Think Ahead

Technical factsheet:

General Data Protection Regulation (GDPR)

April 2018

CONTENTS

1. What is GDPR?

A new European Union (EU) data protection framework, the General Data Protection Regulation (GDPR), takes effect from 25 May 2018. From this date onwards all organisations, including accountancy practices and their business clients, will have to be able to show they have systems in place that meet the GDPR standards.

The GDPR builds on the *concepts and principles* in the current Data Protection Act (DPA). In addition to the GDPR, the UK will have a new Data Protection Act. The new act:

a) supplements the GDPR in the UK
b) implements the Law Enforcement Directive
c) extends data protection laws to areas not covered by GDPR.

The government has confirmed that the UK's decision to leave the EU will not affect the commencement of the GDPR. Affected organisations therefore need to act now to ensure they are compliant by May 2018.

2. How GDPR is different to the old Data Protection Act?

The GDPR includes a number of data protection principles, which set out the main responsibilities for organisations. GDPR takes a holistic view of personal data security, which will require accountancy practices to carefully match their compliance efforts to their

particular circumstances. These principles are similar to those in the DPA, but with some added detail.

A key change is that the GDPR introduces a new principle of:

Accountability

This requires organisations to actively show how they comply with data protection principles, for example by:

- having effective policies and procedures in place
- providing comprehensive, clear and transparent privacy policies
- appointing a data protection officer (DPO) where appropriate
- implementing technical and organisational measures to show that they have considered and integrated data protection into their processing activities (referred to as data protection by design and default)
- Carrying out data protection impact assessments (also known as privacy impact assessments) in certain high-risk circumstances.

Other important new measures and changes introduced by the GDPR include:

Lawful bases for processing personal data

Under the GDPR, organisations have to identify and *document* their lawful basis for processing data. The basis has to be included in the organisation's privacy notice (ie the information given to an individual when the organisation is collecting their data), and can affect the rights that individuals have.

Consent

The GDPR tightens the rules around consent given by data subjects:

- Consent must be specific, informed, unambiguous and given freely.
- There must be a positive opt-in; consent cannot be inferred from silence, inactivity or pre-ticked boxes.
- All requests for consent must be separate from other terms and conditions.
- It must be as easy for individuals to withdraw consent as it is to provide it.

Individuals generally have more rights where an organisation relies on consent as a lawful basis. Existing consents will only be acceptable under the GDPR if they meet these new, stricter requirements.

Children's data

The GDPR brings in special protections for dealing with the personal data of children if information society services are offered directly to children (eg through social networks). Further guidance is available from the Information Commissioner's Office (ICO).

- The privacy notice must be written in a clear, plain way that the child will understand.
- If consent is the legal basis for processing, a parent or guardian's consent may be required to process the data. The UK's proposed age limit for valid consent is 13.

Transfer of data

The GDPR imposes a *prohibition on the transfer of personal data outside the European Economic Area*. Transfers can only be made where certain conditions are met, including that the receiving organisation has provided adequate safeguards (such as standard contractual clauses).

Transfers may also be made where derogations apply, such as with the individual's informed consent to the transfer or that it is necessary for the performance of a contract. However, the derogations should only be used in exceptional circumstances for one-off transfers. They should not be used as the basis for regular transfers of personal data outside the EU.

Data breaches

Organisations must notify the ICO within 72 hours of any personal data breach that is likely to result in a risk to the rights and freedoms of individuals.
Individuals also need to be informed directly and without undue delay if there is likely to be a high risk to their rights and freedoms as the result of a breach.

3. Why does it apply to members?

The GDPR applies to both data controllers and processors of *personal data* which either:

- operate within the EU,
- operate outside the EU but their activities relate to EU individuals, or
- process personal data in the context of an establishment within the EU, regardless of whether the actual processing takes place within the EU.

The definition of personal data has, however, been expanded, and can now include online identifiers such as IP addresses and data that is given a pseudonym (for example, key coding, where names etc are changed into numbers based on a key). The GDPR provides more rights to individuals than before.

Data controllers determine how and why personal data is processed. Data controllers are not relieved of their obligations where a processor is involved; instead, the GDPR imposes further obligations regarding the contracts they hold with processors.

Data processors process personal data under the instruction of controllers. The distinction is not always clear, and it is advisable for members to ensure that they meet the requirements for both data controllers and processors.

Member firms are a data processor or data controller when providing services to clients, eg audit, review, AUP, non-audit assurance etc, depending upon the contractual relationship. A firm can be a data controller for one processing activity but a data processor for another. This should be decided on a case-by-case basis.

As per the ICO guidance a firm will always be a data controller because accountants and similar providers of professional services work under a range of professional obligations, which oblige them to take responsibility for the personal data they process. 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

For example, if the accountant detects malpractice while doing the firm's accounts they may, depending on its nature, be required under his monitoring obligations to report the malpractice to the police or other authorities. In doing so an accountant would not be acting on the client's instructions but in accordance with its own professional obligations and therefore as a data controller in their own right.

Where specialist service providers are processing data in accordance with their own professional obligations, they will always be acting as the data controller and cannot agree to hand over or share data controller obligations with the client in this context.

For instance:

Tax advisers may be both data controllers and data processors. Historically, tax advisers have been required to register with the ICO as data controllers where they process any data electronically.

Payroll processors: where they prepare payroll calculations and submissions for employers, it is generally accepted that the employer is the data controller and the payroll provider is the data processor as they are processing information on behalf of the controller.

Subcontractors: members may also be data processors where they are purely processing the information at the direction of the firm contracting with the client.
Anyone currently subject to the DPA is very likely to also be subject to the GDPR. GDPR also does not apply to processing *'…by a natural person in the course of a purely personal or household activity'.* This is the equivalent of the 'domestic purposes' exemption under section 36 of the current DPA.

4. What do organisations need to do now?

Any businesses that are data controllers or processors need to consider what new obligations they will have under the GDPR and what changes they may need to make before May 2018 to ensure they are compliant.

As an initial step, they should raise awareness of the impending changes with key decision-makers and personnel in the business.

In terms of practical steps, organisations are recommended by the ICO to:

- **document** what personal data they hold, where it came from and who it is shared with, and maintain these records going forwards
- **review** current privacy notices to see what changes are needed
- **check** that procedures cover all the new and expanded rights individuals have
- **identify** their lawful basis for processing data and create an updated letter of engagement and privacy policies specifying the firm's obligations and responsibilities to communicate to clients.

- review how they seek, record and manage **consent** to see if this is up to the GDPR standard
- make sure the right **procedures** are in place to report data breaches
- designate a **data protection officer** if necessary.

The ICO website has a number of helpful webinars and documents to assist organisations, including:

- a more detailed Overview of the GDPR
- a 12 steps to take now summary
- a Getting ready for the GDPR toolkit.

The ICO checklist indicates that organisations should document what personal data is held, where it comes from and who the organisation shares it with. An information audit will be an important step to form the basis of the 'records of processing' required under Article 30 of the GDPR.

The ICO has not produced information audit templates but one suggested approach might be to:

- Note down all the computer systems used by the organisation and understand what personal data is held on those systems.
- Contact all principals and members of staff and ask them to list out all information they hold outside these systems including:
    - where the data is stored
    - how it is named
    - what it is used for
    - what types of information are held
    - who makes sure this information is kept up to date
    - who can access the information
    - what security settings are there on the information
    - how/when old files are deleted and disposed of.

5. What records should organisations retain?

The short answer is the *minimum amount* necessary.

Under the GDPR, as with the DPA, data has to be *'adequate, relevant and limited to what is necessary in relation to the purpose for which they are processed*'. That obligation applies to the amount of personal data collected, the extent of their processing, the period of their storage and their accessibility.

The GDPR applies to both electronic personal data and to manual filing systems where personal data are accessible according to specific criteria. This now includes chronologically ordered sets of manual records containing personal data.

Personal data that has been pseudonymised – eg key-coded – falls within scope of the GDPR, with the pseudonymisation acting as a safety measure. Truly anonymised data, however, does not fall within scope (ie it is not possible to re-identify the individual to whom the data originally related).

Certain types of personal data are defined as 'special categories' under GDPR. These are broadly the same as 'sensitive personal data' under the DPA, but with some additional categories, such as biometric data in some circumstances, and genetic data. Data controllers need to be able satisfy additional conditions to be able to process special categories of personal data. These are listed in Article 9 of the GDPR, which also lists the types of personal data considered to be 'special categories'.

6. How long should members hold client data under the GDPR?

The GDPR does not set specific limits on data retention. It requires that the period for which personal data are stored is no longer than necessary for the task performed. This requirement is essentially the same as the requirement under Principle 5 of the DPA.
The ICO says that is good practice to regularly review the personal data held, and if more than small amounts of personal data are held members should establish standard retention periods for different categories.

When deciding how long to retain data, you should:

- consider legal retention period requirements
- the period of time during which actions may be brought in the courts, and which records and working papers might be needed as evidence, factoring in whether the likelihood of this makes the retention period justifiable
- rhe period of time for which information in the working papers might be required for use in compiling tax returns
- review the length of time you keep personal data
- consider the purpose or purposes you hold the information for in deciding whether (and for how long) to retain it
- the current and future use and relevance of the information
- the costs, risks and liabilities associated with retaining it
- the ease or difficulty of making sure it remains accurate and up to date
- securely delete information that is no longer needed for this purpose or these purposes; update, archive or securely delete information if it goes out of date.

ACCA Rulebook guidance for the retention of working papers states that a professional accountant shall use their own judgement in determining the period for which working papers should be retained. The minimum periods for which a professional accountant shall retain working papers are as follows:

Audit working papers	7 years
Files on clients' or former clients' chargeable assets and gifts	8 years (then return them to the client or former client or obtain authority from the client or former client for their destruction)
Files of professional accountant as trustee (other than trustee in bankruptcy)	For the period of trusteeship and 7 years thereafter
Investment business advice	For the life of the policy and 3 years thereafter

Tax files and other papers that are legally the property of the client or former client shall be returned to the client (or former client) after seven years or specific authority obtained for their destruction.

Where it is possible that a defect in advice rendered to clients or former clients may not become apparent for a longer period than those set out above, the professional accountant may consider it prudent to retain working papers for at least this period of time. For example, the professional accountant shall consider retaining advice given on the creation of a trust for the period until the trust comes to an end.

A similar guidance from the Chartered Institute of Taxation and the Assocation of Taxation Technicians, *Professional Rules and Practice Guidelines 2011,* states that members should implement a policy for retention of documents and records in their files. It is recommended that members should keep records and working papers for at least **seven** years from the end of the tax year, or accounting period, to which they relate or such longer period as the rules of self-assessment may require, which reflects the Statute of Limitations.

Retention schedules must be robust and justifiable, and differentiate legal requirements from professional best practice. Members need to factor in any specific obligations with respect to HMRC time limits for discovery assessments, information requests etc with practical factors such as clients often not keeping copies of information which they have provided to their adviser.

The ICO acknowledges that there are various legal requirements and professional guidelines about keeping certain kinds of records – such as information needed for income tax and audit purposes. As such guidelines are based on solid foundations, an organisation is unlikely to be deemed to have kept the information for longer than necessary. Whatever is decided upon, the retention period or criteria used to determine the retention period have to be included in your privacy statement under the GDPR. Members may choose to adopt different data retention policies for different types of client and these should be included in the privacy policy and made clear to the client.

Ex-clients' records

There are no specific limits or guidance on this but it may depend, in part, upon the lawful basis for processing that data and what is necessary (rather than just useful) for that purpose.

If members are relying on consent rather than because processing is necessary for contract, they need to check this extends to situations where individuals are no longer clients:

- The GDPR does not set a specific time limit for consent.
- Consent is likely to degrade over time, but how long it lasts will depend on the context; members will need to consider the scope of the original consent and the individual's expectations.

As noted above, for general data retention policies, members need to balance the requirement to only keep data for the minimum amount of time with their obligations to HMRC, clients etc.

Anti-money laundering rules require members to keep records for **five** years after the relationship ends. Furthermore, the updated money laundering regulations (The Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017) set out in Regulation 40 (5) that any personal information obtained for the purposes of the regulations must be deleted after five years from the end of a business relationship unless

- the business is required to retain it under statutory obligation, or
- the business is required to retain it for legal proceedings, or
- the data subject has consented to the retention.

The ICO's data protection guidance acknowledges that it may not be necessary to delete all personal data when the relationship ends. Members may need to keep some information so that they can confirm that the relationship existed – and that it has ended – as well as some details. Under the GDPR, individuals have a right to have personal data erased, known as the 'right to be forgotten'. This could apply where processing is no longer necessary for the purpose; where the data subject withdraws consent; if the individual objects to processing undertaken for legitimate interests; or where there are legal requirements to do so. There are exemptions from this right and members should seek further guidance as required.

If a client leaves and asks for all personal information to be deleted, members should assess whether further retention is necessary and respond to the client within **one month**, explaining the next steps and rationale.

Delete data

ICO information on deleting information is available here. ICO guidance states that 'The word 'deletion' can mean different things in relation to electronic data.

- There is a significant difference between deleting information so it cannot be retrieved and merely archiving data, which is not deletion and therefore still subject to the same data protection rules as 'live' data.
- There has to be a justification for retention more than 'just in case'.
- Members need to review the data they currently hold, consider whether they need to keep it or not, and delete records where appropriate. Following these review members may need to contact clients and agree with them the ongoing retention of records in some cases.
- If you use a professional to delete records on your behalf, you may ask for a certificate for its secured deletion.

Note that the GDPR introduces a right to erasure. The circumstances where the right applies are set out in Art17 (1). If any of those apply, and there are no overriding considerations from Art17 (3), then the data would have to be erased.

In terms of Art17 (3)(e), there would have to be some sort of reasonable expectation of a legal claim. Just that there might be a claim at some point for some unforeseeable reason isn't going to be enough, otherwise everyone could justify retaining anything.

7. What are the suggested secure ways to communicate personal data?

A risk-based approach should be adopted when deciding what level of security is needed in relation to information. The ICO guidance indicates that 'The GDPR requires personal data to be processed in a manner that

- ensures its security,
- protects against unauthorised or unlawful processing and
- protects against accidental loss, destruction or damage.

ICO guidance is a good starting point and can be found here under the heading 'Security'. The ICO's guidance on information security indicates that there will not be a 'one-size-fits-all' solution to information security.

ICO's stand on using various communication means is as below:

Portal: These days many firms use portals to receive information from clients and send out tax returns. Use of portals is not mandatory but it can be a useful tool in maintaining data security. Find out more here.

Emails: GDPR does not introduce a ban on the transfer of personal data or tax returns by email but there are risks in using this method. The client should be made aware of these risks and the organisation should consider where additional security is appropriate. Find out more here.

Dropbox: Members need to take their own view on the security of using programs like Dropbox. The ICO suggests that the more sensitive the data, the less appropriate it will be to use 'off-the-shelf' cloud storage where the data controller is not in control of the terms and conditions.

Encryption: When firms are communicating on emails, their software provider may be able to provide more details about the various security measures that are available – for example, encryption. Encryption is not mandatory under the DPA or GDPR but it can be one method that organisations can use to protect against accidental loss, destruction or damage of data. Further guidance on encryption is included on the ICO website. ICO guidance also includes details on accredited products for data encryption.

8. What records need to be kept to be GDPR compliant?

A key change under the GDPR is accountability: members need to demonstrate that they comply with the principles and the GDPR states explicitly that this is their (ie members') responsibility.

This includes:

- providing clear and transparent privacy policies
- if relying on consent, being able to demonstrate that the data subject has given a valid consent. This should include keeping records to show:
    - who consented
    - when they consented
    - what they were told at the time
    - how they consented, eg for written consent a copy of the relevant document
    - whether they have withdrawn consent, and if so when.
- If members have 250 or more employees, keeping additional written records of all processing activities including:
    - name and details of organisation, and, where applicable, other controllers, the member's firm's representative and data protection officer
    - purposes of the processing
    - description of the categories of individuals and personal data
    - categories of recipients to whom the personal data has been or will be disclosed
    - details of transfers to third countries (ie outside the EU), including the safeguards in place
    - retention schedules (where possible)
    - description of technical and organisational security measures (where possible).
- There is a limited exemption if members have fewer than 250 employees. Detailed records of processing activities only have to be kept where one of the following applies:
    - higher risk processing, such as processing personal data that could result in a risk to the rights and freedoms of an individual
    - processing that is not occasional
    - processing of special categories of data (including that revealing race or ethnic origin, religious beliefs, political opinions, health data or genetic/ biometric data) or criminal convictions and offences.

- Carrying out and documenting a Data Protection Impact Assessment (DPIA, also known as privacy impact assessment) if processing is likely to result in a high risk to individuals, for example:
    - where new technologies are used
    - where a profiling operation is likely to significantly affect individuals
    - large-scale processing of special categories of data (race, health records, sexual orientation, religion etc) or personal data relating to criminal convictions or offences.
- Appointing a Data Protection Officer (DPO) where the business in question:
    - is a public authority,
    - carries out large-scale systematic monitoring of individuals (eg online behaviour tracking), or
    - carries out large-scale processing of special categories of data such as health records, or data relating to criminal convictions and offences.

Further information can be found here and here on the ICO website, and this includes templates for the documentation of data processing.

9. Do the firms have to issue new engagement letters and privacy policies?

a) Engagement letters: As per *ACCA Rulebook* guidance on 'section B9 Professional liability of accountants and auditors', 'A professional accountant shall record in writing and send to their client a letter of engagement which sets out the terms under which they are agreeing to be engaged by their client before any work is undertaken or, if this is not possible, as soon as practicable after the engagement commences.

Normally firms will be processing data on a contractual basis in order to supply a service to a client, rather than on the basis that the client has given consent for data to be processed. However, members do need to be clear within the business about the basis on which information is being processed for different purposes.

Whatever the legal basis for processing, members must also consider the fairness and transparency requirements, ie explaining to the clients how their personal data will be processed.

Firms should review their existing processing regarding 'Consent' and 'Lawful basis for processing data' as below:

- As the GDPR tightens the rules around **consent** given by data subjects, all consents in engagement letters (and elsewhere) will need to reflect these stricter conditions. If existing consents don't meet GDPR standards, members will need to seek fresh GDPR-compliant consents from clients.
- It is a requirement of the GDPR that the lawful basis for processing data is established, so this is an exercise members need to undertake anyway.
- The data is necessary for performance of a contract with the individual: for example, to supply goods or services they have requested, or to fulfil your obligations under an employment contract.
- Legitimate interests: private sector organisations can process personal data without consent if they have a genuine and legitimate reason (including commercial benefit), unless this is outweighed by harm to the individual's rights and interests.

The ICO has published guidance on consents under the GDPR, and guidance on the lawful bases for processing within its Guide to the GDPR.

b) Privacy policies: requirements for privacy policies (also referred to as privacy notices) are more detailed under the GDPR, so existing ones need to be reviewed to make sure they are compliant:

- They need to be in clear and plain language, transparent and easily accessible.
- Some further information is required in privacy policies under GDPR – lawful basis for processing, data retention policies and the fact that individuals have a right to complain to the ICO if they think there is a problem with the way you are handling their data.
- Privacy policies should be updated as necessary for the introduction of the GDPR in May 2018.

The ICO believes that if the good practice recommendations in it Privacy notices code of practice is followed, the adviser will be well placed to comply with the GDPR regime. HMRC's data protection policy and procedures refer to the way in which it may use information and share it with others including tax agents.
Tax agents will need to ensure that their privacy policy is provided to clients and reflects the fact that they may give information to HMRC.

10. What are the penalties for non-compliance with GDPR?

The non-compliance of GDPR can be very expensive due to the strict rules to follow for the security of personal data. Sometimes the costs may push the SME out of business. The administrative fines are discretionary rather than mandatory; they must be imposed on a case-by-case basis and must be 'effective, proportionate and dissuasive'.

There are two tiers of administrative fines that can be levied:
1) up to €10m, or 2% annual global turnover – whichever is higher
2) up to €20m, or 4% annual global turnover – whichever is higher.

The fines are based on the specific articles of the regulation that the organisation has breached. Infringements of the organisation's obligations, including data security breaches, will be subject to the lower level, whereas infringements of an individual's privacy rights will be subject to the higher level.

When deciding whether to impose a fine and the level, the ICO must consider:

- the types of personal data involved
- the nature, gravity and duration of the infringement
- the intentional or negligent character of the infringement
- the way the regulator found out about the infringement
- any action taken by the organisation to mitigate the damage suffered by individuals
- technical and organisational measures that have been implemented by the organisation
- any previous infringements by the organisation or data processor
- the degree of cooperation with the regulator to remedy the infringement.

Besides the power to impose fines, the ICO has a range of corrective powers and sanctions to enforce the GDPR. These include issuing warnings and reprimands; imposing a temporary or permanent ban on data processing; ordering the rectification, restriction or erasure of data; and suspending data transfers to third countries.

It is therefore important to make sure that you have a robust breach-reporting process in place to ensure you detect and can notify a breach, on time, and to provide the necessary details.