPA, its IRR, issuances by the NPC, and other applicable laws and regulation relating to privacy and data protection.

The Company shall also appoint COP(s) for its subsidiaries where appropriate to assist the supervising DPO in the performance of the latter's functions.

6.1.1.1 Functions of the DPO, COP and/or any other responsible personnel with similar functions

A DPO shall, among others:

1. Monitor the Company's compliance with the DPA, its IRR, issuances by the NPC, and other applicable laws and policies.

2. Ensure the conduct of Privacy Impact Assessments relative to activities, measures, projects, programs, or systems of the Company.
3. Advice the Company regarding complaints and/or the exercise by data subjects of their rights.
4. Ensure proper data breach and security incident management by the Company, including the latter's preparation and submission to the NPC of the reports and other documentation concerning security incidents or data breaches within the prescribed period.
5. Inform and cultivate awareness on privacy and data protection within the Company.
6. Advocate for the development, review and/or revision of policies, guidelines, projects, and programs of the Company relating to privacy and data protection, by adopting a privacy by design approach.
7. Serve as the contact person of the Company vis-à-vis data subjects, the NPC and other authorities in all matters concerning data privacy or security issues or concerns.
8. Cooperate, coordinate and seek advice of the NPC regarding matters concerning data privacy and security.
9. Perform other duties and tasks that may be assigned by the Company that will further the interest of data privacy and security and uphold the rights of the data subjects.

Except for items 1 to 3, a COP shall perform all other functions of a DPO.

6.1.1.2 Obligations of the Company relative to the DPO and/or COP

The Company should:

1. Effectively communicate to its personnel, the designation of the DPO or COP and his or her functions.
2. Allow the DPO or COP to be involved from the earliest stage possible in all issues relating to privacy and data protections.
3. Provide sufficient time and resources (financial, infrastructure, equipment, training and staff) necessary for the DPO or COP to keep himself or herself updated with the developments in data privacy and security and to carry out his or her task effectively and efficiently.
4. Grant the DPO or COP appropriate access to the personal data it is processing, including the processing systems.
5. Where applicable, invite the DPO or COP to participate in meetings of senior and middle management to represent the interest of privacy and data protection.

6. Promptly consult the DPO or COP in the event of a personal data breach or security incident.
7. Ensure that the DPO or COP is made a part of all relevant working groups that deal with personal data processing activities conducted inside the Company, or with other Company.

6.1.2 Conduct of Trainings or Seminars and Continuing Education on Data Privacy

All employees of the Company shall be required to read this Privacy Manual upon employment, and/or upon effectivity of this Manual, whichever is applicable.

An Inter-office Memo shall be disseminated to inform employees of any update or issuances of the NPC on data privacy and security, as well as of any update or amendment of this Privacy Manual.

The Company shall sponsor a mandatory training on data privacy and security for at least once a year. For employees directly involved in the processing of personal data, management shall ensure their attendance and participation in relevant trainings and orientations, as often as necessary.

6.1.3 Conduct of Privacy Impact Assessment (PIA)

The Company through its Process Owners and DPO shall conduct a Privacy Impact Assessment relative to all activities, projects and systems involving processing of personal data.

6.1.4 Duty of Confidentiality

All employees will be asked to sign a Non-Disclosure Agreement (NDA). 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. This obligation shall continue upon termination of their employment or contractual relations.

6.1.5 Contracts with Personal Information Processors (PIPs)

The Company shall only engage those PIPs that provide sufficient guarantees to implement appropriate security measures specified in the DPA, its IRR, and other issuances of the NPC, and ensure the protection of the rights of the data subject.

6.1.6 Review of Privacy Manual

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

6.2. Physical Security Measures

6.2.1 Format of data to be collected

Personal data in the custody of the Company may be in digital/electronic format and paper-based/physical format.

6.2.2 Storage type and location

All personal data being processed by the Company shall be stored in a secured data room, whether it be a physical or virtual. Paper-based documents are kept in locked filing cabinets where only authorized personnel shall be allowed access. While the digital/electronic files are stored in password protected computers provided and installed by the company.

6.2.3 Access procedure of employees

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

6.2.4 Monitoring and limitation of access to room or facility

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

6.2.5 Design of office space/work station

Computers shall be positioned with considerable spaces between them to maintain privacy and protect the processing of personal data.

6.2.6 Duties and responsibilities of employees involved in processing

Employees involved in processing shall always maintain confidentiality and integrity of personal data. All employees, whether authorized or not, shall not be allowed to bring their own gadgets or storage device of any form when processing personal data or entering the data storage room.

6.2.7 Modes of transfer of personal data within the Company, 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.

6.2.8 Retention and disposal procedure

The Company shall retain the personal data in its custody and control in accordance with the retention limit set by our industry standards. Upon expiration of such period, all physical and electronic copies of the personal data shall be destroyed and disposed of using secure technology.

6.3 Technical Security Measures

6.3.1 Monitoring for security breaches

6.3.1.1 The Company through its IT Department shall monitor its information and communication system/s through the employment of file integrity monitoring.

6.3.1.2 The IT Department shall run vulnerability scans periodically to detect outdated versions of software and misconfigured networks.

6.3.1.3 The IT Department shall use an intrusion detection system to monitor security breaches and to alert of any attempt to interrupt or disturb its information and communication system/s.

6.3.1.4 The IT Department shall regularly read the firewall logs to monitor security breaches and alert itself of any unauthorized attempt to access the Company network.

6.3.2 Security features of the software/s and application/s used

6.3.2.1 The IT Department 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.

6.3.2.2 The IT Department shall procure and install antivirus software for all Company devices where personal data are stored, including tablets and smartphones that regularly access the internet.

6.3.2.3 The IT Department shall use web application firewall to protect its servers and databases from malicious online attacks.

6.3.3 Process for regularly testing, assessment and evaluation of effectiveness of security measures

The Company shall review security policies, conduct vulnerability assessments and perform penetration testing within the company on regular schedule to be prescribed by the IT Department.

6.3.4 Encryption, authentication process, and other technical security measures that control and limit access to personal data

Encryption. The Company shall employ encryption of personal data most especially sensitive personal data by encoding them into scrambled text using algorithms that render it unreadable unless a cryptographic key is used to convert it.

Authentication. Each employee with access to personal data shall verify his or her identity using a secure encrypted link and multi-level authentication. Any passwords or passcodes used to access personal data should be of maximum strength to deter any password attacks.

Other technical measures. The Company shall use or procure such other technical security measures to keep its software security tools up-to-date.

Section 7. Breach and Security Incidents

7.1. Creation of a Security Incident Response Team

A Security Incident Response Team (SIRT) 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. Other employees/personnel may be called on to join the team on a per incident basis when their expertise or background is appropriate and necessary to effectively address the incident, as recommended by the team officers and approved by the CEO.

7.2. Duties and Responsibilities of the Security Incident Response Team

The team is generally responsible for the following:

1. Implementing security incident management policy of the PIC or PIP;
2. Managing security incidents and personal data breaches; and
3. Compliance by the Company with the relevant provisions of the Act, its IRR, and all related issuances by the Commission on personal data breach management.

Further duties and responsibilities include:

1. Investigate, assess and evaluate security incidents and personal data breaches in coordination with all concerned departments of the Company;
2. Restore integrity to the information and communication system;
3. Recommend mitigation and remedial measures to be performed by the Process Owner/s and other concerned departments;
4. Accomplish of a written report detailing the actions taken in compliance with the DPA;
5. Serve as the contact person/s for all reports of security incidents or personal data breaches; and
6. Act as custodian of all reports and documents submitted or prepared in relation to all security incidents and personal data breaches.

7.3. Measures to prevent and minimize occurrence of breach and security incidents

The Company through its Security Incident Response Team and Process Owner/s 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. A periodic review of policies and procedures being implemented in the Company shall also be conducted.

7.4. Procedure for recovery and restoration of personal data

The Company shall always maintain a backup file for all personal data under its custody and control. 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 security incident or data breach.

7.5. Notification protocol

7.5.1 Mandatory Notification: for the National Privacy Commission

Notification shall be required upon knowledge of or when there is a reasonable belief by the Company that a personal data breach requiring notification has occurred, under the following conditions:

1. It involves sensitive personal information or any *other information*[1] that may be
   used to enable identity fraud;
2. There is reason to believe that the information may have been acquired by an unauthorized person; and
3. There is reason to believe that the unauthorized acquisition is likely to give rise
   to a real risk of serious harm to any affected data subject.

Where there is uncertainty regarding the need to notify the NPC, the following additional factors shall be considered by the Company:

1. The likelihood of harm or negative consequences on the affected data subjects;

[1] "Other information" shall include, but not be limited to: data about financial or economic situation of the data subject; usernames, passwords and other login data; biometric data; copies of identification documents, licenses or unique identifiers like Philhealth, SSS, GSIS, TIN numbers; or other similar information, which may be made basis of decisions concerning the data subject, including the grant of rights or benefits.

2. Notification could reduce the risks arising from the personal data breach reasonably believed to have occurred;
3. The data breach would likely affect national security, public safety, public order, or public health;
4. The data breach affects at least one hundred (100) individuals;
5. The personal data involved is required by applicable laws or rules to be confidential; and
6. The personal data belongs or refers to vulnerable groups.

The DPO shall notify the NPC within seventy-two (72) hours after the Company has determined that a confirmed data breach meets the conditions set out in this Section.

For this purpose, the DPO shall send a notification letter to the NPC via email. The DPO shall make sure to obtain a confirmation from the NPC that it has received the notification letter.

7.5.2 Personal Data Breach Notification to the Data Subject(s)

The Company must also notify the affected data subject within the same period, unless there are grounds recognized by law that allow the Company to forego with such notification.

In determining whether a valid ground exists for not notifying or postponing the notification of the affected data subjects, the Company, through the DPO, may consult with the NPC.

The notification shall include, but not be limited to:

1. Nature of the breach;
2. Personal data possibly involved;
3. Measures taken to address the breach;
4. Measures taken to reduce the harm or negative consequences of the breach;
5. Representative of the PIC, including his or her contact details, from whom the data subject can obtain additional information regarding the breach; and
6. Any assistance to be provided to the affected data subjects.

7.6. Documentation and reporting procedure of security incidents or a personal data breach

All security incidents and personal data breaches shall be documented through written reports, including those not covered by the notification requirements.

The Security Incident 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.

For detailed guidelines, refer to the Security Incident Management Policy.

Section 8. Rights of Data Subject

The right to be informed

The data subject have the right to be informed that his or her personal data will be, are being, or were, collected and processed.

The right to access

The data subject shall have the right to find out whether a Company holds any personal data about him and if so, gain "reasonable access" to them. Through this right, a data subject may also ask to be provided a written description of the kind of information that a Company have about him or her as well as its purpose/s for holding them.

The right to object

The data subject shall have the right to object to the processing of his or her personal data, including processing for direct marketing, automated processing or profiling. The data subject shall also be notified and given an opportunity to withhold consent to the processing in case of changes or any amendment to the information supplied or previously declared to the data subject.

When the data subject object or withhold consent, the Company should no longer process the personal data, unless the processing is pursuant to a subpoena, for obvious purposes, or a result of a legal obligation.

The right to erasure or blocking

The data subject shall have the right to suspend, withdraw or order the blocking, removal or destruction of his or her personal data from the personal information controller's filing system.

This right may be exercised upon discovery and substantial proof of any of the following:

1. The personal data is incomplete, outdated, false, or unlawfully obtained;
2. The personal data is being used for purpose not authorized by the data subject;
3. The personal data is no longer necessary for the purposes for which they were collected;
4. The data subject withdraws consent or objects to the processing, and there is no other legal ground or overriding legitimate interest for the processing;
5. The personal data concerns private information that is prejudicial to data subject, unless justified by freedom of speech, of expression, or of the press or otherwise authorized;
6. The processing is unlawful; or
7. The personal information controller or personal information processor violated the rights of the data subject.

The right to damages

The data subject shall be indemnified for any damages sustained due to such inaccurate, incomplete, outdated, false, unlawfully obtained or unauthorized use of personal data, taking into account any violation of his or her rights and freedoms as data subject.

The right to file a complaint

The data subject through the National Privacy Commission can file complaint when his data privacy is breached.

The right to rectify

The data subject has the right to dispute the inaccuracy or error in the personal data and have the personal information controller correct it immediately and accordingly, unless the request is vexatious or otherwise unreasonable. Once corrected, the personal information controller shall ensure the accessibility of both the new and the retracted information and the simultaneous receipt of the new and the retracted information by the intended recipients thereof. PIC should also furnish third parties with said information, upon reasonable request of the data subject.

The right to data portability

Where personal data is processed by electronic means and in a structured and commonly used format, the data subject shall have the right to obtain from the personal information controller a copy of such data in an electronic or structured format that is commonly used and allows for further use by the data subject.

The exercise of this right shall primarily take into account the right of data subject to have control over his or her personal data being processed based on consent or contract, for commercial purpose, or through automated means.

Section 9. Inquiries

9.1. Who may inquire

Any employee, client, customer, partners, stakeholders or persons may inquire with the Company, as long as it involves a data processing system of the Company and/or personal data under its control or custody.

9.2. Format

An inquiry may be sent or forwarded to the Company's Data Protection Officer through:

Postal address: 15/F L.V. Locsin Building 6752
Ayala Ave., cor. Makati Ave.,

Makati City
Attention to: Data Protection Officer
Email address: alhidataprivacy@anchorland.com.ph

To properly address the inquiry, the DPO will collect basic information about the inquiring party, such as his or her name, email address, contact number, date of inquiry and details of the inquiry. If necessary, submission of relevant document or information in relation to the inquiry may also be required. Upon receipt of the inquiry, the DPO shall send a confirmation email to the inquiring party. An inquiry is not deemed filed without such confirmation.

The DPO may seek the assistance or advice of the relevant Process Owner/Department Head in order to properly address the inquiry.

9.3. Procedure

The inquiry must state clearly the question/s or concern/s. The inquiring party should include all relevant facts and details that would allow the DPO to properly address or resolve the matter.

The DPO shall make an initial assessment of the inquiry:

1. If certain matters need clarifications, the DPO shall contact the inquiring party via email to seek clarification. If the inquiring party fails to respond within five (5) working days, the inquiry will be archived.
2. If the subject of the inquiry does not involve issue/s or concern/s on data privacy and security, the DPO shall inform the inquiring party. However, the DPO may also refer the matter to the appropriate Process Owner or Department, if necessary.

The DPO shall respond to all inquiries within fifteen (15) working days from receipt thereof. However, if the inquiry involves a complicated issue or if additional time is needed to fully address the inquiry, the inquiring party shall be informed.

9.4. Inappropriate Inquiries

The DPO may refrain from answering an inquiry if it is found to be inappropriate, such as:

1. The subject or question has little merit or is of trivial nature;
2. It is frivolous or vexatious; or
3. It concerns the same subject matter which is (a) under investigation or pending before the Security Incident Response Team, any other Department of the Company, the NPC, or other public authorities, law enforcement agencies, or the courts.

9.5. Storage, Retention and Disposal

All inquiries and its corresponding responses will be stored in a safe and secure manner. The same may be disclosed or shared internally only for the purpose of addressing the inquiry. Any information obtained will be held in strict confidentiality and will not be shared with third parties, unless it is necessary to comply with a legal obligation.

All inquiries and related documents or records shall be disposed of in a secure manner within one (1) year after it has been acted upon or answered by the Company.

Section 10. Complaints

10.1. Who may file Complaints

Any employee, client, customer, partners, stakeholders, or persons who are subject of a privacy violation or personal data breach may file complaints for violation of the DPA.

10.2. Format

A complaint may be sent or forwarded to the Company's Data Protection Officer through:

Postal address: 15/F L.V. Locsin Building 6752
Ayala Ave., cor. Makati Ave.,

Makati City
Attention to: Data Protection Officer
Email address: alhidataprivacy@anchorland.com.ph

The DPO will also collect basic information about the complainant, such as his or her name, email address, contact number, date of complaint and details of the complaint. The complaint shall include a brief narration of the material facts and any supporting documents.

Upon receipt of the complaint, the DPO shall send a confirmation email to the complainant. A complaint is not deemed filed without such confirmation.

10.3. Procedure

Evaluation. Upon receipt of the complaint, the DPO shall evaluate the complaint to determine whether its allegations involve a violation of the Data Privacy Act or related issuances by the NPC.

Investigations. If there is a reason to believe that there is a privacy violation or personal data breach, the DPO shall refer the matter to the Security Incident Response Team (SIRT) and conduct an official investigation.

Recommendations. Upon the termination of the investigation, the SIRT shall produce a fact-finding report, which shall include the results of the investigation, the evidence gathered and any recommendations. The report shall be submitted to the management for approval.

10.4. Storage, Retention and Disposal

All complaints and its corresponding responses will be stored in a safe and secure manner. The same may be disclosed or shared internally only for the purpose of addressing the complaint. Any information obtained will be held in strict confidentiality and will not be shared with third parties, unless it is necessary to comply with a legal obligation.

All complaints and related documents or records shall be disposed of in a secure manner within one (1) year after it has been acted upon or answered by the Company.

Section 11. Effectivity

This Privacy Manual was approved by the Board of the Directors of the Company on 28 October 2021 and shall take effect immediately.

ANNEXES

Annex "A" Request for Exercise of Rights

Annex "B" Acknowledgment of Data Subject Request Template

Annex "C" Inquiry/Complaint Form

Annex "D" Incident Report Form (for ALHI employees only)

Annex "E" Mandatory Notification: Personal Data Breach for the National Privacy Commission

Annex "F" Mandatory Notification: Personal Data Breach Notification for the Data Subjects

Annex "G" Annual Security Incident Reports for PICs

Annex "H" Privacy Impact Assessment Template