Lawful Processing

MDDUS
UK INDEMNITY, ADVICE & SUPPORT

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. Organisations have to be able to detect, report and investigate a personal data breach. Reputation management should be considered as part of the process.

What are the bases for legal processing?

These are not so different from the conditions of processing in the DPA 1998 but, under the GDPR, you need to actively identify the lawful bases for processing personal data, document it and explain it in your privacy notice. You must allocate *at least* one legal basis to each processing activity. If you don't have a lawful basis for processing the data then the processing is not deemed to be legal. There are six bases for legal processing of personal data, one of which is consent.

Consent here should not be confused with the consent that is required for a clinician to carry out a procedure which is quite separate.

The 6 lawful bases for processing personal data are:

- The data subject has given consent to the processing of his or her personal data for one or more specific purposes
- Processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract
- The processing is necessary for compliance with a legal obligation to which the controller is subject
- Processing is necessary in order to protect the vital interests of the data subject or of another natural person
- 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
- Processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms, particularly in the case of a child

The lawful basis that covers the NHS work carried out practices when processing direct healthcare data is highlighted in red. Practices would have to pick another lawful basis to process private work.
If you are processing Special Category data, which healthcare information is, then you have to identify *both* a lawful basis *and* an additional Condition for processing this type of data.

The 10 special category Conditions are:

- Explicit consent
- Employment and social security and social protection law
- Protecting vital interests where the data subject is physically or legally incapable of giving consent
- Management of not-for-profit membership organisations
- Processing relates to personal data which are manifestly made public by the data subject
- Processing is necessary for the establishment, exercise or defence of legal claims or whenever courts are acting in their judicial capacity
- Processing is necessary for reasons of substantial public interest, to safeguard the fundamental rights and the interests of the data subject
- Healthcare, occupational health and public health and safety
- Processing is necessary for reasons of public interest in the area of public health
- Scientific, historical archiving, research or statistical purposes

The special category Condition highlighted in red is an appropriate Condition for processing patient healthcare data. This Condition in full reads:
'Processing is necessary for the purposes of preventive 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 on the basis of Union or Member State law or pursuant to contract with a health professional and subject to specific conditions and safeguards'
The full wording for the 6 lawful bases and the 10 Conditions can be found on the ICO website.

How do you know which lawful basis to use?

This depends on your specific purposes and the context of the processing. Remember, you have to pick one or more lawful bases for processing your employee data too.

You should consider which lawful basis best fits the circumstances and the type of data. You might consider that more than one basis applies, in which case you should identify and document all of them *from the start* and tell the data subject which one you are relying upon. You would do this via your Privacy Notice.

You must not adopt a one-size-fits-all approach. No one basis should be seen as always better, safer or more important than the others, and there is no hierarchy in the order of the list in the GDPR.

If you were entering into a contract or performing a contract with the individual then you could use the basis of 'necessary for the performance of a contract'. You could use 'necessary for compliance with a legal obligation' as a basis where you're obliged to process information under a piece of legislation, such as sending personal data to the HMRC after each payroll run. The basis of 'necessary to protect someone's vital interest' would be used where there was a life or death situation and it is necessary to protect the vital interests of the data subject or another individual (e.g. their children) where the data subject is physically or legally incapable of giving consent. The basis of 'necessary for the performance of a task in the public interest' would mainly be used by public sector organisations and is unlikely to be appropriate to a medical or dental practice.

Note that if you are going to rely upon any of the "necessary" conditions you will have to be able to explain to the ICO if challenged *why* such use of data is indeed "necessary" rather than simply desirable or because you think it is a good idea.

The 'legitimate interests' is useful because it can cover such a wide number of areas and would be valid provided the legitimate interests of the business don't outweigh those of the data subject. You must balance your interests against the individual's. If they would not reasonably expect the processing, or if it would cause unjustified harm, their interests are likely to override your legitimate interests. However, legitimate interests is not available to GP and dental practices as a basis for lawful processing of special category data i.e. healthcare data.

Consent as a legal basis for processing personal data

We would advise that consent as a legal basis should not be used when processing healthcare data.

In the healthcare sector, patient data is held under a duty of confidence. Healthcare providers generally operate on the basis of implied consent to use patient data for the purposes of direct care, without breaching confidentiality.

Implied consent for direct care is industry practice in that context. This 'implied consent' in terms of duty of confidence is not the same as consent to process personal data in the context of a lawful basis under the GDPR.

Any requirement to get consent to the medical treatment itself does not mean that there is a requirement to get GDPR consent to associated processing of personal data, and other lawful bases are likely to be more appropriate.

Nothing has changed in this regard an practitioners should carry on as before.

You're more likely to rely on consent when sending out communications for marketing purposes or to impart information that is not related directly to patient healthcare such as health promotion.

When relying on consent, your method of obtaining it should:

- be displayed clearly and prominently;
- Be to ask individuals to positively opt-in, in line with good practice; and
- give them sufficient information to make a choice. If your consent mechanism consists solely of an "I agree" box with no supporting information then users are unlikely to be fully informed and the consent cannot be considered valid.

In addition if you are processing information for a range of purposes you should:

- explain the different ways you will use their information; and
- provide a clear and simple way for them to indicate they agree to different types of processing.
- Give them a clear and simple way to opt out in the future

Good practice would be to list the different purposes with separate unticked opt-in boxes for each or Yes/No buttons of equal size and prominence. Opt-in boxes can be prominently placed in your privacy notice.

More detailed information about lawful processing can be found on the ICO's website ico.org.uk

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.