mercia
incorporating swat
Wilmington Professional

# GDPR is Here to Stay - Everything You Need To Know

*As many know, GDPR came into force in May 2018. However, the Information Commissioner has confirmed that a relatively light touch will be operated for 12 months, to allow firms to get to grips with the regulations. This is not an excuse for firms to do nothing and all would be well advised to make a clear and documented plan for compliance in this area, even if some aspects have yet to be finalised.*

## Understanding the size of the problem

The first step towards compliance is to understand the size of the problem. It is hard to implement a plan and think about the areas that need to be dealt with and where problems might arise. It would appear then that the task is twofold: firms need to ensure they have done some training; and then need to review their own digital records.

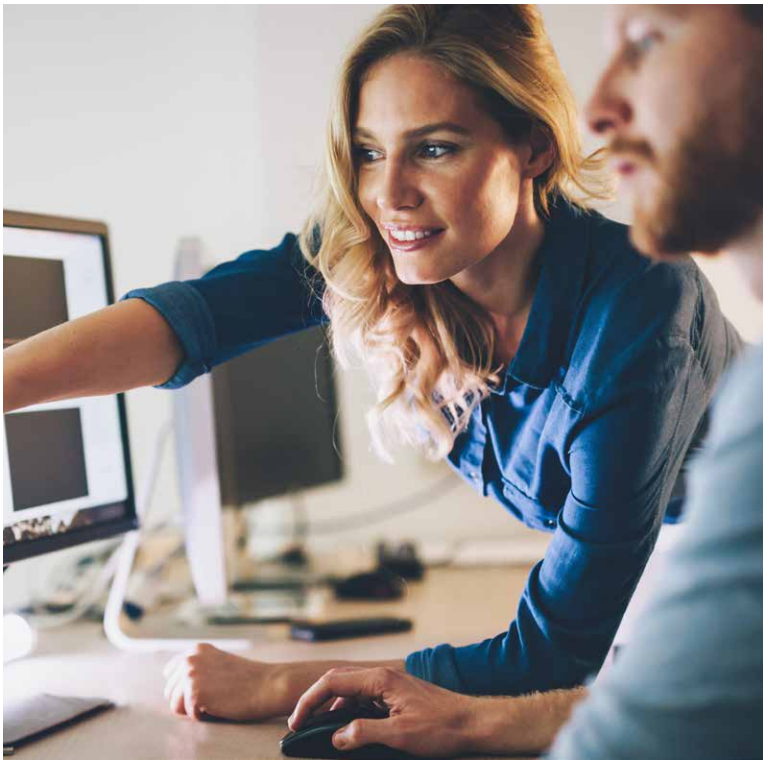
In terms of training, staff generally should be made aware of the fact that GDPR is now in force and the kind of issues they are likely to face. This could be done by general reading or through attending training.

The person responsible for GDPR compliance would generally need a higher level of training and this could be done by using a specialist company or reading through the documentation on the Information Commissioners website. Of course, once the firm's appointed person was sufficiently knowledgeable they could run their own training for the teams in the office.

Once firms know what to look for, it would be sensible to do an audit of the firm's data and consider how much of an issue this brings to light. This would need to be done partly by looking at the IT setup generally (where is the data? What form is it in? Why is it used and who can access it?). But also more broadly by talking to staff. For example, do staff use spreadsheets? How is information stored? How is data sent to clients? Can data be accessed remotely?

Once the firm has a good understanding of the rules, what data they have and how it is used, they can then look to other issues they need to tackle.

In terms of guidance for firms visit the **ICAEW GDPR hub and the Information Commissioners website**. Certainly, the latter has been well received by many individuals as the material is widely applicable to other businesses as well as accountants; and of course it's all free.



# Communication with clients

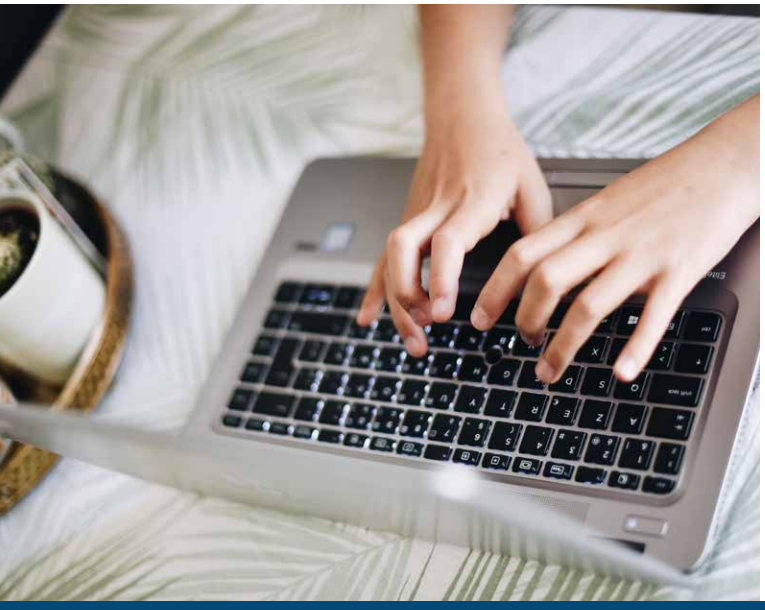
Once the firm has trained staff and understood what data it has, the firm should then be ensuring that engagement letters have been updated or an addendum has been sent out so that clients are aware of the firm's policies with regard to data protection and data retention. Much of this documentation is standard and will not need to be signed by the client – the firm is just stating how it collects and processes data.

For example, the firm will produce a paragraph (often called a Privacy Notice) that confirms how the firm will deal with data if engaged to prepare a tax return. This standard wording can be found on the **ICAEW GDPR hub** and will be repeated for other services.

Firms will also need to develop data retention policies to describe how long they should keep data. This can be specific to the firm and does not have to be a standard period, but the firm will presumably start by looking at how long HMRC can look back at the data and PII providers might also have opinions on how long to keep data. The firm's policy will need to be communicated to staff and consideration given to how this is implemented in practice, along with how often data is purged from the system.

# Communication with others

Firms should also be confirming with key suppliers and subcontractors how they should deal with data. For example, there is little point in the firm being GDPR compliant if it then sends data to an external processor or IFA for them to not be compliant in the way they handle data. Firms should also ensure that any cloud software providers have confirmed they are GDPR compliant. This is particularly important for non-EEA providers as they will have no automatic requirement to comply with this European regulation.



Firms might also be getting questions from clients who are looking for confirmation that they are compliant, often clients will not rely on the engagement letter and so firms will need to reply carefully.

To enable the firm to demonstrate to the wider world that it has good procedures, it could look to get its procedures certified. This will help the firm to review its procedures and enable it to stand out from its competitors. ISO 27001 is certainly an option, but Cyber Essentials might be a better starting point.

# Cyber Essentials

In conjunction with the government, the ICAEW launched Cyber Essentials to help UK businesses protect themselves.

Cyber Essentials aims at the most basic technical controls (5 in total) and doesn't supersede other standards, such as ISO27001, but is a base level of cyber hygiene which all businesses should have in place. It won't prevent all security breaches, but it will raise the bar significantly for many firms who are currently very vulnerable.

It incorporates a 'badge' system to demonstrate compliance with the controls. To get a Cyber Essentials badge, a business fills in a questionnaire on the controls, which is then validated by a qualified professional.

The firm has to consider how it communicates to all parties it interacts with and the above points need to be dealt with. A certification like Cyber Essentials can help promote a powerful message that the firm is good with data, which might be a vital message in this digital world.

There are a number of ways in which firms may wish to communicate with clients. For example, in relation to the service directly provided, to impart information about regulatory changes or to encourage them to engage the firm in new products and services.

In principle, firms should have good justification as to why they are communicating with individuals and how they are using that person's data. For example, with updated engagement letters in place, firms can communicate with individuals regarding services they have been engaged to perform, such as personal tax returns. It would be crazy to suggest that a firm cannot contact an individual about his tax returns if the firm has been asked to prepare it!

However, things get a little bit more challenging where the firm is looking to communicate another service or issue. In principle though, if the firm is communicating to an existing client about issues that will affect that client, then that would be a lawful basis for communication and so no consent is needed (although it is recommended to try and encourage existing clients to 'opt-in' to your marketing communications nevertheless, as this provides you with an increased level of security). This would cover newsletters and other direct mailing about related services offered by the firm, this is

referred to as 'legitimate interest'. Making Tax Digital is a prime example of this – clients would expect you to tell them how MTD affects them and how you can help, even if they had not specifically asked for information on it. However, the basis of communicating with clients (by way of 'legitimate interest' alone) is of course over-ruled where the client has specifically opted-out (i.e. asked to be removed from communications).

The other way to justify communicating with clients is to obtain their permission or consent. This is often discussed in the press and you will have no doubt been contacted about this problem by various online retailers, but most accountants do not have the systems to properly record consent. If you do want to consider recording consent, it must be specific and documented.

Where you have had no contact at all with a prospective client, it will be much harder to justify any lawful basis for sending marketing communications. Great care should be taken in such circumstances to avoid sending communications to non-clients who have not opted-in to your communications or engaged with you in some way. Ensuring you have documented opt-in's for such prospective clients is therefore critical.

On the other hand, informing existing clients of related services that the firm can provide, carries far less risk than attempting to send marketing communications to prospective clients with whom the firm has had no dealings with at all.

# Policies and procedures

While much of the focus of GDPR is on the marketing and document retention issues, the regulations also refer to ensuring that data protection (i.e. data security) is part of your firm's processes by design. Firms should therefore ensure that they have good procedures not just for contacting clients but also for generally handling data and devices that can access the firm's network.

For example, firms should have clear policies about encrypting and securing laptops, being able to remotely wipe mobile devices, ensuring staff cannot use their personal devices on the network without suitable security and, of course, making sure the ubiquitous USB memory sticks are destroyed or encrypted.

Firms might want to also think about physical security over digital devices as well as the office environment and paper records themselves. For example, in Mercia incorporating SWAT, we are told that laptops must be removed from vehicles before being left overnight as they are not insured, and all filing cabinets should be closed at night if they contain client records inside them. There has even been a case at a firm whose cleaner was questioned, as she had unlimited access to the office when everyone else had left!

When firms are visited, it is often found that there is no clear guidance as to the use of IT, the security of those devices and the way in which emails or the internet are used by staff. It is also recommended that firms stipulate what software can be installed and used by staff. Firms would do well to document the thoughts in these areas and to then communicate them to staff. The QAD in the review of firms often question whether firms have properly trained staff in their procedures in such a way that staff understand it.

The process should also include confirmation that staff understand a data breach and the need to internally report. For example, recently an IT consultant suggested that whenever unencrypted USB devices, mobile phones or other devices are lost then that would be reported as a data breach even though we are not sure that the data has been accessed by a third party.

There have been other firms take the opportunity of reminding staff to take great care over emails and making sure they are actually from the client before actioning them. There are at firms where an email supposedly from a client tried to instigate transfer from the clients account and yet it turned out it was fake. So firms should ask themselves are all the staff suitably data savvy as part of all aspects of professional life and not just thinking data protection is about marketing or emailing.

It is not just deliberate attacks, many people receive an email meant for somebody else. It is very easy to send an email to the software suggested recipient only to realise it is the wrong David. If the email includes personal data that may be a data breach.

# How we can help

We provide a range of tools to help support your firm. Please contact our team for information about our range of products and courses **enquiries@mercia-group.co.uk** or **0330 058 7141**.