

CHECKLIST | LEGITIMATE INTERESTS UNDER THE GDPR

Presented by MacKay Corporate Insurance Brokers

In order for your organisation to process individuals' personal data, you must have a lawful basis (or bases). One of these bases is legitimate interests, which the Information Commissioner's Office (ICO) defines as:

'[Data processing which] 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.'

Out of the six lawful bases, legitimate interests is the most flexible, yet that does not mean that it is the most appropriate. It is likely to be most appropriate when you use people's data in ways they would reasonably expect and 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. The legitimate interests can be your own interests or the interests of third parties—a wide range of interests may be legitimate interests. 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. If you don't need consent under the Privacy and Electronic Communications Regulations (PECR), 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 that people would not be surprised or likely to object. See the [ICO's guide to PECR](#) for more information on when you need consent for electronic marketing.

Before you decide that legitimate interests is the most applicable basis, complete a legitimate interests assessment (LIA). An LIA is a type of risk assessment based on the specific context and circumstances that will help you ensure that your processing is lawful. LIAs 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?

Complete the three-part LIA checklist and the general considerations checklist below to determine whether you can rely on the legitimate interests clause to process personal data under the GDPR.

Legitimate Interests Assessment:

STEP 1: CONDUCTING A PURPOSE TEST	YES	NO	ADDITIONAL NOTES
We know why we want to process the data and what we are trying to achieve.	<input type="checkbox"/>	<input type="checkbox"/>	
We understand who benefits from the processing and in what way.	<input type="checkbox"/>	<input type="checkbox"/>	
We have investigated whether there are any wider public benefits to the processing and how important those benefits are.	<input type="checkbox"/>	<input type="checkbox"/>	
We have evaluated what the impact would be if we couldn't go ahead with the processing.	<input type="checkbox"/>	<input type="checkbox"/>	
We have scrutinised whether our use of the data would be unethical or unlawful in any way.	<input type="checkbox"/>	<input type="checkbox"/>	

This checklist is of general interest and is not intended to apply to specific circumstances. It does not purport to be a comprehensive analysis of all matters relevant to its subject matter. The content should not, therefore, be regarded as constituting legal advice and not be relied upon as such. In relation to any particular problem which they may have, readers are advised to seek specific advice. Further, the law may have changed since first publication and the reader is cautioned accordingly.

Contains public sector information published by the ICO and licensed under the Open Government Licence v3.0.

Design © 2018 Zywave, Inc. All rights reserved.

STEP 2: CONDUCTING A NECESSITY TEST	YES	NO	ADDITIONAL NOTES
We have determined that our processing helps to further the legitimate interest that we have identified.	<input type="checkbox"/>	<input type="checkbox"/>	
We agree that our plans are a reasonable way to go about processing individuals' data.	<input type="checkbox"/>	<input type="checkbox"/>	
We have considered whether there is a less intrusive way to achieve the same result.	<input type="checkbox"/>	<input type="checkbox"/>	

STEP 3: CONDUCTING A BALANCING TEST	YES	NO	ADDITIONAL NOTES
We have identified the nature of our relationship with the individuals.	<input type="checkbox"/>	<input type="checkbox"/>	
We have determined whether any of the data is particularly sensitive or private.	<input type="checkbox"/>	<input type="checkbox"/>	
We have considered whether people would expect us to use their data in this way.	<input type="checkbox"/>	<input type="checkbox"/>	
We are happy to explain to people how we use their data.	<input type="checkbox"/>	<input type="checkbox"/>	
We have considered whether some people are likely to object or find it intrusive.	<input type="checkbox"/>	<input type="checkbox"/>	
We have considered the possible impact on the individual and how big that impact would be.	<input type="checkbox"/>	<input type="checkbox"/>	
We have determined whether we process any children's data.	<input type="checkbox"/>	<input type="checkbox"/>	
We have considered whether any of the individuals are vulnerable in any way.	<input type="checkbox"/>	<input type="checkbox"/>	
We have examined whether we can adopt any safeguards to minimise the impact our processing would have on individuals.	<input type="checkbox"/>	<input type="checkbox"/>	
We have examined whether we can offer an opt-out to individuals.	<input type="checkbox"/>	<input type="checkbox"/>	
Does the impact of our processing override our interests?	<input type="checkbox"/>	<input type="checkbox"/>	

Once you have undertaken the three-part LIA, be sure to keep a record of it 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 often not be the most appropriate basis for processing that is unexpected or high risk. If

you do rely on legitimate interests to process data, remember that you must tell people in your privacy notice that you are relying on legitimate interests and explain what those 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. In this case, the ICO still recommends that you conduct a new LIA, as this will help you demonstrate compatibility.

If you rely on legitimate interests for direct marketing, the right to object is absolute and you must stop processing when someone objects.

After conducting your three-part LIA, complete the general considerations checklist below to identify anything else that may prevent you from relying on the legitimate interests clause to process data.

GENERAL CONSIDERATIONS FOR USING LEGITIMATE INTERESTS	YES	NO	ADDITIONAL NOTES
We have checked that legitimate interests is the most appropriate basis for processing data.	<input type="checkbox"/>	<input type="checkbox"/>	
We understand our responsibility to protect the individual's interests.	<input type="checkbox"/>	<input type="checkbox"/>	
We have conducted an LIA and kept a record of it to ensure that we can justify our decision.	<input type="checkbox"/>	<input type="checkbox"/>	
We have identified the relevant legitimate interests.	<input type="checkbox"/>	<input type="checkbox"/>	
We have checked that the processing is necessary and there is no less intrusive way to achieve the same result.	<input type="checkbox"/>	<input type="checkbox"/>	
We have done a balancing test and are confident that the individual's interests do not override our legitimate interests.	<input type="checkbox"/>	<input type="checkbox"/>	
We only use individuals' data in ways they would reasonably expect, unless we have a very good reason.	<input type="checkbox"/>	<input type="checkbox"/>	
We are not using people's data in ways they would find intrusive or that could cause them harm, unless we have a very good reason.	<input type="checkbox"/>	<input type="checkbox"/>	
If we process children's data, we take extra care to make sure we protect their interests.	<input type="checkbox"/>	<input type="checkbox"/>	
We have considered safeguards to reduce the impact where possible.	<input type="checkbox"/>	<input type="checkbox"/>	
We have considered whether we can offer an opt-out.	<input type="checkbox"/>	<input type="checkbox"/>	
If our LIA identifies a significant privacy impact, we have considered whether we also need to conduct a data protection impact assessment (DPIA).	<input type="checkbox"/>	<input type="checkbox"/>	
We keep our LIA under review, and repeat it if circumstances change.	<input type="checkbox"/>	<input type="checkbox"/>	
We include information about our legitimate interests in our privacy notice.	<input type="checkbox"/>	<input type="checkbox"/>	