ICAEW
BUSINESS LAW / IT FACULTY

FAQs

GDPR FOR ACCOUNTANTS: YOUR QUESTIONS ANSWERED

Updated May 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 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. Members are advised to seek specific legal advice before taking or refraining from taking any action in relation to the matters outlined

GDPR: WHAT DOES IT MEAN FOR ACCOUNTANTS?

Introduction

This guide is designed as an introduction to the GDPR for members and member firms and explains what the changes will mean for accountants. It is part of a series designed to answer the questions that members have been asking about the GDPR. The first of these are: What is the GDPR? an overview of the key terms and concepts of the GDPR and A GDPR Checklist suggests the key steps members should take to get themselves GDPR ready by 25 May 2018. More FAQs are planned and will be available on the ICAEW GDPR webpage.

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 the 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 contact our Technical Advisory Service.

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.

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 a new approach. It will therefore replace the UK's Data Protection Act 1998 (DPA 98).

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, a new UK Data Protection Act (currently the Bill is going through Parliament) will incorporate all of the GDPR as well introducing some new provisions. This is so the UK will be GDPR compliant post Brexit.

An overview of the impact of the GDPR

In this section we will consider how the GDPR will impact members and member firms. This should be read in conjunction with What is the GDPR? (for definitions of the key terms and concepts) and A GDPR Checklist (for practical tips on how to get ready for the GDPR).

Please note: this is a living document and will be amended as we receive more guidance from the ICO.

Does the GDPR still apply just to Personal Data?

Yes. As before 'personal data' 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, any indication of the intentions of the data controller or any other person in respect of the individual.

What is now included as Personal Data?

The GDPR has added to the type of data that can identify a living individual to reflect changes in technology. So as well as name, address, date of birth it now includes IP addresses, location data and cookie identifiers as well as genetic data. What is also new is that the GDPR covers both paper and electronic data. The GDPR, however, continues to apply to personal data within an automated systems and to hard-copy documents that are contained in as 'relevant filing system' (meaning a structured set of personal data that can be searched by reference to certain criteria).

Please note: the GDPR specifically excludes the processing of personal data if performed by a natural person for a purely personal or household activity such as the private use of social media.

What about the personal data processed by accountants and accountancy firms?

Accountants and accountancy firms typically process two different types of personal data: client data and firm data.

- 'Client data' is personal data received from clients in relation to professional engagements and practice.
- 'Firm data' is personal data held by a firm in relation to its own management, employees and affairs generally, including marketing databases.

The GDPR will not change this.

Are there any changes to the definition of 'processing?'

No. As under the DPA 'processing' means:

- obtaining, recording or holding information or data;
- or carrying out any operation on the information or data, including organising, adapting or altering, using, disclosing (by any means), combining with other data, blocking or removing in any other way from the record.

Does the GDPR only apply to digital processing?

No. Manual/paper records are also included if they are part of a 'relevant filing system'. This means papers stored systematically, for example, in a filing cabinet are included but ad hoc paper files are not. Members should ensure that they apply the same levels of diligence to paper records as they do digital

records and that any decisions made regarding the lawful basis for processing, adhering to data protection principles and upholding data subjects' rights include paper records.

Does the GDPR create a conflict with the ICAEW's code of Ethics and the concept of client confidentiality?

No. The core requirements for professional confidentiality and integrity will apply in all cases.

What are the GDPR's data protection principles? Is this a change?

As with the DPA, the GDPR stipulates that the processing of personal data must be in accordance with the data protection principles (see FAQs - What is the GDPR?). These have not changed, although the principle of accountability has been added.

How can I prove accountability?

Under Article 5(2) of the GDPR controllers will be responsible for, and must be able to demonstrate, compliance with the GDPR's data protection principles. This is the accountability principle. It means that internal mechanisms and control systems are put in place to ensure compliance with the GDPR and 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).

Members should, therefore, have written policies and procedures set out in a Data Protection Policy and all staff will need 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. Members are advised to consider the various schemes available that can be used to demonstrate this such as the National Cyber Security Centre's Cyber Essentials and Cyber Essentials Plus or IASME and ISO 27001

Are the lawful bases for processing the same?

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 (see What is the GDPR?). The GDPR, however, states that you must identify upfront the lawful basis, document the reasoning and inform the data subject of it. Members will therefore need to decide which of the lawful bases are applicable, document this and inform the data subject (via a privacy notice, engagement letter or contract).

- In relation to 'client data', a lawful basis might be to meet a legal obligation (eg, a statutory audit) or legitimate interest or for the performance of a contract (if the contract is with a data subject). This will need to be specified in the engagement letter for the service offering.
- In relation to 'firm data', it may be appropriate to obtain consent to hold and process personal data for marketing purposes but for employees the basis is more likely to be legitimate interest. This is because the relationship between employer and employee is such that the employee (i.e. the data subject) is unable to give consent freely. For employees the lawful basis must be specified in the employment contract; for marketing contacts members will need to ensure they have documented how they obtained 'consent' that is GDPR compliant (see below for more on 'consent' under the GDPR).

Before you can process data you must satisfy all the principles and at least one processing condition. This must be documented.

Please note: the ICO's guidance on lawful bases includes a lawful basis interactive guidance tool to give tailored guidance on which lawful basis is likely to be most appropriate for your processing activities.

When and how can I use 'consent' as a lawful basis for processing?

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 not be assumed but should be:

- freely given;
- unambiguous;
- not obtained under duress;
- not bundled together with other services;
- renewable (ie, for a fixed period);
- revocable (and withdrawing consent must be as easy as giving consent); and
- specific.

The processor must also be able to prove that consent has been given in this way: this means the fact of consent must be documented or in the case of oral consent evidenced in some way.

Remember consent is not the only way to prove that you have the right to process personal data – there are others (see the section on lawful bases above) that may be more appropriate. For example because of the imbalance of power between an employer and employee, consent cannot be given freely but the employer does have a legitimate interest in holding personal data about its employees but only the data that is necessary to fulfil this legitimate interest.

We advise that members should review whether they are relying on consent to hold personal data, check if this is still appropriate and seek other grounds for lawfully processing personal data if necessary. In case of doubt we advise members to seek legal advice.

Please note: The ICO has now published its final guidance on consent.

Definition of data processors and data controllers – any change?

No. 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. This is a complex area and legal advice may be required. This has not changed.

If I am data processor or data controller now will I remain one under the GDPR?

Yes. The definitions have not changed for either a data controller or a data processor but it is important to be aware that the responsibilities of both have changed (see below) and will require action to ensure GDPR compliance.

Under the GDPR member firms will still be data controllers with regard to their firm data.

In respect of client data, however, it is possible, as under the DPA, that firms could be considered a processor rather than a controller. However with reference to the DPA the ICO has previously advised that an accountancy firm is always a data controller - this can, however, be solely or jointly with the client. This is because the firm will usually have flexibility over the manner in which it provides services to its clients and may not be simply acting on their instructions. We do not expect the ICO to change this view because of the GDPR, although we are seeking clarification from them. If there is any doubt regarding your status as a processor or controller we advise you to take legal advice.

What are the new responsibilities of data processors under the GDPR?

These will include the following:

- a duty to maintain records of all processing activities (and the ICO can inspect these);
- a duty to identify and document under what basis they are processing data; and
- a duty to inform your data controller if there is a breach.

Under the GDPR a processor can only act on the documented instructions of a controller (see below for more on contracts between processors and controllers).

The most significant change however is that under the GDPR data processors, not just data controllers, can be held responsible for a breach and therefore subject to sanctions and/or fines. So as well as

recording their activities and documenting the rationale for processing, processors must also have a breach plan in place so that they can inform the data controller if there is a breach.

What about data controllers? Will their role and responsibilities change once the GDPR comes into force?

The definition and role of a data controller has not changed but under the GDPR data controllers must ensure that any processors they deal with are also GDPR compliant. In line with the accountability principle this must be documented.

A new fee structure has been proposed for data controllers post 25 May 2018. See the ICO's guidance on the proposal. Before 25 May 2018 the ICO advises that data controllers should register and pay in accordance with the DPA 98.

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.

Members should review (or draw up) contracts between themselves and any third party who is either their data controller or who processes data on their behalf. This will also include cloud storage providers. If any of these are based outside of the EU (cloud storage providers frequently are) members will need to obtain a GDPR compliance statement confirming in writing that any data transferred out of the EU to or by the cloud storage provider is in line with the GDPR's equivalence rules (see below).

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 but as this is a complex area we would advise that, if in any doubt, members seek legal advice.

The GDPR refers to a Data Protection Officer (DPO) but what is a DPO and do I need to appoint one?

The DPO is a new role established by 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.

Under the GDPR a DPO must:

- possess sufficient and expert knowledge of data processing (including the relevant legislation);
- be able to avoid any conflicts of interest between their role as a DPO and any other role they perform within the organisation; and
- be able to act independently ie, they must not be instructed on how to carry out their functions or how to interpret the legislation.

To ensure a DPO can act with the necessary degree of autonomy the GDPR states that a DPO cannot dismissed or penalised for performing their task.

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.

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, for example, are 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.

The GDPR does not define 'large-scale' but the latest EU Article 29 Working Party guidance suggests that the following would constitute 'large-scale' processing:

- processing of patient data in the regular course of business by a hospital;
- processing of travel data of individuals using a city's public transport system (e.g. tracking via travel cards);
- processing of real time geo-location data of customers of an international fast food chain for statistical purposes by a processor specialised in these activities;
- processing of customer data in the regular course of business by an insurance company or a bank;
- processing of personal data for behavioural advertising by a search engine; or
- processing of data (content, traffic, location) by telephone or internet service providers.

The following are given as examples of what would not constitute large-scale processing:

- processing of patient data by an individual physician; or
- processing of personal data relating to criminal convictions and offences by an individual lawyer.

This suggest that most accountancy practices would not be involved in large –scale processing and so will not need to appoint a DPO but if you are unsure whether you need to appoint a DPO we advise you to seek legal advice.

Can I appoint a DPO even if I don't need to under the GDPR?

Yes but the responsibilities of and protections afforded to a DPO means this may not always be the best way forward. A Head of Privacy may be more appropriate but whatever the title the person appointed or assigned must have sufficient authority to ensure GDPR compliance is achieved.

Please note: If you don't need to appoint a DPO our advice, nonetheless, is that you must appoint someone senior to oversee and monitor GDPR compliance both pre and post 25 May2018.

How will the new rights of individuals affect my accountancy practice?

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 – see below);
- Right to restrict processing (see below);
- Right to data portability (see below);
- Right to object (see below); and
- Rights re: automated decision making and profiling.

All these rights require processes to be in place to ensure that they can be met. It is worth bearing in mind, however, that not all the rights are absolute and you can take a risk based approach and decide

not to have procedures for certain rights if it is very unlikely that a data subject will ask you to enforce them. For accountancy practices we believe this is most likely in regard to the new rights regarding automated decision making and profiling but that all the other rights may be enforceable in certain circumstances.

Can my clients or employees ask for erasure?

Under the right to erasure (or 'right to be forgotten') a data subject is entitled to ask a data processor to delete/erase the personal data held by them (and by any third party) and the processor must comply with this request. This right is not, however, absolute unless the data processor is relying solely on the consent of the data subject as the legal basis to process the data. In addition, where the personal data is no longer necessary in relation to the purpose for which it was originally collected then the right to be forgotten can be applied.

If the data is processed under any other processing condition, such as legitimate interest, then there is no automatic right to be forgotten. This would apply to client data held for audit, tax, anti - money laundering or other regulatory purposes.

Where the personal data is held under a lawful basis other than consent and is no longer necessary in relation to the purpose for which it was originally collected (eg, personal data held as part of an audit assignment but the period it has been held exceeds the statutory requirements) then the right to be forgotten can be applied. Likewise, if there are no other overriding legitimate grounds for the processing (including storage) or where the data has been processed for direct marketing purposes, then the right to be forgotten can be enforced.

If you have to respond to a request for erasure, then you will need to ensure that all the personal data of the data subject is erased. This will include data held by third parties such as a cloud provider whether in the UK, EU or anywhere else. It will not necessarily include archived data as the ICO has indicated that only reasonable endeavours should be undertaken to ensure all data is deleted. It is therefore advisable to put in place policies to deal with such requests now rather than waiting until you receive such a request.

Who has the right to object to processing?

The right to erasure should not be confused with a data subject's right to object to all further processing, including the storage, of their personal data ('right to object'. This includes data collected for the purposes of direct marketing and profiling. The processor must agree to a data subject's objection to processing if there is no lawful reason for them to continue to hold the data. Again it is advisable to put in place policies to deal with such requests now rather than waiting until you receive such a request.

What is the right to restrict processing?

Under this right a data subject can ask for all future processing of data to stop. Data can still be stored but cannot be further processed. This right existed under the DPA so is not new but should not be confused with the right to erasure. Again it is advisable to put in place policies to deal with such requests now rather than waiting until you receive such a request.

Who has a right to data portability?

The right to data portability allows individuals to obtain and reuse their personal data for their own purposes across different services. This means they should be able to move, copy or transfer personal data easily from one IT environment to another in a safe and secure way. This right is primarily designed to enable consumers to take advantage of applications and services which can use their data to find them a better deal, or help them understand their spending habits and as such we believe it is unlikely (but not impossible) that accountancy firms will be asked to deal with such a request.

Are there any changes to the rules about Subject Access Requests (SARs)?

Yes. Data subjects will still be able to make a SAR but an organisation may no longer charge a fee for them and must now respond within 30 days (previously 40 days). All SARs must be responded to unless a controller can show that the request is manifestly unfounded or excessive. Again members should establish procedures to deal with SARs.

How does the GDPR change the rules on document retention?

The GDPR, like the DPA, stipulates that data must only be held for the purpose for which it was collected and only for 'as long as necessary', although it does not specify what is meant by '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.

How long is 'necessary' for client data?

This is likely to be determined and/or affected by a number of factors as follows:

- Audit files and papers containing personal data – statutory audit regulations;
- Tax files – HMRC regulations;
- Criminal cases e.g. money laundering – legal requirements;
- Contracts – for the life of the contract; and
- Employee details – statutory requirements.

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 review decisions must be made whether they do need to hold it and polices drafted accordingly.

Please note: if a firm drafts a policy on how long, for example, the personal data of former and prospective employees should be held, the data held must only be that which it is necessary ie, not all the personal data. For example, a firm may determine that name and address may be all that is necessary to hold to enable the firm to contact a former employee, for a specific purpose (eg, changes to a pension scheme, employment opportunity) in the future.

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.

The new fines are very high – what I can do to reduce the risk of a potentially ruinous fine?

The fines are potentially very large but the ICO has indicated that the Information Commissioner will not automatically impose the top level of fines as their aim is to encourage organisations to take their data responsibilities seriously rather than bankrupt organisations. So if an organisation has done everything it could to mitigate a breach then this will be taken into account by the ICO. This is why the most effective action for members to take now is to review and enhance their cyber security, document their policies and process action taken and to update or create processes that document when and how policies are implemented and maintained.

Is it true that employees and clients could claim compensation for a breach?

Yes. Clients and employees, as data subjects, can make a claim against both data processors and data controllers if they can prove they have suffered damage or distress as a result of the breach. The mere fact of a breach, therefore, will not automatically mean you will have pay out compensation but it does mean that any breach response plan should include an assessment of just who could be impacted (and how) by the breach.

Do all breaches have to be notified to the ICO within 72 hours?

Yes and No. Any breach should be recorded (including the action taken) but it only has to be reported to the ICO if is likely to result in a risk to the rights and freedoms of individuals. These include the risk of discrimination, damage to reputation, financial loss, loss of confidentiality or any other significant economic or social disadvantage as a result of the breach.

The ICO has advised that this needs to be assessed on a case by case basis and has given the following examples of when and when not to notify them:

- you will need to notify the ICO about a loss of customer details where the breach leaves individuals open to identity theft; but

- you will not need to notify them if the breach has resulted in the loss or inappropriate alteration of a staff telephone list.

We advise that members should put in place a plan of action to deal with breaches and test it before any breach occurs.

Do I have to notify anyone else of a breach?

- Data Processors must now inform their data controller.
- Data Controllers must inform the data subjects if there is a high risk that they will be impacted adversely by the breach.

In both cases this must be as soon as feasibly possible and without undue delay.

What is Data Governance?

The GDPR imposes on organisations the need to reduce the risk of any breaches and to prove that they take data governance seriously by, for example, putting in place and following proportionate data governance procedures. Data Privacy Impact Statements, Privacy notices and the concept of Privacy by Design are all ways to embed data governance in to the operations of an organisation.

What is a (Data) Privacy Impact Assessment? When will I have to prepare one?

These must be carried out to assess the risk to an individual's rights when, for example, introducing new technology or new working practices.

Please note: The ICO has issued guidance on completing Privacy Impact Assessments (PIA) under the DPA 98. It is currently updating this guidance to reflect the provisions of the GDPR but has advised organisations that its existing guidance is a good starting point for organisations.

What does 'Privacy by Design' mean and will it apply to my practice?

This is a new concept and means that the protection of privacy must be built into all decision making processes and at the start of any new service development or process development. It covers both technological and organisational measures and applies to all organisations. So if a firm is considering, for example, changes to working practices (eg, homeworking), an office redesign or installing new technology then means to protect the privacy of data subjects must be included in the decision making process and the rolling out of the change. This would include, but is not limited to, a consideration of how home workers will ensure any personal data is held securely on any personal equipment used (if this is permitted), or how the disposal of old filing cabinets, paper records and computer equipment should be undertaken to ensure that personal data does not fall into the wrong hands.

What is a Privacy Notice?

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. The ICO has issued guidance on privacy notices and ICAEW have issued a helpsheet and template for members.

Will engagement letters have to change?

Yes. All engagement letters will have to be updated to inform clients that the GDPR (and the new Data Protection Act once it comes into force) is the applicable legislation and as before explain how you will use the personal data of your clients in line with the GDPR and other applicable legislation. Care should be taken to ensure that there is no bundling of services eg, an engagement letter for an audit assignment should not also imply that by accepting the terms of this service offering the client is also consenting to the receipt of marketing or promotional material from your practice.

ICAEW has prepared a helpsheet and pro forma paragraphs to include in engagement letters issued after 25 May 2018 and a covering letter to amend engagement letters issued before 25 May 2018.

Further Information

- ICO's Guide to the GDPR for a continually updated guide to the GDPR
- ICO guidance for Small Organisations
- The EU's Article 29 Working Party news page for updates on their latest guidance
- ICAEW's Guide to the GDPR – a webpage dedicated to the GDPR with our guidance and articles from third parties
- ICAEW's FAQS GDPR for Accountants: Your Questions Answered – 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
- Technical Advisory Service Data Protection Helpsheets
- Engagement Letters and Privacy Notices guidance and templates
- ICAEW Webinars – see Events webpage for details

ICAEW connects over 150,000 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 ethics@icaew.com