Version	Date Published	Review Status
1.0	Feb 2018	New document

Belford Medical Practice
Data Protection & GDPR

This document explains the provisions of the GDPR, helping practices understand and comply with its requirements.

The new Data Protection Bill (DPB) currently going through Parliament will transpose the GDPR into UK law, and FPM will continue to add further updates and resources to this document as more information becomes available.

The information in this section will help you and your practice comply with data protection regulations by protecting the information that is stored, collected and shared by the organisation.

The *Data Protection Act 1998* is an act of UK Parliament that ensures information collected by organisations is used fairly, stored safely and not disclosed to any other person unlawfully.

The *GDPR* is European Union (EU) legislation through which the European Parliament, the Council of the EU and the European Commission intend to strengthen and unify data protection for all individuals within the EU. This change in legislation intends to strengthen and unify data protection rights for all citizens residing within the EU, as well as addressing the export of data outside of the EU.

It will be implemented into UK law before the UK leaves the EU, and will almost certainly remain in place after Brexit.

Hold Ctrl on your keyboard and click on the links below to go directly to each section.

1. **What is the current position?** The principles under the Data Protection Act

Anyone processing personal data must comply with the eight enforceable principles of good practice:

- **One:** The information to be contained in personal data shall be obtained, and personal data shall be processed, fairly and lawfully.
- **Two:** Personal data shall be held only for one or more specified lawful purposes.
- **Three:** Personal data held for any purpose or purposes shall not be used or disclosed in any matter incompatible with that purpose or those purposes. The data shall be adequate, relevant and not excessive in relation to that purpose or those purposes.
- **Four:** Personal data shall be accurate and, where necessary, kept up to date.
- **Five:** No data shall be kept for longer than is necessary for those purposes.
- **Six:** An individual shall be entitled, at reasonable intervals and without undue delay or expense, to be informed by any data user whether they hold personal data of which that individual is the subject; and they can have access to any such data held by a data user, which may incur an administration charge.
- **Seven:** An individual shall be entitled, where appropriate, to have such data corrected or erased. Appropriate security measures shall be taken against unauthorised access to, or alteration, disclosure or destruction of, personal data and against accidental loss or destruction of personal data.
- **Eight:** Personal data held for any purpose or purposes shall not be transferred to countries without adequate protection.

In accordance with the Data Protection Act 1998, the Practice will only process data on the following basis:

- If the data subject has given consent
- If it is necessary in relation to the performance or formation of contracts in relation to the data subject
- If it is required under a legal obligation
- If it is necessary to protect the vital interests of the data subject
- If it is necessary to carry out public functions
- If it is necessary to pursue the legitimate interests of the data controller or third party (unless it could prejudice the data subject's interests)

Sensitive personal data will only be processed:

- With explicit consent of the data subject, if the data subject has made the information public
- If the data is required by law and is in respect of employment purposes
- If it is necessary in order to protect the vital interests of the data subject or another in relation to the administration of justice or legal proceedings for medical purposes by health professionals in order to safeguard racial equality

2 Introducing the General Data Protection Regulations (GDPR)

A new Data Protection Bill ("DPB") in the UK will enact the General Data Protection Regulations with effect from 25 May 2018. The Information Commissioners Office, responsible to regulating data use in the UK, has stated that the introduction of the new legislation is *"the biggest change to data protection law for a generation"*. They go on to say that *"if your organisation cannot demonstrate that good data protection is a cornerstone of your business policy and practices, you are leaving your organisation open to enforcement action that can damage both public reputation and bank balance."*

They have advised that their primary focus will be safeguarding customer and client data, and most organisations have good grounds for requesting, retaining and processing employee data. However, this does not exempt GP practices from having to comply. In addition to the financial risks of the practice not complying with data protection law, individuals will also have greater rights to challenge the organisation's use of their data, which could lead to costly legal action.

Introduction to the GDPR (ICO): ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/

12 Steps to Prepare for GDPR (ICO): ico.org.uk/media/1624219/preparing-for-the-gdpr-12-steps.pdf

If you are having trouble opening this link copy and paste it into your internet browser search bar

3 What is changing? The principles under the General Data Protection Regulations

Below are the key principles under GDPR, which all organisations must comply with when processing employee personal data:

Three of these are consistent with the Data Protection Act:

- **Purpose Limitation** - Personal information is collected for specific, explicit and legitimate purposes
- **Storage Limitation** - Personal information is retained for only as long as is necessary
- **Integrity and Confidentiality** - Personal information is processed in a way that ensures appropriate security of the data

Three of these have been further strengthened under GDPR:

- **Lawfulness, fairness and transparency** – The fair, lawful and transparent processing of personal information
- **Data minimisation** – Stored personal information is "adequate, relevant and limited to what is necessary."
- **Accuracy -** Stored personal information is "accurate and, where necessary, kept up to date"

A new principle has also been introduced:

- **Accountability** - "the controller shall be responsible for, and be able to demonstrate, compliance with the principles."

4 a) What is changing under the GDPR? Obligations

Privacy measures will now need to be built into all data processing activities to identify privacy problems at an early stage. These measures will be embedded throughout the employee life cycle.

Practices will need to show that they have considered and integrated data protection into processing activities at every level, including raising awareness of privacy and data protection within the practice. The result is that your activities are less likely to be privacy intrusive, enabling you to meet your legal obligations and avoid breaching GDPR.

Checklists for Data Controllers and Data Processors (ICO):

ico.org.uk/for-organisations/resources-and-support/data-protection-self-assessment/getting-ready-for-the-gdpr/

Self-Assessment Tool (ICO):

ico.org.uk/for-organisations/resources-and-support/data-protection-self-assessment/

4. **b) What is changing under the GDPR?** Consent and the lawful processing of personal data

In order to process employee data, you must meet at least **one** of the following criteria for each piece of data:

- The data subject has given explicit written consent to their data being processed, which they have the right to withdraw.
- The data is being processed for the performance of a contract with the data subject (such as staff administration), or the data is being processed at the request of the data subject prior to entering into a contract (such as reference checks)
- The data is being processed in compliance with a legal obligation (such as HMRC. PAYE, sick pay and auto enrolment)
- The data is being processed to protect the individual's 'vital interests'. This condition only applies in cases of life or death, such as where an individual's medical history is disclosed to a hospital's A&E department treating them after a serious road accident.
- The data is being processed in the exercise of official authority, covering public functions and powers that are set out in law, or to perform a specific task in the public interest that is set out in law.
- The data is being processed in pursuit of the employer's 'legitimate interests' (such as transmitting personal data within the company for internal admin purposes)

The ICO have advised employers not to use consent as the basis to process employee data if they have another legal basis under GDPR, e.g. 'the performance of the contract' or 'compliance with a legal obligation' are likely to be the strongest grounds, depending on the type of data.

4. c) What is changing under the GDPR? Enhanced employee privacy and individual rights

Under the new legislation, the employee will have the following personal data rights:

- *The right to be informed* – data processors must provide 'fair processing information', usually through a privacy notice.
- *The right of access* – GDPR gives enhanced rights of Data Subject access. They are entitled to more information than under the DPA. In general, no fee can be charged by a Data Controller for providing a Data Subject with copies of their personal data and the timescale for a Data Controller to respond to a request will now be one month.
- *The right to rectification* - The GDPR gives individuals the right to have personal data rectified if it is inaccurate or incomplete.
- *The right to erasure* - GDPR provides Data Subjects with a new enhanced right to request erasure of their personal data.
- *The right to restrict processing* - Individuals have a right to 'block' or suppress processing of personal data.
- *The right to data portability* - The right to data portability allows individuals to obtain and reuse their personal data for their own purposes across different services. It allows them to move, copy or transfer personal data easily from one IT environment to another in a safe and secure way, without hindrance to usability.
- *The right to object* - Individuals have the right to object to: processing based on legitimate interests or the performance of a task in the public interest/exercise of official authority (including profiling); direct marketing (including profiling); and processing for purposes of scientific/historical research and statistics.
- *Rights in relation to automated decision making and profiling* - for example, if you use the Bradford Factor for absence monitoring).

Privacy and Enhanced Individual Rights

There are several scenarios facing employers with regard to how they store and manage employee information:

1. All employee information is held centrally on a server.
2. Some employee information is held electronically on a central system and some information is held electronically in managers' sub-folders.
3. Some employee information is held electronically on a central system and some information is held electronically in managers' sub-folders. Information is also held manually across a variety of different sites.
4. Some employee information is held electronically on a central system and some information is held electronically in managers' sub-folders. Information is also held manually across a variety of different sites. Further information about the employee is stored at home or on managers' computers.

You should audit your employee information to see what data you have and how it is stored. You can then use this data map to carry out a minimisation exercise - consider what information you need to store and how it can comply with the enhanced responsibilities.

5. **What is the current position under the DPA?** The employee file & data protection

- Ensure that all workers are aware of the nature and source of any information kept about them, how it will be used and who it will be disclosed to.
- Nominate a member of staff to be responsible for keeping and maintaining this file on each employee.

In principle, employee files must be kept to satisfy statutory requirements. These cover, for example:

- Hours of work (employment law legislation);
- Holidays taken (employment regulation inspections/health and safety);
- Statutory Sick Pay, Maternity Pay, Adoptive Parental Leave and Pay, time-off taken for dependant emergencies, time off without Pay for Parental Leave;
- Recovery from the Inland Revenue of Maternity, Adoption and / or Paternity Pay Disciplinary action and the outcome of grievances (employment legislation);
- Minimum wage compliance (employment legislation);
- Accidents at work (Health and Safety regulations)

Perhaps more importantly, they can help the growth and development of the practice because they are a record of how the talents and skills of the individual are being developed.

They can also help employers to:

- Identify any patterns of absence, lateness and / or sickness;
- Ensure disciplinary matters are dealt with consistently throughout the Practice;
- Assist with identification of training needs;
- Defend the Employer's actions if Employee's claims are made to Employment Tribunals or the Courts
- Supply information to insurers and others for them to handle claims e.g. accidents.

The following information and documents should be kept on the employee file as appropriate:

- Completed Application for Employment and Equal Opportunity Forms.
- Interview notes.
- Job offer letter and acceptance.
- Any references.
- Any checks made, such as CRB (if applicable), right to work in UK.
- Any medical reports.
- Completed induction checklist.
- Copy of the written Statement of Terms and Conditions of Employment and any subsequent notes issued which amend it (e.g. salary changes – amounts & dates).
- Details of any Probationary arrangements, reviews and related correspondence.
- Any holiday request forms for the relevant periods.

- Individual employee absence record, coded by reason for absence.
- Copies of any disciplinary warnings, appeals, agreed actions and outcomes.
- Copies of any grievances raised and outcomes.
- A copy of the 'Details of Employee' Form.
- The file should contain a signed copy of the Written Statement of Terms and Conditions of Employment which should be issued with the Employee Handbook.
- Any and all agreed amendments to their Written Statement of Terms and Conditions of Employment should also be placed on the Employee's file.
- Ensure that all workers are aware of the nature and source of any information kept about them, how it will be used and who it will be disclosed to.

The Information Commissioner has yet to update the Employment Practices Code and other existing codes, and has not confirmed when it will published revised versions in line with GDPR. Practices are therefore encouraged to familiarise themselves with the current codes and ensure they are complying with current law. The codes are available at the following links:

Employment Practices Code ico.org.uk/for-organisations/guide-to-data-protection/employment/

6. Breach Notification

A personal data breach is any breach of security, either accidental or deliberate, that leads to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data.

Circumstances in which a breach may occur

- Loss of control/limitation of employee rights
- Discrimination
- Identity theft or fraud
- Financial loss
- Damage to reputation
- Loss of confidentiality
- Other significant social disadvantage

Under the regulations, employers must document any breach, specifically:

- Facts relating to the breach
- The effect of the breach
- Any remedial action taken to prevent recurrence.

To notify or not to notify – that is the question!

- You must notify the relevant supervisory authority (ICO and NHS) within 72 hours of becoming aware of a breach **IF** the breach is likely to result in a risk to the rights and freedoms of individuals. In the HR context, this is unlikely.
- You need to notify individuals without undue delay **IF** the breach is likely to result in a high risk to the rights and freedoms of the employee.

7. Accountability

You need to be able to demonstrate that any processing is carried out in accordance with *the first 6 GDPR principles.*

Specifically, you will need to update your written policies and processes and be able to provide evidence of an audit process of your own internal processes (e.g. a data map) and those of third parties (e.g. a data map or statement from any third parties such as payroll providers). You also need to make sure that any policies are adhered to or risk falling to meet your accountability obligations as per the legislation.

Public authority bodies that process personal information to appoint a nominated Data Protection officer (DPO), who will be responsible for GDPR compliance. The DPO should report to the highest level of management and must be informed of all data protection issues within the organisation.

The DPO may be an employee of the practice, or an individual who represents several practices at a federated/CCG/health board/LMC level.

8. Data Subject Access Requests

Under the Data Protection Act, any individual can make a 'subject access request' to any organisation that s/he believes is processing his or her personal data. This request must be in writing, for example by letter or e-mail. Once an organisation receives such a request it must respond promptly, or at the most within 40 calendar days. It must produce copies of the information it holds in an intelligible form. The organisation can charge up to £10 for doing this.

Under the GDPR, the right to submit a Subject Access Request and receive the information without undue delay is shortened to within 1 month. An extension of 2 months can be allowed if necessary taking into account the complexity of the request. A fee cannot be charged unless the request is "manifestly unfounded or excessive", in which case a fee may be charged or the request refused.

Retention and disposal of staff records

The Data Protection Act 1998 itself does not specify any particular retention periods for employment data and records. However, it does specify that personal data should not be kept longer than necessary for the purpose for which it was processed and this is consistent with the GDPR.

It is recommended that employers assess retention times for different categories of employment data for job applicants, current employees and former employers. The retention times should be based on business needs, taking into account relevant professional guidelines and a risk analysis approach. When records are disposed of, this should be done securely and effectively, particularly with sensitive information.

9. Data Protection Definitions

Data subject: A living individual who can be identified from that data or other data/information in (or likely to come into) the possession of the data controller, such as employees, candidates, workers, contractors, freelancers and ex-employees.

Personal data: Any information relating to an identified of identifiable living individual e.g. name, address, date of birth, NI number, etc.

Special category of personal data: Racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data, biometric data, health, sexual life and sexual orientation data, commission (alleged commission) of an offence, any proceedings in respect of an offence (alleged offence) or, relevant criminal convictions. Examples include but are not limited to: sickness absence data, diversity monitoring, photographs etc.

Data controller: A person who determines the purposes and has overall responsibility for the manner in which personnel data is or will be processed, in essence, the employer.

Data processor: A person who processes employee data on behalf of the Data Controller e.g. payroll, benefits and pensions providers.

Processing: The conduct of any operations in relation to data, including obtaining, recording, storing, adapting, altering, disclosing, transmitting, disseminating, aligning, continuing, blocking, erasing or destroying data. Processing activities can include recruitment, the performance of the contract, monitoring equality and diversity, health and safety, etc.

Relevant filing systems: Manual or electronic records stored not only in paper or electronic personnel files but also emails, hard drives, work phones and so on.