UK data protection law: the GDPR, DPA 2018 and PECR

The **EU GDPR General Data Protection Regulation)** superseded the Data Protection Directive 1995 and all member state law based on it on **25 May 2018.**

The **UK DPA (Data Protection Act) 2018** came into force at the same time, modifying the EU GDPR by filling in sections that were left to individual member states to interpret and implement.

The DPA 2018 also applies “a broadly equivalent regime” – which it calls “the applied GDPR” – to certain types of personal data processing that fall outside the EU GDPR’s scope, including processing by public authorities. It also sets out data processing regimes for law enforcement and intelligence purposes.

Because the DPA 2018 supports the GDPR rather than enacting it, the two laws should be read together.

What is GDPR?

The EU General Data Protection Regulation (GDPR) comes into force on 25th May 2018; the scope of the changes under the new regulation means that preparing for the GDPR should now be a very high priority for general practices and all other organization who holds personal data. GDPR will need to be implemented alongside the new Data Protection Act 2018 both of which came into force on May 25, 2018.

All organisations will need to carry out audits of the employee and customer/patient personal data that they collect and process to ensure that it meets GDPR conditions for consent. New governance and record-keeping requirements mean that organisations will also have to create or amend policies and processes relating to privacy notices, data breach responses and subject access requests.

NHS Guidance and briefing on GDPR and accountability focuses on **changes to data protection legislation: why this matters to you**.

This covers:

- data protection, accountability and governance;
- privacy by design and default;
- implications of the GDPR for Health and Social Care research;
- health and social care research: legal basis and safeguards;
- transparency, consent and subjects' rights;
- consent;
- pseudonymisation;
- personal data breaches and notification;
- profiling and risk management;
- what's new and what changes.

What is The Data Protection Act 2018?

The **Data Protection Act 2018** is a United Kingdom Act of Parliament which updates data protection laws in the UK. It is a national law which complements the European Union's General Data Protection Regulation (GDPR).

The Data Protection Act 2018 achieved Royal Assent on 23 May 2018. It applies the EU's GDPR standards. Whereas the GDPR gives member states limited opportunities to make provisions for how it applies in their country, one element of the DPA 2018 is the details of these, applying as the national law.

The Data Protection Act 2018 controls how your personal information is used by organisations, businesses or the government.
The Data Protection Act 2018 is the UK's implementation of the General Data Protection Regulation (GDPR).

Everyone responsible for using personal data has to follow strict rules called 'data protection principles'. They must make sure the information is:

- used fairly, lawfully and transparently
- used for specified, explicit purposes
- used in a way that is adequate, relevant and limited to only what is necessary
- accurate and, where necessary, kept up to date
- kept for no longer than is necessary
- handled in a way that ensures appropriate security, including protection against unlawful or unauthorised processing, access, loss, destruction or damage

There is stronger legal protection for more sensitive information, such as:

- race
- ethnic background
- political opinions
- religious beliefs
- trade union membership

- genetics
- biometrics (where used for identification)
- health
- sex life or orientation

There are separate safeguards for personal data relating to criminal convictions and offences.

Your rights

Under the Data Protection Act 2018, you have the right to find out what information the government and other organisations store about you. These include the right to:

- be informed about how your data is being used
- access personal data
- have incorrect data updated
- have data erased
- stop or restrict the processing of your data
- data portability (allowing you to get and reuse your data for different services)
- object to how your data is processed in certain circumstances

You also have rights when an organisation is using your personal data for:

- automated decision-making processes (without human involvement)
- profiling, for example to predict your behaviour or interests

The Act introduces new offences that include knowingly or recklessly obtaining or disclosing personal data without the consent of the data controller, procuring such disclosure, or retaining the data obtained without consent. Selling, or offering to sell, personal data knowingly or recklessly obtained or disclosed would also be an offence.

Essentially, the Act implements the EU Law Enforcement Directive, it implements those parts of the GDPR which 'are to be determined by Member State law' and it creates a framework similar to the GDPR for the processing of personal data which is outside the scope of the GDPR. This includes intelligence services processing, immigration services processing and the processing of personal data held in unstructured form by public authorities.

Under section 3 of the European Union (Withdrawal) Act 2018, the GDPR will be incorporated directly into domestic law immediately after if the UK exits the European Union.

What is PECR ?

The Privacy and Electronic Communications Regulations (PECR) sit alongside the Data Protection Act and the GDPR. They give people specific privacy rights in relation to electronic communications.

There are specific rules on:

- marketing calls, emails, texts and faxes;
- cookies (and similar technologies);
- keeping communications services secure; and
- customer privacy as regards traffic and location data, itemised billing, line identification, and directory listings.

Who does the GDPR apply to?

The GDPR applies to all individuals and organisations with day-to-day responsibilities for data protection. It therefore applies to GP practices, as 'data controllers', and their clinicians and administrative staff.

Will it be affected by Brexit?

The UK will still be part of the EU in May 2018 and practices must therefore comply with the GDPR. The Data Protection Bill 2017 debated in Parliament and it becomes an Act- The data Protection Act 2018, it sets most of the GDPR regulations

What are the main changes?

The key regulation changes that affect practices are summarised below.

Definition of personal data has been expanded

Personal data is any information relating to an identified or identifiable natural person. It includes names, addresses, telephone numbers, dates of birth and GP and hospital numbers. Under GDPR, the definition has been expanded to include information processed via digital media.

In addition, special categories of personal data (formerly 'sensitive' data) – covering health, race, ethnicity, sexual orientation, religion and political views – now also include genetic and biometric data.

Practices must establish their legal basis for processing data

Practices must document both a *lawful basis* for processing personal data and also a *condition* for processing special categories of data.

The GDPR has six lawful bases for processing personal data – for general practice the relevant ones are explicit patient consent, that processing is necessary for the provision of a service/performance of a contract, or that processing is necessary in the vital interests of the data subject.

Meanwhile one of 10 conditions must be met for processing special categories of data – here the relevant options are explicit patient consent or that processing is necessary for provision of healthcare.

However, where 'consent' is chosen, the GDPR sets a high standard – it has to be specific, freely given, informed and should constitute an unambiguous indication of the patient's wishes, by clear affirmative action to the processing of their data. Pre-ticked boxes, for example on new patient registration forms, would not count as valid consent for data protection purposes and there must be a positive opt-in process. Patients must also be provided with an easy way to withdraw their consent.

Given these requirements, rather than relying on explicit consent to process data, practices are likely to use another appropriate lawful basis and special category condition for the processing of personal and special categories of data, respectively. The ICO has published specific guidance on this.

For practices, this will mostly mean relying on 'necessary for the provision of healthcare' for processing sensitive data. As long as patients have been appropriately informed how their personal data will be used, in 'privacy notices', it would usually be reasonable for GPs to rely on implied consent for sharing relevant information in order to provide direct patient care – for example, when a patient agrees to a referral to another healthcare professional.

However, for some other purposes – for example, a request for confidential data from a third party such as an employer or insurance company, explicit consent will be needed.

Practices must provide more information in 'privacy notices'

Practices must inform individuals what they are doing with their data.[4] Privacy notices informing patients at the time of collecting their data should be available on the practice website, on posters in the practice and perhaps within leaflets provided at patient registration. The following information must be provided within such notices:

- **Practice name (identified as data controller)**
- **Data protection officer's contact details**
- **Purpose of processing patient data**

- **Lawful basis for processing personal data**
- **The categories of personal data concerned**
- **Potential recipients of personal data**
- **How long data will be retained**
- **A list of the patient's rights**
- **Safeguards if data transferred to a country outside the EU.**

Patients are informed that they can complain to the ICO if they are unhappy with how their data are being handled.

Practices will rarely be able to charge for access to medical records

You will no longer be able to charge patients for subject access requests, unless the request is 'manifestly unfounded or excessive' or is a repetitive request for copies of the same information, previously disclosed. Such situations are expected to be rare. The timescale for compliance with a patient's request will also be reduced, from 40 days to one month. If practices refuse a subject access request, they must tell the patient the reasons and inform them that they have a right to complain to the ICO.

Practices must report data breaches, and these incur bigger financial penalties

In the event of a data breach affecting a patient's privacy rights (for example, breach of confidentiality), data controllers must notify the ICO 'without undue delay', and where feasible no later than 72 hours after becoming aware of the breach. Practices will also have to notify the patient of the breach if it is likely to result in a high risk to their privacy rights. This is in addition to the duty of candour to inform patients of such breaches. The ICO will also be able to impose much higher fines for breaches and non-compliance.

Practices must demonstrate compliance with the GDPR

Accountability was always implicit in data protection law, but the GDPR makes it mandatory for practices to be able to demonstrate that they are compliant with GDPR. They should maintain accurate records of all data processing activities, document all advice provided by the DPO and data protection impact assessments (DPIAs) undertaken. Now is the time to revise and update internal data protection policies, and arrange and document staff training.

DPIAs are recommended, as a way of assessing the levels of protection in place to safeguard personal patient data. Whilst considered good practice in any case, DPIAs will be mandatory when the processing of personal data involves high risks to

confidentiality, such as when practices engage in data sharing arrangements, or where new technologies are being used, for example a new computer system.

Practices need to designate a data protection officer

General practices will be required to appoint a Data Protection Officer to advise and monitor data security. The Data Protection Officer can be an employee or external to the practice, and should have professional experience and knowledge of data protection law; this should be proportionate to the type of processing the practice carries out, taking into consideration the level of protection the personal data requires.

Patients will have more rights

Individuals will have stronger rights to control their data under the GDPR, including the right to erasure, the right to rectification, the right to object to processing and the right to restrict processing. These rights are complex and not absolute. Practices should ensure they understand when they apply and have a process in place, should patients wish to exercise them.

Where can you get further information?

The ICO has published comprehensive guidance on the GDPR and how organisations must comply. However, the recommendations are not completely finalised and you should check the ICO website regularly to review updates.

The ICO has also published the Data Protection Self-Assessment tool, with helpful checklists to assess your compliance and identify what steps you need to take now to be GDPR compliant on 25 May 2018.

References

1. GDPR Portal https://www.eugdpr.org/

3. Information Commissioner's Office. Guide to the General Data Protection Regulation: Lawful basis for processing

5. Information Commissioner's Office

6.Information Commissioner's Office. Resources and support: Data protection and self assessment

7. "Data Protection Act 2018". *ico.org.uk*. 2018-07-20. Retrieved 2018-08-29.

8."Data Protection Act 2018". *UK Government*. Retrieved 8 August 2018.

9, "New Data Protection Act finalised in the UK". *www.out-law.com*. Retrieved 2018-08-29.

10.DIRECTIVE (EU) 2016/680 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL

11."European Union (Withdrawal) Act 2018". *UK Government*. Retrieved 8 August 2018.

12.Full text of the Data Protection Act 2018