BRIDGENET SOLUTIONS

Privacy Policy

Policy owner: *Chief Technology Officer ("CTO")*
Policy manager: *Head of Managed Security Services ("HMSS")*
Approver: *Board of Directors*

---

1 Purpose & Scope

The purpose of this policy is to mitigate privacy risks by defining a common set of requirements for managing privacy compliance across Bridgenet Solutions ("the **Company**") and to ensure accountability for privacy compliance at the management level and across the value chain.

This policy shall apply to all processing of Personal Data in the Company, including processing that is carried out by third parties on the Company's behalf.

The Privacy Policy Owner shall advise on and monitor its implementation. This policy shall be implemented by the Company.

2 Requirements

2.1 Governance and Organisation

The Company shall formally delegate and describe the organisational structure, roles, and responsibilities for managing privacy.

The HMSS is responsible to advise and reports on privacy matters to the Privacy Policy Owner and Company senior management and is tasked with independent oversight of privacy compliance, including monitoring.

The Company shall assign privacy resources corresponding to the complexity and level of risk of its processing activities.

2.2 Risk Management

The Company shall identify, mitigate, and report on privacy compliance risks, following the regular risk reporting process internally.

2.3 Controls

The Company shall implement effective internal controls that verify the level of implementation of internal and external privacy requirements.

2.4 Personal Data Inventory

The Company shall maintain an up-to-date inventory of existing processing activities and supporting IT systems.

2.5 Fundamental Data Protection Principles

The Company shall:

- Identify and document the legal basis for all its processing activities.
- Ensure Personal Data is only processed to the extent it is necessary for fulfilling a defined purpose.
- Define and implement retention limits for Personal Data in all relevant processes and systems.
- Be transparent about its processing of data subjects' Personal Data, which data subject rights apply, how data subjects may invoke their rights and how the Company will implement such rights.

2.6 Processes and Technology

The Company shall implement technical, organisational, operational, and contractual measures as necessary to mitigate privacy risk and ensure privacy compliance in the development and procurement of its processes, systems, products, and technologies.

The Company shall identify privacy related high-risk activities, processes and technologies and ensure the conduct of Data Protection Impact Assessments in which the privacy impact is assessed, documented, and managed.

2.7 Cross-Border Transfers

The Company shall maintain an overview and ensure the legality of all cross-border transfers of Personal Data, considering local restrictions or conditions.

2.8 Business Partner Privacy Management

The Company shall assess and manage privacy risks related to the Personal Data processing performed by its Business Partners.

The Company shall adopt contractual clauses that govern the processing of Personal Data by its Business Partners, wherever applicable.

2.9 Training and Awareness-Raising Activities

The Company shall ensure the general knowledge and awareness of all employees on fundamental privacy principles and the main obligations to respect individuals' privacy.

The Company shall provide additional, role-based training to specific employees, where relevant.

2.10 Privacy Incident Management

In the event of a Privacy Incident leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access to Personal Data, the Company shall identify and assess, record, resolve, and report the Privacy Incident to the HMSS, ensuring this is an integrated part of its regular incident management processes.

2.11 Regulatory Management

The Company shall have mechanisms in place to identify and assess changes to external requirements and their impact.

The Company shall have procedures in place on how to handle inquiries, requests and inspections from data protection authorities and other relevant authorities as applicable.

3 Reporting

The Privacy Policy Owner shall be immediately notified of severe Privacy Incidents including breaches to this policy, related manuals, and applicable privacy laws.

In order to maintain communication effectiveness and transparency within the Company, the Policy Owner is responsible for setting privacy performance management and reporting requirements.

4 Reference Documents

Internal

- Business Partner Management Policy
- Enterprise Risk Management Policy
- PDPA Acceptance Form

External

- Personal Data Protection Act 2010
- General Data Protection Regulation (GDPR)

5 Definitions and Abbreviations

Business Partner: see definition in the Business Partner Management Policy.

Cross-Border Transfer (of personal data): Communication, disclosure or otherwise making available Personal Data by one legal entity to another legal entity (data recipient), conducted with the knowledge or intention of the involved legal entities.

Personal Data: any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, national registration identification card, telephone/mobile number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural, or social identity of that natural person. Communications content data is considered to be personal data, and metadata from the telecommunications network is considered to be personal data to the extent the Group connects these data with an individual.

Privacy Incident: Any adverse event pertaining to the unauthorised use or disclosure of personal data that happens as a result of violating privacy legislation including but not limited to the Malaysian Personal Data Protection Act 2010 or this policy and related manuals.