



MEGA SQUARE SDN. BHD.

PRIVACY POLICY

MSSB-008 Rev.00.202305

PRIVACY POLICY

INTRODUCTION

This Privacy Policy outlines how Mega Square Sdn Bhd ("the Company") collects, uses, retains, and discloses limited third-party contact details in compliance with the Personal Data Protection Act 2010 ("PDPA") of Malaysia. The Company is committed to protecting the privacy and confidentiality of employee personal data and any personal data received from third party engagement and ensuring its proper handling and security.

A. POLICY FOR EMPLOYEE DATA PROCESSING

1. Collection and Use of Personal Data

1.1. Purpose of Collection

The Company collects and processes personal data of employees for the purposes of employment management, human resources administration, payroll processing, benefits administration, performance evaluation, compliance with legal obligations, and other employment-related activities.

1.2. Types of Personal Data Collected

The personal data collected by the Company may include, but is not limited to:

- Employee identification information (name, employee number, photograph, identification card/passport details)
- Contact information (address, email address, phone number)
- Employment details (job title, department, employment history, performance records)
- Compensation and benefits information
- Financial information (bank account details for payroll processing)
- Medical and health information (where necessary for occupational health and safety)
- Leave and attendance records
- Training and development records
- Disciplinary and grievance records (if applicable)
- Emergency contact information

1.3. Consent for Data Collection

By entering into an employment contract with the Company or by signing the consent form, employees provide consent for the collection, use, and processing of their personal data as outlined in this Privacy Policy.

1.4. Use and Retention of Personal Data

The Company shall use employee personal data solely for the purposes specified in this Privacy Policy or as required by applicable laws and regulations. Personal data shall be retained for as long as necessary to fulfill the purposes for which it was collected, or as required by law.

2. Disclosure of Personal Data

2.1. Internal Disclosure

Employee personal data may be disclosed internally to authorized personnel within the Company on a need-to-know basis for the purposes outlined in this Privacy Policy.

2.2. External Disclosure

The Company may disclose employee personal data to third parties outside the Company under the following circumstances:

- Compliance with legal obligations, court orders, or government requests
- Facilitation of payroll processing or benefits administration with authorized third-party service providers
- Verification of employment history or reference checks with previous employers
- Compliance with tax, social security, or other statutory requirements
- application of work permits and immigration requirements

3. Security and Data Protection

The Company shall implement appropriate technical and organizational measures to safeguard employee personal data against unauthorized access, disclosure, alteration, or destruction. These measures may include physical security, access controls, encryption, regular system audits, and staff training on data protection. The details of the technical and organizational measures are set out in the relevant sections of the Company's Employee Principles.

4. Employee Rights

Employees have the following rights regarding their personal data:

- Right to access: Employees may request access to their personal data held by the Company.
- Right to correction: Employees may request the correction of inaccurate or incomplete personal data.
- Right to withdrawal of consent: Employees may withdraw their consent for the collection, use, or processing of their personal data, subject to legal obligations.
- Right to erasure: Employees may request the deletion or removal of their personal data when it is no longer necessary for the purposes for which it was collected, subject to legal obligations.
- Right to restriction: Employees may request a restriction on the processing of their personal data in certain circumstances.
- Right to data portability: Employees may request the transfer of their personal data to another organization in a structured, commonly used, and machine-readable format.

5. Questions or Concerns

For any questions or concerns regarding this Privacy Policy or the Company's data protection practices, please contact the General Manager, the P&A Manager, email your concern through **concern@megasquare.com.my**, or raise a concern through “Let’s talk” portal (for MSSB’s employee) or the reporting portal available at **www.megasquare.com.my/concern** (for third party). Both internal and external portals provide an option to raise the concern anonymously.

B. POLICY FOR LIMITED THIRD-PARTY CONTACT DETAILS PROCESSING

1. Collection and Use of Limited Third-Party Contact Details

1.1. Purpose of Collection

The Company may collect and process limited third-party contact details for the purpose of communication and collaboration with external entities, such as business partners, suppliers, vendors, contractors, or other relevant parties.

1.2. Types of Limited Third-Party Contact Details Collected

The limited third-party contact details collected by the Company may include, but are not limited to:

- Name
- Position or job title
- Business email address
- Business phone number

1.3. Consent for Data Collection

The collection and processing of limited third-party contact details are based on the legitimate interests of the Company in conducting its business operations and establishing communication with relevant external entities. The Company ensures that such collection and processing are reasonable, necessary, and conducted in compliance with applicable laws and regulations.

1.4. Use and Retention of Limited Third-Party Contact Details

The Company shall use limited third-party contact details solely for the purposes of business communication, collaboration, and relationship management with external entities. These contact details will be retained only for as long as necessary to fulfill the purposes for which they were collected or as required by law.

2. Disclosure of Limited Third-Party Contact Details

2.1. Internal Disclosure

Limited third-party contact details may be disclosed internally to authorized personnel within the Company on a need-to-know basis for the purposes outlined in this Privacy Policy.

2.2. Third-Party Disclosure

The Company may disclose limited third-party contact details to external entities under the following circumstances:

- Business communication and collaboration: Sharing contact details with relevant external entities to facilitate effective communication and collaboration.
- Contractual relationships: Sharing contact details with contracted vendors, suppliers, or service providers to enable the provision of goods or services.
- Compliance with legal obligations: Disclosing contact details when required by law, court order, or governmental regulation.

3. Security and Data Protection

The Company shall implement appropriate technical and organizational measures to safeguard limited third-party contact details against unauthorized access, disclosure, alteration, or destruction. These measures may include physical security, access controls, encryption, regular system audits, and staff training on data protection.

4. Rights of Individuals

Individuals whose limited contact details are processed by the Company have the right to:

- Request access to their personal data.
- Request correction of inaccurate or incomplete personal data.
- Object to the processing of their personal data, where applicable.
- Request the deletion or removal of their personal data, subject to legal obligations.

5. Questions or Concerns

For any questions or concerns regarding this Privacy Policy or the Company's data protection practices, please contact the General Manager, the P&A Manager, email your concern through concern@megasquare.com.my, or raise a concern through “Let’s talk” portal (for MSSB’s employee) or the reporting portal available at www.megasquare.com.my/concern (for third party). Both internal and external portals provide an option to raise the concern anonymously.

C. INCIDENT MANAGEMENT PROCEDURE

In the event of a privacy-related incident involving the processing of personal data by the relevant team at Mega Square Sdn Bhd, the following incident management procedure shall apply:

1. Incident Reporting: Once identified, the relevant team/employee must immediately report any privacy-related incidents to the General Manager or the P&A Manager.
2. Incident Assessment: Upon receiving an incident report or any incident received through concern@megasquare.com.my, the internal reporting channel or the external reporting channel, the General Manager and the P&A Manager will assess the incident to determine its severity and potential consequences and report to the Managing Director
3. Incident Response: Based on the severity of the incident, the Company will take appropriate actions to address and mitigate it, including containment, notification, restoration, investigation, and remedial measures as necessary.
4. Incident Documentation: All incidents and related actions will be thoroughly documented for future reference, audits, and continuous improvement.
5. Communication: The Company will maintain open and transparent communication regarding privacy-related incidents, including notifying affected individuals or relevant authorities if required by law or if the incident poses significant risks.
6. Review and Continuous Improvement: The Company shall review its incident management procedure to ensure its effectiveness and make necessary improvements.