Privacy Notice or Privacy Policy?

When working for a potential client, the first thing that I look at is the company's website. This is the shop window for that company, and a quick sign of how compliant or not they may be with GDPR. One thing I see time and time again which gives a clue that the company might not have fully grasped GDPR compliance, is having a page on the website for their 'Privacy Policy'.

'But you're wrong!' I hear you cry. My website has a Privacy Policy and it tells my potential clients where we got their data from, what types of data we might use, how we will use their data and why, how long we will hold it for, the lawful basis for using their data, who we might share their data with, and how long we will keep it for. It also informs them of all their data protection rights.

Maybe that's right, and if it contains all of that information, then that's excellent. But you're actually talking about a Privacy *Notice* rather than a Policy.

If you're a financial adviser who holds all client data on a wealth platform, you may rely on your network or an external compliance company's Privacy Notice and have nothing on your own website or available for your clients that can be posted or emailed to them if you don't have a website.

Quite often, these external service providers will have a specific section in their Privacy Notice which states something like *If you access our services as a client of our customer (e.g. your financial advisor), this privacy notice does not apply, and your financial advisor's privacy notice explains how your personal information is used. We will process your personal data only as directed or permitted by our customer. Please contact your financial advisor to obtain a copy of their privacy notice*.

If your financial advice network or platform provides you with your own website, then they may provide you with a generic Privacy Notice, which is a start, but you will still need to have one of your own that you can provide to your clients.

The UK GDPR regulator (the ICO) states that if your company holds any form of personal data, such as client names, addresses, contact numbers, email addresses, etc, and processes (or uses) them, even to just store them, then you must have some sort of Privacy Notice that explains how you will use it in advance. Every time you send a client an email, you are processing that data and so you must have a Privacy Notice that you can send to them or that they can view on your website.

So what's the difference between a Privacy Notice and a Privacy Policy? Very simply, a Privacy Policy is your internal procedure document that explains why you are using client data, how long you will keep it for, store and dispose of it, how you will use ADM fairly, and what you will do if you have a data breach or if someone makes a Subject Access Request or exercises any of their other 'data rights'. It will also hold records of when you carried out checks on any company you use to process client data, and data flow maps to show how data flows or moves around your company. A Privacy Notice is how you tell your clients and employees how your company uses their personal data.

About



Sarah Hodgkin-Bates is a qualified GDPR Practitioner and director of Fintect Limited www.fintect.co.uk If you have any comments or questions about this article or GDPR in general, please email her at sarah@fintect.co.uk

© Fintect Limited