Maitland

Personal Data Security Protection

Table of Contents

The EU's General Data Protection Regulation (GDPR) requires Maitland to secure and protect the confidentiality, integrity, availability and privacy of personal data. Maitland has been reviewing and enhancing its existing Information Security framework in readiness for the implementation of the GDPR on 25th May 2018.

Maitland will continue with implementations, refinement and development of its privacy framework to meet client, regulatory and best practice requirements.

Maitland Group Information Security uses reasonable measures and continues to improve, refine and implement such measures to safeguard sensitive and personal data.

1. PRIVACY AND INFORMATION SECURITY

1.1 ICT and Group Information Security at Maitland treat privacy and the security of personal data very seriously and the Maitland Group continues to invest in information security to ensure compliance with GDPR and other applicable privacy laws.

1.2 Information security in the Maitland Group is based on the ISO/IEC 27001:2013 Information Security Management System (ISMS) as an overarching framework to manage privacy and personal data as part of the broader management of information risks, information security and related compliance, incident management and business continuity issues.

1.3 Following a risk based approach, the measures that have been and continue to be selected are deemed appropriate to the type of information maintained, and always consider applicable laws regarding safeguarding any such information under our control, in particular personal data.

1.4 Existing information security controls are maintained and new controls have been designed and implemented to detect or prevent unauthorized access to, modification or destruction of personal data, whether accidental or deliberate. These controls are based on the requirements of the business and conform to commonly accepted industry standards as well as contractual and legal requirements.

2. INFORMATION SECURITY MANAGEMENT SYSTEM

2.1 The Information Security Management System that is in place, is based on the ISO/IEC 27000 set of standards for information security, in particular ISO/IEC 27001:2013.

2.2 Information Security in the Maitland Group is embedded through participation in various forums and structures and the Group Information Security Head provides regular reporting directly to the Board and the Audit and Risk Committee.

2.3 The Group Information Security policy is regularly reviewed and updated to ensure continued information security compliance to legal and regulatory requirements.

3. INFORMATION SECURITY AWARENESS TRAINING

3.1 Information Security awareness training is implemented and forms part of the Induction programme for all new joiners.

3.2 Information security and data protection training is compulsory for all staff.

4. ENCRYPTION AND NETWORK PROTECTION

4.1 Maitland recognises how important it is to protect the confidentiality, authenticity and/or integrity of information.

4.2 Maitland uses Secure Socket Layer (“SSL”) or Transport Layer Security (“TLS”) encryption technology and encrypts communications to enhance data privacy and help prevent loss, misuse, or alteration of personal data.

4.3 Security is managed with mechanisms to protect entry points to the network and the network is segregated to provide security and protect the confidentiality and availability of personal data.

5. DATA TRANSFER

Due to the global nature of the Maitland Group, appropriate steps are taken to manage the risks associated with cross border transfer of personal data and we continue to monitor legislative and regulatory requirements in order to comply with data flow requirements.

6. ICT AUDITS

6.1 Internal audits of ICT and Information Security are performed at Maitland by the internal audit department.

6.2 ISAE 3402 audits are performed for an independent assurance opinion on controls for financial reporting.

7. DATA CLASSIFICATION

Maitland has implemented a data classification and handling policy to manage and protect personal data, which governs the operational measures that we have in place to detect and prevent unauthorized disclosure, modification, removal or destruction of data, including the management, detection and control of the use of removable media and email.

8. ACCEPTABLE USE OF ICT

8.1 Our Acceptable Use policy governs the acceptable use of information assets including mobile devices.

8.2 Maitland ICT continually reviews its management of assets and continues to identify information assets and maintaining an inventory of assets.

9. USER ACCESS CONTROL TO SYSTEMS AND APPLICATIONS

9.1 User registration and de-registration follows a defined process and users of Maitland’s information assets only receive access to the Maitland network and related services for which approval has been given.

9.2 User access reviews are performed periodically to ensure and to reduce the risk of unauthorized access to systems and services.

9.3 The Acceptable Use policy makes users accountable for safeguarding their authentication information. The Acceptable Use policy is presented to users at log on and requires acceptance before authenticating a user to Maitland's network.

9.4 To prevent unauthorized access to systems and applications, access to information and application system functions are restricted and log-on is secure on all relevant applications and systems, with quality passwords that meet or exceed current standards.

10. PHYSICAL AND ENVIRONMENTAL SECURITY

10.1 All data processed by Maitland and the technology used are hosted in secure data centres.

10.2 Physical protection measures, to safeguard against unauthorized physical access, damage and interference to the organization's information and information processing facilities are in place.

10.3 Data centres have the necessary environmental controls, access control, back-up and uninterrupted power supplies, to reduce the risk of loss, damage, theft, compromise and likelihood of an interruption to Maitland's operations.

11. OPERATIONS SECURITY

11.1 Information security operating procedures are continually developed, refined and reviewed to meet existing and new client, regulatory and best practise requirements. This is to ensure correct and secure operations of information processing facilities.

11.2 The Maitland Change Management policy governs changes, including security changes, to Maitland business processes, information processing facilities and systems, and requires that all changes follow the change management process.

11.3 Development, testing, and production environments are physically or logically separated, where it is required, to reduce the risks of unauthorized access or changes to the operational environment.

12. MALWARE AND VULNERABILITY MANAGEMENT

12.1 Maitland's information processing facilities are protected against malware and the implemented anti-malware technologies detect, prevent, and can recover against known malware.

12.2 The Information Security Office have controls in place to prevent the exploitation of technical vulnerabilities, by managing technical vulnerabilities and performing regular vulnerability scans to identify technical vulnerabilities of information systems being used. Maitland's exposure to such vulnerabilities is evaluated and the appropriate measures are taken to address the associated risk.

13. BUSINESS CONTINUITY AND DISTASTER RECOVERY

13.1 Business continuity, disaster recovery and security continuity are part of Maitland's business continuity management system. The business continuity processes are documented, implemented and maintained.

13.2 IT disaster recovery is tested regularly to ensure availability of information processing facilities. The major information processing facilities (data centres) have appropriate standby recovery facilities (data centre).

14. INCIDENT MANAGEMENT

Maitland has an established incident management process to identify, record and manage incidents including data breaches. The incident management process is continually improved to allow for additional business, regulatory, or best practise requirements and developments.

15. DATA RETENTION AND DESTRUCTION

15.1 Maitland has a Data Protection, Retention and Destruction policy, that sets out its policy with respect to data protection, data and document retention, archiving and destruction and applies to all staff across Maitland.

15.2 ICT performs backups of Maitland's information hosted on the ICT managed infrastructure, software and systems. Backups are tested regularly to protect against loss of data and in accordance with the Maitland backup policy.

Maitland
16 May 2018