Privacy Notices (GDPR)

Background

The GDPR, or General Data Protection Regulation, is a new piece of European legislation which replaced the Data Protection Act (DPA) 1998 on 25 May 2018. A new Data Protection Act 2018 also came into force at the same time. The purpose of the new DPA 2018 is to apply the GDPR in the UK.

The underlying data protection principles have not changed significantly from those of the DPA 1998 – but there is the new principle of 'accountability' (see below). The GDPR also requires organisations to adopt the philosophy of 'Data Protection by Design and Default'. This means that the organisation must be able to demonstrate compliance with the data protection principles. The principles are the backbone of the regulation.

Processing principles

The GDPR requires that personal data shall be:

- processed lawfully, fairly and in a transparent manner ('lawfulness, fairness and transparency')
- collected for specified, explicit and legitimate purposes ('purpose limitation')
- adequate, relevant and limited to what is necessary ('data minimisation')
- accurate and up-to-date ('accuracy')
- kept in a form which permits identification for no longer than is necessary/archiving ('storage limitation')
- processed with appropriate technical and organisational measures to ensure security of personal data ('integrity and confidentiality').

The GDPR also requires that the data controller must be *responsible for and able to demonstrate compliance with* the principles ('accountability'). This means having the right procedures and processes in place from the point of data collection, so that there is clarity as to the legal basis for data processing at every stage of the life cycle of the data. So organisations have to be able to detect, report and investigate a personal data breach. Reputation management should be considered as part of the process.

Why do I need a privacy notice?

It was always best practice to have a privacy notice under the Data Protection Act 1998 but the new legislation now makes it compulsory. The first processing principle is that personal data must be processed fairly and lawfully. The GDPR says that the information that you provide to people about how you process their personal data must be concise, transparent, intelligible and easily accessible. As the data controller, you will have to demonstrate compliance and you are accountable by law.

What is a Privacy Notice for?

The point of a privacy notice is to tell people in plain English (or possibly another language):

- Who you are
- What you do with their information
- Who it will be shared with.

These are the basics upon which all privacy notices should be built. However, they can tell people more than this and should do so where you think that not telling people will make your processing of that information unfair. For example if an individual is unlikely to know that you use their information for a particular purpose or where their personal data has been collected by observation or inference.

What do you need to do first?

You should conduct an information audit to clarify what personal data your practice holds:

- Who do you hold information about?
- What information do you hold about them?
- What is the purpose of the processing
- Who do you share it with?
- How long do you hold it for?
- How do you keep it safe?

What does a Privacy Notice look like?

The GDPR uses the term 'privacy notice' to describe all the privacy information that you make available. The privacy notice doesn't have to be one big document. If it becomes too unwieldy, you might consider using a layered approach where key privacy information is provided immediately and more detailed information could be provided elsewhere, such as on your shared drive for employees or on your website for patients, as printed notices, on forms, in emails and on signs. Wherever it is, the location must be obvious and easy to access.

What does legal basis for processing mean?

To be able to process personal data legally, you have to be able to show that you can justify the processing against at least one of the 6 GDPR processing conditions. For example, you may need to process an employee's personal data to comply with a legal obligation such as sending information to the HMRC, or providing a copy of a patient record under a subject access request. The basis here could be 'compliance with a legal obligation'.

Other implications

Among other practical implications for consideration is how you monitor staff activities. Do you have CCTV in your practice? Why is it installed and did you carry out an impact assessment before you installed it? Do you allow staff to make personal phone calls from the practice phone system or send personal emails from their business account? Do you have a fair use policy which outlines when staff can access the internet for personal use (e.g. at lunchtime) and are staff aware that you can monitor their usage and the sites they access through their computer's IP address? Can they access personal email accounts and online banking from their work PC? If you have call recording, do staff know that you might use this for training and assessing their performance?

Why would you want to monitor these things? You could argue that your legal basis for this is that you have a 'legitimate interest' in protecting your business: for example you have the right to try to prevent viruses infecting your IT system. However, you also need to respect the personal privacy of your staff. It is a balancing act between a legitimate interest in monitoring and the right to privacy for staff.

What must the Privacy Notice include?

- Who is collecting the information (i.e. the name and contact details of the data controller)
- The name and contact details of the Data Protection Officer
- What personal information do you hold?
- How is the information collected by you?
- Why is it collected – the purpose? – this would include your lawful basis for processing
- How will it be used?
- Who will it be shared with?
- What will be the effect of this on the individuals concerned?
- Is the intended use likely to cause individuals to object or complain?
- What are you doing to ensure the security of personal data?
- Information about the individual's right of access to their data.
- The retention period for the data.

How should the Notice be presented?

- Use clear, straightforward language and avoid jargon.
- Adopt a style that is easy to read.
- Don't assume that everybody has the same level of understanding as you.
- Be truthful.

Before roll-out, test the privacy notice with users, amend if needed and keep it under review. If in doubt contact either the Information Commissioner's Office on 0303 123 1113/Option 4 or call MDDUS on 0333 043 4444 for advice.