ICAEW
BUSINESS LAW / IT FACULTY

FAQs

GDPR FOR ACCOUNTANTS: YOUR QUESTIONS ANSWERED

June 2018

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 thechanges 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

WHAT IS THE GDPR?

Introduction

This guide is designed as an introduction to the GDPR for members and member firms. It is part of a series designed to answer the questions that members have been asking about the GDPR.

It is **not** definitive guidance on all aspects of the GDPR. The Information Commissioner's Office (ICO) has issued some guidance and will continue to do so. Members are 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. The ICAEW's Essential Guide to GDPR is a useful starting point for members**.** 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**. We will be publishing a summary of the questions asked by members (and the answers) in due course as well as further guidance and webinars. This guide will also be updated as necessary.

If in doubt members are advised to seek legal advice. 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 does 'GDPR' stand for?

GDPR is short for the General Data Protection Regulation came into force on 25 May 2018. It is an overhaul of existing EU legislation on data protection, not new legislation. In addition, in the UK, the Data Protection Act 1998 (DPA) will be replaced by the Data Protection Act 2018.

Does it apply to all accountants and accountancy firms?

Yes. The GDPR applies to all EEA countries and any individual or organisations trading with them, irrespective of their size or location. As it comes into force before the UK leaves the EU, UK individuals & organisations must ensure compliance with the new regime by and after 25 May 2018.

What about Brexit?

Post Brexit if a UK organisation or individual processes the personal data of an EU data subject then they will have to do this in accordance with the GDPR. To ensure that the UK will be GDPR compliant post Brexit, the new Data Protection Act 2018 will incorporate all of the GDPR as well introducing some new provisions.

Is the GDPR a completely 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 existing legislation (the DPA). It is an update, not a wholesale revision, to meet the changes in technology and data use over the last twenty years or so. As a result consumers' privacy and data were not as well protected as they could be. The GDPR rectifies this this by increasing the responsibility on organisations to use personal data appropriately and to hold it securely.

The ICO has indicated that if you are already compliant with the DPA then you are well on the way to being GDPR ready. 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, although the GDPR does allow organisations to take a risk based approach.

But even if the approach is familiar, hasn't the detail changed?

No. As with the DPA it only applies to personal data, not company data. The principles remain the same, although a new principle of 'accountability' has been added. Similarly anyone who processes 'personal data' must still have a lawful basis for processing. Where the GDPR differs from its predecessors is that it is intended to make all those who process data consider data protection at every stage.

Hasn't the reach of data protection been expanded by the GDPR?

Yes, in the sense that everyone needs to take data protection seriously and the territorial reach of the GDPR is worldwide (as far as EU data subjects are concerned). But it still only applies to personal data and the following types of processing are out of scope:

- if by a natural person for a purely personal or household activity such as the private use of social media;
- if by a law enforcement agency; and
- if by EU institutions.

GDPR – key terms and concepts

In this section we will explain the key terms and concepts under the GDPR of which you need to be aware. Most are the same as under the DPA but not all. We have highlighted those that are completely NEW but as many others have been 'tweaked' we would encourage members to familiarise themselves with all the key terms and concepts.

Personal Data

As under the DPA, the GDPR only applies to 'personal data.' This means data which relates to a living individual who can be identified from:

- the data; or
- the data and other information which is in the possession of, or is likely to come into the possession of, the data controller.

It also includes any expression of opinion about the individual and any indication of the intentions of the data controller or any other person in respect of the individual.

The GDPR has extended the type of data that can be deemed to identify an individual. As well as the name, address or date of birth of an individual, the GDPR includes things such as location data or online identifiers (eg, IP address).

The GDPR also refers to 'sensitive data.' This is defined in Article 9 as "special categories of personal data" and now includes genetic data and biometric data if processed to uniquely identify an individual.

Processing

Processing means:

- obtaining, recording or holding personal data; or
- carrying out any operation or set of operations on personal data, including organising, adapting, altering, using, disclosing (by any means) or removing (by any means) from the records (manual and digital).

Under the GDPR processing covers both automated personal data and manual/paper records if part of a 'relevant filing system.'

Data Protection Principles

As with the DPA, the GDPR (Article 5) stipulates that the processing of personal data must be in accordance with the data protection principles. These have not changed, although the principle of accountability has been added.

The principles are that personal data shall be processed in a way that is:

- fair, lawful and transparent;
- only for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes;
- adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;
- accurate and up to date;
- kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; and
- processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

NEW The Accountability Principle

Article 5(2) requires that controllers should be responsible for and be able to demonstrate compliance with the other principles outlined above. This is the accountability principle and means that internal mechanisms and control systems are put in place to ensure compliance with the GDPR and that there is (documentary) evidence to prove this. This evidence may need to be produced to external stakeholders, including supervisory authorities (such as the ICO in the UK).

The best way to demonstrate accountability is to have written policies and procedures in place and to ensure that all staff receive training (appropriate to their role) to ensure they understand these policies and procedures. The policies and procedures will need to be regularly updated, as will staff training. The ICO has indicated that staff training should be repeated at least every two years.

Demonstrating that the business has sought confirmation of the suitability of their systems will also provide valuable evidence. Examples of schemes to demonstrate this include the National Cyber Security Centre's Cyber Essentials or Cyber Essentials Plus, IASME and ISO 27001

Lawful Basis for Processing

As under the DPA, the GDPR stipulates that before you can process data you must establish that you have a lawful basis for doing so. The GDPR, however, states that you must identify upfront the lawful basis, document the reasoning and inform the data subject of it.

Under the GDPR (Article 6) the lawful bases for processing are:

- consent of the data subject.
- performance of a contract with the data subject or to take steps to enter into a contract with a data subject e.g. personal data relevant to the provision of a specific service.
- compliance with a legal obligation, e.g. data required to fulfil a statutory requirement such as maintaining books of records, statutory audits, submitting tax returns or satisfying AML regulations.
- protection of the vital interests of a data subject or another person, e.g. medical data where the health of a data subject is at risk.
- for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller e.g. Public Authority duties.
- legitimate interests pursued by the controller or a third party, except where such interests are overridden by the interests, rights or freedoms of the data subject. Eg, marketing of services to existing clients where the balance of rights favours the business over the data subject (the client) would not constitute a legitimate interest.

Before you can process data you must satisfy (and document how you satisfy) all the principles and at least one processing condition.

The ICO's guidance includes useful checklists. See here for our guidance on the implications for ICAEW members.

Consent

The GDPR will strengthen the rules regarding when 'consent' can be deemed to have been given by a data subject. Under the GDPR 'consent' must be freely given, explicit, affirmative, finite and documented. All data subjects must be informed that their consent can be withdrawn at any time and withdrawing consent must be as easy as giving consent.

Definition of Data Processors and Data Controllers

This is unchanged. Generally a controller determines the purposes and means of processing personal data whereas a processor is responsible for processing personal data on behalf of a controller. As this is a complex area, legal advice may be required to determine your status.

NEW Responsibilities of Data Processors

The GDPR will give processors responsibilities and liabilities in their own right, and processors as well as controllers may now be liable to pay damages or be subject to fines or other penalties. This is because processors will, under the GDPR, be as responsible as controllers for ensuring that personal data is kept secure.

NEW Contracts between Data Processors and Data Controllers

The GDPR stipulates that data processors and data controllers must have in place a written contract. Furthermore it sets out in detail what should be included in contracts between data controllers and data processors. These include the subject matter of the processing, its duration, and purpose, type of personal data and categories of data subjects.

Please note: the ICO is still finalising its guidance on this area. In the meantime it has produced a useful checklist of what to include in contracts. As this is a complex area we are currently advising to seek legal advice if in doubt.

NEW Data Protection Officer (DPO).

This is a new role under the GDPR. A DPO is the person within an organisation who:

- advises the organisation on its data protection obligations;
- monitors the organisation's compliance with the GDPR; and
- is the first point of contact with the ICO and data subjects.

The GDPR specifies that a DPO must be appointed when:

- the processing is performed by a public authority or body; or
- the core activities of the controller or processor consist of regular and systematic monitoring of data subjects on a 'large' scale; or
- the processing relates to sensitive data or criminal offences, again if on a 'large' scale.

See also ICAEW's guidance on DPOs.

Please note: The GDPR does not define what a public authority is but the UK government, in its Data Protection Bill, has stated that the definition of a public authority or body in this instance will be in accordance with the Freedom of Information Act (FOI). This would suggest that accountancy firms are unlikely to be considered as a 'public authority' but all academy schools are, for example, as they are specifically included under the FOI as a public authority or body. However, this is not necessarily the case as the Bill includes a qualification: a public authority will only be treated as a public authority for the purposes of the GDPR when it is carrying out a task in the public interest or in the exercise of official authority vested in it

NEW Rights of Individuals

The GDPR has enhanced the rights of individuals (data subjects) and so all organisations need to be aware of these and set up policies and procedures to deal with them. The rights are now:

- Right to be informed
- Right of access
- Right to rectification
- Right to erasure ('right to be forgotten')
- Right to restrict processing
- Right to data portability
- Right to object
- Rights re: automated decision making and profiling

Please Note: Not all rights apply in all circumstances. For further details see the ICO's guidance.

Subject Access Requests (SARs)

Data subjects will still be able to make a SAR but an organisation will no longer be able to charge a fee for them and must now respond within 30 days (previously 40 days). All SARS must be honoured unless they are deemed to be malicious.

Transferring Data out of the EU

As under the DPA, the personal data of EU data subjects can only be transferred out if the EU if there is equivalence. For further details see the ICO's guidance. Legal advice may be required.

Document retention

The GDPR, like the DPA, stipulates that data must only be held for 'as long as necessary'. This means that 'just in case' is not a justification for retaining data but at the same time it is not necessary to delete all personal data as a matter of course.

It is recommended that members and member firms should review all the data they hold and on what grounds the data is held (by category). Following on from this, it will be easier to decide whether it is still appropriate for the data to be held and draft retention polices.

Please note: We will be updating our guidance Documents and records: ownership, lien and rights of access and the Helpsheet Document Retention to reflect the requirements of the GDPR and the new Data Protection Act in due course.

NEW Data Privacy Impact Statement (DPIA)

These must be carried out to assess the risk to an individual's rights when, for example, introducing new technology or new work practices. See the ICO's guidance on completing DPIA.

NEW Privacy by Design This is a new concept and means that the protection of privacy must be built into all decision making processes. It covers both technological and organisational measures and it is particularly important to consider privacy design at the start of any new service development or process development.

Please note: The ICO has published guidance on privacy by design and will be updating this to reflect the provisions of the GDPR. In the meantime, the existing guidance is a good starting point for members.

Privacy Notices

A Privacy Notice is a document explaining to data subjects their rights and how their personal data will be used. They are not new but the GDPR is more prescriptive as to what they should include and how they should be prepared. In particular they must be easy to understand and not excessively long.

NEW Registration

Under the DPA all data controllers have to register with the ICO. The GDPR removed this requirement but it is one of the areas where the derogations for individual countries apply. The UK government has, accordingly, included a provision in the Digital Economy Act making it a legal requirement for data controllers to pay the ICO a data protection fee. See the ICO blog for further details.

Breaches

A breach is defined as a breach of security leading to the destruction, loss, alteration, unauthorized disclosure of, or access to, personal data. It is, therefore, more than the loss of personal data.

NEW Reporting Requirements re: Breaches

The GDPR will introduce a duty on both data processors and data controllers to report data breaches (within 72 hours) to the relevant supervisory authority where it is likely to result in a risk to the rights and freedoms of individuals.

Where a breach is likely to result in a high risk to the rights and freedoms of individuals, controllers and processors must also notify those concerned directly.

Fines and Sanctions

The GDPR has introduced much higher fines and a wider range of sanctions for data breaches. See the ICO's blog on their approach to this issue.

Further Information

- ICO's Data Protection Reform webpage for a continually updated guide to the GDPR
- The EU's Article 29 Working Party news page for updates on their latest guidance
- ICAEW's Guide to the GDPR
- ICAEW's FAQS GDPR for Accountants: Your Questions Answered (all available here)
    - What is the GDPR
    - GDPR – What does it mean for Accountants?
    - A GDPR Checklist
    - GDPR: Your Questions Answered Webinar Q and A Part One – General
    - GDPR Your Questions Answered Webinar Q and A Part Two – Consent and Marketing
    - Pension Funds
    - Engagement Letters and Privacy Notices
- ICAEW Webinars – see Events webpage for details

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.

Chartered Accountants' Hall
Moorgate Place, London
icaew.com

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