LAWFUL BASIS FOR DATA PROCESSING

# Lawful basis for data processing guidance

## How should I use my lawful basis for data processing document?

This guidance document is designed to assist your company in determining the appropriate lawful basis which applies to each type of data your company processes.

## Will I need to update my lawful basis for data processing document?

Yes. You should review this document at least every 3 months, and amend as necessary to ensure your company remains GDPR compliant. The lawful basis your company applies to data should be recorded and documented in your Controller Processing Activities Register.

# The aims of this document

The purpose of this document is to provide your company with an explicit explanation regarding lawful basis as it applies to GDPR, and how to appropriately select a lawful basis to support your company’s lawful right to process data.

Your company should define the legitimate (or lawful) basis in its Controller Processing Activities Register document for each processing activity that occurs – demonstrating the lawful basis you are choosing to apply to each activity or instance of processing.

# GDPR, lawful basis and legitimate interests

Under GDPR legislation, companies wishing to process data are permitted to do so if they can justify the relevant processing activities under at least one of the following six **categories of lawful basis**:

* The data subject has given your company consent to process their data for a specific reason
* Processing data is necessary to carry out the delivery of a contract with the data subject
* Processing data is necessary to protect the vital interests of the data subject or another individual
* Processing data is necessary for the delivery of a task that is being carried out in the public interest
* Processing data is required to meet your company’s compliance with legal obligations
* Processing is required for a legitimate interest being pursued by your company or a relevant third-party (note this category does not apply if your company’s legitimate interests clash with the individual rights of the data subject)

There is no established hierarchy in terms of the lawful bases you can apply as your reason for processing data. Different bases can be applied to different activities, and may depend upon the types of personal data being processed at any given time. Consent is often considered the most explicit and strongest form of legal basis.

It’s also worth noting that “legitimate interests” is not a phrase defined by the European Union’s GDPR legislation, and so is subject to limited interpretation.

For the purpose of GDPR compliance, the legitimate interests of your company or data controllers operating on behalf of your company generally provides a legal basis for processing data. This is the most common form of lawful basis; however, this category of lawful basis cannot be applied in any situation in which the processing activity in question could impair an individual’s rights or freedoms.

If your company decides to use legitimate interest to support the lawful basis of any processing activity, you must carefully assess whether the data subject would reasonably expect the processing activity for which you have collected data to take place. If the data subject would not reasonably expect further data processing to take place that is supplemental to the rationale originally applied, it could negate your company’s ability to claim legitimate interests as a reason for processing data.

Please note there may be situations in which the legitimate interests of your company or data controller may overlap with other bases for lawful processing. For example, under GDPR, it is acknowledged within the legislation that data controllers can apply a legitimate interest for any processing activity required to ensure the security of information systems, or as part of a task that is being carried out in the public interest.

Likewise, any data processing activity relating to public health can be lawfully carried out both in the legitimate interest of a data controller or company, but also to protect the vital interests of the data subject in question.

Finally, you must bear in mind that regardless of the legal basis you choose to support each data processing activity, that basis can be removed if the data subject decides to object to processing.

Your company must consider what tools are in place to allow individuals to submit their objections. For example, the right to object to direct marketing activities such as email communications could be extended through inclusion of an unsubscribe link or online communications preferences centre.

Your company should always assess the impact of a potential objection prior to identifying how you should handle an objection and implement tools offering data subjects the opportunity to submit an objection.

# The processing activities that are justified by legitimate interests

Your company and data controllers processing data on behalf of your company are legally permitted to do so based on the following legitimate interests:

## Processing of customer or client data (including direct marketing)

If there is an appropriate and relevant relationship between your company and/or data controllers acting on behalf of your company with the data subject, you may be able to apply the processing of customer or client data as a legitimate interest for processing that data. Use of the legitimate interest basis must be carefully assessed, and must include whether the data subject can reasonably expect at the point of data collection/submission that the data provided will be processed.

As previously outlined, utilising this category as a legitimate interest for processing data can be overridden in the event that the processing activity in question conflicts in any way with the personal rights or liberties of the data subject.

Your company must carefully consider whether to assume the processing of data applies to direct marketing activities. This can generally be applied through documentation; however, it is considered best practice under GDPR to obtain explicit consent for any processing activities associated with marketing (both direct and indirect).

## Processing of data to ensure network or information security

There may be scenarios in which the processing of an individual’s personal data is essential to ensure network security or information security. These activities must generally be carried out to prevent any potential data breaches or data security incidents that have the potential to compromise the availability, the integrity or the confidentiality of data that is being stored or processed.

## One-off data transfers

One-off data transfers are ‘ad hoc’ transfers that are not repetitive in nature. They tend to include only a limited number of data subjects. Use of one-off or ad hoc data transfer as a legitimate basis to support lawful processing. Again, this use of legitimate interest can be overridden in the event that such a data transfer conflicts with any one of the data subjects’ personal liberties or rights under GDPR, the Data Protection Act 2018 or any other piece of legislation.

One-off data transfers must only be applied and carried out where no other grounds for transfer can be applied to the situation.

# Assessing and communicating legitimate interests

It isn’t enough to simply state your company’s legitimate interest to support the lawful processing of data. Under GDPR legislation you must also undertake an assessment to clearly determine the legitimate interest as a legal basis for processing, as well as how and why it applies to the relevant activity.

This assessment, known as a legitimate interest assessment (LIA), should include be carried out in the following 3 steps:

1. You must identify the legitimate interest your company is choosing to apply
2. You must carry out a necessity test to decide whether the processing activity in question is necessary
3. You must carry out a balancing test to ensure the personal liberties and rights of the data subject do not outweigh the reasons your company has outlined as being necessary

Whilst there is no specific or formal format in which this assessment must be carried out, it is essential that each assessment includes the following information:

* Information regarding whether the data subject in question should reasonably expect the processing of their data, and why that expectation is present
* Information regarding whether the legitimate interests of your company and/or the data controller acting on behalf of your company are overridden by the individual rights or personal liberties of the data subject in question

When conducted correctly, a legitimate interests assessment will be able to prove that the privacy rights of any given data subject have been given due consideration prior to the carrying out of any processing activities.

If assessment of the scenario demonstrates that the data subject may not have had a reasonable expectation that their personal data would be processed for the activity in which you are attempting to apply it to, the individual’s personal rights will outweigh your legitimate interests and the activity cannot and should not be carried out.

It’s also worth noting that GDPR legislation includes transparency requirements dictating how you articulate and inform data subjects about the activities in which their personal data may be processed under relevant legitimate interests. Because individuals have a right to know how their personal data is being processed, your company has a legal obligation to communicate this in a clear and concise manner, which is easily accessible and easy to understand.

The information about legitimate interests your company applies can and should be included within your company’s online privacy policy. For guidance on what to include in your privacy policy, please consult the Privacy statement and consent template.