QNET GDPR Compliance Statement

Introduction

The EU **General Data Protection Regulation** ("**GDPR**") comes into force across the European Union on 25th May 2018, and brings with it the most significant changes to data protection law in two decades. Based on privacy by design and taking a risk-based approach, the GDPR has been designed to meet the requirements of the digital age. It aims to standardise data protection laws and processing across the EU, affording individuals stronger, more consistent rights to access and control their personal information.

Our Commitment

QNET (including its affiliated companies that collects or processes data of EU persons, and whom we refer to as 'we' or 'us' or 'our') are committed to ensuring the security and protection of the personal information that we process, and to provide a compliant and consistent approach to data protection. We have always had a robust and effective data protection program in place which complies with existing laws and abides by the data protection principles. However, we recognise our obligations in updating and expanding this program to meet the demands of the GDPR in addition to the applicable national data protection laws across the European Union.

QNET is dedicated to safeguarding the personal information under our remit, and in developing a data protection regime that is effective, fit for purpose and demonstrates an understanding of, and appreciation for, the GDPR. Our preparation and objectives for the GDPR compliance have been summarised in this Statement, and include the development and implementation of new data protection roles, policies, procedures, controls and measures to ensure maximum and ongoing compliance.

How We're Preparing for the GDPR

QNET already has a consistent level of data protection and security across our organisation. However it is our aim to be fully compliant with the GDPR; therefore, in this respect, please be informed that our preparations towards that aim include:

- **Information Audit** – carrying out a company-wide information audit to identify and assess what personal information we hold, where it comes from, how and why it is processed and if and to whom it is disclosed.

- **Policies and Procedures** – revising and/or implementing new data protection policies and procedures to meet the requirements and standards of the GDPR and any relevant data protection laws, including:

    (a) **Data Protection** – our main Policies and Procedures document for data protection will be reviewed to meet the standards and requirements of the GDPR. Accountability and governance measures will be put in place to ensure that we understand, adequately disseminate and evidence our obligations and responsibilities, with a dedicated focus on privacy by design and the rights of individuals.

(b) **Data Retention and Erasure** – we will ensure that we meet the 'data minimisation' and 'storage limitation' principles, and that personal information is stored, archived and destroyed compliantly and ethically. We will be putting erasure procedures in place to meet the new 'Right to Erasure' obligation, along with any exemptions, response timeframes and notification responsibilities.

(c) **Data Breaches** – our breach procedures ensure that we have safeguards and measures in place to identify, assess, investigate and report any personal data breach at the earliest possible time. Our procedures are robust and have been disseminated to all employees, making them aware of the reporting lines and steps to follow.

(d) **International Data Transfers and Third Party Disclosures** – where a third party transfers personal information outside the EU, we have robust procedures and safeguarding measures in place to secure, encrypt and maintain the integrity of the data. Our procedures include a continual review of the countries with sufficient adequacy decisions, as well as provisions for binding corporate rules, standard data protection clauses and/or approved codes of conduct. We carry out strict due diligence checks with all recipients of personal data to assess and verify that they have appropriate safeguards in place to protect the information, ensure enforceable data subject rights and have effective legal remedies for data subjects where applicable.

- **Legal Basis for Processing** – we will be reviewing all processing activities to identify the legal basis for processing and ensuring that each basis is appropriate for the activity it relates to. Where applicable, we will also be maintaining records of our processing activities.

- **Privacy Notice/Policy** – we will be revising our Privacy Notice(s) to comply with the GDPR, ensuring that all individuals whose personal information we process will be informed of why we need it, how it will be used, what their rights are, who the information is disclosed to, and what safeguarding measures are in place to protect their information.

- **Obtaining Consent** – we will be revising our consent mechanisms for obtaining personal data, ensuring that individuals understand what they are providing, why and how we use it and giving clear, defined ways to consent to us processing their information. We will be enhancing our processes for recording consent, including maintaining time and date records, and an easy way to see, access or withdraw consent at any time.

- **Direct Marketing** – we will be revising the wording and processes for direct marketing, including clear opt-in mechanisms for marketing subscriptions, a clear notice and method for opting out and providing unsubscribe features on all subsequent marketing materials.

Data Subject Rights

In addition to the preparations mentioned above that will ensure individuals can enforce their data protection rights, we will be providing easy access to information via our website at http://www.qnet.net.my/ informing an individual's right to access any personal information that **QNET** processes about them, and to request information about:

- What personal data we hold about them
- The purposes of the processing
- The categories of personal data concerned
- The recipients to whom the personal data has/will be disclosed
- How long we intend to store your personal data for
- If we did not collect the data directly from them, information about the source
- The right to have incomplete or inaccurate data about them corrected or completed and the process for requesting this
- The right to request erasure of personal data (where applicable) or to restrict processing in accordance with data protection laws, as well as to object to any direct marketing from us and to be informed about any automated decision-making that we use
- The right to lodge a complaint or seek judicial remedy and who to contact in such instances

Information Security & Technical and Organisational Measures

QNET takes the privacy and security of individuals and their personal information very seriously and take every reasonable measure and precaution to protect and secure the personal data that we process. We have robust information security policies and procedures in place to protect personal information from unauthorised access, alteration, disclosure or destruction and have several layers of security measures, including:

- SSL
- Access controls
- Password policy
- Encryptions
- Authentication

GDPR Roles and Employees

QNET understands that continuous employee awareness and understanding is vital to the continued compliance of the GDPR, and we will be involving our employees in our preparation plans.

QNET has a designated Data Protection and data privacy team to develop and implement our roadmap for complying with the new data protection Regulation. The team are responsible for promoting awareness of the GDPR across the organisation, assessing our GDPR readiness, identifying any gap areas and implementing the new policies, procedures and measures. If you have any questions about our preparation for the GDPR, please send us an email at dpo@qnet.net.