Impressive Communications Sdn. Bhd.
Personal Data Protection Policy

1. Overview

This policy outlines the steps and best practices for managing and protecting personal data in compliance with the **Malaysia Akta Perlindungan Peribadi 2010 [Akta 709]**, hereby will be referred to as PDPA. The PDPA sets out the framework for personal data processing and establishes the rights and responsibilities of both data users and data subjects. This procedure ensures that all data processing activities are performed in accordance with legal requirements while maintaining the privacy and security of personal data.

2. Purpose

The implementation of a data protection standard is with the purpose for:

- **Compliance with PDPA:** Ensuring that ICSB employees meets its legal obligations under the Akta Perlindungan Peribadi 2010 [Akta 709].
- **Preventing Data Breaches:** Minimizing the risk of unauthorized access or disclosure of personal data.
- **Building Trust:** Demonstrating commitment to data privacy to customers, clients, and stakeholders.
- **Risk Management:** Avoiding penalties, fines, and reputational damage due to non-compliance.

3. Scope

The scope of this policy document is in adherence also the policy requirement of Impressive Communications Sdn Bhd compliance to the Information Security Management System (ISO 27001:2022) as part the obligation to maintain certification and compliance to the ISO standard.

4. Policy

- General Requirements

  ICSB is committed to protecting the privacy and personal data of our employees, clients, and end-users. In compliance with the Malaysian Personal Data Protection Act 2010 (PDPA), we ensure that all personal data processed during our software development lifecycle—from design to deployment—is handled with the highest standards of security, transparency, and integrity. This also includes during execution of any Maintenance and Support contract that gives ICSB the indirect access to clients and user information.

  ICSB approach ensures that data protection is not an afterthought but a core component of every line of code we write and every system we architect as well ensuring our staff that supports the client's status during the Software Development Life Cycle (SDLC)

- Intended Audience

  The following groups must comply with the data protection mechanism under the PDPA:

  - **Data Users (Organizations):** Any organization or individual who contracted by ICSB that processes personal data as part of its business or operations.
  - **Employees:** Individuals within the ICSB who handle personal data, either directly or indirectly.
  - **Third-Party Processors:** External entities contracted by the ICSB to process personal data (e.g., vendors, service providers).
  - **Data Subject Representatives:** Legal representatives who act on behalf of data subjects in specific circumstances.

    Note:

    - ICSB Partners, Vendors and Subcontractors are required to sign a Non-Disclosure Agreement (NDA) prior to any pre-sales or pre projects activities that involves ICSB existing or potential customers.
    - Prior to any contract and/or project execution ICSB Partners, Vendors and Subcontractor are required to signed a PDPA agreement to ensure user data received are maintained and preserved as required by this procedure.

5. Procedural Content

All the following procedural content with the policy document is subjected to Impressive Communications Sdn Bhd having access and/or required to process the personal data of the clients or its customer. Which in lieu of these requirements only applicable procedural content is determine to be complied with based on Impressive Communication discretion.

- Data Categorization

  Data should be categorized based on its sensitivity to ensure appropriate handling. Categories of personal data include:

  - **Basic Data:** Includes name, contact details, and basic information.
  - **Restricted Data:** Data that needs additional protection, such as financial details.
  - **Sensitive Data:** Includes health data, racial or ethnic origin, religious beliefs, and political opinions. This data requires the highest level of protection under the PDPA.

- Data Inventory

  Maintain an up-to-date data inventory that includes:

  - **Data Type:** Identify and document the personal data being collected and processed.
  - **Data Source:** Specify where the data is collected (e.g., directly from data subjects, through third parties).
  - **Purpose of Processing:** State the specific purpose(s) for collecting and processing each type of data.
  - **Retention Period:** Record the retention period for each data type, ensuring compliance with data retention policies.
  - **Access and Usage:** Define who has access to personal data and how it will be used.

- Data Protection Impact Assessment (DPIA)

  A **Data Protection Impact Assessment** (DPIA) is required for new projects or data processing activities that could impact the privacy of data subjects. The DPIA process includes:

  - **Assessing Risks:** Evaluate the potential impact on data subjects' privacy.
  - **Identifying Mitigation Measures:** Propose actions to minimize or eliminate identified risks.

  - **Approval and Documentation:** Ensure that DPIA results are documented and approved before processing begins.

- Basis for Processing

  Personal data must be processed based on one of the lawful bases outlined in the PDPA:

  - **Consent:** Obtaining explicit consent from data subjects.
  - **Contractual Necessity:** Processing required to fulfill contractual obligations with the data subject.
  - **Legal Obligation:** Processing necessary to comply with legal requirements.
  - **Legitimate Interest:** Processing based on the legitimate interests of the data user or third parties.
  - **Vital Interests:** Processing necessary to protect someone's life.
  - **Public Interest:** Processing for the performance of a task carried out in the public interest.

- Transparency

  The organization must ensure that data subjects are informed about the processing of their personal data:

  - **Privacy Notice:** Provide clear, concise, and easily accessible privacy notices that describe the purpose, scope, and use of the data.
  - **Right to Withdraw Consent:** Inform data subjects of their right to withdraw consent at any time.
  - **Information Access:** Allow data subjects to access and understand the data being processed.

- Purpose Limitation

  Personal data should only be collected for specific, legitimate, and lawful purposes, and not processed further in a manner incompatible with those purposes. Any change in the purpose of data processing must be communicated to the data subject, and their consent must be obtained if required.

- Minimization

  Personal data collection should be limited to what is necessary for the specified purpose. Data should not be excessive or irrelevant to the intended use. Periodically review data collection practices to ensure that only essential information is gathered.

- Accuracy

  Organizations must ensure that personal data is:

  - **Accurate:** Data should be correct and up-to-date.
  - **Correctable:** Provide mechanisms for data subjects to correct inaccurate data.
  - **Reviewable:** Regularly assess the accuracy of personal data and implement processes to address inaccuracies

- Storage Limitation

  Personal data should not be kept in a form that permits identification of data subjects for longer than necessary. Implement a data retention policy that:

  - Defines Retention Periods: Clearly outline how long data will be stored.
  - Ensures Secure Deletion: Data should be securely deleted or anonymized when no longer required

- Security (For Basic / Restricted / Sensitive Data)

  Different levels of security measures must be applied depending on the data classification:

  - Basic Data: Apply access controls and standard security protocols.
  - Restricted Data: Use encryption, firewalls, and strong access controls.
  - Sensitive Data: Implement additional security measures such as multi-factor authentication, advanced encryption, and restricted access by designated personnel.

- Data Breach

  In the event of a data breach, the following steps must be followed:

  - **Immediate Notification:** Notify the **Personal Data Protection Commissioner (PDP Commissioner)** and affected data subjects within 72 hours of discovering the breach.
  - **Containment:** Stop the breach, secure the compromised data, and prevent further unauthorized access.
  - **Investigation:** Determine the scope, nature, and cause of the breach.
  - **Corrective Action:** Implement corrective measures to prevent future breaches, including a review of security protocols.
  - **Record and Report:** Maintain a record of the breach and report it to relevant regulatory bodies.

- Data Subject Rights Management

  Under the PDPA, data subjects have the following rights:

  - Right to Access: Allow data subjects to access their personal data upon request.
  - Right to Correct: Data subjects can request corrections to inaccurate or incomplete data.
  - Right to Withdrawal of Consent: Data subjects can withdraw consent at any time, with no detriment.

6. Training & Communication

Regular training must be provided to employees, contractors, and third-party vendors on:

- Data Protection Practices: Ensure awareness of the PDPA and its impact on data processing activities.
- Internal Policies: Training on organizational policies related to data security, handling of personal data, and response to data subject rights requests.
- Updates and Refresher Courses: Conduct periodic updates and refresher training sessions to address changes in laws, technologies, or organizational

Note: Training requirements are subjected to the contractual requirements of the clients in such cases where ICSB does not handle or have access to personal data this will be void. If the clients does require ICSB staff to be trained in the requirements this will need to be formally informed and requested.

7. Compliance Measurement

The ICSB IT Department will verify compliance with this policy through various methods, including but not limited to, periodic walk-through, video monitoring, business tool reports, internal and externalaudits, and feedback to the policy owner.

- Exceptions

  Any exception to the policy must be approved by the IT Department in advance.

- Non-Compliance

  An employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

8. Related Standards, Policies and Processes

- ISMS Manual for ISO27001