D1 – GDPR

Compliance legislation (data protection, GDPR)
Applicant to confirm details of their organisation's approach to ensure the confidentiality of data is maintained. Applicants to confirm how they ensure compliance to GDPR & Data Protection Act as part of their response.
Please also confirm how you keep abreast of changes in GDPR / Data Protection legislation?

2 page A4 Arial 11 2%

Excellent scores will be awarded where Applicants;
• Demonstrate robust capabilities and compliance with UK/EU Data Protection legislation and meeting GDPR regulations with supporting evidence, policy and procedures.
• Provide their detailed processes for maintaining all relevant regulatory compliance for data protection and information security
• Details a thorough approach to how the applicant manages any changes in these legislations.
• Demonstrates a robust process to how the applicant ensures the confidentiality of data is maintained and how any breaches of process are communicated and managed to its customers.

INTRODUCTION

Morrison Water Services (MWS) is committed to ensuring that all company and client information is managed securely and in compliance with applicable national and international legislation. MWS holds ISO 27001 and Cyber Essentials accreditations as part of our security compliance, which is managed in house by the M Group Services (MGS) InfoSec team. This team also manages both internal (or via third parties) and external audits.
We implement a range of measures across our organisation that will, together with any bespoke procedures necessary, ensure all UU data is managed in compliance with GDPR requirements. These are described below.

DATA PRIVACY

We regularly review our Privacy Notice to ensure our processing of personal data is conducted fairly and lawfully. To ensure GDPR compliance operates optimally across our whole organisation and each of our contracts, we ensure all necessary legal and procedural aspects of compliance are in place – and are tested and operational. We also heavily invest across the organisation in regular GDPR training and awareness campaigns and communications.

Data privacy is reported via the quarterly Cyber Security Forum, which includes various representatives of the business, including the Risk Committee and IT services. Regular reviews and vulnerability testing are carried out via the Group InfoSec team who ensure that where improvements can be made, these are fully implemented. Regular risk reviews are also conducted on behalf of the Cyber Security Forum and following any individual changes or new processes.

Data privacy training is mandatory for all staff.

CORPORATE IT POLICIES AND PROCEDURES

Our integrated business management system (BMS) contains robust policies for data protection and retention, and access control. These govern IT service provision for staff and ensure access to information is based on the principle of least privilege; enabling staff to complete tasks relevant to their roles and responsibilities and ensuring data is only processed for the purpose specified. In line with our responsibility for data governance and accountability, we conduct data protection impact assessments (DPIA) to evidence any identified data protection risks.

To further embed the data protection policies and processes across the business, employees are required to adhere to our procedure 'Data Protection Breach Procedure', which lists a series of questions to complete as the first stage of the process.

GENERAL IT SECURITY

All lost IT equipment is suspended from the network or wiped remotely using mobile device management software to protect data storage. If a data breach occurs or suspicious behaviour is discovered or suspected, the user account is reviewed and suspended. We implement multi-factor authentication to reduce the likelihood and impact of account credential compromises.

Network and mobile passwords are changed every 180 days. Multiple incorrect log-in attempts result in the user's account being locked; with access only being regained via the IT Service Desk and a password reset following independent verification. Login attempts are monitored via our infrastructure support and IT Service Desk supplier to identify trends and potential attempted break-ins, ensuring data remains protected.

All data, whether office/site based or in transit is encrypted using a range of measures including Microsoft options, Intune for remote devices, and services such as Mimecast encrypted email, TLS and Bitlocker for discs.

We ensure each individual contract encompasses any client data retention requirements, such as defined storage limitations, which differ from those stipulated in the MGS Retention Policy.

We conduct data processing impact assessments, where necessary, to ensure information is adequately appraised and risks effectively managed.

All company data and client data processed by MWS is held within the UK/EU/EEA.

LEADERSHIP, MANAGEMENT AND COLLABORATION

We recognise that our data security and GDPR compliance is crucial in ensuring our clients deliver their regulatory requirements. The senior management team responsible for each of our contracts work closely with MGS and client teams to fully understand their needs and any sensitivities. This enables us to then develop bespoke approaches to ensure compliance, for example, on our contract with Thames Water, we have collaborated with the client to create a 'Data Subject Rights Policy'.

All directors and managers are directly responsible for implementing the relevant IT policies, procedures and standards within their business units. All users have access to relevant IT documentation via 'Stay Connected', the MGS corporate intranet.

TRAINING

All staff receive mandatory IT training including data privacy, document protection and security of IT equipment. This training is managed via an online service called 'Learn With Us', which is accessible to all MWS employees and our sister MGS companies.

We monitor the successful completion of all mandatory IT courses through the MGS InfoSec team and our competency cloud system 'Train With Us'. This helps us identify any requirements for additional support, reinforcement or improvement actions.

We also provide ongoing Toolbox Talks and staff awareness campaigns to reinforce compliance with data legislation, regulations and procedures. For example, we have recently focused on IT passwords and access, and have improved security through embedded credentials. All employees have an individual username and password with rights to access only those areas of the network appropriate to their job role and approved by line management.

KEEPING TRACK OF CHANGES IN LEGISLATION

We are aware that the data protection landscape is always evolving especially with the changing political landscape, we therefore stay abreast with updates from our in-house legal counsel on data protection issues. We further receive data protection legislation updates from legal partners with whom we work closely. Our data protection officer also attends seminars, conferences, conventions and other allied data protection outreach programs to enrich the knowledge on data protection as well as sharing best practices with other industry leaders.

We have our legal framework where we do an in-depth self-audit of our data protection posture and we also employ the services of an outsourced consulting firm who conduct (at least) an annual audit on our data protection posture to ensure we are operating within the required legal framework.

RELEVANT DOCUMENTS

The following documents form part of our BMS and are available on request:

- MGS-POL-DP-001 Data Protection Policy
- MGS-POL-DP-003 Data Breach Policy
- MGS-PRO-DP-001 Data Protection Breach Procedure