What does data protection mean?

The UK GDPR/Data Protection Act [DPA] 2018 provide a set of rules or a framework that any company that handles or 'processes' an individual's 'personal data' or information must follow. There are additional rules if a company is handling an individual's 'sensitive personal data'.

Data protection covers all your company's procedures for processing personal data by paper, telephone, email and computer/digital. There are also rules around how you store physical/paper and digital information or computer files as storage is also counted as processing data.

What is 'personal data'?

It's any piece of information that can be used to identify a living individual. This might be just one piece of information, such as an unusual name, or it might be a combination of different pieces of information which, when put together, can identify an individual. Examples of this might be name, postal address, date of birth, bank details and perhaps an email address.

It does not cover people in their profession/work within a company, unless they are a 'sole trader', in which case those individuals are also covered by the UK GDPR/DPA 2018.

What is 'sensitive personal data'?

This is information about an individual that the UK GDPR/DPA 2018 requires a company to take extra care of and might include images, gender, race, political views, medical history, etc.

Why is data protection important?

There is the threat of enforcement action or fines from the ICO, but a financial penalty isn't the only problem a financial adviser might face. The FCA might also take action for non-compliance.

A direct follow-on from any regulatory action would be a drop in your company's reputation The ICO regularly publishes any enforcement action or fines it makes, and this information is freely available on their website.

By ensuring that your systems for handling personal data are up to date, with no duplication of work or unnecessary work, a company can often find efficiencies in time and costs. Firms often find that reviewing their systems and processes can result in efficiencies by cutting out unnecessary work, or handling personal data more efficiently by using new technologies.

Following on from this, any client can make a Subject Access Request [SAR] at any time. This is a formal request for a firm to provide an individual with a copy of all the personal data the firm is using. In addition, a client has the right to request that their personal data is given to them in an electronic format that can be transferred to another firm if they move their business. If you know where a client's personal data is stored, you can retrieve it relatively quickly and easily and not be faced with overwhelming time and effort (and associated costs) to provide the information.

If your IT systems are properly secure, you will reduce the risk of being hacked and the personal data you use being stolen or lost, and also reduce the risk of a 'ransomware' attack.

Compliance with the DPA 2018 can mean that your professional indemnity and cyber liability insurance premium is reduced, resulting in a direct cost saving to your firm.

And finally, the general public seem generally to be more aware of how their personal data can or cannot be used as they have certain 'rights' under the UK GDPR/DPA 2018. Data protection is just

© Fintect Limited

one way that an adviser can engage with their clients, and demonstrate a level of customer care by showing that the company takes the security and use of their clients' personal information seriously.

What action should my company take to comply with the UK GDPR/DPA 2018?

1. Complete a **Data Inventory** covering paper and electronic records which states what personal data the company has, why it is used, how it is used, and how long it can be kept for.
2. Carry out any **Data Protection Impact Assessments** that you might need to. This is a review of any processing of data that is likely to result in high risk to individuals, including use of CCTV, 'sensitive personal information', large scale processing, etc.
3. Carry out any **Legitimate Interest Assessments** that might be necessary. This is a process whereby you judge if your reasons for processing someone's personal data is more important than their rights. An example might be carrying out any marketing activities to potential clients who have not already contacted you or given their consent for you to send information to you.
4. Produce **Data Flow Maps** which show how data 'flows' (enters, is used and stored) around a company in an easily understandable way.
5. **Review contracts** you may have with any suppliers or contractors who you use to process personal data. Are their own data protection procedures adequate or do they need to improve?
6. Following on from this, produce a **Data Protection Policy** which documents how the company will process an individual's personal data and includes all items in points 1-5 above. This should also include information for employees on how you will use their personal information during their employment contract with you, as well as a list of all suppliers used.
7. Provide the Data Protection Policy to all employees and give **adequate training**. They should understand what they are permitted and forbidden to do with personal data that they process, and signing an **Employee Declaration** is one way of demonstrating this.
8. Produce a fully compliant **Privacy Notice** for your website or any individual that asks for a copy of it. This tells an individual how the company will be using their personal data, why they are using it, and other required information.
9. Carry out a **Data and System Inventory** of your company IT systems. Ensure your IT systems are secure and able to be accessed only by authorised people. Use this information to produce your **IT Security Policy** which records all details about the IT system.
10. **Review your website**.
    a. Make sure you have a **cookie banner** and **cookie policy** which explains what cookies your website uses and gives individuals the ability to choose which types of cookie they are happy to allow while they are visiting the site.
    a. Ensure your **Privacy Notice** is able to be easily accessed, and is ICO compliant.
    b. If you are asking individuals to complete a **contact form**, is it secure and does it tell the user why you are asking for the information with a clear consent statement?

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