GDPR – general core principles

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. The GDPR makes GP partners and dental principals legally accountable for ensuring compliance with data protection law.

The Data Protection Act 2018 also came into force on 25 May 2018. The purpose of the DPA 2018 is to apply the GDPR in the UK. It introduced UK-specific provisions in some areas such as processing of special category data. Health data is included in special category data.

All GP and dental practices which were registered with the Information Commissioner's Office (ICO) under the DPA 1998 will still be registered under the DPA 2018 but need to update their processes and policies to comply with the new legislation.

New principles

The new processing principles of the GDPR require 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 be able to demonstrate compliance with the principles *('accountability').*

Basic requirements

There are certain requirements that data controllers need to know about to ensure they comply with the GDPR and DPA 2018.

- A privacy notice should be made available to patients. This is now compulsory. The purpose of a privacy notice is to let your patients know who you are; who your data controller and data protection officer are; what information you collect about your patients and what you do with it.
- Organisations must carry out an information audit to identify exactly what personal data you process; how you process it; why you process it; who you share it with; how long you hold it for and how you keep it safe.

- There are lawful bases and special category conditions which allow for the processing of personal and sensitive data under the new regulations. You must be able to demonstrate compliance with at least one lawful basis and one special category condition.
- The ICO expects all organisations in the UK to take a 'privacy by design' approach to data protection. This means considering how to address the privacy risks inherent in processing the data you hold. Carrying out a data protection impact assessment (DPIA) for any new system or process that you intend to implement would help you do this. A DPIA is a risk assessment tool which helps you to identify potential privacy and related risks in your new system; identify solutions to those risks and let you decide whether to accept the risks or whether to take action to reduce or eliminate them.
- The rules for dealing with a data breach have changed. Organisations are required to have a policy in place for breach identification and reporting and also a written breach management plan. A breach log should be created to include both reported and non-reported breaches. The ICO could ask to see your breaches log.
- Data subject rights have also been enhanced. The one that is most relevant to practices is subject access. This is commonly known as a subject access request or SAR. Patients have the right to access the personal data that you hold about them. The main changes are that you must now comply with the request within one month and you can no longer charge a fee for doing so. If you refuse to comply with a request you must tell the patient and advise them how to complain to the ICO about you.

There are other issues that must also be considered when processing a SAR. Our guidance sheet, listed below, gives more detail.

Common Pitfalls

- Not having identified a data protection officer
- Not notifying the ICO of a breach when it is appropriate to do so
- Not complying with the new SAR requirements
- Not making available to patients and staff a privacy notice which includes all of the required information.

All of the above could lead to financial penalties or reprimands being imposed by the ICO.

Key points

Work your way through the MDDUS GDPR checklist and read our guidance sheets to help you through what you need to do:

- Lawful processing
- Privacy notices
- Privacy impact assessments
- Breaches
- Data subject rights

Further guidance

- ICO. *Guide to the General Data Protection Regulation (GDPR)*: https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr
- ICO. *Data protection impact assessments*: https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/data-protection-impact-assessments-dpias
- ICO. *Guide to data protection audits*: https://ico.org.uk/media/for-organisations/documents/2787/guide-to-data-protection-audits.pdf

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