GDPR – privacy notices

The GDPR, or General Data Protection Regulation, is a 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.

Compulsory compliance

It was best practice to have a privacy notice under the DPA 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 requires the information you provide to people about how you process their personal data to be concise, transparent, intelligible and easily accessible. Data controllers will have to demonstrate compliance and are accountable by law.

The point of a privacy notice is to tell people in simple language:

- who you are
- what you do with their personal information
- who it will be shared with.

These are the basics upon which all privacy notices should be built. However, you can go into more detail 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.

Step-by-step guide

What do you need to do first?
You should conduct an information audit to clarify what personal data your organisation 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 is available elsewhere. This could be 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 six GDPR processing conditions. The most appropriate lawful basis for processing health data for direct healthcare is: "processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller".

This basis is applicable for clinicians who carry out NHS work. Private practitioners will need to find an alternative lawful basis.

Because of the sensitive nature of healthcare data, it is classified as special category data under the GDPR. Data controllers must establish both a lawful basis for processing and a special category condition for processing. The special category condition for processing direct healthcare is that processing is "necessary for the purposes of preventative or occupational medicine for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services".

Both the lawful basis and the special category condition should be shown in your privacy notice.

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.

Common Pitfalls

- Organisations do not carry out an information audit, so they don't know exactly what information they are processing, how they process it and why. This means they can't create a meaningful privacy notice.
- Failing to appreciate that GDPR covers *all* personal data that they process, including employee data. Privacy notices have to be created for staff too.

Key points

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

Further guidance

- ICO. *Make your own privacy notice:* https://ico.org.uk/for-organisations/make-your-own-privacy-notice/

MDDUS Training & CPD resources: https://www.mddus.com/training-and-cpd/training-for-members

MDDUS GDPR checklist and guidance sheets: https://www.mddus.com/training-and-cpd/training-for-members/gp-risk-toolbox/gdpr