Klarity Systems

DATA PROTECTION & PRIVACY POLICY

Klarity Systems Sdn Bhd (1584729-A)
3003, Level 30, Menara Prestige, Jalan Pinang, Kuala Lumpur,
50450 Kuala Lumpur, Federal Territory of Kuala Lumpur

1. Introduction

Klarity Systems is committed to protecting the privacy and security of personal data we collect from our customers, employees, and partners. This policy outlines our practices concerning the collection, use, disclosure, and protection of personal information in compliance with applicable data protection laws and regulations.

2. Scope

This policy applies to all personal data processed by Klarity Systems, regardless of the medium on which that information is stored or whether it relates to past or present employees, workers, customers, clients or supplier contacts, shareholders, website users or any other Data Subject.

3. Definitions

a) "**Personal data**" means any information relating to an identified or identifiable natural person ('data subject').

b) "**Processing**" means any operation performed on personal data, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

c) "**Data Controller**" means the entity that determines the purposes and means of processing personal data.

d) "**Data Processor**" means the entity that processes personal data on behalf of the Data Controller.

4. Data Protection Principles

Klarity Systems adheres to the following principles when processing personal data:

a) Lawfulness, fairness, and transparency: All processing must be legal, fair, and transparent to the data subject.

b) Purpose limitation: Data should only be collected for specified, explicit, and legitimate purposes and not further processed in a manner incompatible with those purposes.

c) Data minimization: Only personal data that is adequate, relevant, and limited to what is necessary should be processed.

d) Accuracy: Personal data must be accurate and, where necessary, kept up to date.

e) Storage limitation: Data should be kept in a form which permits identification of data subjects for no longer than is necessary.

f) Integrity and confidentiality: Processing should ensure appropriate security of the personal data.

g) Accountability: The data controller is responsible for and must be able to demonstrate compliance with these principles.

5. Legal Bases for Processing

We will only process personal data where we have a lawful basis to do so. The lawful bases we rely on are:

a) Consent: The individual has given clear consent for you to process their personal data for a specific purpose.

b) Contractual necessity: The processing is necessary for a contract you have with the individual.

c) Legal obligation: The processing is necessary for you to comply with the law.

d) Vital interests: The processing is necessary to protect someone's life.

e) Public interest: The processing is necessary for you to perform a task in the public interest or for your official functions.

f) Legitimate interests: The processing is necessary for your legitimate interests or the legitimate interests of a third party, unless there is a good reason to protect the individual's personal data which overrides those legitimate interests.

6. Rights of Data Subjects

We respect the rights of data subjects and will respond to requests to exercise those rights in accordance with applicable laws. These rights may include:

a) Right to be informed: Individuals have the right to know how their data is being collected and used.

b) Right of access: Individuals can request access to their personal data.

c) Right to rectification: Individuals can have inaccurate or incomplete personal data rectified.

d) Right to erasure: Also known as 'the right to be forgotten', individuals can request the deletion of their personal data in certain circumstances.

e) Right to restrict processing: Individuals can request the restriction or suppression of their personal data.

f) Right to data portability: Individuals can obtain and reuse their personal data for their own purposes across different services.

g) Right to object: Individuals can object to the processing of their personal data in certain circumstances.

h) Rights related to automated decision making and profiling: Individuals have rights related to automated individual decision-making (making a decision solely by automated means without any human involvement) and profiling (automated processing of personal data to evaluate certain things about an individual).

7. Data Collection and Use

We collect and use personal data for specified, explicit, and legitimate purposes. These purposes include:

a) Providing products and services: This includes processing orders, delivering products, services and providing customer support.

b) Managing customer relationships: This could involve maintaining customer accounts, handling inquiries, and personalizing user experiences.

c) Processing payments: This includes billing, collecting payments, and maintaining financial records.

d) Marketing and communications: This might involve sending promotional materials, newsletters, or conducting market research, always in compliance with applicable marketing laws.

e) Improving products and services: This could include analysing usage data to enhance user experience or develop new features.

f) Complying with legal obligations: This includes maintaining records for tax purposes, responding to legal requests, or fulfilling regulatory reporting requirements.

We will not use personal data for purposes incompatible with those for which it was originally collected.

8. Data Retention

We retain personal data only for as long as necessary to fulfil the purposes for which it was collected, including for the purposes of satisfying any legal, accounting, or reporting requirements.

9. Data Security

We implement appropriate technical and organizational measures to ensure a level of security appropriate to the risk, including:

a) Encryption of personal data.

b) Ensuring ongoing confidentiality, integrity, availability and resilience of processing systems and services.

c) The ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident.

d) A process for regularly testing, assessing and evaluating the effectiveness of technical and organizational measures for ensuring the security of the processing.

10.Data Breaches

In the event of a personal data breach, we will notify the relevant supervisory authority without undue delay and, where feasible, not later than 72 hours after having become aware of it, unless the breach is unlikely to result in a risk to the rights and freedoms of natural persons.

11.International Data Transfers

When transferring personal data outside the jurisdiction in which it was collected, we ensure appropriate safeguards are in place in compliance with applicable laws and regulations.

12.Data Protection Impact Assessments

We will carry out Data Protection Impact Assessments (DPIAs) for processing operations that are likely to result in a high risk to the rights and freedoms of natural persons.

13.Training

We provide data protection training to our employees and ensure they understand their responsibilities when handling personal data.

14.Third-Party Processors

We only appoint processors who can provide sufficient guarantees to implement appropriate technical and organizational measures in such a manner that processing will meet the requirements of applicable data protection laws and regulations and ensure the protection of the rights of the data subject.

15.Children's Privacy

We do not knowingly collect or process data relating to children under the age of 16 without parental consent, except where local law allows for a different age of consent.

16.Changes to This Policy

We may update this policy from time to time in response to changing legal, technical or business developments. We will take appropriate measures to inform you about any material changes.

17.Contact Information

If you have any questions about this policy or our data protection practices, please contact info@klaritysytems.com.