15 May 2018

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.

Our Commitment

Southwest Medical Ltd is 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. However, we recognise our obligations in updating and expanding this program to meet the demands of the **GDPR.**

Southwest Medical Ltd 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 new Regulation.

Preparing for GDPR

Southwest Medical Ltd 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** by *25th May 2018***.**

Our preparation includes: -

- ***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 -*** revising/implementing 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.
- ***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.
- ***Privacy Notice/Policy*** – we have revised/are revising 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.
- ***Obtaining Consent*** - we have revised/are 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 have developed stringent processes for recording consent, making sure that we can evidence an affirmative opt-in, along with time and date records; and an easy to see and access way to withdraw consent at any time.
- ***Direct Marketing*** – *Southwest Medical Ltd* does not engage in Direct Marketing activities.
- ***Data Protection Impact Assessments (DPIA)*** – *Southwest Medical Ltd* does **not** process personal information that is considered high risk, involves large scale processing or includes special category/criminal conviction data.
- ***Processor Agreements*** – where we use any third-party to process personal information on our behalf (*i.e. Payroll*), 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.

Data Subject Rights

In addition to the policies and procedures mentioned above that ensure individuals can enforce their data protection rights, we provide information via our website, office, of an individual's right to access any personal information that *Southwest Medical 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
- The right to lodge a complaint and who to contact

Information Security & Technical and Organisational Measures

Southwest Medical Ltd takes the privacy and security of individuals and their personal information very seriously and takes 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

GDPR Roles and Employees

Southwest Medical Ltd has designated Louise Bennett as our Data Protection Officer (**DPO**) appointed person.

Southwest Medical Ltd understands that continuous employee awareness/understanding is vital to the continued compliance of the **GDPR** and has involved its employees in the preparation and ongoing training plan.

Southwest Medical Ltd is a Data Controller, as defined by the Data Protection Act/**GDPR**. Our **ICO** registration number is Z3227488. Data we hold is maintained in accordance with the Act, and we may contact you from time to time to verify and update this data. *Southwest Medical Ltd* is PCI DSS merchant compliant for payment card industry data security standards (Security Metrics).