ENVIROS Data Protection Policy

ENVIROS is required to gather, process, and use personal data of individuals such as employees, clients, suppliers, and other third-party vendors. This policy outlines how personal data is collected, used, stored, and protected in compliance with the Personal Data Protection Act (PDPA) 2010.

This data protection policy ensures that ENVIROS:

- Complies with Personal Data Protection Act 2010 (PDPA 2010) regulations and follows best practices.
- Protects the rights and privacy of individuals whose data it collects.
- Is transparent about how it collects, processes, and manages personal data.
- Minimizes risks associated with data breaches and unauthorized disclosures.

Personal Data Collection

ENVIROS will collect various types of personal data from you, including but not limited to the following:

- Personal information to establish your identity and background such as your full name, identity card number or passport, nationality and religion.
- Contact information such as permanent & correspondence address, telephone or mobile number and email address.
- Family member details such as full name, relationship, passport or identity card number, and their employer's name (if applicable)
- Payment information such as your bank account details & bank statement.
- Sensitive information such as health medical history or checkups.
- Resume or CVs when you apply job with us.

Rights of Data Subjects:

Under the Personal Data Protection Act 2010 (PDPA 2010), individuals have the following rights to:

- Right to access - you can request access to your personal data held by ENVIROS.
- Right to correct - if your data is found to be inaccurate, incomplete, misleading or not up to date, you can request to correct your personal data.
- Right to withdraw consent - you can withdraw consent for the collection, use, or disclose of your personal data.
- Right to prevent processing - you can request to restrict the use of your personal data.

Data Protection Principles

ENVIROS complies by the seven PDPA 2010 principles relating to the processing of personal data, i.e., that it should be:

- **General Principle**: We will process personal data legally and only with consent, unless the law allows otherwise.
- **Notice and Choice Principle**: We will inform individuals about why their data is being collected and give them the choice to consent.
- **Disclosure Principle**: We will not share personal data with others without consent, unless the law requires it.
- **Security Principle**: We will take steps to keep personal data safe.
- **Retention Principle**: We will only keep personal data for as long as we need it.

Copyright: © ENVIROS 2022

ENVIROS Data Protection Policy

- **Data Integrity Principle**: We will ensure that personal data is correct and up to date.
- **Access Principle**: Individuals can request to see or update their personal data.

Data Processing by Third Parties

Third parties who works with ENVIROS has the responsibilities to ensure that the personal data is collected, stored, and secure properly. Data Processing Agreements (DPA) will be in place, specifying third-party's responsibilities on handling personal data & to ensure compliance with the PDPA 2010.

Transferring Data Outside Malaysia

Individuals will be informed if their personal data will be transferred to outside of Malaysia if necessary for ENVIROS's business operations. Adequate safeguards are in place to protect the personal data, including encryption transfer protocols, and to ensure compliance with the PDPA 2010.

Data Retention & Disposal

Personal data collected by ENVIROS must align with the ENVIROS Data Retention Policy (ENV-POL-15). Personal data will not be retained longer than necessary to fulfill its original purpose. Upon reaching the end of its retention period, personal data must be securely deleted using data wiping or any encryption methods to ensure that it cannot be recovered.

Data Protection & Security

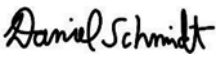
ENVIROS is dedicated to protecting personal data from unauthorized access, loss, destruction, or misuse. To achieve this, access is limited to authorized personnel using Multi-Factor Authentication (MFA), while physical data storage areas are secured with locked cabinets and restricted server rooms.

To protect our IT infrastructure, we deploy firewalls, Intrusion Detection Systems (IDS), and conduct vulnerability assessments. Data Loss Prevention (DLP) systems are implemented to monitor and prevent unauthorized sensitive personal data sharing. Additionally, employees receive regular data protection and cybersecurity training to reduce the risk of human error and ensure secure data handling.

Enforcement

Any employee, contractor, or third party found in violation of this policy may face disciplinary action, including termination of employment or contract. All employees are required to report any suspected breaches or unauthorized disclosures of personal data immediately to the IT Department. If a data protection issue is identified, corrective actions will be taken promptly to prevent recurrence, including updating procedures, providing additional training, or enhancing security controls.

Signed



Daniel Schmidt (President)

Date

14th Nov 2024

Copyright: © ENVIROS 2022