MARNIX EUROPE LTD

(part of the Marubeni Group Companies)

DATA PROTECTION POLICY

Data Protection Policy

Date of issue: 16th March 2015

1. POLICY STATEMENT

1.1 Everyone has rights with regard to how their personal information is handled. During the course of its activities, Marnix Europe Ltd (the "**Company**") will collect, store and process personal information about members of Staff (as defined in paragraph 3.10 below), and the Company recognises the need to treat it in an appropriate and lawful manner.

1.2 The types of information that the Company may be required to handle include details of current, past and prospective members of Staff, suppliers, customers and other individuals that the Company communicates with. The information, which may be held on paper or on a computer or other media, is subject to certain legal safeguards specified in the Data Protection Act 1998 (as amended from time to time) (the "**Act**") and other regulations.

The Act imposes restrictions on how the Company may use that information.

1.3 This policy does not form part of any employee's contract of employment and it may be amended at any time. Any breach of, or non-compliance with, this policy will be taken seriously, may be regarded as gross misconduct and may result in disciplinary action up to and including dismissal.

2. STATUS OF THE POLICY

2.1 This policy has been approved by the Managing Director of the Company. It sets out our rules on data protection and the legal conditions that must be satisfied in relation to the obtaining, handling, processing, storage, transportation and destruction of personal information.

2.2 The Company's Managing Director is responsible for ensuring compliance with the Act and with this policy.

Any questions or concerns about the operation of this policy should be referred in the first instance to the Managing Director.

2.3 If you consider that the policy has not been followed in respect of personal data about yourself or others you should raise the matter with your line manager or the Managing Director

3. DEFINITION OF DATA PROTECTION TERMS

3.1 **Data** is information which is stored electronically, on a computer, or in certain paper-based filing systems.

3.2 **Data subjects** for the purpose of this policy include all living individuals about whom we hold personal data. A data subject need not be a UK national or resident. All data subjects have legal rights in relation to their personal data.

3.3 **Personal data** means data relating to a living individual who can be identified from that data (or from that data and other information in our possession). Personal data can be factual (such as a name, address or date of birth) or it can be an opinion (such as a performance appraisal).

3.4 **Data controllers** are the people who or organisations which determine the purposes for which, and the manner in which, any personal data is processed. They have a responsibility to establish practices and policies in line with the Act. We are the data controller of all personal data used in our business.

3.5 **Data users** include employees whose work involves using personal data. Data users have a duty to protect the information they handle by following our data protection and security policies at all times.

3.6 **Data processors** include any person who processes personal data on behalf of a data controller. Employees of data controllers are excluded from this definition but it could include suppliers which handle personal data on our behalf.

3.7 **Main Offices** mean the registered office of the Company; the branch offices of the Company; and the liaison offices of the Company.

3.8 **Processing** is any activity that involves use of the data. It includes obtaining, recording or holding the data, or carrying out any operation or set of operations on the data including organising, amending, retrieving, using, disclosing, erasing or destroying it. Processing also includes transferring personal data to third parties.

3.9 **Sensitive personal data** includes information about a person's racial or ethnic origin, political opinions, religious or similar beliefs, trade union membership, physical or mental health or condition or sexual life, or about the commission of, or proceedings for, any offence committed or alleged to have been committed by that person, the disposal of such proceedings or the sentence of any court in such proceedings. Sensitive personal data can only be processed under strict conditions, and will usually require the express consent of the person concerned.

3.10 **Staff** means any director, officer or employee (of the Company unless otherwise stated).

4. DATA PROTECTION PRINCIPLES

Anyone processing personal data must comply with the eight enforceable principles of good practice. These provide that personal data must be:

(a) Processed fairly and lawfully.

(b) Processed for limited purposes and in an appropriate way.

(c) Adequate, relevant and not excessive for the purpose.

(d) Accurate.

(e) Not kept longer than necessary for the purpose.

(f) Processed in line with data subjects' rights.

(g) Secure.

(h) Not transferred to people or organisations situated in countries without adequate protection.

5. FAIR AND LAWFUL PROCESSING

5.1 The Act is intended to ensure that the processing of personal data is done fairly and without adversely affecting the rights of the data subject, rather than to prevent such processing. The data subject must be told who the data controller is (in this case

Marnix Europe Ltd), the purpose for which the data is to be processed by us, and the identities of anyone to whom the data may be disclosed or transferred.

5.2 The Company will usually only process a member of Staff's personal data where he/she has given his/her consent or where the processing is necessary to comply with the Company's legal obligations. In other cases, processing may be necessary for the protection of a member of Staff's vital interests, for the Company's legitimate interests or the legitimate interests of others. The full list of conditions is set out in the Act.

5.3 The Company will only process sensitive personal data where a further condition is also met. Usually this will mean that the relevant member of Staff has given his/her explicit consent, or that the processing is legally required for employment purposes. The full list of conditions is set out in the Act.

6. PROCESSING FOR LIMITED PURPOSES

The Company will only process a member of Staff's personal data for the specific purpose described in the Annex or purposes notified to the member of Staff or for any other purposes specifically permitted by the relevant Act.

7. ADEQUATE, RELEVANT AND NON-EXCESSIVE PROCESSING

Each member of Staff's personal data will only be processed to the extent that it is necessary for the specific purposes described in the Annex or otherwise notified to the relevant member of Staff.

8. ACCURATE DATA

Personal data must be accurate and kept up to date. Information which is incorrect or misleading is not accurate and steps should therefore be taken to check the accuracy of any personal data at the point of collection and at regular intervals afterwards. Inaccurate or out-of-date data should be destroyed.

9. TIMELY PROCESSING

Personal data should not be kept longer than is necessary for the purpose. This means that data should be destroyed or erased from our systems when it is no longer required.

10. PROCESSING IN LINE WITH DATA SUBJECT'S RIGHTS

Data must be processed in line with data subjects' rights. Data subjects have a right to:

(a) Request access to any data held about them by a data controller.

(b) Prevent the processing of their data for direct-marketing purposes.

(c) Ask to have inaccurate data amended.

(d) Prevent processing that is likely to cause damage or distress to themselves or anyone else.

11. DATA SECURITY

11.1 The Company must ensure that appropriate security measures are taken against unlawful or unauthorised processing of personal data, and against the accidental loss of, or damage to, personal data.

11.2 The Act requires us to put in place procedures and technologies to maintain the security of all personal data from the point of collection to the point of destruction. Personal data may only be transferred to a third-party data processor if he/she agrees to comply with those procedures and policies, or if he/she puts in place adequate measures himself/herself.

11.3 Maintaining data security means guaranteeing the confidentiality, integrity and availability (for authorised purposes) of the personal data.

11.4 All personal data should therefore be transferred securely including, where appropriate, with password protection and the use of encryption technologies.

12. WHERE WE STORE YOUR PERSONAL DATA

The data that we collect from you may be transferred to, and stored at, a destination outside the European Economic Area ("**EEA**"). It may also be processed by Staff operating outside the EEA who work for us or for one of our suppliers. By submitting your personal data, you agree to this transfer, storing or processing. The Company will take all steps reasonably necessary to ensure that your data is treated securely and in accordance with this data protection policy. These steps include complying with legally binding data transfer agreements which are in place with Marubeni group companies.

13. DEALING WITH SUBJECT ACCESS REQUESTS

A formal request from a data subject for information that we hold about them must be made in writing. A fee is payable by the data subject for provision of this information. Any member of Staff who receives a written request should forward it to the Managing Director immediately.

14. ANTI-CORRUPTION HOTLINE

14.1 Marubeni Group has established an Anti-Corruption Hotline called EthicsPoint (available at https://secure.ethicspoint.eu/domain/media/en/gui/100659/index.html). EthicsPoint is operated by NAVEX Global, Inc. on behalf of Marubeni Group.

14.2 EthicsPoint is a comprehensive and confidential reporting tool to assist Marubeni Group's management and employees to work together to address fraud, abuse and other misconduct in the workplace, all while cultivating a positive work environment.

14.3 **The operation of EthicsPoint may involve the processing of personal data about both Marubeni Group's Staff and third parties.** Any personal data collected through EthicsPoint will be processed fairly and lawfully in accordance with applicable data protection laws for the sole purpose of identifying and investigating allegations of illegal activity and/or non-compliance with Marubeni Group policies.

15. MONITORING AND REVIEW OF THE POLICY

15.1 We will continue to review the effectiveness of this policy to ensure it is achieving its stated objectives.

15.2 If you have any queries or concerns regarding this data protection policy, please contact the relevant Data Protection Compliance Manager in accordance with paragraph 2.2 above.

ANNEX

Purposes of the processing

Marnix Europe may process personal data for the following purposes:

- For recruitment, job application management, human resources planning and management by the Company and Marubeni Corporation, including, head count analysis and senior Staff succession planning, management development and talent retention strategies.
- For the Company or any other Marubeni Group company to provide information technology and information processing support, IT applications and systems maintenance, data storage, and IT facilities (including cloud-based solutions) in support of the Company's activities relating to its business including internal management and administration.
- As required to operate the "Marubeni Anti-Corruption Hotline", including to enable Marubeni Corporation to process, analyse, recognise, resolve and/or otherwise address any issues or circumstances in which the Company and/or any of its Staff have actually or allegedly been involved in any acts relating to bribery, money laundering, illegal accounting treatment, violation of securities laws such as insider trading, and other actual or potential criminal or unethical activity.