

Legitimate interests

At a glance

- Legitimate interests is the most flexible lawful basis for processing, but you cannot assume it will always be the most appropriate.
- It is likely to be most appropriate where you use people's data in ways they would reasonably expect and which have a minimal privacy impact, or where there is a compelling justification for the processing.
- If you choose to rely on legitimate interests, you are taking on extra responsibility for considering and protecting people's rights and interests.
- Public authorities can only rely on legitimate interests if they are processing for a legitimate reason other than performing their tasks as a public authority.
- There are three elements to the legitimate interests basis. It helps to think of this as a three-part test. You need to:
 - identify a legitimate interest;
 - show that the processing is necessary to achieve it; and
 - balance it against the individual's interests, rights and freedoms.
- The legitimate interests can be your own interests or the interests of third parties. They can include commercial interests, individual interests or broader societal benefits.
- The processing must be necessary. If you can reasonably achieve the same result in another less intrusive way, legitimate interests will not apply.
- 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.
- Keep a record of your legitimate interests assessment (LIA) to help you demonstrate compliance if required.
- You must include details of your legitimate interests in your privacy information.

Checklists

- We have checked that legitimate interests is the most appropriate basis.
- We understand our responsibility to protect the individual's interests.
- We have conducted a legitimate interests assessment (LIA) and kept a record of it, to ensure that we can justify our decision.
- We have identified the relevant legitimate interests.
- We have checked that the processing is necessary and there is no less intrusive way to achieve the same result.

- We have done a balancing test, and are confident that the individual's interests do not override those legitimate interests.
- We only use individuals' data in ways they would reasonably expect, unless we have a very good reason.
- We are not using people's data in ways they would find intrusive or which could cause them harm, unless we have a very good reason.
- If we process children's data, we take extra care to make sure we protect their interests.
- We have considered safeguards to reduce the impact where possible.
- We have considered whether we can offer an opt out.
- If our LIA identifies a significant privacy impact, we have considered whether we also need to conduct a DPIA.
- We keep our LIA under review, and repeat it if circumstances change.
- We include information about our legitimate interests in our privacy information.

In brief

- [What's new under the GDPR?](#)
- [What is the 'legitimate interests' basis?](#)
- [When can we rely on legitimate interests?](#)
- [How can we apply legitimate interests in practice?](#)
- [What else do we need to consider?](#)

What's new under the GDPR?

The concept of legitimate interests as a lawful basis for processing is essentially the same as the equivalent Schedule 2 condition in the 1998 Act, with some changes in detail.

You can now consider the legitimate interests of any third party, including wider benefits to society. And when weighing against the individual's interests, the focus is wider than the emphasis on 'unwarranted prejudice' to the individual in the 1998 Act. For example, unexpected processing is likely to affect whether the individual's interests override your legitimate interests, even without specific harm.

The GDPR is clearer that you must give particular weight to protecting children's data.

Public authorities are more limited in their ability to rely on legitimate interests, and should consider the 'public task' basis instead for any processing they do to perform their tasks as a public authority. Legitimate interests may still be available for other legitimate processing outside of those tasks.

The biggest change is that you need to document your decisions on legitimate interests so that you can demonstrate compliance under the new GDPR accountability principle. You must also include more information in your privacy information.

In the run up to 25 May 2018, you need to review your existing processing to identify your lawful basis and document where you rely on legitimate interests, update your privacy information, and communicate it to individuals.

What is the 'legitimate interests' basis?

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



“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.”

This can be broken down into a three-part test:

1. **Purpose test:** are you pursuing a legitimate interest?
2. **Necessity test:** is the processing necessary for that purpose?
3. **Balancing test:** do the individual's interests override the legitimate interest?

A wide range of interests may be legitimate interests. They can be your own interests or the interests of third parties, and commercial interests as well as wider societal benefits. They may be compelling or trivial, but trivial interests may be more easily overridden in the balancing test.

The GDPR specifically mentions use of client or employee data, marketing, fraud prevention, intra-group transfers, or IT security as potential legitimate interests, but this is not an exhaustive list. It also says that you have a legitimate interest in disclosing information about possible criminal acts or security threats to the authorities.

'Necessary' means that the processing must be a targeted and proportionate way of achieving your purpose. You cannot rely on legitimate interests if there is another reasonable and less intrusive way to achieve the same result.

You must balance your interests against the individual's interests. In particular, if they would not reasonably expect you to use data in that way, or it would cause them unwarranted harm, their interests are likely to override yours. However, your interests do not always have to align with the individual's interests. If there is a conflict, your interests can still prevail as long as there is a clear justification for the impact on the individual.

When can we rely on legitimate interests?

Legitimate interests is the most flexible lawful basis, but you cannot assume it will always be appropriate for all of your processing.

If you choose to rely on legitimate interests, you take on extra responsibility for ensuring people's rights and interests are fully considered and protected.

Legitimate interests is most likely to be an appropriate basis where you use data in ways that people

would reasonably expect and that have a minimal privacy impact. Where there is an impact on individuals, it may still apply if you can show there is an even more compelling benefit to the processing and the impact is justified.

You can rely on legitimate interests for marketing activities if you can show that how you use people's data is proportionate, has a minimal privacy impact, and people would not be surprised or likely to object – but only if you don't need consent under PECR. See our [Guide to PECR](#) for more on when you need consent for electronic marketing.

You can consider legitimate interests for processing children's data, but you must take extra care to make sure their interests are protected. See our detailed guidance on [children and the GDPR](#).

You may be able to rely on legitimate interests in order to lawfully disclose personal data to a third party. You should consider why they want the information, whether they actually need it, and what they will do with it. You need to demonstrate that the disclosure is justified, but it will be their responsibility to determine their lawful basis for their own processing.

You should avoid using legitimate interests if you are using personal data in ways people do not understand and would not reasonably expect, or if you think some people would object if you explained it to them. You should also avoid this basis for processing that could cause harm, unless you are confident there is nevertheless a compelling reason to go ahead which justifies the impact.

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. However, if you have 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.

See our [guidance page on the lawful basis](#) for more information on the alternatives to legitimate interests, and how to decide which basis to choose.

How can we apply legitimate interests in practice?

If you want to rely on legitimate interests, you can use the three-part test to assess whether it applies. We refer to this as a legitimate interests assessment (LIA) and you should do it before you start the processing.

An LIA is a type of light-touch risk assessment based on the specific context and circumstances. It will help you ensure that your processing is lawful. Recording your LIA will also help you demonstrate compliance in line with your accountability obligations under Articles 5(2) and 24. In some cases an LIA will be quite short, but in others there will be more to consider.

First, identify the legitimate interest(s). Consider:

- Why do you want to process the data – what are you trying to achieve?
- Who benefits from the processing? In what way?
- Are there any wider public benefits to the processing?
- How important are those benefits?
- What would the impact be if you couldn't go ahead?
- Would your use of the data be unethical or unlawful in any way?

Second, apply the necessity test. Consider:

- Does this processing actually help to further that interest?
- Is it a reasonable way to go about it?
- Is there another less intrusive way to achieve the same result?

Third, do a balancing test. Consider the impact of your processing and whether this overrides the interest you have identified. You might find it helpful to think about the following:

- What is the nature of your relationship with the individual?
- Is any of the data particularly sensitive or private?
- Would people expect you to use their data in this way?
- Are you happy to explain it to them?
- Are some people likely to object or find it intrusive?
- What is the possible impact on the individual?
- How big an impact might it have on them?
- Are you processing children's data?
- Are any of the individuals vulnerable in any other way?
- Can you adopt any safeguards to minimise the impact?
- Can you offer an opt-out?

You then need to make a decision about whether you still think legitimate interests is an appropriate basis. There's no foolproof formula for the outcome of the balancing test – but you must be confident that your legitimate interests are not overridden by the risks you have identified.

Keep a record of your LIA and the outcome. There is no standard format for this, but it's important to record your thinking to help show you have proper decision-making processes in place and to justify the outcome.

Keep your LIA under review and refresh it if there is a significant change in the purpose, nature or context of the processing.

If you are not sure about the outcome of the balancing test, it may be safer to look for another lawful basis. Legitimate interests will not often be the most appropriate basis for processing which is unexpected or high risk.

If your LIA identifies significant risks, consider whether you need to do a DPIA to assess the risk and potential mitigation in more detail. See our [guidance on DPIAs](#) for more on this.

What else do we need to consider?

You must tell people in your privacy information that you are relying on legitimate interests, and explain what these interests are.

If you want to process the personal data for a new purpose, you may be able to continue processing under legitimate interests as long as your new purpose is compatible with your original purpose. We would still recommend that you conduct a new LIA, as this will help you demonstrate compatibility.

If you rely on legitimate interests, the right to data portability does not apply.

If you are relying on legitimate interests for direct marketing, the right to object is absolute and you must stop processing when someone objects. For other purposes, you must stop unless you can show that your legitimate interests are compelling enough to override the individual's rights. See our guidance on [individual rights](#) for more on this.

Further Reading

 [Relevant provisions in the GDPR - See Article 6\(1\)\(f\) and Recitals 47, 48 and 49](#) 
External link

In more detail – ICO guidance

We have produced more detailed guidance on [legitimate interests](#)

We have produced the [lawful basis interactive guidance tool](#), to give tailored guidance on which lawful basis is likely to be most appropriate for your processing activities.

In more detail - European Data Protection Board

The European Data Protection Board (EDPB), which has replaced the Article 29 Working Party (WP29), includes representatives from the data protection authorities of each EU member state. It adopts guidelines for complying with the requirements of the GDPR.

There are no immediate plans for EDPB guidance on legitimate interests under the GDPR, but [WP29 Opinion 06/2014 \(9 April 2014\)](#) gives detailed guidance on the key elements of the similar legitimate interests provisions under the previous Data Protection Directive 95/46/EC.