Medipro Limited

General Data Protection Regulations Policy

1. Introduction

This policy sets out how Medipro Ltd handles the data of both employees, students, patients and customers. The General Data Protection Regulations came into force on 25th May 2018, replacing the Data Protection Act 1998. The GDPR extends the rights given to individuals in previous legislation and requires Data Controllers (people or organisations that hold and process the details of living individuals) to comply with the seven principles and to bear in mind the rights and freedoms of those individuals when processing their details. This policy requires staff to ensure that the HR Dept be consulted before any significant new data processing activity is initiated, to ensure that relevant compliance steps are addressed.

Whilst legislation places certain responsibilities and requirements on Medipro to protect personal data, we are also conscious of the sensitivity of people with regards to the information held about them, and will always adhere to a responsible as well as lawful attitude towards the processing of data acquired. Being transparent and providing accessible information to individuals about how we will use their personal data is important for us.

Medipro Ltd aim to ensure that all appropriate staff are properly trained, fully informed of their obligations under the GDPR and are aware of their personal responsibilities. Any information sharing arrangements will be based upon formal protocols and will be in accordance with the GDPR principles, but we will also secure and maintain data in accordance with the regulations.

All staff are expected to comply with the policy and seek advice from HR when required. This policy covers all personal information that is stored in a relevant filing system (in various different forms i.e. electronic, paper copy etc).

2. Scope

This policy is applicable to all staff, companies and other third parties holding, storing or using information on or behalf of Medipro Ltd. This policy supplements our other policies relating to internet and email use. We may supplement or amend this policy by additional policies and guidelines from time to time.

3. Objectives

The main aims of this policy is to provide a framework to manage General Data Protection Regulations requirements by answering the following questions:

- What information is being collected?
- Who is collecting it?
- How is it collected?
- Why is it being collected?
- How will it be used?
- Who will it be shared with?
- Identity and contact details of any data controllers
- Details of transfers to third country and safeguards
- Retention period

But also, to provide guidance to Medipro staff and third parties that explains the requirements of the regulations and their responsibilities with regard to managing an individual's personal information.

4. Principles

Fair and lawful processing

Medipro Ltd will process personal data fairly and lawfully in accordance with individuals' rights. This generally means that we will not process personal data unless the individual whose details we are processing has given consented to this happening.

Sensitive personal data

In most cases where we process sensitive personal data we will require the data subject's explicit consent to do this unless exceptional circumstances apply or we are required to do this by law (e.g. to comply with legal obligations to ensure health and safety at work). Any

such consent will need to clearly identify what the relevant data is, why it is being processed and to whom it will be disclosed.

Sensitive personal data consists of information as to:

- the racial or ethnic origin of the data subject;
- his/her political opinions;
- his/her religious beliefs or other beliefs of a similar nature;
- whether he/she is a member of a trade union;
- his/her physical or mental health or condition;
- his/her sexual life;
- Patient/Medical details;
- the commission or alleged commission by him/her of any offence; or
- any proceedings for any offence committed or alleged to have been committed by him/her, the disposal of such proceedings or the sentence of any court in such proceedings.

Accuracy and relevance

We will ensure that any personal data we process is accurate, adequate, relevant and not excessive, given the purpose for which it was obtained. We will not process personal data obtained for one purpose for any unconnected purpose unless the individual concerned has agreed to this or would otherwise reasonably expect this.

Individuals may ask that we correct inaccurate personal data relating to them. If you believe that information is inaccurate you should record the fact that the accuracy of the information is disputed and inform the HR Dept.

Staff personal data

All staff must take reasonable steps to ensure that personal data we hold about them is accurate and updated as required. For example, if their personal circumstances change, they should inform the HR Dept so that they can update their records.

Data security

Medipro will keep personal data secure against loss or misuse. Where other organisations process personal data as a service on our behalf, the HR Dept will establish what, if any, additional specific data security arrangements need to be implemented in contracts with those third party organisations.

Storing data securely

- In cases when data is stored on printed paper, it should be kept in a secure place where unauthorised personnel cannot access it
- Printed data should be shredded when it is no longer needed
- Data stored on a computer should be protected by strong passwords that are changed regularly. The ICT Rep will store passwords.
- Data stored on CDs or memory sticks must be locked away securely when they are not being used
- The MD must approve any cloud used to store data
- Servers containing personal data must be kept in a secure location, away from general office space
- Data should be regularly backed up in line with the company's backup procedures
- Data should never be saved directly to mobile devices such as laptops, tablets or smartphones
- All servers containing sensitive data must be approved and protected by security software and strong firewall.

Data retention

Personal data should be retained for no longer than is necessary. What is necessary will depend on the circumstances of each case, taking into account the reasons that the personal data was obtained, but should be determined in a manner consistent with our data retention guidelines. The following points are purely for guidance:

- Actuarial valuation reports - permanently.
- Application forms and interview notes (for unsuccessful candidates) - 6 months to a year. (Because of the time limits in the various discrimination Acts, minimum retention periods for records relating to advertising of vacancies and job applications should be at least 6 months.

- Assessments under health and safety regulations and records of consultations with safety representatives and committees - permanently.
- Inland Revenue/HMRC approvals - permanently.
- Money purchase details - 6 years after transfer or value taken.
- Parental leave - 5 years from birth/adoption of the child or 18 years if the child receives a disability allowance.
- Pension scheme investment policies - 12 years from the ending of any benefit payable under the policy.
- Pensioners' records - 12 years after benefit ceases.
- Personnel files and training records (including disciplinary records, medical records and working time records) - 6 years after employment ceases.
- Redundancy details, calculations of payments, refunds, notification to the Secretary of State - 6 years from the date of redundancy
- Senior executives' records (that is, those on a senior management team or their equivalents) - permanently for historical purposes.
- Statutory Sick Pay records, calculations, certificates, self-certificates - 6 years after the employment ceases, for a contractual claim for breach of an employment contract.
- Student records – 10 years after the completion of their training programme

Transferring data internationally

No data may be transferred outside of the EEA without first discussing it with the HR Dept. Specific consent from the data subject must be obtained prior to transferring their data outside the EEA.

Responsibilities

The HR Dept's responsibilities:

- Keeping the policy updated about data protection responsibilities, risks and issues
- Reviewing all data protection procedures and policies on a regular basis
- Offering advice for all staff members and those included in this policy
- Answering questions on data protection from staff and other stakeholders

- Responding to individuals such as clients and employees who wish to know which data is being held on them by Medipro Ltd
- Checking and approving with third parties that handle the company's data any contracts or agreement regarding data processing i.e. Live Drive, Shiftboard

Responsibilities of LiveDrive, Shiftboard & Administrate:

- Ensure all systems, services, software and equipment meet acceptable security standards
- Checking and scanning security hardware and software regularly to ensure it is functioning properly
- Ensuring that they themselves adhere to GDPR.

Responsibilities of the Marketing Manager:

- Approving data protection statements attached to emails and other marketing copy
- Addressing data protection queries from clients, target audiences or media outlets
- Coordinating with the HR Dept to ensure all marketing initiatives adhere to data protection laws and the company's GDPR Policy

The processing of all data must be:

- Necessary to deliver our services
- In our legitimate interests and not unduly prejudice the individual's privacy
- In most cases this provision will apply to routine business data processing activities.

Our Terms of Business contains a Privacy Notice to clients on data protection.

The notice:

- Sets out the purposes for which we hold personal data on customers and employees
- Highlights that our work may require us to give information to third parties such as expert witnesses and other professional advisers
- Provides that customers have a right of access to the personal data that we hold about them

5. Medipro's procedure for processing data

Conditions for processing

We will ensure any use of personal data is justified using at least one of the conditions for processing and this will be specifically documented. All staff who are responsible for processing personal data will be aware of the conditions for processing. The conditions for processing will be available to data subjects in the form of a privacy notice.

Justification for personal data

We will process personal data in compliance with all six data protection principles.

We will document the additional justification for the processing of sensitive data and will ensure any biometric and genetic data is considered sensitive.

Consent

The data that we collect is subject to active consent by the data subject. This consent can be revoked at any time.

Criminal record checks

Any criminal record checks are justified by law. Criminal record checks cannot be undertaken based solely on the consent of the subject.

Right to be forgotten

A data subject may request that any information held on them is deleted or removed, and any third parties who process or use that data must also comply with the request. An erasure request can only be refused if an exemption applies. This request would be relevant for unsuccessful candidates or ex-employees.

Medipro GDPR Compliance Tool

Regular data audits to manage and mitigate risks will inform the Compliance Tool. This contains information on what data is held, where it is stored, how it is used, who is responsible.

Reporting breaches

All members of staff have an obligation to report actual or potential data protection compliance failures (computer hacking or information used for other purposes that are not authorised) to the HR Dept. This allows us to:

- Investigate the failure and take remedial steps if necessary
- Maintain a Risk Register
- Notify the ICO of any compliance failures that are likely to risk the rights and freedoms of individuals i.e. financial loss, reputational damage, discrimination etc.

External sharing

On occasion, Medipro may have a legal or policy-based obligation to share certain information held in the course of operation and/ or co-operation with external agencies.

In the event that access to controlled data is needed by an external authority, the external authority must request the information correctly and Medipro will then apply a set test to consider the request.

The process is as follows:

- The external authority makes a request for controlled data by way of an official letter. Telephone and email requests are never acceptable.
- The letter must detail the reason(s) for the request, what the organisation intends to do with it or how it will use the information, and how it will protect the information once provided to them.
- We will acknowledge the request in writing and will then consider the request, with appropriate legal advice if necessary.

- If the request is deemed reasonable, the data subject will be informed in writing of the decision to release the data.
- The information will be provided to the external authority via a mutually agreeable method that is safe and trusted.
- If the request is denied a letter detailing the reasons for the decision will be sent to the external authority.

There are specific instances where this framework will not apply, for example, with regards to the course of a police or medical investigation. Such instances require by law that we co-operate with the concerned body if we believe the data will be used responsibly to prevent or deter crime.

Internal sharing

Controlled information, at all times, needs to be shared internally within Medipro and its departments for the purposes of operations and general enquiries.

On such occasions members of staff are required at all time to respect and keep safe personal data and only share it with other staff who must have access to it. Data is always transferred between departments securely and confidentially with the use of electronic methods, password protected computer and database access and encryption to ensure that only authorised staff are able to view information.

6. Subject access requests

Where Medipro Ltd hold any data about a person then that person has a right to request access to this data and to know what details we hold about them.

Employee details will be for purposes connected with employment, including recruitment and termination of employment. The sort of information we will hold includes information for payroll purposes, references, contact names and addresses and records (including, for example, disciplinary records) relating to your career with the Company, information about health for the purposes of compliance with health and safety and occupational health

obligations; considering how an employee's health affects ability to do the job and, if disabled, whether any reasonable adjustments to be made to assist at work.

In order to find out if we hold any information about a person a 'Subject Access Request' must be made to Medipro Ltd in writing.

You have the right, on written request to the following:

- to be informed whether personal data about you is being processed, whether by the company or someone else on its behalf;
- to be given a description of the personal data that is being processed, a description of the purposes for which the data is being processed and details of all recipients or classes of recipients to whom they are or may be disclosed;
- to have communicated, in an intelligible form, any information held about you by the company, as well as any information available to the company as to the source of this information. If the information is not in an intelligible form, for instance if it contains codes, you will be given an explanation of the information. The information will be provided in a permanent form unless this is impossible, would involve a disproportionate effort or you agree to some other form. The copy will usually be a printed paper copy, but can also be provided in other ways, for example, on disk or via e-mail;

As per the GDPR there will be no charge to cover administration costs. The company will comply with the request within 30 days.

If the company has already complied with an identical or similar request then we will not respond to repeated demands until a reasonable period has elapsed or new information has been added to the file, for example, if the individual has been subject to an investigation or disciplinary hearing.

If you receive a subject access request, you should refer that request immediately to the HR Dept. We may ask you to help us comply with those requests.

5 GDPR Principles

Medipro adheres to the seven Principles within the GDPR:

- Lawfulness, fairness and transparency - Personal data shall be processed lawfully, fairly and in a transparent manner in relation to the data subject
- Purpose limitation - Personal data shall be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes
- Data minimisation - Personal data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed
- Accuracy - Personal data shall be accurate and, where necessary, kept up to date
- Storage limitation - Personal data shall be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed
- Integrity and confidentiality - Personal data shall be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures
- Accountability - The controller shall be responsible for, and be able to demonstrate compliance with the GDPR

7. Consequences of failing to comply

We take compliance with this policy very seriously. Failure to comply puts both you and Medipro at risk.
The importance of this policy means that failure to comply with any requirement may lead to disciplinary action under our procedures which may result in dismissal.

8. Definitions

Business purposes

The purposes for which personal data may be used by us:

- Personnel, administrative, financial, regulatory, payroll and business development purposes.

Business purposes include the following:

- Compliance with our legal, regulatory and corporate governance obligations and good practice
- Gathering information as part of investigations by regulatory bodies or in connection with legal proceedings or requests
- Ensuring policies are adhered to (such as policies covering email and internet use)
- Operational reasons, such as recording transactions, training and quality control, ensuring the confidentiality of commercially sensitive information and checking
- Investigating complaints
- Checking references, ensuring safe working practices, monitoring and managing staff access to systems and facilities and staff absences, administration and assessments
- Monitoring staff conduct, disciplinary matters
- Marketing our business
- Improving services

Personal data

Information relating to identifiable individuals, such as job applicants, current and former employees, agency, contract and other staff, clients, suppliers and marketing contacts.

Personal data we gather may include: individuals' contact details, educational background, financial and pay details, details of certificates and diplomas, education and skills, marital status, nationality, job title, and CV.

Medipro Limited

Annex A
dated 12 Feb 18

GDPR Initial Data Questionnaire

Name:

Role:

Date:

The questions below form the core of a review of GDPR compliance regarding the storage and processing of data but are a generic approach to cover key points. They are only a tool to inform the process of achieving compliance.
This will allow us to provide a brief report outlining areas you should work on to ensure GDPR compliance which would need further detailed investigation.

Who do you store personal data about? E.g. Customers, patients, students, suppliers, staff, business partners/collaborators - personal data means you can identify an individual

What personal data do you store? E.g. name, telephone, address, bank details, PRF's, email, etc

Why are you storing the data?

Where is the personal data stored? E.g. on a mobile phone, filling cabinet, server etc.

Who has access to the personal data?

How do you secure your data?E.g. passwords, different levels of access for different staff, keys etc.

Does your job description justify your access to this data?

Do you have procedures in place to deal with lost passwords, or leaks in information?

Do you store data on your computer?

Do you hold data as paper copies?

Do you have any data stored on a mobile phone?

Are staff allowed to bring their own computers or mobile phones to work?

Are staff allowed to take company mobile devices (laptops/tablets/phones) home or whilst travelling?

Do people know what data you hold on them?

Do people know what you do with the data you hold on them?

Have people given permission for you to hold and use their data?

Have you reviewed all data collection to ensure permission is always asked for?

Do you have systems in place to monitor for data breaches?

Do you have procedures for notifying people if their data may be leaked?

Does your job description justify how you use the data?

Do you use any outside companies to hold or use any data?

Do you hold or use data that may go outside of the EU?

Do you hold medical data on individuals?

Are you aware of any other data concerns?

Medipro Limited

Remarks:

Medipro Limited

Annex B
dated 12 Feb 18

Privacy Notice

How your information will be used

As your employer, the Company needs to keep and process information about you for normal employment purposes. The information we hold and process will be used for our management, medical, educational and administrative use only. We will keep and use it to enable us to run the business and manage our relationship with you effectively, lawfully and appropriately, during the recruitment process, whilst you are working for us, at the time when your employment ends, when your studies have finished and after you have left. This includes using information to enable us to comply with the employment contract, to comply with any legal requirements, pursue the legitimate interests of the Company and protect our legal position in the event of legal proceedings. If you do not provide this data, we may be unable in some circumstances to comply with our obligations and we will tell you about the implications of that decision.

As a company pursuing the education of medical students or the care of patients, we may sometimes need to process your data to pursue our legitimate business interests, for example to prevent fraud, administrative purposes or reporting potential crimes. The nature of our legitimate interests are to run education training courses for the medical profession and supply a medical service to our customers and patients. We will never process your data where these interests are overridden by your own interests.

Much of the information we hold will have been provided by you, but some may come from other internal sources, such as your manager, or in some cases, external sources, such as referees.

The sort of information we hold includes your application form and references, your contract of employment and any amendments to it; correspondence with or about you, for example letters to you about a pay rise or, at your request, a letter to your mortgage company confirming your salary; information needed for payroll, benefits and expenses purposes; contact and emergency contact details; records of holiday, sickness and other absence; information needed for equal opportunities monitoring policy; and records relating to your

career history, such as training records, appraisals, other performance measures and, where appropriate, disciplinary and grievance records.

You will, of course, inevitably be referred to in many company documents and records that are produced by you and your colleagues in the course of carrying out your duties and the business of the company. You should refer to the GDPR Policy which is available from the HR Dept or in paper format from Medipro Ltd, Faraday House, Sopwith Close, Stockton on Tees, TS18 3TT.

Where necessary, we may keep information relating to your health, which could include reasons for absence and GP reports and notes. This information will be used in order to comply with our health and safety and occupational health obligations – to consider how your health affects your ability to do your job and whether any adjustments to your job might be appropriate. We will also need this data to administer and manage statutory and company sick pay.

Where we process special categories of information relating to your racial or ethnic origin, political opinions, religious and philosophical beliefs, trade union membership, biometric data or sexual orientation, we will always obtain your explicit consent to those activities unless this is not required by law or the information is required to protect your health in an emergency.

Where we are processing data based on your consent, you have the right to withdraw that consent at any time.

In addition, we may monitor computer and telephone use, as detailed in our Monitoring Policy, available from the HR Dept or in paper format from Medipro Ltd, Faraday House, Sopwith Close, Stockton on Tees, TS18 3TT. We also keep records of your hours of work by way of our shift system, Shiftboard, as detailed in the company handbook.

Other than as mentioned below, we will only disclose information about you to third parties if we are legally obliged to do so or where we need to comply with our contractual duties to you, for instance we may need to pass on certain information to our pension or health insurance schemes.

We may transfer information about you to other group companies for purposes connected with your employment or the management of the company's business.

In limited and necessary circumstances, your information may be transferred outside of the EEA or to an international organisation to comply with our legal or contractual requirements. We have in place safeguards including secure premises, secure storage, electronic security and limited access to ensure the security of your data.

Your personal data will be stored for a period of 6 years after your cessation of contract.
If in the future we intend to process your personal data for a purpose other than that which it was collected we will provide you with information on that purpose and any other relevant information.

Your rights

Under the General Data Protection Regulation (GDPR) and The Data Protection Act 2018 (DPA) you have a number of rights with regard to your personal data. You have the right to request from us access to and rectification or erasure of your personal data, the right to restrict processing, object to processing as well as in certain circumstances the right to data portability.

If you have provided consent for the processing of your data you have the right (in certain circumstances) to withdraw that consent at any time which will not affect the lawfulness of the processing before your consent was withdrawn.

You have the right to lodge a complaint to the Information Commissioners' Office if you believe that we have not complied with the requirements of the GDPR or DPA 18 with regard to your personal data.

Identity and contact details of HR Dept

Medipro Ltd is the controller and processor of data for the purposes of the DPA 18 and GDPR.
If you have any concerns as to how your data is processed you can contact:

Brian English, Managing Director at brian.english@medipro.co.uk
Kirsty Wharton, Clinical Director at kirsty.wharton@medipro.co.uk
or you can write to these individuals using the address of Medipro Ltd, Faraday House, Sopwith Close, Stockton on Tees, TS18 3TT.

Medipro Limited

Please sign to confirm that you have read and give your consent to the requirements detailed in this Privacy Notice and the GDPR Policy.

Name:

Date:

Signature:

Version number	001	**Used by**	**All**
Version date	15 June 2018	**Business Area**	HR
Version expiry	15 June 2020	**Document ID number**	HR **000**
Version status	Live document	**Document classification**	Internal Use