

# GDPR IS COMING 25 MAY 2018

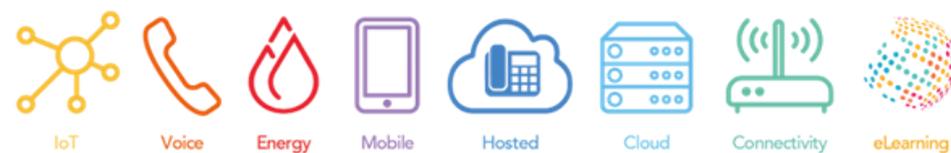
QUICK GUIDE TO GET YOU READY





## LEGAL BASIS FOR PROCESSING PERSONAL DATA

You must have a valid lawful basis in order to process personal data. Processing data basically means collecting, holding or using personal data. There are six legal bases for processing and you will have to show that the need for processing is necessary. Meaning you could not achieve the same result without processing the data. If the processing is not necessary, you won't have a lawful basis. You should decide on your lawful basis before you begin and you should document it. Your privacy notice, which should be included in email correspondence, should include your lawful basis for processing, as well as the purposes of the processing.





## What are the 6 Legal Bases?

The lawful bases for processing are set out in Article 6 of the GDPR. At least one of these must apply whenever you process personal data.

- (1) Consent: the individual has given clear consent for you to process their personal data for a specific purpose.
- (2) Contract: the processing is necessary for a contract you have with the individual, or because they have asked you to take specific steps before entering into a contract.
- (3) Legal obligation: the processing is necessary for you to comply with the law (not including contractual obligations).
- (4) Vital interests: the processing is necessary to protect someone's life.
- (5) Public task: the processing is necessary for you to perform a task in the public interest or for your official functions, and the task or function has a clear basis in law.
- (6) Legitimate interests: the processing is necessary for your legitimate interests or the legitimate interests of a third party unless there is a good reason to protect the individual's personal data which overrides those legitimate interests.

We believe that in the majority of cases companies operating in the B2B environment will either opt for consent or legitimate interests as the lawful basis for processing personal data. This does not mean that any of the others should be discounted, but for the sake of this article we will only address these.



IoT



Voice



Energy



Mobile



Hosted



Cloud



Connectivity



eLearning



## Legitimate Interest

Legitimate interest is a more flexible lawful basis, it can be used when you process data in ways that people would reasonably expect, and your use will have a minimal privacy impact. You can rely on legitimate interest 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.

You should avoid using legitimate interest 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.

When using legitimate interest as a lawful basis for processing data you will still need to show why. You can use a legitimate interest assessment (LIA); which is a light-touch risk assessment, to assess whether it applies. The Data Protection Network have an excellent guide and template for an LIA. 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.

If you are relying on legitimate interest for direct marketing, the right to object is absolute and you must stop when someone objects.





## Consent

In a nutshell, to obtain consent you need to ask people to positively opt in, this can be verbally or via email. You cannot use pre-ticked boxes or methods of default consent. You need to say why you need the data and what you will do with it, make it easy to understand and give a clear means of opting out. You need to name your organisation and any 3rd parties you may share the data with, you need to keep records to document consent.

## Disclaimer

We have given a very brief overview of the GDPR here. Any comments are our own and not in any way legal advice. Both the ICO (Information Commissioners Office) and the DPN (Data Protection Network) have produced excellent guides and templates for GDPR compliance and we would recommend visiting both sites and downloading the resources available.

With anything new there is always a degree of fear, and also companies who would look to stoke up this fear to generate profit. We do not believe the GDPR will mean the end of direct marketing within a B2B environment. Taking sensible measures to ensure your compliance and paying particular attention to how you document your lawful reason(s) for processing personal data should ensure you comply with the GDPR.

