Lawful basis myths

Myth #1

“This lawful basis stuff is all new.”

Reality

It’s not new. The six lawful bases for processing are very similar to the old ‘conditions for processing’ under the Data Protection Act 1998.

In more detail…

The requirement to have a lawful basis in order to process personal data is not new. It replaces and mirrors the previous requirement to satisfy one of the ‘conditions for processing’ under the Data Protection Act 1998 (the 1998 Act). However, the GDPR places more emphasis on being accountable for and transparent about your lawful basis for processing.

The six lawful bases for processing are broadly similar to the old conditions for processing, although there are some differences. You now need to review your existing processing, identify the most appropriate lawful basis, and check that it applies. In many cases it is likely to be the same as your existing condition for processing.

DPA 1998 processing conditions (Schedule 2)	**GDPR lawful bases (Article 6)**
Data subject has given consent to the processing	Data subject has given consent to the processing for one or more specific purposes
Processing is necessary for performance of a contract to which the data subject is a party or for the taking of steps at the request of the data subject with view to entering into a contract	Processing is necessary 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
Processing is necessary for compliance with any legal	Processing is necessary for compliance with a legal obligation

obligation to which the data controller is subject, other than an obligation imposed by contract	to which the controller is subject
Processing is necessary in order to protect the vital interests of the data subject	Processing is necessary in order to protect the vital interests of the data subject or of another natural person
The processing is necessary for: the administration of justice; the exercise of any functions conferred by or under any enactment; the exercise of functions of the Crown/Minister of the Crown/government department; the exercise of any other functions of a public nature exercised in the public interest	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 data controller or by the third party (ies) to whom the data are disclosed, except where the processing is unwarranted due to prejudice to the rights and freedoms or legitimate interests of the data subject	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 of the data subject which require protection of personal data, in particular where the data subject is a child

The biggest change is for public authorities, who have more limited scope to rely on consent or legitimate interests and may need to consider the 'public task' basis for more of their processing.

You can choose a new lawful basis if you find that your old condition for processing is no longer appropriate under the GDPR, or decide that a different basis is more appropriate. You should try to get this right first time. Once the GDPR is in effect, it will be much harder to swap between lawful bases at will if you find that your original basis was invalid. You will be in breach of the GDPR if you did not clearly identify the appropriate lawful basis (or bases, if more than one applies) from the start.

The GDPR brings in new accountability and transparency requirements. You should therefore make sure you clearly document your lawful basis so that you can demonstrate your compliance in line with Articles 5(2) and 24.

You must now inform people upfront about your lawful basis for processing their personal data. You need therefore to communicate this information to individuals by 25 May 2018, and ensure that you include it in all future privacy notices.

Myth #2

"The GDPR says legitimate interests covers all direct marketing activities."

Reality

The GDPR suggests direct marketing **may** be a legitimate interest. But you still need to assess the three-part test for legitimate interests, and in some cases you need consent to comply with PECR.

In more detail...

Recital 47 of the GDPR says:

> "…The processing of personal data for direct marketing purposes may be regarded as carried out for a legitimate interest."

This means that direct marketing **may** be a legitimate interest. However the GDPR does not say that direct marketing always constitutes a legitimate interest, and whether your processing is lawful on the basis of legitimate interests depends on the particular circumstances.

In terms of the purpose test, some forms of marketing may not be legitimate if they do not comply with other legal or ethical standards or with industry codes of practice. However, as long as the marketing is carried out in compliance with e-privacy laws and other legal and industry standards, in most cases it is likely that direct marketing is a legitimate interest.

However this does not automatically mean that all processing for marketing purposes is lawful on this basis. You still need to show that your processing passes the necessity and balancing tests.

You may also need to be more specific about your purposes for some elements of your processing in order to show that processing is necessary and to weigh the benefits in the balancing test. For example, if you use profiling to target your marketing.

When looking at the balancing test, you should also consider factors such as:

- whether people would expect you to use their details in this way;
- the potential nuisance factor of unwanted marketing messages; and
- the effect your chosen method and frequency of communication might have on more vulnerable individuals.

Given that individuals have the absolute right to object to direct marketing under Article 21(2), it is more difficult to pass the balancing test if you do not give individuals a clear option to opt out of direct marketing when you initially collect their details (or in your first communication, if the data was not collected directly from the individual). The lack of any proactive opportunity to opt out in advance would arguably contribute to a loss of control over their data and act as an unnecessary barrier to exercising their data protection rights.

If you intend to process personal data for the purposes of direct marketing by electronic means (by email, text, automated calls etc) legitimate interests may not always be an appropriate basis for processing. This is because the e-privacy laws on electronic marketing – currently the Privacy and Electronic Communications Regulations (PECR) – require that individuals give their consent to some forms of electronic marketing. It is the GDPR standard of consent that applies, because of the effect of Article 94 of the GDPR.

If e-privacy laws require consent, then processing personal data for electronic direct marketing purposes is unlawful under the GDPR without consent. If you have not got the necessary consent, you cannot rely on legitimate interests instead. You are not able to use legitimate interests to legitimise processing that is unlawful under other legislation.

If you have obtained consent in compliance with e-privacy laws, then in practice consent is also the appropriate lawful basis under the GDPR. Trying to apply legitimate interests when you already have GDPR-compliant consent would be an entirely unnecessary exercise, and would cause confusion for individuals.

If e-privacy laws do not require consent, legitimate interests may well be appropriate. Based on the current legislation (PECR), and depending on the outcome of your three-part test, legitimate interests may be appropriate for 'solicited' marketing (ie marketing proactively requested by the individual), or for unsolicited marketing in the following circumstances:

Marketing method	**Is legitimate interests likely to be appropriate?**
Post	✓
'Live' phone calls to TPS/CPTS registered numbers	✗
'Live' phone calls to those who have objected to your calls	✗
'Live' phone calls where there is no TPS/CTPS registration or objection	✓
Automated phone calls	✗
Emails/text messages to individuals – obtained using 'soft opt-in'	✓
Emails/text messages to individuals – without 'soft opt-in'	✗
Emails/text messages to business contacts	✓

You also need to remember that Article 21 specifically gives the data subject the right to object to processing of their personal data for the purposes of direct marketing, and you must inform them of that right. If the data subject objects then this overrides your legitimate interests and you need to stop processing their data for direct marketing purposes.

The EU is in the process of replacing the current e-privacy law (and therefore PECR) with a new ePrivacy Regulation (ePR). However the new ePR is yet to be agreed. The existing PECR rules continue to apply until the ePR is finalised, with some changes for GDPR (chiefly the definition of consent).

Myth #3

"The six lawful bases are:

Consent

Contract
Legal obligation
Vital interests
Public interest task or official authority
Legitimate interests"

Reality

Consent is not always the best answer. It is one lawful basis for processing, but there are alternatives. Consent is not inherently better or more important than these alternatives.

In more detail…

Consent is appropriate if you can offer people real choice and control over how you use their data, and want to build their trust and engagement. But if you cannot offer a genuine choice, consent is not appropriate. If you would still process the personal data without consent, asking for consent is misleading and inherently unfair.

You should always consider which lawful basis (or bases) best fits the circumstances. 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.

You may need to consider a variety of factors, including:

- What is your purpose – what are you trying to achieve?
- Can you reasonably achieve it in a different way?
- Do you have a choice over whether or not to process the data?

Several of the lawful bases relate to a particular specified purpose – a legal obligation, a contract with the individual, protecting someone's vital interests, or performing official functions or public interest tasks.

If you are processing for these purposes then the appropriate lawful basis may well be obvious, so it is helpful to consider these first.

If you are processing for purposes other than legal obligation, contract, vital interests or public task, then the appropriate lawful basis may not be so clear cut. In many cases you are likely to have a choice between using legitimate interests or consent. You need to give some thought to the wider context, including:

- Who does the processing benefit?
- Would individuals expect this processing to take place?
- What is your relationship with the individual?
- Are you in a position of power over them?
- What is the impact of the processing on the individual?
- Are they vulnerable?
- Are some of the individuals concerned likely to object?
- Are you able to stop the processing at any time on request?

You may prefer to consider legitimate interests as your lawful basis if you wish to keep control over the processing and take responsibility for demonstrating that it is in line with people's reasonable expectations and wouldn't have an unwarranted impact on them. On the other hand, if you prefer to give individuals full control over and responsibility for their data (including the ability to change their mind as to whether it can continue to be processed), you may want to consider relying on individuals' consent.

Myth #4

"We can use another basis as a back-up to consent."

Reality

It's true you can have more than one lawful basis for your processing. But if you choose to ask for consent, you must respect the individual's choice. You cannot do it anyway on a different basis if they don't consent.

In more detail...

It may be that more than one lawful basis applies to the processing if you have more than one purpose. However, this does not mean you can use another basis as a back-up for consent.

If you offer people a choice, you must respect that choice. It is fundamentally misleading and unfair to tell people they have a choice, then process the data anyway – it presents individuals with a false choice and only the illusion of control.

You should also remember that the GDPR gives a specific right to withdraw consent. You need to tell people about their right to withdraw, and offer them easy ways to withdraw consent at any time. You must then stop any processing based on consent once consent is withdrawn.

If you need to retain the data for another purpose after consent is withdrawn, you need to be open and honest about your reasons (and lawful basis) for doing this from the start.

Myth #5

"Public authorities are banned from using legitimate interests."

Reality

There is no absolute ban. Public authorities can still rely on legitimate interests for any processing which is not to perform their tasks as a public authority.

In more detail…

If you are a public authority, you cannot rely on legitimate interests for any processing you do to perform your tasks as a public authority. Other lawful bases such as public task or legal obligation are likely to apply.

For other legitimate purposes outside the scope of your tasks as a public authority, you can consider legitimate interests where appropriate. This will be particularly relevant for public authorities with commercial interests.

The Data Protection Bill will define 'public authority' and the final text of those provisions may also have some impact here. We will publish more guidance on the effect of relevant Bill provisions when they are finalised.

Example

A university that wants to process personal data may consider a variety of lawful bases depending on what it wants to do with the data.

Universities are likely to be classified as public authorities, so the public task basis is likely to apply to much of their processing, depending on the detail of their constitutions and legal powers. If the processing is separate from their tasks as a public authority, then the university may instead wish to consider whether consent or legitimate interests are appropriate in the particular circumstances, considering the factors set out below. For example, a University might rely on

public task for processing personal data for teaching and research purposes; but a mixture of legitimate interests and consent for alumni relations and fundraising purposes.

The university however needs to consider its basis carefully – it is the controller's responsibility to be able to demonstrate which lawful basis applies to the particular processing purpose.

Myth #6

"Vital interests can cover anything really important"

Reality

Vital interests only applies to matters of life and death.

In more detail...

It's clear from Recital 46 that vital interests are intended to cover only interests that are essential for someone's life. So this lawful basis is very limited in its scope, and generally only applies to matters of life and death.

It is likely to be particularly relevant for emergency medical care, when you need to process personal data for medical purposes but the individual is incapable of giving consent to the processing.

Example

An individual is admitted to the A & E department of a hospital with life-threatening injuries following a serious road accident. The disclosure to the hospital of the individual's medical history is necessary in order to protect his/her vital interests.
It is less likely to be appropriate for medical care that is planned in advance. Another lawful basis such as public task or legitimate interests is likely to be more appropriate in this case.

Processing of one individual's personal data to protect the vital interests of others is likely to happen more rarely. It may be relevant, for example, if it is necessary to process a parent's personal data to protect the vital interests of a child.

Vital interests is also less likely to be the appropriate basis for processing on a larger scale. Recital 46 does suggest that vital interests might apply where you are processing on humanitarian grounds such as monitoring epidemics, or where there is a natural or man-made disaster causing a humanitarian emergency.

However, if you are processing one person's personal data to protect someone else's life, Recital 46 also indicates that you should generally try to use an alternative lawful basis, unless none is obviously available. For example, in many cases you could consider legitimate interests, which will give you a framework to balance the rights and interests of the data subject(s) with the vital interests of the person or people you are trying to protect.

In most cases the protection of vital interests is likely to arise in the context of health data. This is one of the special categories of data, which means you will also need to identify a condition for processing special category data under Article 9.

There is a specific condition at Article 9(2)(c) for processing special category data where necessary to protect someone's vital interests. However, this only applies if the data subject is physically or legally incapable of giving consent. This means explicit consent is more appropriate in many cases, and you will need a different condition for special category data (including health data) if the data subject refuses consent, unless they are not competent to do so.

Myth #7

“For special category data, it’s Article 9 instead of Article 6.”

Reality

You must still have a lawful basis for your processing under Article 6, in exactly the same way as for any other personal data. The difference is that you will also need to satisfy a specific condition under Article 9.

In more detail…

In order to lawfully process special category data, you must identify both a lawful basis under Article 6 and a separate condition for processing special category data under Article 9.

Your choice of lawful basis under Article 6 does not dictate which special category condition you must apply, and vice versa. For example, if you use consent as your lawful basis, you are not restricted to using explicit consent for special category processing under Article 9. You should choose whichever special category condition is the most appropriate in the circumstances – although in many cases there may well be an obvious link between the two. For example, if your lawful basis is vital interests, it is highly likely that the Article 9 condition for vital interests will also be appropriate.

The conditions are listed in Article 9(2) of the GDPR:

> (a) the data subject has given explicit consent to the processing of those personal data for one or more specified purposes, except where Union or Member State law provide that the prohibition referred to in paragraph 1 may not be lifted by the data subject;
>
> (b) processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the controller or of the data subject in the field of employment and social security and social protection law in so far as it is authorised by Union or Member State law or a collective agreement pursuant to Member State law providing

for appropriate safeguards for the fundamental rights and the interests of the data subject;

(c) processing is necessary to protect the vital interests of the data subject or of another natural person where the data subject is physically or legally incapable of giving consent;

(d) processing is carried out in the course of its legitimate activities with appropriate safeguards by a foundation, association or any other not-for-profit body with a political, philosophical, religious or trade union aim and on condition that the processing relates solely to the members or to former members of the body or to persons who have regular contact with it in connection with its purposes and that the personal data are not disclosed outside that body without the consent of the data subjects;

(e) processing relates to personal data which are manifestly made public by the data subject;

(f) processing is necessary for the establishment, exercise or defence of legal claims or whenever courts are acting in their judicial capacity;

(g) processing is necessary for reasons of substantial public interest, on the basis of Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject;

(h) 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 the conditions and safeguards referred to in paragraph 3;

(i) processing is necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of quality and safety of health care and of medicinal products or medical devices, on the basis of Union or Member State law which provides for suitable and specific measures to safeguard the rights and freedoms of the data subject, in particular professional secrecy;

(j) processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) based on Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and

specific measures to safeguard the fundamental rights and the interests of the data subject.

Some of these conditions make reference to UK law, and the GDPR also gives member states the scope to add more conditions. The Data Protection Bill includes proposals for additional conditions and safeguards, and we will publish more detailed guidance here once these provisions are finalised.

Myth #8

"Only public authorities can use the public task basis"

Reality

It is most relevant to public authorities, but it can apply to any organisation that exercises official authority or carries out tasks in the public interest.

In more detail...

Article 6(1)(e) gives you a lawful basis for processing where:

> "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 can apply if you are either:

- carrying out a specific task in the public interest which is laid down by law; or
- exercising official authority (for example, a public body's tasks, functions, duties or powers) which is laid down by law.

Any organisation who is exercising official authority or carrying out a specific task in the public interest can use this public task basis. The focus is on the nature of the function, not the nature of the organisation.

Example

Private water companies are likely to be able to rely on the public task basis even if they do not fall within the definition of a public authority in the Data Protection Bill. This is because they are considered to be carrying out functions of public administration and they exercise special legal powers to carry out utility services in the public interest. See our guidance on Public authorities under the EIR for more details.

However, if you are a private sector organisation you are likely to be able to consider the legitimate interests basis as an alternative. Use our interactive tool to help you choose.

The Data Protection Bill includes a draft clause clarifying that the public task basis will cover processing necessary for:

- the administration of justice;
- parliamentary functions;
- statutory functions; or
- governmental functions.

However, this is not intended as an exhaustive list. If you have other official non-statutory functions or public interest tasks you can still rely on the public task basis, as long as the underlying legal basis for that function or task is clear and foreseeable.

For accountability purposes, you should be able to specify the relevant task, function or power, and identify its basis in common law or statute. You should also ensure that you can demonstrate there is no other reasonable and less intrusive means to achieve your purpose.