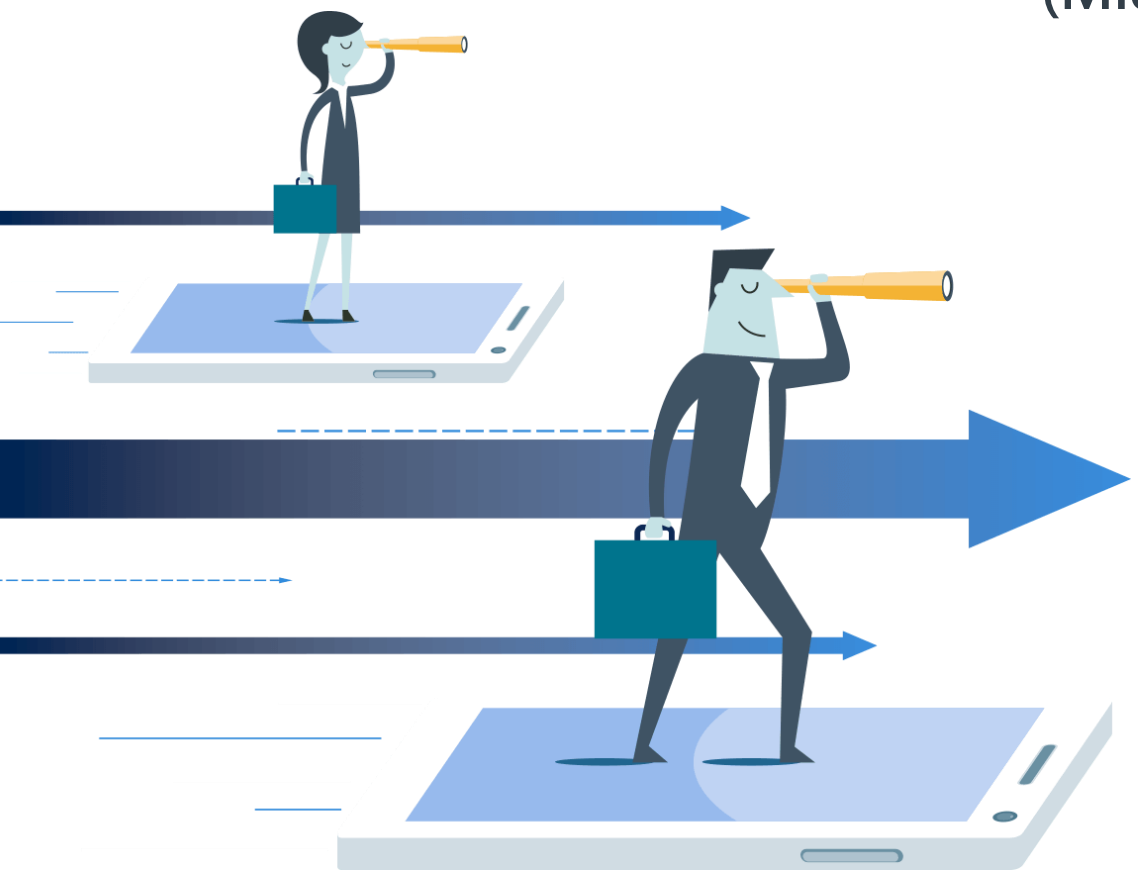
technology management

GDPR Compliance Statement

Technology Management (Midlands) Ltd



Date: 08/05/2018

Version: 1.0.1

Contents

1.1 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.

The 21st Century brings with it broader use of technology, new definitions of what constitutes personal data, and a vast increase in cross-border processing. The new Regulation aims to standardise data protection laws and processing across the EU; affording individuals stronger, more consistent rights to access and control their personal information.

1.2 Our Commitment

Technology Management (Midlands) Ltd 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 law and abides by the data protection principles (Certified ISO27001). However, we recognise our obligations in updating and expanding this program to meet the demands of the GDPR.

Technology Management (Midlands) Ltd are 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 new Regulation. Our preparation and objectives for 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.

1.3 How we have prepared for the GDPR

Technology Management (Midlands) Ltd already have a consistent level of data protection and security across our organisation, however it is our aim to be fully compliant with the GDPR by **25th May 2018**.

Our program included:

- **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 & Procedures –** We have implemented new data protection policies and procedures to meet the requirements and standards of the GDPR and any relevant data protection laws, including:
  - **Data Protection –** our main policy and procedure document for data protection has been overhauled to meet the standards and requirements of the GDPR. Accountability and governance measures are in place to ensure that we understand and adequately disseminate and evidence our obligations and responsibilities; with a dedicated focus on privacy by design and the rights of individuals.
  - **Data Retention & Erasure –** we have updated our retention policy and schedule to ensure that we meet the '*data minimisation*' and '*storage limitation*' principles and that personal information is stored, archived and destroyed compliantly and ethically. We have dedicated erasure procedures in place to meet the new '*Right to Erasure*' obligation and are aware of when this and other data subject's rights apply; along with any exemptions, response timeframes and notification responsibilities.
  - **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. We also hold insurance to cover for any fraudulent use of data contained within our systems.
  - **Subject Access Request (SAR) –** we have revised our SAR procedures to accommodate the revised 30-day timeframe for providing the requested information and for making this provision free of charge. Our new procedures detail how to verify the data subject, what steps to take for processing an access request, what exemptions apply and a suite of response templates to ensure that communications with data subjects are compliant, consistent and adequate.
- **Legal Basis for Processing -** we are 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 also maintain records of our processing activities, ensuring that our obligations under Article 30 of the GDPR and Schedule 1 of the Data Protection Bill are met.
- **Privacy Notice/Policy –** we have revised our Privacy Notice(s) to comply with the GDPR, ensuring that all individuals whose personal information we process have been informed of why we need it, how it is used, what their rights are, who the information is disclosed to and what safeguarding measures are in place to protect their information.
- **Direct Marketing -** we have revised 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 Protection Impact Assessments (DPIA) –** where we process personal information that is considered high risk, involves large scale processing or includes special category/criminal conviction data; we have developed stringent procedures and assessment templates for carrying out impact assessments that comply fully with the GDPR's Article 35 requirements. We have implemented documentation processes that record each assessment, allow us to rate the risk

posed by the processing activity and implement mitigating measures to reduce the risk posed to the data subject(s).

- **Processor Agreements –** where we use any third-party to process personal information on our behalf (*i.e. EDI, Hosting etc*), we have drafted compliant Processor Agreements and due diligence procedures for ensuring that they (*as well as we*), meet and understand their/our GDPR obligations. These measures include initial and ongoing reviews of the service provided, the necessity of the processing activity, the technical and organisational measures in place and compliance with the GDPR.

1.4 Data Subject Rights

In addition to the policies and procedures mentioned above that ensure individuals can enforce their data protection rights, we will provide easy to access information via our website, of an individual's right to access any personal information that **Technology Management (Midlands) Ltd** 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

1.5 Information Security & Technical and Organisational Measures

Technology Management (Midlands) Ltd 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 all in line with our ISO27001 accreditation.

[We implement measures such as SSL, access controls, password policy, encryptions, 2 factor authorisation, and regular reviews]

1.6 GDPR Roles and Employees

Technology Management (Midlands) Ltd have designated **James Crowter** as our **Data Protection Officer (DPO)** and have appointed a 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.

Technology Management (Midlands) Ltd understands that continuous employee awareness and understanding is vital to the continued compliance of the GDPR and have involved our employees in our preparation plans. We have implemented an employee training program specific to the which will be provided to all employees prior to May 25th, 2018, and forms part of our induction and annual training program.

If you have any questions about our preparation for the GDPR, please contact **James Crowter (DPO)** or email **gdpr@tecman.co.uk**.

Data Processing under GDPR at Technology Management

The data we collect, how its used and managed securely

Data set	Data source	Purpose	Description	Where held?	Legal basis for processing	Additional information on legal reason for processing	Retention period	Additional information
Customer details	Customer	To keep customers informed & educated as well as deliver the services we are contracted to provide	Company name, address, telephone number, software installed. Contact names, email address, telephone number, email communications, meeting & telephone call notes. Support call records.	Microsoft Dynamics 365/CRM	Contractual	N/A	1 year of non-use unless request to unsubscribe or right to be forgotten is received	Information protected to ISO 27001 standards
Customer details	Customer	To send emails to customers and process event bookings	Contact name, email address and company name	CommuniGator	Contractual	N/A	1 year of non-use unless request to unsubscribe or right to be forgotten is received	Information protected to ISO 27001 standards & GDPR Processor agreement in place for CommuniGator
Prospective customer details	Data purchase, website enquiries, exhibitions/events, direct calling	To market to and inform potential customers about the services we provide in our key areas of expertise	Company name, address, telephone number, software installed. Contact names, email address, telephone number, email communications, meeting & telephone call notes	Microsoft Dynamics 365/CRM	Legitimate interest	A contact at a prospective customer will only be part of an industrial sector campaign that our solution can support. Any company contacted has the option to Unsubscribe at any time.	1 year of non-use unless request to unsubscribe or right to be forgotten is received	Information protected to ISO 27001 standards
Prospective customer details	As above	To email prospective customers and process events bookings	Contact name, email address and company name	CommuniGator	Legitimate interest	as above	1 year of non-use unless request to unsubscribe or right to be forgotten is received	Information protected to ISO 27001 standards & GDPR Processor agreement in place for CommuniGator
Prospective customer/customer contact details	As above	We use third party mailing houses to send customer and prospective customer physical mailings	Exported list from Dynamics 365/CRM containing contact name, company name and address details	Third party mailing houses own databases (currently Sorted Direct Mail & Baker Goodchild)	Contractual & Legitimate interest	as above	All data is deleted by the third party mailings houses directly after execution of agreed mailing	Information protected to ISO 27001 standards & GDPR Processor agreements signed with Sorted Direct Mail & Baker Goodchild
Prospective customer/customer web chat conversation records	Customer/prospective customer	To respond to click to chat enquiries from customers/prospective customers	Customer/prospective customer name, email address and enquiry details	Live Chat software	Contractual & Legitimate interest	as above	5 years	Information protected to ISO 27001 standards
Prospective customer/customer webform enquiries	Customer/prospective customer	To respond to enquiries from website customers/prospective customers when they fill in a form on our website	Customer/prospective customer name, email address and enquiry details	Joomla! software	Contractual & Legitimate interest	as above	5 years	Information protected to ISO 27001 standards