PHILKOEI INTERNATIONAL, INC.
CONSULTANTS • PLANNERS • ENGINEERS

DATA PRIVACY MANUAL

Approved by the Management Team
January 1, 2025

Implementation Date
January 1, 2025

ARTICLE I: INTRODUCTION

Philkoei International, Inc. (hereby referred to as the "Company") created and implements this Data Privacy Manual (hereby referred to as the "Manual"), pursuant to Republic Act No. 10173, or *An Act Protecting Individual Personal Information in Information and Communication Systems in the Government and the Private Sector, Creating for this Purpose a National Privacy Commission and for Other Purposes*, hereby referred to as the "Act", its Implementing Rules and Regulations or the "IRR", and other relevant policies of the National Privacy Commission or the "Commission".

The Republic Act No. 10173, also known as the Data Privacy Act of 2012, was enacted during the Second Regular Session of the Fifteenth Congress of the Republic of the Philippines, and was signed into law on August 15, 2012 by His Excellency President Benigno S. Aquino III. The Act aims to protect the fundamental human right of privacy and of communication while ensuring free flow of information to promote innovation and growth. The Act also recognizes the vital role of information and communications technology in nation-building and its inherent obligation to ensure that personal information in the information and communications systems in the government and in the private sector are secured and protected. The said Act also ensures that organizations processing personal data establish policies, and implement measures and procedures that guarantee the safety and security of personal data under their control or custody, thereby upholding an individual's data privacy rights. Personal information controllers (PICs) and/or personal information processors (PIPs) are therefore instructed to implement reasonable and appropriate control framework to protect personal data against natural dangers such as accidental loss or destruction, and human dangers such as unlawful access, fraudulent misuse, unlawful destruction, alteration, and contamination.

The Company stands by this Manual in implementing its principal businesses and client transactions to ensure that personal information under its management has its safeguards and is secured while being handled and processed during its business processes and operations following data privacy principles of transparency, legitimate purpose, and proportionality. This Manual also aims to inform the Company's employees, consultants, partners, clients, and stakeholders regarding its safety measures and provides direction in the exercise of their rights in adherence to the Act and other relevant policies and guidelines.

This Manual was reviewed and duly approved by the Management of the Company and shall take effect on January 1, 2025, and supersedes all previous policies, guidelines, rules and regulations, practices, or agreements in relation to data privacy.

The Company reserves the right to add, delete, and adjust any of the policies or procedures indicated in this Manual at any time and will notify employees through a release of the modified guidelines by way of memorandum and notices.

ARTICLE II: DEFINITION OF TERMS

Commission	-	refers to the National Privacy Commission created by virtue of Republic Act No. 10173 also known as the Data Privacy Act of 2012.
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 personal information about

		and/or relating to him or her. Consent shall be evidenced by written, electronic or recorded means. It may also be given on behalf of the data subject by an agent specifically authorized by the data subject to do so.
Data Subject	-	refers to an individual whose personal information is processed.
Filing System	-	refers to any act 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 person 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 or 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 Information (considered as Personal Data)	-	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 (PIC)	-	refers to a person or organization who controls the collection, holding, processing or use of personal information, including a person or organization who instructs another person or organization to collect, hold, process, use, transfer or disclose personal information on his or her behalf. The term excludes: (1) A person or organization who performs such functions as instructed by another person or organization; and (2) An individual who collects, holds, processes, or uses personal information in connection with the individual's personal, family or household affairs.
Personal Information Processor (PIP)	-	refers to any natural or juridical person qualified to act as such under this Act to whom a personal information controller may outsource the processing of personal data pertaining to a data subject.
Processing	-	refers to any operation or any set of operations performed upon personal information including, but not limited to, the collection, recording, organization, storage, updating or modification, retrieval, consultation, use, consolidation, blocking, erasure, or destruction of data.
Privacy Impact Assessment (PIA)	-	a Privacy Impact Assessment (PIA) helps PIC and PIP navigate the process of understanding the personal data flows in the organization. It identifies and provides an assessment of various privacy risks, and proposes measures intended to address them.
Privileged Information (considered as Personal Data)	-	refers to any and all forms of data which under the Rules of Court and other pertinent laws constitute privileged communication.
Sensitive Personal	-	refers to personal information: (1) About an individual's race, ethnic origin, marital status, age, color, and religious, philosophical or political affiliations; (2)

Information (considered as Personal Data)		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 person, 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 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.

ARTCLE III: SCOPE AND LIMITATIONS OF THIS MANUAL

This Data Privacy Manual provides information on data protection, safeguard measures, and security incident procedures. This Manual directs the processing of personal data of data subjects and covers all personnel of the Company, regardless of the type of employment, its applicants, consultants, and applicants and must comply with the terms and provisions set out in this Manual.

ARTCLE IV: APPOINTMENT OF DPO AND COP

Section 1: Data Protection Officer (DPO)
Appointing a DPO is a legal requirement for PICs and PIPs under NPC Advisory No. 2017-01. The Management of the Company shall therefore assign one (1) DPO. The DPO is primarily responsible for ensuring the company's compliance to Republic Act No. 10173 also known as the Data Privacy Act of 2012, its IRR, and other relevant policies and issuances related to this Act by the Commission.

Section 2: Compliance Officer/s for Privacy (COP)
The Management of the Company shall appoint a COP on each department or group who shall assist the DPO in supervising the activities of their respective departments and/or areas of responsibility ensuring that their members comply with the Data Privacy Act of 2012, its IRR, and other relevant policies and issuances related to the Act by the Commission.

Section 3: General Qualifications of the DPO and COP
The DPO and COP must be a regular/ permanent employee of the Company and must have sufficient knowledge acquired from adequate and appropriate trainings and workshops regarding the Data Privacy Act of 2012, its IRR, and relevant policies and issuances related to the Act by the Commission. The DPO and COP must demonstrate truthfulness and reliability in the performance of their respective duties and responsibilities and should also understand the processes being carried out in each department with regard to handling personal data.

Section 4: Tenure and Vacancy
The duration of term of the appointed DPO and COPs shall be for at least three (3) years. Once the terms of the DPO and COP expire and the positions become vacant, the Management of PKII shall appoint, reappoint, or hire a replacement personnel within thirty (30) from the notice of vacancy or resignation provided that the personnel possess the general qualifications of the posts.

ARTICLE V: FUNCTIONS OF THE DPO AND COP

A COP shall perform all other functions of a DPO, and where appropriate, he or she shall also assist the DPO in the execution and performance of its duties and functions regarding data privacy and protection. The following are the duties and responsibilities of the appointed DPO and COP.

1. Monitor the PIC's or PIP's compliance with the Data Privacy Act of 2012, its IRR, issuances by the Commission and other applicable laws and policies as well as the following activities. (i) collect information to identify the Processing, Program, Project, Measure, System, and Technology (PPPMST) of PICs or PIPs and maintain a record thereof; (ii) analyze and check the compliance of processing systems and compliance by third-party service providers, if any; (iii) inform, advise, and issue recommendations to PICs or PIPs regarding data privacy and its protection; (iv) ascertain renewal of accreditations and/or certifications necessary to maintain the required standards in personal data processing; and (v) advice the PIC or PIP regarding the necessity of executing data sharing and outsourcing agreements with third parties, and ensure its compliance with the Act;
2. Oversee the conduct of privacy impact assessments relative to the PPPMST of PICs or PIPs;
3. Assist in the development, review, and/or revision of policies, guidelines, programs, and/or systems of PICs or PIPs relating to data privacy;
4. Promote awareness on data privacy within the organization, including updates on all relevant laws, rules, and regulations and well as on issuances and other directives of the Commission;
5. Advise PICs or PIPs regarding the exercise by the data subjects of their rights as well as security incidents and complaints;
6. Ensure proper incident management by PICs or PIPs, including the preparation and submission to the Commission of necessary reports and other documentation concerning data breaches or security incidents within the given timeframe;
7. Act as the point person of PICs or PIPs concerning data subjects, the Commission, and other authorities in all matters concerning data privacy, concerns of the PICs or PIPs, and security issues;
8. Cooperate, coordinate, and seek advice of the Commission regarding matters concerning data privacy; and
9. Perform other duties and tasks together with the PICs or PIPs that will further promote and uphold data privacy and the rights of the data subjects.

ARTICLE VI. THE DATA PRIVACY TEAM

Section 1. Data Privacy Team

The Data Privacy Team of the Company shall be composed of the DPO and the COPs and shall be responsible for ensuring immediate action on any event or circumstances that concerns data privacy and data breach and security incidents relating to personal data.

Section 2. Duties and Responsibilities of the Data Privacy Team

The duties and responsibility of the members of the Data Privacy Team are the following:

1. Guarantee the implementation of the Data Privacy Act of 2012, its IRR, and all government-related memorandum and issuances by the Commission as well as the execution of the Company's Data Privacy Manual in workplaces and/or project sites;
2. Assess and evaluate incidences of data breach and security incidents;

3. Execute mitigation and security measures to prevent data breach and security incidents; and
4. Comply with the government-mandated and legal documents and reports.

Section 3. Prevention of Data Breach and Security Incidents
The Data Privacy Team shall regularly conduct PIAs to identify risks in the processing systems of the Company. The Team will also regularly conduct review of existing policies and procedures to ensure the Company's adherence to the Data Privacy Act of 2012, its IRR, and other relevant policies and issuances related to this Act by the Commission.

ARTICLE VI: RIGHTS OF THE DATA SUBJECT

The Republic Act No. 10173 or the Data Privacy Act of 2012 specified several rights of data subjects regarding the processing of his or her personal data. As such, all employees of the Company shall respect the rights of all data subjects. Prior to the effectivity of this Manual and start of employment of new hires regardless of employment status and tenure, all employees of the Company shall accomplish and sign the **Consent Form** which indicates the rights of an employee regarding the processing of his or her personal data by Company.

Section I. Right to be Informed
The data subject has the right to be informed regarding the processing of his or her personal data by the Company. The data subject shall be notified with the following information: (i) Purpose and description of personal data to be entered and processed into the Company's system; (ii) Method of gathering and the scope of the processing of personal data; (iii) Recipients to whom the personal data are or may be disclosed; (iv) Identity and contact information of the PIC and its representative; (v) Period for which personal data will be retained in the Company's filing system; and (vi) Existence of rights of the data subjects.

Section 2. Right to Damages
The data subject has the right to be covered for any damages sustained due to inaccurate, incomplete, outdated, false, unlawfully obtained, or unauthorized use of his or her personal data.

Section 3. Right to Access
The data subject has the right to obtain confirmation on whether data relating to the data subject is being processed.

Section 4. Right to File a Complaint
The data subject has the right to file a complaint with the Commission if his or her personal data has been misused, maliciously disclosed, or improperly disposed, or that any of the data privacy rights have been violated.

Section 5. Right to Object
The data subject has the right to object to the processing of his or her personal data where such processing is based on consent or legitimate interest for the following reasons: (i) If there is any significant change or amendment to the information provided in the **Consent Form**, where the data subject should be notified and given the opportunity to object and/or withdraw consent, if consent was previously given for such

personal data processing; (ii) If the processing of personal data is for by any other means; and (iii) In cases of automated processing where personal data will, or is likely to be made as the sole basis for any decision that significantly affects or will affect the data subject.

Section 6. Right to Rectify
The data subject has the right to correct any inaccuracies in his or her personal data and the Company should consider and rectify any wrong information entered in the information systems provided that the data subject provides proof of information to back up and the correct data.

Section 7. Right to Erasure or Blocking
The data subject has the right to request for the suspension, withdrawal, blocking, removal, or destruction of personal data from the PIC's information management and filing systems. The data subject can exercise his or her right to erasure or blocking upon discovery and substantial proof of any of the following: (i) If the data subject disapproves to the processing of his or her personal data; (ii) If the processing is unlawful and without consent; (iii) If the personal data is incomplete, incorrect, outdated, or illegally obtained; (iv) If the personal data is being used for an unauthorized purpose; (v) If the personal data is no longer necessary for the purpose/s for which they were collected; and (vi) If the PIC or PIP violated the rights of the data subject.

A PIC may deny the data subject's request for erasure or blocking, wholly or partly, when personal data is still necessary in any of the following instances: (i) For fulfillment of the purpose/s for which the data was obtained; (ii) If it has a legitimate business purpose that is consistent with the industry standard for data retention; (iii) In compliance with a legal obligation that requires personal data processing; (iv) For the establishment, exercise, or in defense of any legal claim; and (v) As may be provided by any existing laws, rules, and regulations.

Personal data that is publicly available online may be subject of request for erasure. The PIC shall communicate with other PICs, including third party service providers, if any, and request them to erase copies or remove or de-list search results or links in relation to the pertinent personal data.

Section 8. Right to Data Portability
The data subject has the right to obtain a copy of his or her personal data, whether in physical and/or electronic format. The data subject can exercise this right when these two conditions concur. First, when the processing is based on consent or contract, and second, if the personal data is processed by electronic means and in a controlled and commonly used format. The right to data portability is limited to the personal data that the data subject has actively and knowingly provided to the Company and observed data that have been acquired by virtue of the use of service or device provided by the Company.

ARTICLE VII: PROCESSING OF PERSONAL DATA

The following section lays out the various data life cycles and processing systems in existence within the Company starting from the collection of personal data, to their actual use, storage, retention, and disposal. This section also includes the type of data collected, mode of collection, person/s collecting personal data, and systems and procedures related to data collection and processing.

Section 1. Data Gathering and Collection

1.1 Conditions

The Company collects personal information of data subjects including their full name, residential address, e-mail address, and contact number through various forms with the following conditions:

1. The Company shall inform the data subject of the following information before the collection of personal data.
    a. The specific purpose for the collection and processing of personal data;
    b. The range and scope of the processing of personal data;
    c. The rights of the data subject under Chapter IV of the Data Privacy Act of 2012.
2. The Company shall obtain the consent of the data subject in relation to gathering and processing of personal data satisfying the following conditions.
    a. In accordance with related laws and government regulations;
    b. Essential part of employment contract with the data subject;
    c. Necessary to protect the interest of the data subject; and
    d. To protect the rights of the Company in any court proceedings.

1.2 Consent Form

The data subject shall receive written notification regarding the gathering and collection of personal data. It will be in a form of **General Consent Form** or **Deployment Consent Form** which will be signed by the data subject. The details that will be included in the form are the following:

1. The specific purpose for the collection and processing of personal data;
2. The range and scope of processing of personal data;
3. The rights of the data subject under Chapter IV of the Data Privacy Act of 2012.

Section 2. Usage of Personal Data

2.1 Purpose of Collecting Personal Data

The use of personal data shall only be for the sole purpose specified and declared to the data subject via the signed **General Consent Form** or **Deployment Consent Form** in carrying out business operations of the Company. Personal data usage also depends on employment status and transactions with the Company as shown below.

1. If the data subject is a prospective employee and/or a consultant, the Company may collect and use personal data to:
    a. To assess compatibility and suitability of candidate to the post that he or she is applying for as well as to explore possible employment opportunities in the future;
    b. For communication between the Company and the data subject;
    c. For training and development;
    d. For performance management and evaluation;
    e. In case of emergencies; and
    f. In the processing of exit interviews and separation pays of resigned employees.
2. If the data subject is a client availing of the Company's services, the Company may collect and use personal data to:
    a. To prepare and execute professional service agreements;
    b. To conducting background investigations and character references;
    c. To updating records, contact details, and mailing addresses for billing purposes.

3. If the data subject is a vendor, supplier, or contractor, the Company may collect and use personal data to:
    a. For communication purposes
    b. For the conduct of due diligence checking;
    c. To evaluate proposals, including technical and financial proposals; and
    d. Any activities that may be required to execute contract obligations.
4. If the data subject is a visitor of the firm or any of its project sites, the Company may collect and use personal data to:
    a. To provide access to the office premises and project sites; and
    b. To ensure the safety and security of the premises and project sites.
5. If the data subject is a stockholder of the firm, the Company may collect and use personal data to:
    a. To maintain and update Company records;
    b. To manage stock transactions; and
    c. For legal and statutory obligations and compliance.

2.2 Statutory and Legal Use of Personal Data

The Company shall use personal data in government-mandated reports and compliance as well as in court orders and proceedings.

2.3 Quality of Personal Data

The Company shall process personal data of data subjects in a precise, accurate, and up-to-date manner. Any incorrect entries in the personal data of data subjects shall be rectified by accomplishing the Company's **Data Privacy Rights Form**. Likewise, supplementation and/or expurgation of personal data should also be processed using the same forms of communication and submission of relevant documents.

Section 3. Retention of Personal Data

3.1 Retention of Personal Data

The personal data of data subjects shall be retained depending on the retention and disposal policies of each department for the continuance of professional and business operations of the Company. The purposes of data collection as prescribed by law shall be considered in processing and retaining personal data.

3.2 Storage of Personal Data

The personal data of data subjects shall be stored in secured management information systems of various departments of the Company. If physical copies of personal data are to be acquired, these are filed in secured storage rooms and inside filling cabinets. Electronic copies of personal data are password-protected and if stored in a software, security measures should be maintained and the software should be up-to-date to its latest version.

Section 4. Disclosure of Personal Data

4.1 Confidentiality of Personal Data

The Company's Authorized Personnel, namely, DPO, COPs, PICs, and PIPs, shall maintain the confidentiality and security of personal data of data subjects that will come to their knowledge and custody from gathering of the data up even after the termination of employment of the data subject.

4.2 Access to Personal Data

The Company's Authorized Personnel, namely, DPO, PICs, PIPs, and COPs are the only ones that are allowed to grant request to access personal data of data subjects. Concerned parties should provide the Authorized Personnel who has the custody of the data that needs to be accessed a written request using the **Data Privacy Rights Form**. Verbal and/or e-mail requests will not be entertained. The Authorized Personnel will then determine if the request will be considered or rejected. If considered, approval will be sought from the DPO. If rejected, explanations will be provided on why the request was disapproved. Access to data should only be done in accordance with its purpose and with security measures in place. Sharing of data is forbidden unless instructed by the Authorized Personnel and with consent of the data subject.

4.3 Sharing of Personal Data

Disclosure of personal data to third party providers including PICs and PIPs shall be with legitimate purpose and/or legal basis. A **Data Sharing Agreement Form** regarding data sharing and disclosure and outsourcing should be signed that would include details and safeguards regarding sharing of personal data. Review of the agreement will be done by the data subject, DPO, COP, and other concerned parties.

A written consent should also be given to data subjects and would include the following information.

a. Information of the PICs and/or PIPs and/or third-party service providers;
b. Purpose of data sharing and disclosure;
c. Duration and extent of data sharing and disclosure; and
d. Rights of data subject.

Section 5. Disposal of Personal Data

Disposal of personal data should be done upon expiration of retention period. Physical and electronic copies of personal data should be discarded using secure means or software that would render the personal data unreadable and unretrievable to prevent breach of data privacy.

ARTICLE VIII. SECURITY OF PERSONAL DATA

The Company shall provide and implement security measures to guarantee data privacy and protection. These measures aim to protect personal data from illegal access, alteration, misuse, loss, and destruction. The Data Privacy Team headed by the DPO and the COPs shall monitor PKII's security compliance and adherence to the Data Privacy Act of 2012.

Section 1. Security Measures – Physical

1. Format of Personal Data
    a. Physical or paper-based form
    b. Electronic or digital form
2. Storage Type and Location of Personal Data
    a. Physical filling rooms and cabinets – where access keys shall be entrusted only to authorized individuals and log details be provided whenever personal data was accessed.
    b. Electronic/ digital storage – where company-provided computer (desktop/ laptop), portable storages (floppy disks/ memory cards/ optical disks/ external hard drives/

universal service bus or USB flash or pen drives), and cloud, shall be protected with passwords/ passcodes.

c. All devices that process personal data should be encrypted with updated and modern encryption methods and standards.

3. Access and Security
   Only the DPO, COPs, PICs, PIPs, and authorized individuals shall have access to personal data.
4. Access Monitoring
   DPO and COPs shall monitor the access of authorized personnel to personal data.
5. Design of Workstations
   Computers in workstations of employees processing personal data should have considerable spaces to maintain privacy and confidentiality and should be positioned in an area with the least volume of foot traffic to minimize risk.
6. Maintenance of Confidentiality
   Confidentiality should always be observed and maintained in processing of personal data. Employees should not be allowed to bring their own gadgets and storage devices and connect and use them to process personal data.
7. Modes of Transfer of Personal Data
   Transfer of personal data via electronic mail including attachments should use a secure facility with encryption of the data.
8. Retention and Disposal of Personal Data
   The Company shall retain and dispose personal data according to the Company's retention and disposal policy (Article VII, Section 3 of this Manual).

Section 2. Security Measures – Organizational

1. Management Information Systems Inventory
   The Data Privacy Team, in collaboration with the PICs, shall conduct Privacy Threshold Analyses (PTAs) and PIAs on various information management systems of the different departments that process personal data.
2. Training and Continuing Education
   Employees, particularly members of the Data Privacy Team, are required to read and understand the Data Privacy Manual and to undergo training and workshop on data privacy once a year or as deemed necessary to keep abreast with the latest updates including directives from the government and its related agencies regarding data privacy.
3. Forms
   The Company shall implement the use of the privacy notice, consent forms, non-disclosure agreements, and data sharing agreements in acquiring and processing of personal, sensitive personal, and privileged information of data subjects.

Section 3. Security Measures – Technical

1. Monitoring of Privacy and Security Incidents
   a. The Company shall monitor access to personal data by maintaining and updating a **Data Privacy Log Sheet** which shall contain log of all issues pertaining to data privacy including requests, incidents, and complains as well as agreements entered by the Company.

b. The Company shall monitor its management information systems through the implementation of file integrity monitoring.
c. The Company shall conduct periodically vulnerability scans to detect outdated versions of software and misconfigured networks.
d. The Company shall use a detection system to monitor for security breaches in its management systems.
e. The Company shall regularly check the firewall logs to monitor for security breaches and unauthorized attempts to access the Company's network.

2. Software and Applications
    a. The Company shall acquire and install anti-virus software for all company devices that process personal data.
    b. The Company shall use firewalls to protect its database and server.
3. Assessment and Evaluation of Security Measures
    a. The Company shall conduct periodic penetration testing of firewall from outside the company's premises and from within to assess vulnerability of the company's systems.
4. Other Technical Measures
    a. Authentication – Employees accessing personal data should verify identity using secure encrypted link and multi-level authentication where passwords should be strong and sufficient enough to prevent password hacking and attacks.
    b. Encryption – Personal data shall be encoded into scrambled text using algorithms that render it unreadable unless a cryptographic key is used to convert it.

ARTICLE IX. DATA BREACH AND SECURITY INCIDENCES

Section I. Procedure for Recovery and Restoration of Personal Data
The Company shall maintain a back-up file for all personal data processes in the company's management systems. In case of security breach, comparison between the back-up file and the compromised file should be done to determine any presence of discrepancies or alterations.

Section II. Documentation and Reporting of Personal Data Breach
Incidents of personal data breach should be reported by the Data Privacy Team to the Management within twenty-four (24) hours using the **Data Privacy Tracker Form**.

Section III. Reporting of Incidents

1. **Annual Security Incident Report**
   An Annual Security Incident Report shall be prepared by the Data Privacy Team and submit to the Commission.
2. **Mandatory Notification to the Management and the Commission**
   Data breach incident shall be reported first to the Management of the Company within twenty-four (24) hours and to the Commission within seventy-two (72) hours after the occurrence of such incident with the following conditions:
    a. If personal data acquired by unauthorized personnel;
    b. If breach in personal data can be used for fraudulent and unlawful activities;
    c. If it causes harm to data subjects;

d. If at least one hundred (100) data subjects are involved in the data breach and/or security incident; and
e. If it concerns national security, public safety, and law and order.

Section IV. Violation and Penalties
Penalties incurred due to data breaches and violation of the Data Privacy Act of 2012 shall follow the HR Policy regarding Disciplinary Regulations found in the PKII Employee Manual.

VIOLATION	PENALTIES			
	FIRST OFFENSE	SECOND OFFENSE	THIRD OFFENSE	FOURTH OFFENSE
Accessing due to Negligence	Verbal Warning	Written Warning	Suspension	Dismissal
Improper Disposal	Verbal Warning	Written Warning	Suspension	Dismissal
Unauthorized Disclosure	Verbal Warning	Written Warning	Suspension	Dismissal
Unauthorized Processing	Written Warning	Suspension	Dismissal	
Unauthorized Access or Intentional Breach	Written Warning	Suspension	Dismissal	
Malicious Disclosure	Written Warning	Suspension	Dismissal	
Concealment of Security Breaches	Written Warning	Suspension	Dismissal	
Combination of Series of Act	Suspension	Dismissal		

1. Verbal Warning – A verbal warning is to be conducted by the immediate superior of the employee concerned together with the members of the Data Privacy Team. It should be structured in a form of focused group discussion and confers the reason behind the issuance of the warning and the impact of the violation committed to the Company, to its stakeholders, and to the business operations.
2. Written Warning – A written warning is to be given and should include the details of the infraction, the number of offenses committed, the reason behind the penalty, and the consequences of such infringement.
3. Suspension – A notice should be given three (3) days prior to start of the suspension of the employee. A suspended employee shall not receive the corresponding salary for the days or weeks that the employee has rendered the penalty of suspension. The number of days will be determined by the Data Privacy Team subject to the approval of the Management depending on the severity of the case.
4. Dismissal – Procedures on employee dismissal will follow HRD's Policy on Disciplinary Regulations.

ARTICLE X. PROCEDURES ON THE USE AND PROCESSING OF PERSONAL DATA

Section 1. Notification on the Use of Personal Data
The data subject should be notified within seventy-two (72) hours before sharing his or her personal data for other purposes other than its originally intended use. Notification should be done through electronic mail to the address provided by the data subject.

Section 2. Request and Inquiries regarding Personal Data

The data subject may appeal to PICs and PIPs to rectify his or her personal data using the **Data Request From**. Inquiries regarding personal data may also request for access from the PICs and PIPs and will be subject for review and approval.

Section 3. Procedures in Reporting and Filing for Complaints

1. Any alleged or actual violation of the Data Privacy Act of 2012, its IRR, and other relevant policies and issuances related to the Act by the Commission should be reported in written form to the Data Privacy Team within twenty-four (24) hours and acknowledgement of the complaint reporting should be given within the same timeframe once received.
2. Once the complaint is received by the Data Privacy Team, the DPO and COPs shall perform the following procedures.
    a. Confirm and verify the alleged or actual violation;
    b. Conduct investigation, if necessary; and
    c. Report the incident to the Management and to the Commission following the timeframe stated in Article IX Section VI of the Data Privacy Manual.
3. Results of the investigation and final decision should be made within seventy-two (72) hours after the acknowledgement of the complaint.

PRIVACY NOTICE

WHO WE ARE AND WHAT WE DO

Philkoei International, Inc. (PKII) was established on October 27, 1989. Since then, PKII has grown gradually to meet the demands of the consulting industry requiring varying degrees of expertise in the field of engineering and other allied professions. Now, PKII boasts its strong and dynamic workforce of highly qualified, experienced, and technically-trained engineers and professionals who are positioned in project sites and offices in the Philippines and overseas. At present, the company aims to achieve a sizeable market share in the industry generating more jobs for Filipino professionals both locally and in the international scene and by providing competitive compensation and additional benefits to all its personnel.

OUR COMMITMENT TO DATA PRIVACY

We at PKII are committed to protect and respect the privacy of your personal data. We are also at the forefront of not only in providing you with employment and consulting opportunities, but also in complying with Republic Act No. 10173 also known as the Data Privacy Act of 2012, its Implementing Rules and Regulations (IRR), and memorandum and circulars issued by the National Privacy Commission (NPC) to ensure the safety and security of your personal data.

HOW WE USE YOUR PERSONAL DATA

Personal information, sensitive personal information, and/or privileged information will and may be collected by PKII for recruitment and selection of prospective candidates, for processing of compensation and benefits and performance appraisal of its employees, as well as for marketing and business promotion, and vendor management purposes.

We shall only retain personal data until it serves its purpose, after which it will be securely disposed of according to the firm's policy on data retention and disposal.

You have the right to be informed, to object, to access, to rectify, to erase or to block the processing of your personal information, as well as your right to data portability, to file a complaint, and be entitled to damages for violation of your rights.

CONTACT US

For questions, comments, and concerns regarding data privacy and your personal data, you may reach out to our Data Protection Team via electronic mail at dpo@philkoei.com.ph.
For more details on our Privacy Notice, you may visit our website at http://www.philkoei.com.ph.

THANK YOU

PRIVACY NOTICE

I. INTRODUCTION

Philkoei International, Inc. (PKII), hereby referred to as the "Company", is committed to protect your personal data privacy. The firm is also at the forefront of not only in providing you with employment and consulting opportunities that the Company offers to its employees, consultants, vendors, and clients but also in complying with Republic Act No. 10173 also known as the Data Privacy Act of 2012, its Implementing Rules and Regulations (IRR), and memorandum and circulars issued by the National Privacy Commission (NPC) to ensure the safety and security of your personal data.

II. SERVICE DESCRIPTION

Personal information, sensitive personal information, and/or privileged information will and may be collected by the Company for recruitment and selection of prospective candidates, for processing of compensation and benefits and performance appraisal of its employees, as well as for marketing and business promotion, and vendor management purposes.

III. COLLECTION OF PERSONAL DATA

Personal information, sensitive personal information, and/or privileged information can be collected using various forms of communication and file sharing means including physical/paper-based documents, electronic mails, messaging applications in personal computers, laptops, and mobile phones, and registration in the Company's database. All forms containing personal data will be stored in a protected information and communications system and shall be disposed in accordance with the Company's Records Retention and Disposal Policy. The Company shall not use or process these collected personal data that is contrary to laws, public policies, morals, and the Data Privacy Act of 2012.

IV. STORAGE AND TRANSMISSION

The Company has introduced policies and procedures to protect personal data it has collected and continues to collect. Measures include securing any files or documents containing personal information and sensitive personal information, and signing and implementation of non-disclosure agreements or NDAs by its employees, clients, and partners, among others. The Company's website is also being scanned on a regular basis to detect potential security breaches and vulnerabilities. The Company also implements various security measures in its database as well as in its information management system where personal information are being maintained. Transmission and exchanges of these data are done using company-provided e-mail addresses and are password protected. As there will always be a risk of unauthorized access to these personal data in the database and server, the Company is strongly committed to provide additional safeguard against these risks to protect your personal data in compliance with the Data Privacy Act of 2012.

V. TRANSFER, SHARING, AND DISCLOSURE

The Company may also share personal information of employees and consultants to clients, funding agencies, and joint venture partners for evaluation of credentials to secure possible deployment opportunities to project sites in the Philippines and overseas. The Company may also share personal information in accordance with any directive coming from relevant government agencies as provided by existing laws, rules, and regulations.

DATA PROCESSING SYSTEMS

The following systems and procedures where personal data is being collected and processed by the process owners of the different departments of Philkoei International, Inc. (PKII) are listed below.

Name of Department	:	
Name of the Data Processing System	:	
Information on whether you manage the DPS as a PIC, PIP, or both?	:	

Type of Data Processing System		- *Manual/ Paper-based?*
		- *Electronic?*
		  o *The process involves fully automated decision*
		  o *The decision will significantly affect the data subject*
		- *Both?*

Purpose(s)/Description of the Data Processing System	:	
Information whether the personal data processed in the Data Processing System will be transferred outside the Philippines	:	
Information on whether the Data Processing System is subcontracted/ outsourced or not	:	*If yes, information on the following:* *a. Personal Information Processor (PIP)* *b. PIP e-mail address* *c. PIP address* *d. PIP contact number and extension number* *e. PIP description*
Categories of data subjects	:	*Employees, students, patients, clients, etc.*
Information as to whom the personal data will be disclosed, including organization type	:	
How long are the personal data being retained?	:	

DATA PRIVACY RIGHTS FORM

Name	:	
Designation/ Position	:	
E-mail Address	:	
Contact Details	:	
Attached Documents	:	

Details of Personal Data

Name of Department where the Personal Data was Processed	:	
Description of Personal Data to be Requested	:	
Date or Period around which the Personal Data was Collected	:	

Rights to be Exercised

☐ Right to be informed where my personal data is being held and used by the Company
☐ Right to be provided with a copy of my personal data being processed by the Company
☐ Right to object to the processing of my personal data of the Company
☐ Right to access my personal data
☐ Right to dispute inaccurate details in my personal data
☐ Right to remove my personal data from the records of Company
☐ Right to obtain a copy of my personal data from the Company

Preferred Means of Accepting the Requested Personal Data

☐ Physical copy to be sent to: _____
☐ Electronic copy to be sent to the following e-mail address: _____
☐ Other means, kindly specify: _____

Confirmation

I hereby confirm that the information stated above are factual and accurate to the best of my knowledge and understand that providing false information shall constitute fraud and deception, by which shall be a ground to file for legal actions against me, who is the requestor of the personal data.

I also confirm that I will indemnify and hold the company, Philkoei International, Inc. or PKII, free from all claims arising from the breach of this warranty, for damages, and for actual legal fees to defend such claims, should there be any.

Name of Requestor: _____

Signature: _____

Date: _____

DATA REQUEST FORM

Name of Requestor	:	
Designation/ Position	:	
E-mail Address	:	
Contact Details	:	
Purpose of Request	:	
Attachments or Proof of Capacity to Access Request	:	

Request for Personal Data

Name of Data Subject	:	
Name of Department where the Personal Data was Processed	:	
Description of Personal Data to be Requested	:	
Date or Period around which the Personal Data was Collected	:	

Preferred Means of Accepting the Requested Personal Data

☐ Physical copy to be sent to: _____

☐ Electronic copy to be sent to the following e-mail address: _____

☐ Other means, kindly specify: _____

Confirmation

I hereby confirm that the information stated above are factual and accurate to the best of my knowledge and understand that providing false information shall constitute fraud and deception, by which shall be a ground to file for legal actions against me, who is the requestor of the personal data.

I also confirm that I will indemnify and hold the company, Philkoei International, Inc. or PKII, free from all claims arising from the breach of this warranty, for damages, and for actual legal fees to defend such claims, should there be any.

Name of Requestor: _____

Signature: _____

Date: _____

DATA PRIVACY TRACKER FORM

DATA PRIVACY RIGHTS

No.	Date of Request	Name of Data Subject	Description of Rights Invoked by the Data Subject	Action Taken by the Company

SECURITY INCIDENTS

No.	Date of Incident	Type of Incident	Number of Incidents	Number of Data Subjects Affected	Description of the Incident

COMPLAINTS

No.	Date of Complaint	Name of Data Subject	Description of Complaint	Measures Taken

REQUEST FOR DATA ACCESS

No.	Date of Request	Name of Data Subject	Description of Request for Data Access	Action Taken by the Company

DATA SHARING AND OUTSOURCING AGREEMENTS

No.	Start Date	Duration	Name of Processor	Purpose	Personal Data that is being Processed

ANNUAL SECURITY INCIDENT REPORT

Period: January _____ to December _____

	TOTAL
Number of Security Incidents and Personal Data Breach	
• Security Incidents	
• Personal Data Breach	

CLASSIFICATION OF SECURITY INCIDENTS

☑	**Types of Incidents**	**No. of Incidents**	☑	**Types of Incidents**	**No. of Incidents**
☐	Theft		☐	Communication Failure	
☐	Identity Fraud		☐	Natural Disaster	
☐	Sabotage / Physical Damage		☐	Design Error	
☐	Malicious Code		☐	User Error	
☐	Hacking		☐	Operations Error	
☐	Misuse of Resources		☐	Software Maintenance Error	
☐	Hardware Failure		☐	Third Party / Service Provider	
☐	Software Failure		☐	Others, please specify: _____	

PERSONAL DATA BREACH

Mandatory Reporting	**Availability Breach**	**Confidentiality Breach**	**Integrity Breach**	**TOTAL**
Required				
Not Required				

SUMMARY OF PERSONAL DATA BREACH

Date of Incident	:	
Processing System Involved	:	
Details	:	
Effects	:	
Measures Taken	:	

Date of Incident	:	
Processing System Involved	:	
Details	:	
Effects	:	
Measures Taken	:	

MANDATORY PERSONAL DATA BREACH REPORT TO DATA SUBJECTS

Philkoei International, Inc.

Units 3301 & 3302, 33rd Floor, Corporate Finance Plaza, Ruby Road,
Ortigas Center, Barangay San Antonio, Pasig City 1605 Metro Manila, Philippines

<Date>

<Name of Data Subject>
<Address>

Subject: DATA BREACH dated *<DATE>*
NPC REGISTRATION NO.

Dear *<Name of Data Subject>*,

I write on behalf of **Philkoei International, Inc.** regarding your data in *<Brief Description of Processing System>*.

We regret to inform you that your personal data has been exposed in this incident. Based on our initial investigation and review, the exposure of your personal data is limited to *<Personal Data Involved in the Data Breach>*.

Nature of the Personal Data Breach

Measures Taken or to be Taken to Address and Prevent the Personal Data Breach

If you need further information and assistance, kindly reach out to our Data Protection Officer/ Data Privacy Team at dpo@philkoei.com.ph

Rest assured that the Company is fully committed to provide you with information and assistance to address and mitigate this issue.

Sincerely,

Data Protection Team

Philkoei International, Inc.

MANDATORY PERSONAL DATA BREACH REPORT TO THE COMMISSION

Philkoei International, Inc.

Units 3301 & 3302, 33rd Floor, Corporate Finance Plaza, Ruby Road,
Ortigas Center, Barangay San Antonio, Pasig City 1605 Metro Manila, Philippines

<Date>

Raymund E. Liboro
Chairman
National Privacy Commission
Pasay City, Metro Manila, Philippines

Subject: DATA BREACH dated *<DATE>*
NPC REGISTRATION NO.

Dear *<Name of Data Subject>*,

I write in behalf of **Philkoei International, Inc.** in relation to the personal data breach that happened last *<Date>*, that involves *<Brief Description of Processing System>*. This notification is made pursuant to the mandatory data breach notification procedure of the National Privacy Commission.

The appropriate details of the Company and the responsible people thereof, are as follows:

Head of the Organization: Peter S. Samoza
President
psamoza@philkoei.com.ph
63 2 534 0325

Data Protection Officer: Jose Adones C. Beringuela
Vice-President, Domestic Consulting Group
jacberinguela@philkoei.com.ph
63 2 534 0325

Process Owner: *<Name of Process Owner>*
<Position>
<E-mail Address>
<Contact Number>

Nature and Description of the Personal Data Breach

Measures Taken or to be Taken to Address and Prevent the Personal Data Breach

In the event that you require additional information regarding this incident, you may reach out to us using the above contact details. Any requested information that is indicated as unavailable will be provided and reported within five (5) days, or as soon as they become available.

Sincerely,

Data Protection Team

Philkoei International, Inc.

GENERAL CONSENT FORM

I. INTRODUCTION

Philkoei International, Inc. (PKII) is committed to provide you with employment and/or project opportunities in the Philippines and/or elsewhere while implementing safeguards to protect your privacy and keep your personal data source in accordance with Republic Act No. 10173 also known as the Data Privacy Act of 2012.

II. PROCESSING OF PERSONAL DATA

a. Types of Data Collected

i. Full Name (First Name, Middle Name, Last Name)
ii. Residential Addresses (Temporary and Permanent)
iii. Contact Details (Landline and/or Mobile)
iv. Birthdate/ Age
v. Civil Status
vi. Nationality/ Citizenship
vii. Educational Background
viii. Work Experiences
ix. Bureau of Internal Revenue (BIR) – Tax Identification Number (TIN)
x. Social Security System (SSS)
xi. Home Mutual Development Fund (HDMF) Pag-IBIG Fund
xii. National Bureau of Investigation (NBI) Clearance
xiii. Philippine National Police (PNP) Clearance
xiv. Physical Examination Results (from accredited hospital and clinics)

b. Type of Processing and Legitimate Purpose, Function, or Activity

PRIMARY PURPOSE	
NAME OF DEPARTMENT	SPECIFIC PURPOSE
Human Resources Department	- *Evaluation, Recruitment, Selection* - *Marketing and Promotion* - *PKII Human Resources Database*
Business Development Department	
SECONDARY PURPOSE	
NAME OF DEPARTMENT	SPECIFIC PURPOSE
Human Resources Department	- *Human Resources Information System* - *Benefits Administration* - *Performance Management* - *Training and Development* - *Employee Engagement Activities*
Finance and Accounting Department	- *Compensation and Benefits* - *Monetary and Benefit Claims*
Health, Safety, Security, Environment Department	- *Medical Advice* - *Fit-to-work Clearances*
Information Technology Department	- *PKII Human Resources Database* - *Human Resources Information System*
Direct Superiors (Vice-Presidents/Managers)	- *Performance Management*

III. DATA PROTECTION

We shall implement reasonable and appropriate organizational, physical, and technical security measures for the protection of personal data which we collected. The security measures shall aim to maintain the availability, integrity, and confidentiality of personal data and are intended for the protection of personal data against any accidental or unlawful destruction, alteration, and disclosure, as well as against any other unlawful processing.

IV. CONFIDENTIALITY

Our employees shall operate and hold personal data under strict confidentiality. They are required to sign non-disclosure agreements and are have received training on the company's privacy and security polices to ensure confidentiality and security of personal data.

V. RIGHTS OF THE DATA SUBJECT

As our data subject, you are entitled to the following rights stipulated in Republic Act No. 10173 also known as the Data Privacy Act of 2012:

Right to be Informed	*Right to Erasure or Blocking*
Right to Object	*Right to File a Complaint*
Right to Access	*Right to Damages*
Right to Rectification	*Right to Data Portability*

VI. CONTACT DETAILS OF THE DATA PRIVACY OFFICER

If you have further questions or concerns, you may contact our Data Privacy Officer through the following details:

Contact Number: 63 (02) 534-03-25

E-mail Address: dpo@philkoei.com.ph

Address: Unit 3301 and Unit 3302, 33rd Floor, Corporate Finance Plaza, Ruby Road, Ortigas Center, Barangay San Antonio, Pasig City 1605 Metro Manila, Philippines

VII. CONFIRMATION OF AGREEMENT AND SIGNATURE

I have read this form, understood its contents and consent to the processing of my personal data. I understand that my consent does not preclude the existence of other criteria for lawful processing of personal data, and does not waive any of my rights under the Data Privacy Act of 2012 and other applicable laws.

_____ _____

Signature Over Printed Name Date

CONSENT FORM FOR CONSULTANTS

I. INTRODUCTION

Philkoei International, Inc. (PKII) is committed to provide you with business prospects pursuant to the available consulting opportunities in the Philippines and overseas while implementing safeguards to protect your privacy and keep your personal data source in accordance with Republic Act No. 10173 also known as the Data Privacy Act of 2012.

II. PROCESSING OF PERSONAL DATA

a. Types of Data Collected

i. Full Name (First Name, Middle Name, Last Name)
ii. Residential Addresses (Temporary and Permanent)
iii. Contact Details (Landline and/or Mobile)
iv. Birthdate/ Age
v. Civil Status
vi. Nationality/ Citizenship
vii. Educational Background
viii. Work Experiences
ix. Bureau of Internal Revenue (BIR) – Tax Identification Number (TIN)
x. National Bureau of Investigation (NBI) Clearance*
xi. Philippine National Police (PNP) Clearance*
xii. Physical Examination Results (from accredited hospital and clinics) *

b. Type of Processing and Legitimate Purpose, Function, or Activity

PRIMARY PURPOSE	
Name of Department	Specific Purpose
Human Resources Department	- Recruitment and Selection - Marketing and Promotion - PKII Human Resources Database - Evaluation of Qualifications (Educational Background and Work/ Project Experiences
Business Development Department	
Vice-Presidents/ Managers (ICG/DCG)	
Clients/ Funding Agencies/ Lead Firms/ Joint Venture Partners/ Project Team Leaders	
SECONDARY PURPOSE	
Name of Department	Specific Purpose
Human Resources Department	- Human Resources Information System - Benefits Administration
Finance and Accounting Department	- Compensation and Benefits - Monetary and Benefit Claims
Health, Safety, Security, Environment Department	- Medical Advice* - Fit-to-work Clearances*
Information Technology Department	- PKII Human Resources Database - Human Resources Information System
Vice-Presidents/ Managers (ICG/DCG)	- Performance Management*
Clients/ Funding Agencies/ Lead Firms/ Joint Venture Partners/ Project Team Leaders	

*if considered and applicable

III. DATA PROTECTION

We shall implement reasonable and appropriate organizational, physical, and technical security measures for the protection of personal data which we collected.

The security measures shall aim to maintain the availability, integrity, and confidentiality of personal data and are intended for the protection of personal data against any accidental or unlawful destruction, alteration, and disclosure, as well as against any other unlawful processing.

IV. CONFIDENTIALITY

Our employees shall operate and hold personal data under strict confidentiality. They are required to sign non-disclosure agreements and are have received training on the company's privacy and security polices to ensure confidentiality and security of personal data.

V. RIGHTS OF THE DATA SUBJECT

As our data subject, you are entitled to the following rights stipulated in Republic Act No. 10173 also known as the Data Privacy Act of 2012:

Right to be Informed	Right to Erasure or Blocking
Right to Object	Right to File a Complaint
Right to Access	Right to Damages
Right to Rectification	Right to Data Portability

VI. CONTACT DETAILS OF THE DATS PRIVACY OFFICER

If you have further questions or concerns, you may contact our Data Privacy Officer through the following details:

Contact Number:	63 (02) 534-03-25
E-mail Address:	dpo@philkoei.com.ph
Address:	Unit 3301 and Unit 3302, 33rd Floor, Corporate Finance Plaza, Ruby Road, Ortigas Center, Barangay San Antonio, Pasig City 1605 Metro Manila, Philippines

VII. CONFIRMATION OF AGREEMENT AND SIGNATURE

I have read this form, understood its contents and consent to the processing of my personal data. I understand that my consent does not preclude the existence of other criteria for lawful processing of personal data, and does not waive any of my rights under the Data Privacy Act of 2012 and other applicable laws.

_____ _____

Signature Over Printed Name Date

NON-DISCLOSURE AGREEMENT

[DATA PROCESSOR]
Full Name: _____
Position/ Designation: _____
Department: _____

To the Data Processor,

The information shared by applicants, employees, vendors, and consultants, via physical and/or digital copies and electronic mails are necessary for recruitment and selection purposes, compensation and benefits administration, and vendor management.

Using and sharing their personal data other than its intended purpose will result to violation of Republic Act No. 10173 or the Data Privacy Act of 2012.

By signing at the bottom of this document, you are hereby reminded of Paragraph A, C, and F of Section 12 (Criteria for the Lawful Processing of Personal Information) of Chapter III and Sections 25-33 of Chapter VIII of this Act which reads:

Chapter III
Sec. A: The data subject has given his or her consent.
Sec. C: The processing is necessary for compliance with legal obligation which the personal information controller is subject.
Sec. F: The processing is necessary for the purposes of the legitimate interests pursued by the personal information controller.

Chapter VIII
Sec. 25: Unauthorized Processing of Personal Sensitive and Sensitive Personal Information.
Sec. 26: Accessing Personal Information and Sensitive Personal Information Due Negligence.
Sec. 27: Improper Disposal of Personal Information and Sensitive Personal Information.
Sec. 28: Processing of Personal Information and Sensitive Personal Information for Unauthorized Purposes.
Sec. 29: Unauthorized Access or Intentional Breach.
Sec. 30: Concealment of Security Breaches Involving Sensitive Personal Information.
Sec. 31: Malicious Disclosure.
Sec. 32: Unauthorized Disclosure.
Sec. 33: Combination or Series of Acts.

Signed by the Data Processor:

_____ _____
Signature over Printed Name Date

Noted by the Data Privacy Officer:

_____ _____
Signature over Printed Name Date

CONFORME

This is to confirm that I personally received, carefully read, and fully understood the contents of the Data Privacy Manual of Philkoei International, Inc. (PKII) and will, to the best of my knowledge and abilities, conform with the rules and regulations stated in the said Manual and to adhere to the provisions stipulated in the Republic Act No. 10173, also known as the Data Privacy Act of 2012.

NO.	SURNAME	GIVEN NAME	MIDDLE NAME	DEPARTMENT	SIGNATURE
1					
2					
3					
4					
5					
6					
7					
8					
9					
10					
11					
12					
13					
14					
15					
16					
17					
18					

Received by:

_____

Data Privacy Officer