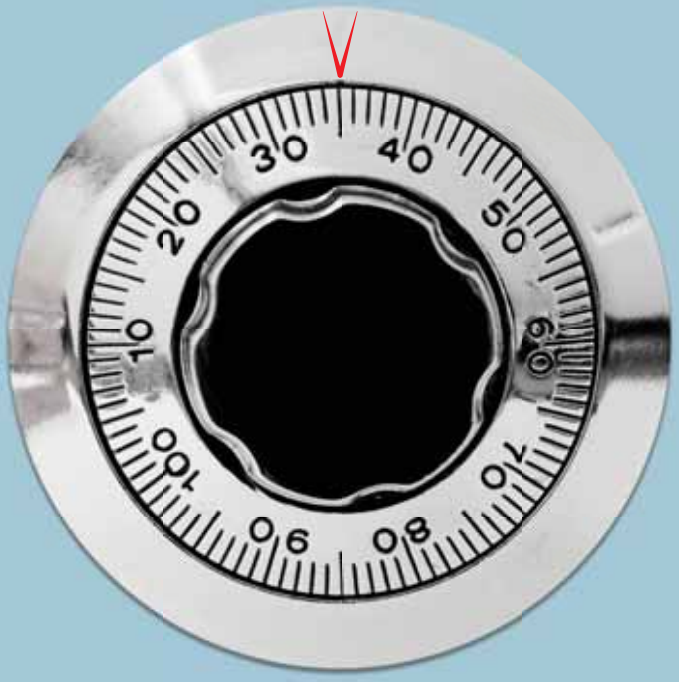
TECH ESSENTIALS
IT FACULTY



The essential guide to GDPR

Getting to grips with the General Data Protection Regulation

The rules governing data protection and personal privacy are changing. Despite the step change in the technical environment and the massive increase in personal data that is being created every day, the regulations have not moved on since the 1998 Data Protection Act.

However, GDPR, or the General Data Protection Regulation, will come into force in May 2018, and will have a major impact on ICAEW members and their organisations; the scale of the new fines alone should have people concerned. ICAEW and the IT Faculty have produced this guide to help members understand the new regulation and what they need to do to prepare.

There are a number of misconceptions about the regulation, some of which were debunked by the information commissioner, Elizabeth Denham, when she presented the IT Faculty Annual Lecture. First is that GDPR does not apply to small business, and second is that it will no longer happen due to Brexit. Both are incorrect; GDPR applies to personal data regardless of the size of the organisation, and the regulation comes into law while the UK is still a member of the EU (and equivalence should follow).

The main advice from the commissioner was to prepare now for the changes that are coming. We hope this guide will help you in that task.

RICHARD ANNING
Head of IT Faculty, ICAEW

INTRODUCING THE TECH ESSENTIALS SERIES

Throughout 2017, the ICAEW IT Faculty will be issuing a series of guides to update members on the latest technology issues affecting the accountancy profession. We aim to bring you practical tips and expert insight on a range of topics, setting you up for any action you'll need to be taking in the coming 18 months.

Words by Tim Phillips

When information commissioner Elizabeth Denham spoke about the forthcoming General Data Protection Regulation to ICAEW on 17 January, she highlighted the opportunities for accountants, the responsibilities facing them in the way they do business and the responsibilities of their clients.

While GDPR, to be introduced in May 2018, is not a break from the current data protection regime, complying will certainly require some work. As Denham says, it "puts an onus on businesses to change their entire ethos to data protection". While GDPR may seem daunting, in part due to the fact that the maximum fine for breaches will go up from £500,000 to €20m (or 4% of annual worldwide turnover, whichever is greater), are there positive implications of compliance?

"On a basic level, your jobs involve handling personal data," said Denham. "It's your responsibility to keep that information secure and ensure that individuals' rights are respected."

CHECK EVERYTHING, AND THEN CHECK IT AGAIN

Richard Kemp, founder of Kemp IT Law, states: "This is an opportunity to check what data you hold, where it comes from, and where precisely it is held. Treat it as an internal project, and check your external stakeholders too.

"You are probably not dealing with large amounts of customer data, but you will still have to deal with the right to be forgotten and comply with data breach notifications," warns Kemp. To do that, you will have to identify what type of data you are holding and why. A benefit of the audit might also be the decision to consolidate or delete data in order to simplify administration. But until a business knows what data it possesses it's impossible to design improved processes.

Whether you are a data processor or a data controller under the GDPR (see page 5), you will have statutory obligations, in contrast to the current regime, in which only data controllers are regulated in this way. "The principle of accountability is that you must show how you comply, not just that you do comply," says Jane Berney, business law manager at ICAEW. "Before, you didn't have to document it, now you do, but that isn't necessarily a bad thing. You could argue that it's part of your general due diligence," she adds.

"Under the Data Protection Act (DPA), data processors don't have any obligations. There will be new obligations for them," says Sam de Silva, partner and head of the IT and outsourcing practice at Nabarro. "From a practical perspective this might not be a big change because in the existing law they would have similar obligations under contract," he explains.

Denham points out that the GDPR gives regulators enforcement power to levy fines based on accountability alone. That means issues like failing to ensure data protection by design, failure to conduct a data protection impact assessment, or a lack of documentation will all incur a penalty.

INITIATE THE CONVERSATION

Denham enlisted accountancy professionals to help her reach businesses through their relationships, and called her speech "a starting point for discussions with the businesses you serve". These are discussions that Steve Williams has been having for a while. As a leader in technology risk and regulation at Moore Stephens – a firm of accountants serving mid-market companies in a number of sectors – he has a background in regulation and technology risk.

"Because we've been paving the way for 18 months and having those conversations, it means that when they are ready we're in a good position," he explains.

The firm has been recruiting and training its employees to cope with GDPR, writing guidance and calling his clients to discuss the topic. Now Williams finds that their need for help has suddenly increased: "Especially over the last month, it's almost as if they came into the new year and everyone wants to talk about GDPR," he says.

Among the topics for further discussion will be the responsibilities that accountants may have as data controllers for their clients, but also the potential to help clients audit their own data, and manage it according to the principles of the GDPR.

IMPACT ON SMALL ORGANISATIONS

Within the UK, 99% of businesses employ fewer than 249 people. This is a huge portion of UK businesses in which ICAEW members are well-placed to offer advice, but also in which awareness might not be as high. "[Small organisations] don't have compliance teams or data protection officers, but often process a lot of personal data, and the reputation and liability risks are just as real. It's harder for me as a regulator to communicate with them," admits Denham.

The idea that small businesses are exempt is "misconception number one", according to Richard Anning, head of the IT Faculty at ICAEW. "You will be affected by this regardless of what size you are," he warns. Small accountancy practices do not escape the demands of compliance. "We have had a lot of meetings with smaller practices and sometimes they say they don't have time for it, but that is more a question of priority than time," Anning adds.

Also, many small businesses have entered into agreements with cloud or managed service providers, and so will have to be sure that the data is stored in a compliant way. "If a third party is holding data on your behalf, you must understand what it is doing with it," Anning explains, "but a lot is about process and people. It's not important how old your system is, it's about knowing what information you have and where it is. We think practices can build trust with customers and clients, and say 'we care about you and your data'."

KNOWLEDGE IS POWER

The most recent government cyber risk survey found that 69% of businesses say their senior management consider cyber security as a very or fairly high priority. However, only just over half of those surveyed had done anything about identifying the risks.

Data protection and cyber risk are brought together in the new regime, not least because those who suffer a breach have 72 hours to report it (see *The importance of preparation*). "You can no longer divorce data protection from data security in the organisation, and most breaches happen in obvious ways, so check your processes for that too," says Anning.

"A lot is about process and people. It's not important how old your system is, it's about knowing what information you have and where it is"

At Moore Stephens, Williams has spent much of the past 18 months building relationships with technology providers and legal firms so that clients get integrated advice not just on what to do, but how to do it.

"In our industry we try to give advance warning of the work they will need to do," he says. "In this case we have three pillars: law, technology and advisory, and the three can work well together. There has to be a role for technologists and the legal profession too. So we have been working hard on our network of contacts, and that's really important."

As Williams points out: offering a value-added service to clients would be undermined if they asked about the legal or technical impact and the accountant didn't know the answer.

DEALING WITH INTERNATIONAL CLIENTS

For the international implications of GDPR, Moore Stephens has been offering its services to its international network. "We don't see many firms doing this, so we have initiatives moving in North America, Asia-Pac and Europe to try to bond the network," says WIlliams.

The global dimension to the GDPR means that international clients who either offer goods and services to EU subjects, or collect data from EU subjects, may have to demonstrate compliance. "This is very much a live area, so it's certainly one that I think both legal and accounting are going to be very busy in for the next few years," says William Long, who leads the EU data protection practice at law firm Sidley Austin. "I think the GDPR is a game changer for many international businesses. Virtually every international company is involved in the collection, use, analysis and transfer of data. We're finding that a lot of US, Indian or Japanese companies will have to develop global processes and global standards."

Therefore accountants who have UK-only relationships with an international client, and who are taking responsibility for data protection, will have to get assurance of their global processes. "It is not limited to changing just notices and consents and policies, and it's not just about legal wording. A lot of the most challenging aspects of the GDPR are the system and process changes, in particular carrying out data inventories, which accounting firms are particularly well adapted to do," Long adds. The alternative to achieving compliance in its global systems would be that the client would segment its European and non-European customer data, which would be costly (and potentially unworkable).

€20,000,000

or 4% of worldwide turnover, whichever is greater – this is the new maximum fine under GDPR, compared with £500,000 under the existing Data Protection Act

PROCESSOR OR CONTROLLER?

While GDPR doesn't alter the already existing definitions of what constitutes a 'controller' or 'processor', it is helpful to revisit the terms.

A controller is a "natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of processing of personal data", while a processor is "a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller".

Both controller and processor will now be jointly held accountable for compliance.

THE IMPORTANCE OF PREPARATION

Managing cyber risk, either for practices or their clients, is not simply about managing data within the perimeter of the organisation. Denham pointed out that the cyber attack on TalkTalk in 2015 exposed 150,000 customers – and the bank details for 15,000 of them – but that many of the exposed records came from Tiscali, which TalkTalk acquired in 2009. When US discount retailer Target was breached in 2013, exposing at least 70 million records, it happened through the company's air conditioning provider. Therefore, it becomes necessary to document the security risks from the supply chain as well as the organisation.

GDPR also specifies a risk-based approach to data protection. For example, clients in high-risk activities (eg those that compile financial profiles of data subjects) would be expected to conduct a detailed privacy impact assessment, and to notify potentially affected individuals if there was a breach. This doesn't just apply to the risk the data might be stolen: if customer data should be anonymous, for example, processes have to ensure that this anonymity cannot be broken.

Risk-based data protection is not about locking down all systems, it's about appropriate responses. "You have to assume you will be breached at some stage, so you will have to work out what information is most important to you and have strong security around that," Anning recommends.

GDPR will also involve maintaining compliance for any data stored in the US Privacy Shield (the successor to Safe Harbor) when storing data in the US. Privacy Shield has already been implemented, but will be reviewed by the Article 29 Working Party (WP29) in summer 2017, and there will be more guidance as to its implementation.

"There's going to be a lot more guidance coming out over the next few months from the WP29 and from the European Data Protection Board, which is yet to be established," says Long. "The way we deal with international transfers of data is still in a state of flux. We will need to see how that will develop in the next year."

ANY POST-BREXIT IMPLICATIONS?

So what impact will Brexit have upon GDPR? Fortunately, there is no practical implication of Brexit at this time for UK accountancy practices and their clients when preparing for GDPR. This is for two reasons: it is implemented before Brexit happens, and it will likely be placed into UK law after Brexit with something similar.

In February 2017, digital minister Matt Hancock told the House of Lords EU Home Affairs Sub-Committee that the current plan is to incorporate the GDPR into UK law. "In a sense, we are matching them rather than asking them to match anything new from the UK," he said. But even if the UK's data protection regime were to deviate from the GDPR over time, anyone doing business in Europe that involves collecting personal data would still be bound by the regulations.

IN THE NOT-SO-DISTANT FUTURE...

In light of Denham's advice, here are some steps you can take in the immediate future:

- **Tomorrow:** Download and consult the ICO's 12-step plan (tinyurl.com/TE1-12Steps) to make sure decision-makers know the law.
- **Next week:** Start getting a more detailed understanding of the new law using the ICO's overview of the GDPR (tinyurl.com/TE1-Overview) which explains similarities to the DPA, and the new and different requirements.
- **Next month:** Start considering how to put privacy by design at the centre of the business processes using the ICO code of practice for conducting privacy impact assessments (tinyurl.com/TE1-PbD).

See our handy guide opposite (page 7) for more detailed steps.

£3,000,000

Largest cost of a breach among Cyber Security Breaches Survey respondents – the average was £36,500

IT IS TIME FOR ACTION

"Accountants should have already started acting. I don't want to scaremonger, but there's a lot of work that needs to be done," says Sam De Silva. "The solutions may not be complicated, but there may be issues that are not straightforward – until you do the work, you can't form a view."

While there is still just over a year to go until the GDPR becomes regulation, Elizabeth Denham suggested accountancy practices – and their clients – look at what steps they should take tomorrow, next week and next month (see below left).

GIVING PRACTICAL ADVICE

"Finance professionals have an important role to play in preparing their organisations for GDPR," says Kirstin Gillon, technical manager in the faculty. "But they can also show leadership and encourage the business to use GDPR as a way of enhancing their brand and building greater customer trust."

There is scope too for sharing of information in the practice-client relationship space. Moore Stephens' clients have responded to the information about GDPR by asking staff to their offices. Steve Williams, technology risk and regulation at Moore Stephens, warns that your expertise needs to add some value to the clients' internal research. While this is an opportunity to deepen the relationship, it has to be on the basis that you can give practical advice.

"There seems to be an appetite in audit committees and some boards to understand what it is," he says. "We expected a wholesale lack of understanding and that's not the case. Our clients are not necessarily moving forward until they understood the implications, but the awareness has been good.

"Typically they will have determined accountability, and now they have an accountable individual they are asking us what they should do next."

Tech Essentials checklist

Your cut-out-and-keep guide to preparing for the May 2018 GDPR implementation

ORGANISING STAFF

- [ ] Identify who in your organisation needs to be aware that data law is changing
- [ ] Designate a data protection officer if required (see GDPR for guidelines)
- [ ] If your business has interests in the US, ensure all relevant staff are aware of the US Privacy Shield

INTERNAL SYSTEMS

- [ ] Consider whether your business needs a risk register, or revisit the existing one
- [ ] Review current privacy notices in accordance with the ICO guidelines on GDPR
- [ ] Check that procedures cover all the new rights that individuals have under GDPR
- [ ] Work out whether you need to organise an information audit and if so across how much of the business
- [ ] If appropriate, ensure you have GDPR-specific procedures in place for gathering young persons' data
- [ ] Ensure you can detect a breach and report and investigate it in a timely fashion in accordance with the new breach notification duty
- [ ] Look at ICO guidance on Data Privacy Impact Assessments (DPIAs) – assess situations where you will be required to conduct a DPIA and what procedures you will put in place
- [ ] Run relevant security checks to ensure your systems are robust around storage of said data in the run-up to May 2018

DATA PROCESSES

- [ ] Document what personal data you hold, where it came from and who you share it with
- [ ] Ensure that you have a process in place to delete client data if requested to do so by the client
- [ ] Review the process that will allow a client to take a copy of the data specific to themselves if requested to do so
- [ ] Plan how you will handle subject access requests in line with GDPR timescales*
- [ ] Look at the data processing you carry out – identify the legal basis for carrying tasks out and document them
- [ ] Review how you are seeking, obtaining and recording consent in line with GDPR – you must be able to demonstrate consent was given and this cannot be inferred from silence or gained from pre-ticked boxes
- [ ] Work out who all the data controllers and data processors in your business are, and plan any relevant training programmes for staff accordingly

STAKEHOLDERS

- [ ] Contact clients to inform/remind them of GDPR obligations and how your processes may be changing
- [ ] Keep a log of all clients who have been contacted
- [ ] Speak to your stakeholders, suppliers and third-party processors about the data you share and their timetables for GDPR implementation. Assess the risks around timeframes that conflict with your own preparations

USEFUL LINKS

ICAEW cyber security resource centre
icaew.com/cyber

Chartech
May/June 2016 – Prepare to protect (page 18)
tinyurl.com/TE1-CH16

Privacy regulation – accountants step forward – blog by Richard Anning
tinyurl.com/TE1-Blog

ICO Guidance: *Overview of the GDPR*
tinyurl.com/TE1-ICOoverview

ICO's *Preparing for the General Data Protection Regulation – 12 steps to take now*
tinyurl.com/TE1-12Steps

ICO Guidance: *What to expect and when*
tinyurl.com/TE1-WhatWhen

ICO blog: *GDPR guidance in 2017*
tinyurl.com/TE1-Guide17

ICO events and webinars
tinyurl.com/TE1-Events

*If your company handles lots of access requests, it could save you money if you develop systems that allow people to access their own information online easily. Conduct a cost/benefit analysis of doing so to work out if it will be beneficial for your business

FACULTY INFORMATION

The ICAEW IT Faculty provides products and services to help its members make the best possible use of IT. It represents chartered accountants' IT-related interests and contributes to IT-related public affairs. It also helps those in business to keep up to date with IT issues and developments. As an independent body, the IT Faculty is able to take an objective view and get past the hype which often surrounds IT, leading and shaping debate, challenging common assumptions and clarifying arguments.

ICAEW connects over 147,000 chartered accountants worldwide, providing this community of professionals with the power to build and sustain strong economies. Training, developing and supporting accountants throughout their career, we ensure that they have the expertise and values to meet the needs of tomorrow's businesses.

Our profession is right at the heart of the decisions that will define the future, and we contribute by sharing our knowledge, insight and capabilities with others. That way, we can be sure that we are building robust, accountable and fair economies across the globe.

ICAEW is a member of Chartered Accountants Worldwide (CAW), which brings together 11 chartered accountancy bodies, representing over 1.6m members and students globally.

ICAEW
IT Faculty
Chartered Accountants' Hall
Moorgate Place
London
EC2R 6EA
UK

T +44 (0)20 7920 8481
E itfac@icaew.com
icaew.com/itfac

in search ICAEW IT Faculty
@icaew_ITFaculty
f facebook.com/icaew

Chartered Accountants Worldwide
Member

GAA
Global Accounting Alliance