# UK GDPR – lawful bases for processing

The GDPR, or General Data Protection Regulation, is a piece of European legislation which replaced the existing Data Protection Act (DPA) 1998 on 25 May 2018. A new UK Data Protection Act 2018 also came into force on the same day. The purpose of the UK Data Protection Act 2018 is to apply the GDPR in the UK, and is now commonly referred to as **'UK GDPR'.**

The legal bases for processing under the UK GDPR are not so different from the conditions of processing in the original DPA 1998. You need to actively identify the lawful bases for processing personal data, document them and explain them 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.

**Bases for Legal Processing**

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 from a patient for a clinician to carry out a procedure. This is quite separate.

The six 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.

If you are processing special category data, which healthcare information is, then you have to identify both a lawful basis and an additional special category 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 is 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 underlined above is an appropriate condition for processing patient healthcare data. This condition states: "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."

**Choosing a lawful basis**

Choosing which lawful basis to use 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 UK GDPR.

**Common Pitfalls**

- Organisations have not carried out an information audit to ascertain why they process information, so they are then unable to justify which lawful basis they are using.
- Organisations fail to identify which lawful basis and special category condition they are using in their privacy notice.

**Key points**

- Ensure that you have carried out an information audit so that you know exactly what personal data you are processing and why you're processing it.
- You need to have a lawful basis for processing staff data too and have that declared on your staff privacy notice.

**Further guidance**

- ICO. *Lawful basis for processing*: https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/

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