The Six Lawful Bases

- Lawful Basis 1 - Consent
- Lawful Basis 2 - Contract
- Lawful Basis 3 - Legal Obligation
- Lawful Basis 4 - Vital Interests
- Lawful Basis 5 - Public Task
- Lawful Basis 6 - Legitimate Interests

Before you can ever begin processing personal data, you must have at least one legitimate and lawful basis for doing so. The GDPR sets out six lawful bases for Data Controllers to consider. None of them are considered "better" than any other; some are better suited for certain kinds of processing, organisations, or Data Subjects and it's the Data Controller's responsibility to decide which one is most appropriate for the work they want to carry out.

iHASCO

Produced to support iHASCO's UK GDPR Training Courses

www.ihasco.co.uk hello@ihasco.co.uk 01344 867088

Lawful Basis 1 - Consent

Being given consent by the Data Subject is a lawful basis for processing their data and while it might seem like the most dependable basis (after all, how much more lawful can you get than being given permission?) that doesn't necessarily mean it's the best option for everyone. The Data Controller needs to weigh up whether it's appropriate and manageable and whether an individual's consent would be considered valid.

If it would be particularly difficult, costly, or time-consuming to gain consent or if consent is necessary in order to provide a service, then it probably isn't the right lawful basis to rely on. Similarly, by asking for consent, people are given a choice. If that choice doesn't really exist (i.e. if their data would still be processed regardless of whether or not they gave consent) then presenting Data Subjects with the option to give or withhold their consent would be considered misleading and unfair.

For consent to be considered valid, it must be freely-given, specific, informed, and clear.

Freely-given means that people should have a genuine choice about whether they allow their data to be processed and shouldn't be forced, coerced, intimidated, pressured, or threatened into giving consent. If a Data Controller is in a position of power over the Data Subject (if they're their employer, a potential employer, or a public authority, for example) then proving that someone wasn't intimidated or pressured might be difficult and so consent should probably be avoided.

Specific means that when consent is requested, it's obvious what it is that's wanted from them. What will happen to their data should be explicitly spelled out for every step of its journey - from the moment it's collected to the moment it's deleted. Requests for data should be obviously separate from any other requests or pieces of information (that means not hiding a request for consent in the middle of a lengthy Terms & Conditions document, for example).

People should be able to make an **informed** decision about whether they want their data to be processed which means providing them with all the information they need. As a minimum, they should be given the name of the Data Controller and, if there are any, the names of any joint Controllers, why their data is needed, what will be done with it, and they should be informed about their rights, including their right to

withdraw their consent at any time.

Lastly, it should be **clear** and obvious that someone is happy for their data to be used. This means that they should be asked to actively opt-in by ticking a box or signing a form; their consent should never be assumed by using pre-ticked or opt-out boxes or by assuming that it's somehow implied.

Lawful Basis 2 - Contract

Processing people's data in order to carry out a contract or as a first step in preparation to signing a contract is a lawful basis for processing people's data. It doesn't have to be a formal contract or even be written down, just as long as there is some agreement on the exchange of services which meet the requirements of contract law in the UK.

Also, the contract doesn't even need to have actually happened for this basis to be used. Imagine that you're an insurance broker. A customer asks you to provide them with a quote. In order to do this, you need to process their personal data. This is the first step on the way to signing a contract of services with them. If, once you give them their quote, they decide not to sign the contract and to go elsewhere, this still would have been an appropriate lawful basis to use.

While processing data doesn't have to be absolutely essential to completing the contract for this basis to apply, it does have to be more than just useful. If there are other more reasonable and less intrusive ways of carrying out the contract, then this basis can't be used. It also can't be used if the contract is with one person but requires the data of somebody else, if the data is reused for unrelated business purposes, or if any further processing takes place that isn't requested by the Data Subject.

Relying on this lawful basis means that the data subject does not have the Right to Object to their data being processed and they lose their Rights regarding Automated Decision Making. If this basis is relied on then the decision making process needs to be properly recorded.

Lawful Basis 3 - Legal Obligation

Having a legal obligation to process data is a lawful basis under the GDPR. The obligation needs to exist somewhere in a UK law, regulation, statute, or a source of guidance or advice given by the government or a related body (for example, in guidance given on the HSE website or by the ICO). Similarly, being given a court order to process data for any reason is also considered a legal obligation.

Processing people's data must be **necessary** in order to comply with the legal obligation, if there's any other way to comply which doesn't involve processing data then this should be done instead.

The source of the legal obligation (whether it's a reference to a law or regulation or a link to a government website) should be recorded in a Privacy Policy and provided to Data Subjects in a Privacy Statement or Notice.

If this basis is relied on then data subjects don't have the Right to Erasure, the Right to Data Portability, or the Right to Object.

Lawful Basis 4 - Vital Interests

Processing a person's data in order to protect their, or someone else's, vital interests is a lawful basis under the GDPR. It's perhaps the most restrictive of the lawful bases as it only applies in a very limited number of cases which tend to relate to healthcare.

By *vital interests*, the Regulation very explicitly means anything that's essential to keeping someone alive (literally only matters of life and death) as it should only be used when there's no other lawful basis to rely on or, in other words, if the person is unconscious and unable to give their consent.

What this means is that this basis can't be relied on for medical care planned in advance (even if it's essential to saving someone's life) or for large scale processing (though there is some scope for using this basis for humanitarian purposes like monitoring an epidemic or providing relief after a natural disaster, for example).

There is one more thing to consider, however. Protecting someone's vital interests is very likely to involve processing their health data. Since this is Special Category Data, it means that using this lawful basis alone often won't be enough and it will have to be used alongside one of the 10 conditions for processing Special Category Data.

Lawful Basis 5 - Public Task

Processing data in order to perform a task which is in the public interest, or in order for an organisation to exercise its official authority as laid down in law, is a lawful basis under the GDPR.

What's important for this basis to apply is not whether an organisation is a public authority, but rather what it is it wants to do. For example, a privately owned energy supplier or a water company isn't a public authority, but if the processing it wants to do is in the public interest (everyone needs energy and water, afterall) or if it has been given the legal authority to carry out certain tasks (like performing utility services, for example) then this basis may be applicable. Whatever the task being performed is or whatever power is being exercised, a record of the law, regulation, or authority which underpins it must be made.

The Data Protection Act provides a short list of examples covered by the public task basis, the list isn't exhaustive, but it includes:

- The administration of justice
- Parliamentary functions
- Statutory functions
- Governmental functions, and
- Activities that support or promote democratic engagement

If this basis is relied on then Data Subjects do not have the Right to Erasure or the Right to Data Portability.

Lawful Basis 6 - Legitimate Interests

The final lawful basis is if processing is necessary for an organisation to achieve its legitimate interests. That may sound like a catch-all term which gives organisations the freedom to justify doing just about anything with people's data and, in a very loose way, it sort of is - though there is a catch. Due to the flexibility of legitimate interests as

a lawful basis, there are extra checks and balances which need to be considered (and documented) before it can be relied on.

Specifically, a Legitimate Interests Assessment (LIA) will need to be carried out. This is a kind of informal risk assessment to help decide and demonstrate whether this basis is appropriate to use.

The LIA is made up of three tests - the Purpose Test, the Necessity Test, and the Balancing Test.

The Purpose Test is all about establishing why people's data needs to be processed. Data Controllers should think about what they're trying to achieve; what the benefits are; who it benefits (to both them & the Data Subject); and what the impact would be if they didn't process the data.

The Necessity Test is fairly straightforward. Data Controllers should think about whether they really need to process data at all - is it essential or is it just useful? And, are there any less intrusive ways of achieving their aims?

Finally, there's the Balancing Test. This is where Data Controllers need to weigh their interests against the Data Subjects' interests. They should consider the impact that processing might have on their rights and freedoms; the impact that a breach might cause; how sensitive their data is; what their relationship with the Data Subject is; and, whether the Data Subject would be likely to object if they'd have been asked for consent instead.

It's easier to justify using this basis if the purpose for processing could be reasonably expected by the data subject.

For example, a customer who gives personal data to their bank to open a current account could reasonably expect that their data might be used to help prevent fraud. This not only benefits the bank, but also the individual and every other customer as well. However, if the bank chose to sell their customers' data to local businesses so that they could send out marketing campaigns not connected with the bank itself, then this wouldn't be justifiable as it couldn't be reasonably expected by customers when they handed over their data.

If this basis is relied on, Data Subjects do not have the Right to Data Portability. However, if this basis is used for Direct Marketing purposes, then people's Right to Object becomes absolute.