

CHECKLIST | LAWFUL BASIS FOR PROCESSING UNDER THE GDPR

Presented by MacKay Corporate Insurance Brokers

The General Data Protection Regulation (GDPR) replaces and mirrors the previous requirement to satisfy one of the 'conditions for processing' under the Data Protection Act. However, the GDPR places more emphasis on being accountable for and transparent about your lawful basis for processing personal data.

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

You must determine your lawful basis before you begin processing, and you should document it. Take care to get it right the first time—you should not swap a different lawful basis at a later date without good reason. If your purpose for processing changes, you may be able to continue processing under the original lawful basis if your new purpose is compatible with your initial purpose (unless your original lawful basis was consent).

To emphasise transparency and accountability, make sure that your privacy notice includes your lawful basis for processing as well as the purposes of the processing. You should also inform people upfront about which lawful basis (or bases) you rely on to process their personal data.

The six lawful bases are outlined below. Click on the title of each lawful basis for more detailed information from the Information Commissioner's Office (ICO). At least one of these must apply whenever you process personal data:

1. [Consent](#)—The individual has given your organisation clear consent for you to process their personal data for a specific purpose.
2. [Contract](#)—The data processing is necessary for a contract that you have with the individual, or because they asked you to take specific steps before entering into a contract.
3. [Legal obligation](#)—The data processing is necessary for your organisation to comply with the law—not including contractual obligations.
4. [Vital interests](#)—The data processing is necessary for your organisation to protect an individual's life.
5. [Public task](#)—The data processing is necessary for you to perform a task in the public's interest or for your organisation's official functions, and the task or function has a clear basis in law.
6. [Legitimate interests](#)—The data processing is necessary for your legitimate interests or the legitimate interests of a third party, unless there is a good reason to protect the individual's personal data that overrides those legitimate interests. (Note: This cannot apply if your organisation is a public authority processing data to perform your own official tasks.)

No single basis is 'better' or more important than the others—which basis is most appropriate to use will depend on your purpose and relationship with the individual. Most lawful bases require that processing is 'necessary'. If you can reasonably achieve the same purpose without the processing, you won't have a lawful basis.

Complete the following checklist to help determine which lawful basis applies. Give some thought to the wider context behind your answers and your processing activities in general. This will help you determine which lawful basis best fits the circumstances.

DETERMINING WHICH LAWFUL BASIS APPLIES	YES	NO	ADDITIONAL NOTES
We have determined what our purpose for processing is and what we are trying to achieve.	<input type="checkbox"/>	<input type="checkbox"/>	
We have determined whether we can reasonably achieve it in a different way.	<input type="checkbox"/>	<input type="checkbox"/>	
We have asked ourselves whether we have a choice over whether or not to process the data.	<input type="checkbox"/>	<input type="checkbox"/>	
We know whether we are a public authority.	<input type="checkbox"/>	<input type="checkbox"/>	
We know who our processing benefits.	<input type="checkbox"/>	<input type="checkbox"/>	
We have considered whether individuals would expect this processing to take place.	<input type="checkbox"/>	<input type="checkbox"/>	
We know our relationship with the individual.	<input type="checkbox"/>	<input type="checkbox"/>	
We have considered whether we are in a position of power over the individuals.	<input type="checkbox"/>	<input type="checkbox"/>	
We know the impact of processing on the individual.	<input type="checkbox"/>	<input type="checkbox"/>	
We have determined whether the individual is vulnerable.	<input type="checkbox"/>	<input type="checkbox"/>	
We have determined whether some of the individuals are likely to object.	<input type="checkbox"/>	<input type="checkbox"/>	
We are able to stop the processing at any time on request.	<input type="checkbox"/>	<input type="checkbox"/>	

GENERAL CONSIDERATIONS FOR DETERMINING LAWFUL BASIS	YES	NO	ADDITIONAL NOTES
We have reviewed the purposes of our processing activities and selected the most appropriate lawful basis (or bases) for each activity.	<input type="checkbox"/>	<input type="checkbox"/>	
We have checked that the processing is necessary for the relevant purpose, and we are satisfied that there is no other reasonable way to achieve that purpose.	<input type="checkbox"/>	<input type="checkbox"/>	
We have documented our decision on which lawful basis applies to help us demonstrate compliance.	<input type="checkbox"/>	<input type="checkbox"/>	
We have included information about both the purposes of the processing and the lawful basis for the processing in our privacy notice.	<input type="checkbox"/>	<input type="checkbox"/>	
Where we process special category data, we have also identified a condition for processing special category data, and have documented this.	<input type="checkbox"/>	<input type="checkbox"/>	
Where we process criminal offence data, we have also identified a condition for processing this data, and have documented this.	<input type="checkbox"/>	<input type="checkbox"/>	

If your purposes for processing data change over time or if you have a new purpose that you did not originally anticipate, you may not need a new lawful basis as long as your new purpose is compatible with the original purpose.

However, the GDPR specifically states that this does not apply to processing based on consent. You need to either get fresh consent, which specifically covers the new purpose, or find a different basis for the new purpose. If you do get specific consent for the new purpose, you do not need to show it is compatible.

In other cases, in order to assess whether the new purpose is compatible with the original purpose, ask yourself the following questions:

- Is there any link between your initial purpose and the new purpose?
- Under what context has the data been collected?
- What is your relationship to the individual?
- What kind of data processing would the individual reasonably expect from your organisation?
- What is the nature of the personal data? Is it special category? Is it criminal offence data?
- What are the possible consequences for individuals of the new data processing?
- Does your organisation have appropriate safeguards to protect the data, such as encryption or pseudonymisation?

This list of questions is not exhaustive and what you need to look at depends on your particular circumstances. As a general rule, if the new purpose is very different from the original, would be unexpected or would have an unjustified impact on the individual, it is unlikely to be compatible with your original purpose for collecting the data. You will probably need to find a new lawful basis to process the data for that new purpose.