Data Protection (GDPR) Policy

General Data Protection Regulation

Regulation on the protection of natural persons with regard to the processing of personal data and on the free movement of such data and repealing Directive 95/46/EC (General Data Protection Regulation) Made by. European Parliament and Council.

Author: C.L. Rees

April 2018

Version: 1.0

Contents

1. Company Background

The Unimed group of companies includes Universal Marine Medical Ltd. (UMM) and FAB Medical Ltd. (FAB) referred to in this GDPR policy as “The Company” &/or “The Company’s”. The Company’s are pharmaceutical wholesalers and distributors of medicinal products, equipment and services to customers on a global basis.

Everybody employed by or used by the Company’s are fully committed to following and maintaining the highest standards of GDP - Good Distribution Practice at all times.

Full compliance of the Company’s policies and procedures is of prime importance in achieving a safe and secure supply chain which will provide an important contribution to the protection of public health.

2. GDPR Background

The Company needs to collect person-identifiable information about individuals in order to carry out its functions and fulfil its objectives. Personal data is defined as ‘information which relates to a living individual and from which they can be identified, either directly or indirectly’.

Personal data at the Company can include employees (present, past and prospective), customers, service providers, contractors, third parties, and suppliers private and confidential information as well as sensitive information, whether in paper, electronic or other form.

Irrespective of how information is collected, recorded and processed person-identifiable information must be dealt with properly to ensure compliance with the Data Protection Act (DPA) 1998 and the General Data Protection Regulations (GDPR).

The DPA gives rights to data subjects (people that we hold information about) to access their own personal information, to have it corrected if wrong, in certain permitted circumstances to ask us to stop using it and to seek damages where we are using it improperly.

The lawful and correct treatment of person-identifiable information by the Company is paramount to the success of the organisation and to maintaining the confidence of its employees, customers, service providers, contractors, third parties and suppliers.

This policy will help the Company ensure that all person-identifiable information is handled and processed lawfully and correctly.

3. Data Protection Act & GDPR Principles

The Company has a legal obligation to comply with all relevant legislation in respect of data protection and information / IT security. The Company also has a duty to comply with all relevant guidance issued by issued by statutory bodies and professional groups.

All legislation relevant to an individual's right to the confidentiality of their information and the ways in which that can be achieved and maintained are paramount to the Company. Significant penalties can be imposed upon the Company or its employees for non-compliance.

The aim of this policy is to outline how the Company meets its legal obligations in safeguarding confidentiality and adheres to information security standards. The obligations within this policy are principally based upon the requirements of the Data Protection Act 1998 and the GDPR, as the key legislative and regulatory provisions governing the security of person-identifiable information.

4. What Information is Covered?

Personal data within the respective legislative and regulatory provisions covers 'any data that can be used to identify a living individual either directly or indirectly'. Individuals can be identified by various means including but not limited to, their address, telephone number or e-mail address.

Anonymised or aggregated data is not regulated by the provisions, providing the anonymisation or aggregation of the data is irreversible.

5. Policy Statement

This document defines the data protection policy for the Company. It applies to all person-identifiable information obtained and processed by the Company and its employees, customers, service providers, contractors, third parties and suppliers.

It sets out:

- The Company policy for the protection of all person-identifiable information that is processed.
- Establishes the responsibilities (and best practice) for data protection.
- References the key principles of the Data Protection Act 1998 and GDPR.

6. Principles

The objective of this policy is to ensure the protection of the Company information in accordance with relevant legislation, namely:

- **To ensure NOTIFICATION** - Annually notify the Information Commissioner about the Company's use of person-identifiable information.

- **To ensure PROFESSIONALISM** - All information is obtained, held and processed in a professional manner in accordance with the principles of the Data Protection Act 1998 and the provisions of the GDPR.

- **To preserve SECURITY** - All information is obtained, held, disclosed and disposed of in a secure manner.

- **To ensure AWARENESS** - Provision of appropriate training and promote awareness to inform all employees of their responsibilities.

- **Data Subject ACCESS** - Prompt and informed responses to subject access requests.

The policy will be reviewed periodically by the Company's senior management. Where review and updates are necessary due to legislative changes these will be done immediately. In accordance with the Company's discrimination and equality policy, this procedure will not discriminate, either directly or indirectly, on the grounds of gender, race, colour, ethnic or national origin, sexual orientation, marital status, religion or belief, age, union membership, disability, offending background or any other personal characteristic.

7. Scope of this Policy

This policy will ensure that person-identifiable information is processed, handled, transferred, disclosed and disposed of lawfully. Person-identifiable information should be handled in the most secure manner by authorised staff only, on a need to know basis. The procedures cover all person identifiable information whether electronic, paper or any other form which may relate to employees, customers, service providers, contractors, third parties and suppliers about whom we hold information.

8. Policy

The Company obtains and processes person-identifiable information for a variety of different purposes, including but not limited to:

- **Employees Data** - payroll, emergency contacts, training, disciplinary, performance, holidays, absence, general administration information.

- **Customers Data** - regulatory information in order to maintain the Company's operators licences.

- **Service Providers Data** - regulatory information in order to maintain the Company's operators licences.

- **Contractors Data** - regulatory information in order to maintain the Company's operators licences.

- **Third Parties Data** - regulatory information in order to maintain the Company's operators licences.

- **Suppliers Data** - regulatory information in order to maintain the Company's operators licences.

- **Miscellaneous Data** - requests for information from any of the aforementioned.

Such information may be kept in either computer or manual records. In processing such personal data the Company will comply with the data protection principles within the Data Protection Act 1998.

9. Data Protection Responsibilities

The Company's senior management, permits the Company employees to use computers and relevant filing systems (manual records) in connection with their duties. The Company's senior management have a legal responsibility for the notification process and compliance of the Data Protection Act 1998.

The Company's senior management whilst retaining their legal responsibilities have delegated data protection compliance to the RP (Responsible Person) for the Company.

10. RP (Responsible Person) Responsibilities

- Ensuring that the policy is reviewed and kept up to date.

- Ensuring that the appropriate practice and procedures are adopted and followed by the Company.

- Provide advice and support on data protection issues within the Company.

- Work collaboratively with stakeholders within the Company to help set the standard for data protection.

- Ensure data protection notification with the Information Commissioner's Office is reviewed, maintained and renewed annually for all use of person-identifiable information.

- Ensure compliance with individual rights, including subject access requests.

- Act as a central point of contact on data protection issues within the organisation.

- Implement an effective framework for the management of data protection.

11. Line Managers / Departmental Heads Responsibilities

- Ensuring their employees are made aware of this policy and any notices.

- Ensuring their employees are aware of their data protection responsibilities.

- Ensuring their employees receive suitable data protection training.

12. Employees / General Responsibilities

All of the Company's employees, including temporary and contract staff are subject to compliance with this policy. Under the GDPR, individuals can be held personally liable for data protection breaches.

All of the Company's employees have a responsibility to inform their line manager, departmental head or RP (Responsible Person) of any new use of personal data, as soon as reasonably practicable after it has been identified.

All of the Company's employees will, on receipt of a request from an individual for information held, known as a subject access request or concerns about the processing of personal information, immediately notify the RP (Responsible Person).

13. Monitoring

Compliance with this policy will be monitored by the Company's senior management together with internal audit reviews where necessary.

The RP (Responsible Person) is responsible for the monitoring, revision and updating of this policy document on an annual basis or sooner, should the need arise.

14. Validity of this Policy

This policy will be reviewed at least annually under the authority of the Company's senior management. Associated data protection standards will be subject to an ongoing development and review programme.

15. Data Protection Act 1998 - Data Protection Principles

- Personal data shall be processed fairly and lawfully.
- Personal data shall be obtained for one or more specified and lawful purposes and shall not be further processed in any manner incompatible with that purpose or those purposes.
- Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed.
- Personal data shall be accurate and, where necessary, kept up to date.
- Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes.
- Personal data shall be processed in accordance with the rights of data subjects under this Act.
- Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.
- Personal data shall not be transferred to a country or territory outside the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.

16. Summary of Relevant Legislation & Guidance

17. General Data Protection Regulations (GDPR)

A legal basis must be identified and documented before personal data can be processed. 'Controllers' and 'Processors' will be required to document decisions and maintain records of processing activities.

18. Human Rights Act 1998

This Act binds public authorities including Health Authorities, Trusts and Primary Care Groups to respect and protect an individual's human rights. This will include an individual's right to privacy (under Article 8) and a service user's right to expect confidentiality of their information at all times. Article 8 of the Act provides that "everyone has the right to respect for his private and family life, his home and his correspondence". However, this article also states "there shall be no interference by a public authority with the exercise of this right except as is in accordance with the

law and is necessary in a democratic society in the interests of national security, public safety, or the economic well-being of the country, for the prevention or disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others". Each organisation must act in a way consistent with these requirements. It must take an individual's rights into account when sharing personal information about them.

19. Freedom of Information Act 2000

This Act gives individuals rights of access to information held by public authorities.

20. Regulation of Investigatory Powers Act 2000

This Act combines rules relating to access to protected electronic information as well as revising the "Interception of Communications Act 1985". The aim of the Act was to modernise the legal regulation of interception of communications, in the light of the Human Rights laws and rapidly changing technology.

21. Crime and Disorder Act 1998

This Act introduces measures to reduce crime and disorder, including the introduction of local crime partnerships around local authority boundaries to formulate and implement strategies for reducing crime and disorder in that local area. The Act allows disclosure of person-identifiable information to the Police, Local Authorities, Probation Service or the Health Service but only if the purposes are defined within the Crime and Disorder Act. The Act does not impose a legal requirement to disclose person- identifiable information and responsibility for disclosure rests with the organisation holding the information.

22. The Computer Misuse Act 1990

This Act makes it a criminal offence to access any part of a computer system, programs and/or data that a user is not entitled to access. The Company issues relevant employees with an individual user id and password which will only be known to the individual and must not be divulged to other staff. This is to protect the employee from the likelihood of their inadvertently contravening this Act. The Company will adhere to the requirements of the Computer Misuse Act 1990, by ensuring that its employees are aware of their responsibilities regarding the misuse of computers for fraudulent activities or other personal gain. Any employee found to have contravened this Act will be considered to have committed a disciplinary offence and be dealt with accordingly.

23. The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000

This Act allows employers to intercept and record communications in certain prescribed circumstances for legitimate monitoring, without obtaining the consent of the parties to the communication.