BRP Consulting Ltd

GDPR & the transparency requirement –
compliance for small organisations

Transparency – what the law requires
Why small businesses and organisations need to be transparent about their data processing

What goes in a privacy policy?
The art of producing accurate yet simple information

Are you compliant?
You may not need to do much, but have you done enough?

How we can help
Addressing any gaps with fixed-fee, bespoke documentation

Introduction
Michael Brunker CIPP/E CISM
BRP Consulting

It is tempting to think of GDPR as a 2018 moment in time, and that you have 'ticked all the boxes'. However, many smaller organisations don't realise they aren't properly meeting the 'transparency' requirement of GDPR and wrongly believe their website privacy notice to be adequate.

This paper seeks to explain the law in terms that relate to such organisations, assist you to assess your current level of compliance and, if you need to make improvements, how we can help.

Transparency – what the law requires

Whatever the size or nature of your organisation, if you process the personal data of other people, you must consider the impact of GDPR.

Unless very limited exemptions apply, you are required to tell those people a number of specific facts about your processing – in other words to provide 'transparency'.

The Information Commissioner ('ICO') states that *"Individuals have the right to be informed about the collection and use of their personal data [and] you must provide privacy information to individuals at the time you collect their personal data from them".*

This can be done with the publication of a 'privacy policy' which must accurately and fully describe what you do with personal data. As well as making your organisation look privacy-aware and professional, compliance can be seen as a one-off insurance premium against the risk of regulatory or legal issues and the high legal costs they inevitably incur.

What goes in a 'privacy policy'?

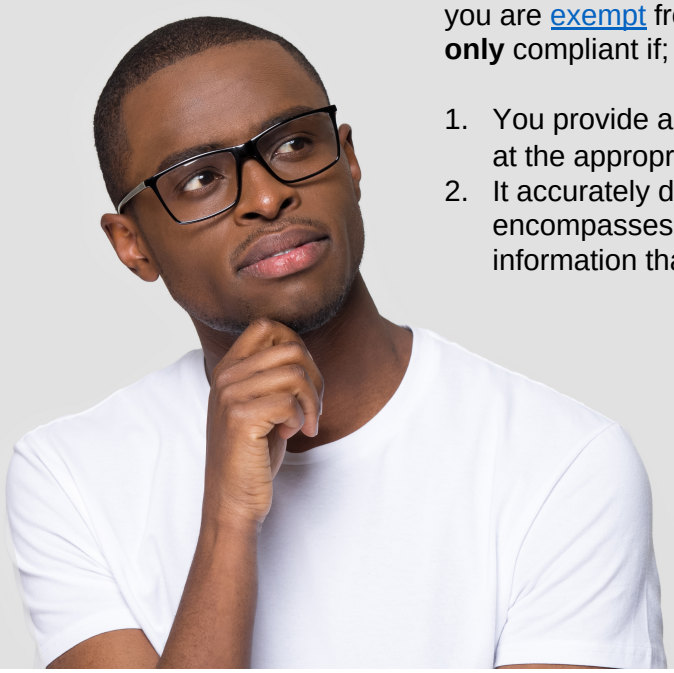
A privacy policy (or privacy notice – they are effectively the same thing) is not a legal contract. It's more of a 'declaration' of how and why you process personal data. Indeed, the ICO requires controllers to provide information which is *"concise, transparent, intelligible, easily accessible, and (in) clear and plain language"*

Crucially, it must contain between seven and sixteen specific pieces of information (depending on the nature of the processing). While any controller can perhaps identify which are relevant, the trick with a privacy policy is to:

a) Fully and accurately catalogue all processing activity;
b) Determine which of the 'legal bases' on which the processing is justified (there are often more than one);
c) Define the 'legitimate interests' of the organisation and balance those with the 'rights and freedoms' of the data subject and;
d) Identify and justify retention periods.

Without a good understanding of privacy laws and knowledge of how specific types of organisation fit within them, producing a fully-compliant policy can be difficult.

Are you compliant?



If the data you process is 'personal' (and unless you are exempt from the requirement) you are **only** compliant if;

1. You provide a privacy policy to data subjects at the appropriate time and;
2. It accurately describes your processing and encompasses all of the transparency information that GDPR requires.

Remember: You may have a 'privacy policy' link on your website. If it came 'off the shelf' with the website design, it will almost certainly **not** be sufficient. Have you checked?

How we can help

Firstly, there are a few reasons why **we** should help!

- DIY internet templates cannot help you make the right choices in compiling a policy and, if you get it wrong, it remains your liability;
- Specialist privacy lawyers are often 'overkill' for smaller organisations and commensurately expensive;
- Using a professionally-qualified practitioner minimises risk and legal liability

What is our approach?

- We will assess anything you already have in place and will **not** try to sell our services where they are not required;
- If you do need one, we will design you a privacy policy bespoke to your actual processing activity;
- The policy will be based on a template which aligns with your particular type of organisation, while ensuring that any individual factors are reflected. This minimises time and costs;
- We charge a one-off, fixed fee - dependent on the complexity of your processing – of between £295-495.

We are more than happy to discuss privacy notices, or any other aspect of GDPR, without obligation. Please feel free to get in touch here or via info@brpconsulting.co.uk