ICAEW
BUSINESS LAW / IT FACULTY

FAQs

GDPR FOR ACCOUNTANTS: YOUR QUESTIONS ANSWERED
A GDPR Checklist

May 2018 Update

Business Law /IT Faculty FAQs are published by ICAEW's Business Law team and the IT Faculty. *GDPR for Accountants: Your Questions Answered* is a series of FAQs designed to provide accountants practical guidance on the implications of the forthcoming changes to data protection legislation arising from the General Data Protection Regulation (GDPR).

This content is not intended to constitute legal advice. Specific legal advice should be sought before taking or refraining from taking any action in relation to the matters outlined.

A GDPR 'TO DO' LIST

Introduction

This guide is designed to explain to members and member firms what they need to do now to get ready for the GDPR. It is part of a series designed to answer the questions that members have been asking about the GDPR and its implications for the services they offer to clients. *What is the GDPR?* provides an overview of the key terms and concepts of the GDPR while *GDPR: What does it mean for Accountants?* explains what the changes will mean for ICAEW members.

It is not definitive guidance on all aspects of the GDPR. The Information Commissioner's Office (ICO) has issued some pieces of guidance and will continue to do so. Members are, therefore, advised to regularly check the ICAEW and ICO webpages for the latest information and guidance from the ICO and the EU's Article 29 Working Party. In addition, ICAEW's Essential Guide to GDPR is a useful starting point for members and ICAEW's dedicated GDPR webpage has more information and links to further resources.

If you have any concerns or questions about how the GDPR may affect your business or practice that are not addressed here then please get in touch with our Technical Advisory Service. This guide will be updated as necessary. We are also running a series of webinars – please see ICAEW's Events webpage for full details – that will be available on demand.

If in doubt, members are advised to seek legal advice as this content is not intended to constitute legal advice. Specific legal advice should be sought before taking or refraining from taking any action in relation to the matters outlined.

Background

What is the GDPR?

The GDPR is the 'General Data Protection Regulation' and will come into force on 25 May 2018. It is an overhaul of existing EU legislation on data protection, not new rules.

Does it apply to all accountants and accountancy firms?

Yes. It will apply to all EEA countries and any individual or organisations trading with them. As it comes into force on 25 May 2018 (before the UK leaves the EU), UK individuals & organisations must ensure compliance with the new regime by then. Furthermore, the Data Protection Bill will incorporate all of the

GDPR as well introducing some new provisions. This is so the UK will be GDPR compliant post Brexit. The Data Protection Bill is currently going through Parliament but is expected to come into force on 25 May 2018.

Is the GDPR a new approach to data protection?

No. There are a number of 'myths' building up around the GDPR but the main thing to remember is that it builds upon the Data Protection Act 1998 (DPA 98). It is an update, not a wholesale revision, to meet the changes in technology and data use over the last twenty years or so.

The ICO has indicated that if you are already compliant with the DPA then you well on the way to being GDPR ready. Even so, although the GDPR is not a major game changer it is more stringent in its application and the fines for non-compliance have been considerably increased. This means that doing nothing is not an option.

Where to start?

It may seem daunting but there are a few key steps accountancy firms should be taking to begin the process to get GDPR ready. These are:

a) appoint someone senior to oversee the process;
b) review and update as necessary existing information and cyber security measures;
c) 'map' your data;
d) review contracts with clients, suppliers (anyone who processes, including storage providers, your data) and employees;
e) draft data protection policies; and
f) train staff.

The 'Checklist below offers some practical steps on what to do for each of these steps.

A word of warning – this is not a one-off event. GDPR compliance requires that all policies, training and procedures are reviewed and updated on a regular basis.

A few words of encouragement:

a) The ICO is not expecting every organisation to have all policies and procedures in place on 25 May 2018 but it will expect every organisation to have made a start and to have a plan on how it will be GDPR ready and when.
b) The GDPR advocates a risk based approach so you can tailor your actions to your circumstances.

GDPR Checklist

1. Appoint someone senior to oversee the process

Getting ready for the GDPR compliance is not just a matter for the IT department, so it is essential that a senior member of staff (director, partner, senior manager) takes responsibility for overseeing the process, allocating funds and resources as necessary.

Please note: This person is not necessarily a Data Protection Officer (DPO) as defined in the GDPR. See the ICO's guidance on when you need to appoint a DPO

Please note: A project team may also be required which may include external support and assistance.

2. Review existing information and cyber security and update as necessary

Having comprehensive levels of information and cyber security is a key step towards building a resilient organisation. We therefore recommend that members should review their existing security and amend or update as necessary. This does not need to be a wholesale (and expensive) revamp but can just be a refresh; either way any review can be tailored in line with the complexity of your organisation and IT set-up.

The following are some relatively straightforward security measures worth considering:

- Encryption
  The GDPR does not mandate the use of encryption technologies for securing data 'at rest' but does suggest that it should be considered. This approach is very similar to the one adopted by principle 7 of the existing DPA, see the ICO advice here. Other controls, such as restricted access to personal data should also be considered.
- Portals
  When sharing documents with a client it is worth considering the use of a web accessible portal, which ideally should be able to store encrypted documents ready for clients to download. Another approach would be to use the 'Encrypt with password' option in Microsoft Office when saving a file.
- Certification
  Certification schemes can both check and prove the robustness of your cyber security. Examples of such schemes include the National Cyber Security Centre's Cyber Essentials, Cyber Essentials Plus, IASME and ISO 27001

Further advice on cyber security from ICAEW can be found here

3. 'Map' your data

Before you can assess what you need to do you need to know ('map') what data you have as this will inform what you do next. To do this:

- Assess what personal data you hold, where it is held, what you do with it, how long you hold it and who you share it with. Is this in accordance with the GDPR? If not how are you going to address this? The ICO have now issued some templates to help you do this – see here
- Do you need to hold it? If you don't, consider deleting it.
- Do you transfer data internationally? Check to where and on what basis – is this still valid under GDPR? You may need to seek legal advice to clarify this.
- Conducting a Data Privacy Impact Assessment (DPIA) may help to assess any risk areas or gaps. The ICO's guidance has some useful tips on when and how to conduct a DPIA.

Once you have 'mapped' your data:

- Assess the lawful basis for you to process all the different types of personal data that you need to process;
- Consider what rights individuals will have with regard to their personal data held by you; and
- Consider whether you a data controller or data processor – you can be both.

4. Review contracts with clients, suppliers (anyone who processes your data) and employees to ensure GDPR compliant.

As the GDPR (Articles28-36) imposes new obligations on data controllers and data processors, you will need to make sure you understand your status and your responsibilities with regard to both client data and firm data. At the very least contracts will need to be updated to reflect the requirements of the GDPR. The ICO has issued a consultation on its draft guidance Contracts and liabilities between controllers and processors and will be issuing final guidance once it has analysed all the responses.

In the meantime the following actions are recommended:

a) Review Contracts with clients :
   i. Where you are the data processor:
      - Obtain documented instructions from any data controller on whose behalf you process data.
      - Check contract clauses on the sharing of data with others for compliance with the GDPR – re-write as necessary

   ii. Where you are a joint controller:
      - Check they are in compliance

- Check contract clauses on the sharing of data with others for compliance with the GDPR – re-write as necessary

iii. Where you are the data controller:

- Ensure any data processors are GDPR compliant

b) Review Engagement letters

- Update to inform clients that the GDPR (and the UK's new Data Protection Act) is the applicable legislation (once they come into force) and as before explain how you will use the personal data of your clients in accordance with the GDPR and other applicable legislation.
- Ensure services are not 'bundled' together.
- Do not assume or include a statement to the effect that by signing the engagement letter a client is also agreeing ('consenting') to receive marketing material from your practice.

Please note: ICAEW has now issued guidance and pro forma paragraphs to include in engagement letters.

c) Review contracts with Suppliers:

- Processors including cloud storage providers – check compliant.
- Establish where data is held – many cloud storage providers, for example, do not store data in the EU so you should obtain confirmation from them that any data stored by them or transferred by them is in accordance with the GDPR.

d) Review Employment contracts (Firm Data):

- Review (and redraft as necessary) employment contracts to include employees' rights as data subjects under the GDPR.
- Employees must also be informed that they can make a complaint to the ICO (or relevant supervisory authority) if they believe their personal data is not being used appropriately or held securely.
- You will not be able to rely on consent as a 'catch-all' so for most employment contracts the lawful basis for processing will be 'legitimate interest.' This must be explained in the revised contract
- It may be possible to rely on 'consent' for one-off circumstances such as bank requests to confirm income for a mortgage application. You should consider whether you need to draft pro-forma consent firms to cover such eventualities.

e) Review marketing contacts (Firm data):

- Review whether you have 'consent' that is GDPR compliant – if not, decide from whom and how you will obtain consent.
- Check 'consent' re: the processing of marketing data is not bundled together with other services (see engagement letters above).

5. Draft (written) data protection policies and procedures.

The GDPR introduces the principle of 'accountability'. This means that all organisations must not only ensure they are compliant with the GDPR but prove this too. The best way to prove this is document your data protection policies and procedures. As the GDPR advocates a risk based approach the policies and procedures need only cover those areas which apply to your use of personal data; if you do not use, for example, automated decision making or profiling then you will not need a policy on how to meet the rights of data subjects with regard to automated decision making or profiling.

We suggest that your policies and procedures should include, but not be limited to, the following:

- Who is responsible for what and reporting lines.

- How to recognise and what to do if there is a breach. As some breaches must be reported within 72 hours to the ICO you will need a plan of action. This is not just so you can notify the ICO but also anyone (including employees) whose data may have been compromised. It is good idea to practice the breach response plan before any breach occurs to prove that it would work! As all breaches, however, must be recorded, a system to record breaches will be necessary.
- How to get consent and when you need consent.
- What to do if consent is withdrawn.
- How to meet requests from data subjects regarding their rights 'to be forgotten,' rectification, data portability etc.
- Document retention policies.
- Privacy notices – what to include, who needs to receive them and when.
- Subject Access Requests –how to respond (including when you do not need to respond).
- A review policy to ensure existing policies and procedures are followed and updated or added to (if necessary) on a regular basis.

6. Train staff

Not all staff will need to understand the GDPR in its entirety but all staff should at least be aware that data protection is an issue for everyone.

- Staff who do not deal with personal data:
  Training can be limited to a (refresher) course on information and cyber–security. This should cover things such as good password practices, not opening emails from unknown senders, how to spot suspicious emails, how to recognise a breach has occurred, knowing when to report, and to whom, any suspected breach, how to ensure the physical security of computers, laptops, thumb drives etc and manual/paper records.
- Staff who do deal with personal data:
  Training should include all of the above regarding security over data plus an awareness of the policies and procedures outlined in section 5 above. Again this can be tailored to their particular role and responsibilities and whether they deal with firm data and/or client data

Further Information

- ICO's Guide to the GDPR webpage for a continually updated guide to the GDPR
- The ICO has also published guidance tailored to meet the needs of small organisations
- The EU's Article 29 Working Party news page for updates on their latest guidance
- ICAEW's FAQs: GDPR for Accountants. Your Questions Answered
- ICAEW's Guide to the GDPR Centre
- ICAEW's Data Protection webpage
- ICAEW Webinars – see Events webpage for details

There are over 1.7m chartered accountants around the world − talented, ethical and committed professionals who use their expertise to ensure we have a successful and sustainable future.

Over 149,000 of these are ICAEW Chartered Accountants. We train, develop and support each one of them so that they have the knowledge and values to help build local and global economies that are sustainable, accountable and fair.

We've been at the heart of the accountancy profession since we were founded in 1880 to ensure trust in business. We share our knowledge and insight with governments, regulators and business leaders worldwide as we believe accountancy is a force for positive economic change across the world.

Chartered Accountants' Hall
Moorgate Place, London
icaew.com

T +44 (0)20 7920 8100
E ethics@icaew.com