# Lawful Basis for Processing Data – Helpful Information.

Before you start processing personal data you have to decide a legal basis for processing. The following questions on the ICO website will help you decide the right basis for you:
[https://ico.org.uk/for-organisations/resources-and-support/getting-ready-for-the-Data Protection Act-resources/lawful-basis-interactive-guidance-tool/](https://protect-eu.mimecast.com/s/8O9hCMwmmiRz7OcRwxAj?domain=ico.org.uk)

## Legitimate Interests

This is the most flexible of the six lawful bases for processing personal data.

“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 Data Protection Act highlights some processing activities where the legitimate interests basis is likely to apply:

* processing employee or client data;
* direct marketing; or
* intra-group administrative transfers.

Although legitimate interests could apply to employee and client data is does not ALWAYS apply and you need to consider the three part test. A template Legitimate Interests Assessments is available to download on the COBRA Network Website.

Legitimate interest could exist where there is a ‘relevant and appropriate relationship’ between you and the individual. For example if the individual is your client or your employee you are more likely to have an evident legitimate purpose for using their personal data. The nature of your relationship means the processing is less likely to be unexpected or unwanted, so the balancing test will be easier.

In some instances it may be that your interests and those of the individual are actually aligned or intertwined for example; dealing with the needs of a customer.

Using this basis for processing helps **avoid bombarding people with unnecessary consent requests** and can help avoid ‘consent fatigue’. It can also, if done properly, be an effective way of protecting the individual’s interests, especially when combined with clear privacy information and an upfront opportunity to opt out.

Legitimate interests can be used for business to business contacts but again you need to apply the three-part test. Remember, you are still processing personal data when you are using and holding the names and details of your individual contacts at other businesses. You must have a lawful basis to process this personal data and if you choose legitimate interests you need to identify your specific interest underlying the processing and ensure that the processing is actually necessary for that purpose.

Assuming you can meet these first two parts of the three-part test, you also need to consider the balancing test. You may find it is straightforward as business contacts are more likely to reasonably expect the processing of their personal data in a business context, and therefore are less likely to object.

**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 do not need consent under PECR.

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 the responsibility of the third party to determine their lawful basis for their own processing.

Some questions that may help:-

* 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?

## Contract

You may have come to the conclusion that Contract is your legal basis for processing data.

A firm can rely on this lawful basis if they need to process someone’s personal data: to fulfil their contractual obligations to them; or because the individual has asked them to do something before entering into a contract (e.g. provide a quote).

“processing is necessary for the 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”

The lawful basis for contracts is likely to apply when:-

* You have a contract with the individual and you need to process their personal data to comply with your obligations under the contract.
* You have not yet got a contract with the individual, but they have asked you to do something as a first step (e.g. provide a quote) and you need to process their personal data to do what they ask.

Contract does not apply if you need to process one person’s details but the contract is with someone else

Also, contract does not apply if you take pre-contractual steps on your own initiative or at the request of a third party. Therefore, if you provide an additional quotation for a product that is recommended to protect the client’s assets but not requested or, if you are acting on the request of another sub broker Contract would not apply.

## Example given by the ICO:

An individual shopping around for car insurance requests a quotation. The insurer needs to process certain data in order to prepare the quotation, such as the make and age of the car.

In this context, a contract does not have to be a formal signed document, or even written down, as long as there is an agreement which meets the requirements of contract law. Broadly speaking, this means that the terms have been offered and accepted, both parties intend them to be legally binding, and there is an element of exchange.

The processing must be necessary to deliver your side of the contract with this particular person. If the processing is only necessary to maintain your business model this lawful basis will not apply and you should consider another lawful basis, such as legitimate interests.

A further consideration is that profiling of an individual’s interests and preferences, based on items purchased, is not necessary for the performance of the contract that the individual requested. Therefore, you cannot rely on Contract as the lawful basis for this processing. Even if this type of targeted advertising is a useful part of your customer relationship and is a necessary part of your business model, it is not necessary to perform the contract itself.

**N.B.//** This does not mean that processing which is not necessary for the contract is automatically unlawful, but rather that you need to look for a different lawful basis.

If the contract is with a child, you may need to consider whether the child has the necessary competence to enter into a contract. If you have doubts about their competence you may wish to consider an alternative basis such as *legitimate interests*, which can help demonstrate that the child’s rights and interests are properly considered and protected.

When processing on the basis of contract, the individual’s right to object and right not to be subject to a decision based solely on automated processing will **not** apply. However, the individual will have a right to data portability.

## Consent

Consent is one lawful basis for processing, and consent (or explicit consent) can also legitimise use of special category data, restricted processing, automated decision-making and overseas transfers of data.

Consent is: “any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her”

Where you want to process personal data for a reason outside your legal basis or you want to process special category data you need to consider whether consent should be obtained.

Consent means offering individuals real choice and control. Genuine consent should put individuals in charge, build customer trust and engagement, and enhance your reputation.

If you are looking to get consent you need to be specific and ‘granular’ so that you get separate consent for separate things. Vague or blanket consent is not enough.

You must always make it easy for peopled to withdraw consent and tell them how this can be achieved. This must be included in all correspondence.

It is important to keep evidence of consent. The evidence should confirm:-

* Who gave the consent,
* When it was given
* How consent was given
* What people were told.

You must ensure that any request for consent is prominent, concise, separate from other terms and conditions, and easy to understand. It must include:

* the name of your organisation;
* the name of any third party controllers who will rely on the consent;
* why you want the data.
* what you will do with it; and
* that individuals can withdraw consent at any time.

## Special Category Data

Remember if you are processing special category data you need to identify both a lawful basis for general processing under article 6 in exactly the same way as for any other personal data but you will also need an additional condition for processing this type of data under article 9 – these do not need to be linked.

This is because special category data is more sensitive, and so needs more protection. Special category data includes information about an individual’s: race, ethnic origin, politics, religion, TU Membership, genetics, biometrics (where used for ID Purposes), health, sex life or sexual orientation.

There are ten conditions for processing special category data in the Data Protection Act itself, but the Data Protection Bill will introduce additional conditions and safeguards. The following are the most likely to apply to Insurance Brokers however for a full list please refer to the Data Protection Bill itself:

1. The data subject has given explicit consent to the processing of those personal data for one or more specified purposes
2. 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
3. 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;
4. Processing relates to personal data which are manifestly made public by the data subject.

**If you have any queries please refer to a member of the compliance team**.