Data Privacy Policy

PROTECTED

DOCUMENT CONTROL NO.: POL.001.003
EFFECTIVITY DATE: 28 August 2024

TABLE OF CONTENTS

1. OVERVIEW

1.1. At EMAPTA, safeguarding personal identifiable information (PII) is paramount. Our Data Privacy Policy reflects our commitment to upholding responsible corporate governance and compliant business practices. We prioritize the protection of PII and ensure that data subjects' rights are respected throughout our privacy management practices.

2. OBJECTIVE

2.1. The objective of our Data Privacy Policy is to establish guidelines for the collection, use, and protection of personal information entrusted to us. We aim to comply with various data privacy regulations and uphold the rights of data subjects. By implementing controls and practices outlined in this policy, we strive to maintain the confidentiality, integrity, and availability of PII.

3. SCOPE

3.1. This policy applies to all aspects of data privacy within EMAPTA, covering the collection, processing, storage, retention, and disposal of personal information. It extends to all employees, clients, and stakeholders involved in handling PII. Additionally, this policy governs data privacy practices on our website and in our business operations, ensuring compliance with international data protection laws.

4. DEFINITION OF TERMS

4.1. **Personal Identifiable Information (PII):** Information that can be used to identify an individual, such as names, contact details, biometric data, government ID numbers, and health information.

4.2. **Data Subjects:** Individuals whose personal information is collected, processed, or stored.

4.3. **Consent:** Informed and active agreement given by individuals for the collection and processing of their personal information.

4.4. **Data Privacy Regulations:** Legal frameworks governing the protection of personal information, such as the General Data Protection Regulation (GDPR), Philippine Data Privacy Act, and Australian Privacy Act.

4.5. **Data Protection Officer (DPO):** Designated individual responsible for overseeing the organization's data privacy compliance and handling inquiries and requests related to data privacy.

5. ROLES AND RESPONSIBILITIES

5.1. **Management:** Responsible for ensuring compliance with data privacy regulations and providing oversight of data privacy practices.

5.2. **Data Protection Officer (DPO):** Oversees the implementation of the Data Privacy Policy, responds to inquiries and requests related to data privacy, and ensures compliance with privacy regulations.

5.3. **Employees:** Required to adhere to data privacy practices outlined in this policy, including obtaining consent, safeguarding personal information, and participating in data privacy awareness training.

5.4. **Stakeholders:** Expected to cooperate with EMAPTA in complying with data privacy regulations and protecting personal information in their possession.

6. DATA SUBJECTS AND RIGHTS

6.1. We take diligent care of the personal information entrusted to us and implement controls designed in compliance with various data privacy regulations. We ensure that we always uphold the rights of our data subjects and secure all personal information collected, used, and stored in our data processing systems. We have mapped our strategies against these requirements to cover as much as possible and isolate any unique requirements. The following are the data subject rights protected by law:

6.1.1. **Right to be Informed.** We treat your PII as our personal property and will not collect, process, or store it without your explicit and informed consent, unless otherwise provided by law as an exemption. We will solicit your informed and active consent through a consent form or through privacy notices and acknowledgement pages incorporated in our data collection tools and portals.

6.1.2. **Right to Access Information.** You have the right to find out whether we hold any personal data about you and gain “reasonable access” to them. You may also request a written description of the information we have about you and our purpose for holding it. We will provide a copy of any information relating to you in an easy-to-access format.

6.1.3. **Right to Object to Processing.** You can assert your right to object if the personal data processing activity is not based on consent or lawful or legitimate interest. When you object or withhold your consent, we will no longer process your personal data, unless the processing is pursuant to a subpoena, for obvious purposes (contract, employer-employee relationship, etc.) or a result of a legal obligation. We will notify you of any change or amendment to the information previously given to you and give you an opportunity to withhold our consent.

6.1.4. **Right to Erasure or Blocking.** You have the right to suspend, withdraw or order the blocking, removal, or destruction of your personal data. You may exercise this right upon discovery and substantial proof that your personal data is incomplete, outdated, false, unlawfully obtained; used for purposes you did not authorize; kept longer than necessary, or processed unlawfully and you have withdrawn your consent.

6.1.5. **Right to Damages**. You may be entitled to claim compensation if you suffered damages due to inaccurate, incomplete, outdated, false, unlawfully obtained,

or unauthorized use of personal data, considering any violation of your rights and freedoms as a data subject.

6.1.6. **Right to Data Portability**. This right allows you to obtain and electronically move, copy, or transfer your data in a secure manner for further use. You may manage your personal data in your private device and transmit it from one location to another.

6.1.7. **Right to Rectify Errors or Inaccuracies**. You have the right to dispute and have corrected any inaccuracy or error in the data we hold about you. We will act on it immediately and accordingly unless the request is vexatious or unreasonable. Once corrected, we will ensure your access and receipt of both new and retracted information.

6.2. We will also furnish third parties with said information, should you request it by contacting our (DPO) at privacy@emapta.com.

7. INFORMATION WE COLLECT AND USE

7.1. As a business, collecting PII is an integral part of our operations. However, we take great care to protect this information as it is not only valuable to us but also to our clients and data subjects. While it is necessary to collect and process PII to deliver services efficiently, we exercise due caution in handling it.

7.2. In our business, PII can be classified into two domains: *Core PII*, collected and used by our support services team, and *Client PII*, which belongs to our clients and is used exclusively by them to conduct their business. For example, Core PII is used by the Core Team to provide compensation and benefits to our employees, assign log in credentials, create project proposals, develop business strategies, and provide tailored solutions as needed. On the other hand, Client PII is collected and processed by our clients and is under their complete control. They are responsible for designing and enforcing controls to manage this set of PII.

7.3. The specific information we may collect as Core PII includes:

7.3.1. **Identifiers and Contacts** - Names, contact numbers, and email addresses that we use to identify and communicate with our stakeholders. We may share this information with clients upon request or when necessary for processing activities and transactions.

7.3.2. **Biometric Information (Fingerprints)** - Collected to provide our employees with physical access to our delivery sites.

7.3.3. **Basic Health Information** - Includes basic health status and wellness information required as part of our pre-employment requirements or from annual physical and wellness exams.

7.3.4. **Location and Addresses** - Collected and used to send correspondence in response to inquiries and requests.

7.3.5. **Government ID Numbers** - Collected from staff to file applications and provide government-mandated benefits. In some cases, we also assist our employees with transactions such as visa applications.

7.3.6. **Work History, Background, and Credentials** - Collected to profile candidates effectively and match requirements for their requested manpower. We verify educational backgrounds, work history and experience, and other credentials like technical certifications, accreditations, and professional licenses through a background check.

8. WHAT DO WE DO WITH CLIENT PII

8.1. We understand the importance of our clients' personal identifiable information (Client PII) and therefore do not store it ourselves. When working with us, our clients maintain full control and flexibility over their business, which is a core part of our brand. This sets us apart from other businesses as we recognize that what is good for our clients is also good for us.

8.2. Customer information of our clients is exclusively housed in their processing portals and systems. Our clients are responsible for securing the confidentiality of Client PII, which includes managing primary identifiers, payment information (such as credit card and bank details), location and addresses, contact details, and other pertinent information used to identify a customer.

9. INFORMATION WE COLLECT ON OUR WEBSITE

9.1. When you visit our website (www.emapta.com), we automatically collect certain information about your device, including information about your web browser, IP address, time zone, and some of the cookies that are installed on your device. Additionally, as you browse our website, we collect information about the individual web pages or products that you view, what websites or search terms referred to us, and information about how you interact with our website. We refer to this automatically collected information as “device information.”

9.2. We collect device information using various technologies such as Cookies, Log Files, and Web Beacons.

9.3. When you complete a contact form through our website, we collect certain information from you, including your name, address, email address, and phone number. We refer to this information as “contact information.” This information is collected so that we can respond to your inquiries and provide you with relevant information about our products and services.

9.4. We may also use this information to send you marketing communications about our products and services, but only if you have given us your consent to do so.

10. DATA PRIVACY PRINCIPLES AND LEGISLATIVE REQUIREMENTS

10.1. We process PII in compliance with regulatory requirements and follow the principles of transparency, legitimate purpose, and proportionality. We determine and declare a specified and legitimate purpose before, or as soon as reasonably practicable after, we initiate the collection and processing of PII. Our processing of personal information is fair, lawful, and necessary for fulfilling our contractual obligations, responding to requests, and delivering services in a timely manner. We keep information only for defined retention periods and dispose of it properly thereafter. The following are the principles we adhere to in processing PII:

10.1.1. **Principle of Transparency**. We obtain informed and active consent prior to collecting and processing PII, except for exemptions provided by laws and regulations. We will inform you of the nature, purpose, and extent of processing of PII, including risks and safeguards involved, your rights, and how to exercise them.

10.1.2. **Principle of Legitimate Purpose**. We ensure that processing of PII is compatible with our declared and specified purpose and not contrary to law, morals, or public policy.

10.1.3. **Principle of Proportionality**. We ensure that the processing of personal information is relevant to and does not exceed the declared purpose or beyond the bounds of the consent we sought for. We collect only what is needed and necessary to carry out processing activities and achieve desired outputs within the bounds of your consent. In certain cases, we may request additional information from you to establish your identity, such as when you exercise your right of access, to ensure that information is not released to unauthorized persons.

11. PROCESSING

11.1. We ensure that the PII we process is adequate, relevant, and not excessive, and we always consider the legitimate purpose for which the information is being collected and processed.

11.2. In order to maintain the privacy and security of the PII we handle, we take the following measures:

11.3. **Consent.** We obtain informed and active consent from individuals prior to collecting their personal information. We use consent forms whenever possible but may also obtain consent through other means such as Privacy Notices incorporated in our data processing systems and data collection portals.

11.3.1. **Privacy Impact and Risks.** We conduct Privacy Impact Assessments and Risk Analysis on a periodic basis to identify gaps and risks in how we manage data privacy. We also conduct these assessments before we implement new processes, acquire, and deploy new data processing systems, and adopt new

strategies that may involve PII. Our Data Protection Officer (DPO) leads these efforts.

11.3.2. **Technical Controls.** We maintain standard technical controls to maintain endpoint security, such as encryption, remote administration, web control filtering, and two- factor authentication for systems as deemed appropriate. Our network design includes secure network segmentations for our clients. We also employ encryption for data in transit and firewall protection.

11.3.3. **Physical Controls.** At our delivery sites, areas such as data centers and server rooms are protected by CCTV recording and monitoring, as well as biometric door access using fingerprint scanners.

11.3.4. **Compliance with Data Privacy Regulations.** We do not draw any conclusions about individuals when processing PII, and no personal evaluation of the data for marketing purposes or profiling takes place. We aim to comply with all applicable data privacy regulations, including but not limited to the General Data Protection Regulation of the European Union, the Philippine Data Privacy Act, and the Australian Privacy Act. When processing PII, we ensure compliance with relevant data privacy regulations in all geographies where we operate.

11.3.5. **Third-Party Data Handling.** When allowing third parties access to personal information, we ensure that data subjects are informed, and their consent is secured before sharing personal information with these entities. We carefully review and approve the data handling practices of third parties to ensure compliance with our privacy policies and applicable regulations. Contracts and agreements are maintained with third parties to establish data protection standards, and regular audits are required to monitor their compliance. This proactive approach guarantees that data subjects are aware of and consent to any use of their personal information by third parties.

12. RETENTION

12.1. We ensure that information is retained for no longer than is necessary, following a defined retention schedule which may be driven by regulatory requirements or our identified needs. We will not keep information longer than is required.

12.2. We respect your right to have your personal information deleted or purged. You can request this by contacting our DPO privacy@emapta.com. Once we receive your request, our DPO will acknowledge it.

13. DISPOSAL

13.1. Our clients have full control over the disposal of their PII since this information is housed entirely in their own portals and applications.

14. OUR DATA PROTECTION OFFICER

14.1. Our DPO is the single point of contact for all matters related to data privacy. The DPO manages the entire Data Privacy Program, responds to requests and inquiries, identifies, and manages risks, develops policies and procedures to secure PII, and ensures compliance with reporting requirements driven by privacy regulations.

14.2. To reach our DPO, you can send inquiries, requests, and queries to privacy@emapta.com.

15. POLICY REVIEW

15.1. As our websites, processes, and technologies continue to develop, it may become necessary to update this privacy policy. We reserve the right to modify this policy at any time, and the version available at the time of your visit to the website will apply.

16. EFFECTIVITY

16.1. This Policy shall take effect upon the approval of the Chief Legal and Operations Officer or the Chief Information Officer.

POLICY/PROCESS OWNER:	**Data Protection Officer**
DOCUMENT CONTROL NO.:	**POL.001.003**
EFFECTIVITY DATE:	**28 August 2024**

	NAME / DESIGNATION	DATE
AUTHOR	Carlo Valencia, Data Protection Officer	March 2023
REVIEWED	Ben van de Beld, Chief Legal and Operations	March 2023
	Luis Sicat, Chief Information Security Officer	August 2024
APPROVED	Ben van de Beld, Chief Legal and Operations	March 2023
	Henry Vassall Jones, Chief Information Officer	August 2024

REVIEW AND REVISION HISTORY

DATE:	ACTION	Control No. (for Revision)	DESCRIPTION / COMMENT
28-Aug-2024	*Review*	*3.1*	*Annual policy review conducted (Jess Macalinao, Data Protection Officer)*