BE PREPARED

Preparing your practice for the new General Data Protection Regulation (GDPR)

October 2017

MyDocSafe™

btc SOFTWARE

INTRODUCTION

The General Data Protection Regulation (GDPR) becomes law on 25 May 2018. It will come into force across the UK and EU and will apply to any organisation that does business with EU citizens. The UK has committed to apply the EU's GDPR standards in its preparation for Brexit. In September 2017 the Government set the UK Data Protection Bill in motion to become law.

In this practical guide, BTCSoftware has joined forces with MyDocSafe to explain how small and medium-sized accountancy practices can prepare for GDPR.

Irrespective of size, location and client spread, all UK accountancy firms will be affected by GDPR. The new regulation seeks to make the UK and EU's data protection laws meet the demands of the digital world we now live in – where an ever growing volume of data is processed. It also wants to empower people to take control of their data, have the right to move or delete their data and establish personal data protection as a basic human right of EU-based individuals.

The Data Protection Bill currently in the process of becoming UK Law sets new standards for protecting data in accordance with the GDPR and will provide clarity on the definitions used in the GDPR in the UK context. It will replace the Data Protection Act 1998.

Does GDPR really affect accountancy practices?

The answer to this is a resounding YES! Data held in an accountancy firm which will be covered by the GDPR includes client data for processing client work, marketing data such as contacts and prospective client details, supplier data and staff data. The Regulation sets out clear requirements to be followed by anyone processing personal data for EU-based individuals.

Failure to comply can result in fines of up to 4% of global annual revenue or 20million Euros – whichever is greater.

It's therefore important to get up to speed both with the implications of GDPR for your firm, and start the process of meeting the compliance criteria. This practical guide will give you key markers for your GDPR Roadmap.

CONTENTS

OVERVIEW

Many of the GDPR's main concepts and principles are very similar to those in the UK's 1998 Data Protection Act. So, if your firm is complying with the current law, then it will face less of a learning/implementation curve. There are, however, a number of new elements which you'll need to build into your data processing, data policies and data security approach.

5 key principles of the GDPR

There are 5 underpinning principles for the GDPR which your firm will need to demonstrate compliance with:

1. Lawfulness, fairness and transparency – you will need to demonstrate you have consent for storing and using a person's data.

2. Purpose – data can only be collected and used for specific, explicit and legitimate purposes. This means any further processing of data is not allowed, although archiving, research and statistical purposes may be ok.

3. Adequate, relevant and limited – this means data has to be kept up to date, the use of it limited to only what is necessary and storage of it only for as long as is necessary.

4. Securely stored – there is a considerable onus in GDPR on the security of storing data. Failure to comply will lead to those hefty fines we mentioned in the Introduction.

5. Controller compliance - your firm will have to have a designated Data Controller and they will need to manage and be able to demonstrate your firm's compliance with GDPR. There is now greater accountability for Data Controllers.

What constitutes personal data?

GDPR focuses on the personal data organisations hold on individuals. It's worth then clarifying what GDPR counts as personal data.

" *Personal data is any information relating to a living, identified or identifiable natural person* "

This could be a person's name, the owner of a business, any information used to identify an individual (such as an ID number), location data, online identifiers or other factors specific to that person's identify. So business contact details are definitely included as are digital information such as IP addresses, cookie strings or mobile device IDS.

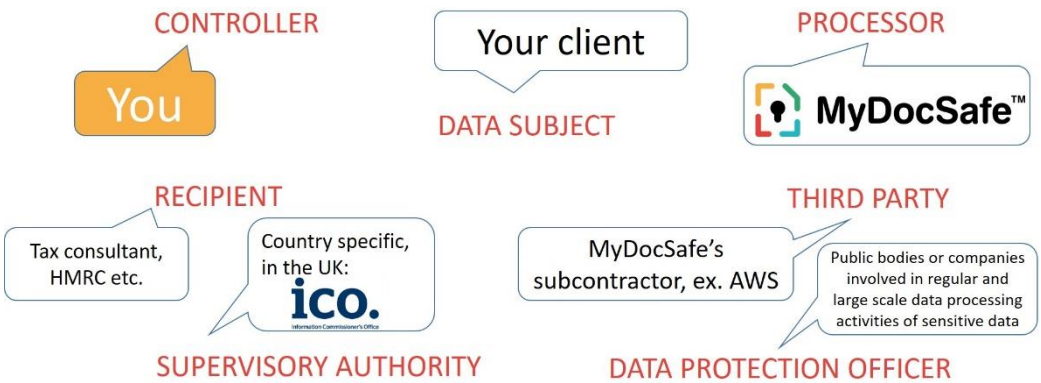
Be also aware that the GDPR has defined a sub-category of personal data which warrants extra protection and care. This is called sensitive data and includes information such as a person's racial or ethic origin, political opinions, religious beliefs, trade union activities, physical or mental health, genetic data, biometric data or details of criminal offences.

ACTION:

Be clear what data you hold within your firm and how you process it. With the GDPR you will need to demonstrate you are processing data legally according to its standards. Knowing what data you hold and use across your firm will help you to comply with the new regulations.

Understanding the GDPR roles in your firm

It is important to understand the different role players involved in the data your firm stores, as defined by the GDPR. We've shown how these roles (marked in red in the diagram) would typically apply to a small or medium accountancy practice and their systems – in this case using MyDocSafe software, although other practice systems' software would count as data processors.



DATA CONTROLLER - A natural or legal person, public authority, agency or any other body who alone or jointly with others determines the purposes and means of the processing of personal data. For example, a Controller can be an organisation or Chief Information Officer.

DATA SUBJECT- A person who can be identified directly or indirectly by means of an identifier. For example, an identifier can be contact details, a national identifier, a credit card number, a username or a web cookie.

THIRD PARTY - A natural or legal person, public authority, agency or any other body other than the Data Subject, the Controller, the Processor and the persons who, under the direct authority of the Controller or the Processor, are authorised to process the data. For example, subcontractors or outsourced support.

DATA PROCESSOR - A natural or legal person, agency or any other body which processes Personal Data on behalf of the Controller. For example, an administrator or secretary. A Processor can also be a cloud service provider or an outsourcing company

DATA PROTECTION OFFICER – This is typically an individual working for a Controller or a Processor with extensive knowledge of the data privacy laws and standards. The Data Protection Officer (DPO) shall advise the controller or the processor of their obligations according to the GDPR and shall monitor its implementation. The DPO acts as a liaison between the controller / processor and the supervisory authority. In a small or medium-sized firm this may be a member of your team or an external specialist/compliance consultant.

SUPERVISORY AUTHORITY - An independent public authority established by a Member State (known as the National Data Protection Authority under the current EU Data Protection Directive) or auditing agency.

RECIPIENT - A natural or legal person, agency or any other body to whom the personal data is disclosed. For example, an individual, a tax consultant, an insurance agent or an agency.

Data Controller vs Data Processor responsibilities

It's important to understand the different roles Data Controllers and Data Processors have under GDPR. See the table below for a brief comparison. It's important that whoever your Data Processors are, you have contracts in place using standard clauses provided by the Information Commissioner's Office).

Area	Data Controller	Data Processor
Responsibilities	• Writes guidelines for the firm, communicates them within the firm and regularly updates them • Subscribes to codes of conduct • Undergoes GDPR certification for the firm • Initiates logs showing who has accessed personal data and monitors them • Restricts access rights to data to those who do not need it • Introduces and monitors data protection measures such as: encryption	• Supports Controller in writing guidelines and following them etc • Subscribes to codes of conduct • Undergoes certification
Data protection compliance by designer and by default	Establishes and monitors: • Pseudonymisation to protect identities • Data minimization procedures Automates data holding period Ensures data sharing cannot be done without data subject's consent	Determines risks posed by processing and the of implementing protective measures

ACTION:

Assign who in your firm will be the designated Data Controller and identify the different data processes in operation in your firm's approach. Ensure the designated Data Controller is familiar with their new responsibilities under GDPR. Give time for training and familiarisation where needed.

Be aware the results of a consultation on GDPR guidance for the contracts and liabilities between controllers and processors is expected to be published later in 2017.

THE IMPORTANCE OF CONSENT

The GDPR gives a new legal basis for processing data. Of course Accountancy firms naturally need to process data as part of their work for clients. Under the GDPR this will still be the case. The difference is the need to inform clients what you are doing with their data and get their consent to do so. Your firm will be expected to demonstrate that it has obtained active consent and is processing data in accordance with that consent.

The GDPR's legal definition of consent is:

"any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her"

Things to bear in mind about consent and your practice's operations.

Consent means offering individuals genuine choice and control. It requires a positive opt-in, so you can't use pre-ticked boxes or any other method of consent by default.

You should check your consent practices and your existing consents and refresh them if they don't meet the GDPR standard. In doing so, remember

- Explicit consent requires a very clear and specific statement of consent.
- Consent requests should be separate from other terms and conditions.
- With consent documentation, be specific and granular. Vague or blanket consent is not enough. So be clear and concise.
- Name any third parties who will rely on the consent.
- Make it easy for people to withdraw consent and tell them how.
- Avoid making consent a precondition of a service.

Going forward it is important to keep evidence of the consents you have obtained – who, when, how, and what you told people. Also keep your client consents under review, and refresh your procedures if anything changes.

ACTION:

It is highly likely that your firm's current privacy notice(s) and policies will need updating in preparation for the GDPR.

GDPR-friendly questions to answer in future consent and privacy notices are:

- Is my data being processed? If so, what under GDPR categories?
- For what purpose?
- Who are the recipients of my data? Where are they located?
- What are the safeguards put in place to ensure compliance with GDPR?
- For how long will the data be stored?
- What rights do I have regarding the data?
- Am I being profiled?

KNOW THE RIGHTS OF DATA SUBJECTS

The GDPR gives people new rights concerning the use of their personal data. These are:

The right to be informed – as a firm your obligation is to provide 'fair processing of information', typically through a privacy notice. You need to be transparent in how you use personal data.

The right of access - Under the GDPR, individuals will have the right to obtain:

- confirmation that their data is being processed
- access to their personal data, and
- other supplementary information – largely corresponding to the information provided in a privacy notice.

The right to rectification - Individuals are entitled to have personal data rectified if it is inaccurate or incomplete. If you have disclosed the personal data in question to third parties, you must inform them of the rectification where possible. You must also inform the individuals about the third parties to whom the data has been disclosed, where appropriate.

The right to erasure - This is also known as 'the right to be forgotten'. The broad principle underpinning this right is to enable an individual to request the deletion or removal of personal data where there is no compelling reason for its continued processing.

The right to restrict processing - individuals have a right to 'block' or suppress processing of personal data. When processing is restricted, you are permitted to store the personal data, but not further process it. You can retain just enough information about the individual to ensure that the restriction is respected in future.

The right to data portability – this allows individuals to obtain and reuse their personal data for their own purposes across different services. It allows them to move, copy or transfer personal data easily from one IT environment to another in a safe and secure way, without hindrance to usability.

The right to object - Individuals have the right to object to:

- data processing based on legitimate interests or the performance of a task in the public interest/exercise of official authority (including profiling)
- direct marketing (including profiling), and
- processing for purposes of scientific/historical research and statistics.

Rights in relation to automated decision making and profiling – here the GDPR provides safeguards for individuals against the risk that a potentially damaging decision is taken without human intervention. It is important to identify whether any of your processing operations constitute automated decision-making and consider whether you need to update your procedures to deal with the requirements of the GDPR.

Source: The ICO

ACTION:

Ensure your firm's procedures and working practices support the rights of individuals under the GDPR. The Information Commissioner's Office has helpful guidance on their website – click here for more information.

SECURITY

How securely your store people's data is also a key concern of the GDPR legislation.

This means you need to have in place robust security measures around your data processing and data storage. Gauge the security risks of your current systems now so you have time to implement changes. You need to be sure your systems are resilient to protect people's confidentiality and keep their personal data safe and secure.

In doing so, consider technical security measures to protect people's identities in your data, such as encryption, pseudonymisation. Talk to your software providers about security measures they have in place. Also introduce a regular secure back-up procedure and regularly test, review and assess the security processes you have in place.

In the case of a data breach...

The GDPR defines a breach of security as one which 'leads to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed".

A breach can take many forms: from a person entering a building and accessing or even taking personal data, to a cyber attack. Also a lost phone, laptop or USB-stick can also be regarded as a data breach. If you experience a data breach the GDPR obligates you to notify your supervising authority within 72hours of becoming aware of the breach, unless risks are minimal. In the UK, the supervising authority is the Information Commissioner's Office. If you are late in reporting you must say why and bear in mind the sizeable fines at stake.

Your firm's Data Processors must notify the Data Controllers of data breaches and in doing so include:

- The nature of breach
- Likely consequences
- Provide point person's contact details ?????
- Proposed measures to mitigate adverse effects

You must also notify the individual whose data has been accessed, if the breach can cause harm. Exemptions here include if stolen data was encrypted, notifying involves disproportionate effort or subsequent measures to minimise harm have already been implemented.

Privacy impact assessments

Going forward your firm should undertake a privacy impact assessment in relation to GDPR when initiating projects, investing in new systems or technology or changing working habits. This will help you to monitor what the data privacy issues are for your firm and the data security risk from these initiatives.

A CHECKLIST TO HELP YOU GET GDPR-READY

As you've probably now concluded, to comply with the GDPR (when it comes into force in May 2018) will require time and preparation. It's important then to start sooner than later. The size of your practice is no excuse, the GDPR will apply to businesses of all shapes and sizes.

1. Make sure your team are aware of GDPR and decide when and how you will go about auditing your current systems and types of data to see if they will comply or not with the GDPR. Assign the Data Controller, Data Processor etc roles.

2. Get up to speed on the information you hold within your firm – what sort is it, where did it come from, who have you shared it with, how is it stored?

3. Confirm what is the legal basis you are using people's data for.

4. Assess whether your document processing activities and data storage comply with GDPR. If not start making changes to ensure they do.

5. Review and if necessary rework your privacy notices and policies so they are GDPR-friendly. Remember the policies and notices **must** be written in plain English.

6. Familiarise yourself with your firm's obligations to individual's rights under GDPR and check out the Information Commissioner's Office Guidelines to evaluate your working practices, systems and procedures.

7. Review and revise the approach you take for obtaining consent from people – you must ensure you're obtaining a positive opt-in, which is specific, informed and not ambiguous. You will need to revisit past consent forms people have completed, if they don't meet the new GDPR standards.

8. If you store details about clients' children who are below the age of 16 (for EU) and 13 (for UK), familiarise yourself with the additional measures you now need to follow under GDPR.

9. Assess your security measures and establish procedures to detect, report and investigate data breaches. Introduce Data Protection Impact Assessments as part of your future firm practices..

10. If you work internationally and send data outside the EU, see if the countries you work with are black listed. Also obtain relevant guarantees from your suppliers regarding data protection.

A HELPING HAND ALONG THE WAY

How BTCSoftware is helping accountancy firms comply with GDPR

Desktop versions of our Software

Privacy by design and security by default– Users are required to log into the software using a password. It is also possible for the system administrator to restrict users to certain client groups and/or activities. They can also password protect individual clients and/or key activities such as tax returns.

Encryption – the database used in our software is encrypted and password protected.

System Back-up – Back ups are conducted by the system administrator in each firm but we recommend the software is set up to automatically backup using an off-site backup product such as Mozy, which is configured to create an incremental back up overnight. We can help our clients set this up.

Cloud versions of our Software

Security by default – At a local level users are required to log into the software using a password. It is also possible for the system administrator to restrict users to certain client groups and/or activities. They can also password protect individual clients and/or key activities such as tax returns, etc. In terms of Public Security, access to the MS SQL Server database server is only permitted via a L2TP VPN connection - using either a pre-shred key or secure certificate. No other internet traffic is permitted to the SQL Server database server. Data held in the software is located in a secure UK-based Amazon data centre

Encryption - the database used in our software is encrypted and password protected.

Back-up – This is performed automatically twice per day with a minimum 14 days retention

A HELPING HAND ALONG THE WAY

How MyDocSafe is helping accountancy firms comply with GDPR

Privacy by design – MyDocSafe clients gain full control over who has access to specific client files and folders and what access level it is.

Security by default - All data stored in MyDocSafe software resides in the EU and is encrypted. No files travel by email and each client is issued with a separate encryption key pair.

Esignature technology – Our esignature technology automates filing and does not leave unencrypted files lingering on email servers.

Data subject rights - Our client portal technology lets accountancy firms manage client consents, provide remote access to client data for easy exercise of 'data access', 'data rectification' and 'data portability' rights.

Customer service – The MyDocSafe client portals remove the need for additional filing and provide a convenient space for sharing best practices, making announcements and even chat securely.

Competitive advantage - MyDocSafe automation engine helps streamline client and employee on boarding processes that include form filling, document upload, identity verification, contract signing, credit card payments or direct debit setup. Automation helps reduce 'time-to-revenue', administrative burden and improves cyber security.

A HELPING HAND ALONG THE WAY

About BTCSoftware

We develop feature-rich, secure and cost-effective software products that make life easier and more rewarding for accounting professionals. Our abiding ethos is that quality, practice grade software should never be expensive.

Suitable for sole practitioners or larger practices, we've designed our software so it's simple to use, whatever the size of your practice.

From start-ups to well-established firms, BTCSoftware's solutions give you the ability to complete Self-Assessment, Corporation Tax and Companies House returns quickly and easily at a price you can afford – and all encompassed within a practice management solution.

w: btcsoftware.co.uk
t. 0345 241 5030
e. sales@btcsoftware.co.uk

About MyDocSafe

We empower companies that sign, manage and transfer access to sensitive documents to do that securely, efficiently and affordably, while maintaining control over their brand exposure and customer experience.

We are the front-office suite for professional services firms that deal with sensitive data. Our encrypted document storage, e-signature and client portal technology form part of the DNA of a modern, cloud enabled, and cyber-security aware accounting practice.

MyDocSafe comes with BTCSoftware integration that allows BTCSoftware users to send documents for approval directly from the practice management console, saving time and resources.

Our flexible pricing plans are suitable to a firm of any size and are based on subscription fees and transaction fees (for ID verification services). We offer a 14-day free trial and 1-to-1 demos.

w: mydocsafe.com
t: 0203 286 7419
e: daniel@mydocsafe.com

SOFTWARE

BTC Software Limited
Lyndale House
24 High Street
Addlestone
KT15 1TN

Freephone: 0345 241 5030
International: +44 1932 840572

www.BTCSoftware.co.uk