General Data Protection Regulation (GDPR) Frequently Asked Questions

22 May 2018

Contents

Introduction 3

What is GDPR? 3

Who does the GDPR apply to? 3

Are tax advisers data controllers or data processors? 4

What are the data protection principles which apply under GDPR? 4

What are the individual's rights under GDPR? 6

What do organisations need to do now? 7

Holding of Data 7

What is the scope of GDPR? A lot of articles relate to digital records only. Does it also cover paper records? 7

What client data should members hold? 8

What should be included in an information audit and is there ICO guidance on what a good audit looks like? 8

How long should members hold client data under the GDPR? 9

How long should members keep information for an advisory client and what about the situation where the client comes and goes for ad hoc advice? 10

What client data should members retain when a client moves to another agent? 10

What does it mean to delete data? 11

What should be done about deleting copies of claims and elections etc submitted for previous clients? HMRC will not keep copies and clients may need them in the future if HMRC raise enquiries, there are Tribunal cases etc. 11

What should be done where a firm has been in operation for a very long time and has retained all records since the start of the business? 12

Contacting Clients 12

What data security is required under GDPR when interacting with clients? 12

Do firms have to use portals to receive information from clients and send out tax returns? 12

What if clients refuse to use secure portals for the exchange of information. Can information still be exchanged by email? 12

Can clients continue to use Dropbox to transfer data? 13

Is it acceptable under GDPR to send pdf versions of tax returns to clients and do returns have to be password protected? 13

Do emails to clients have to be encrypted? If so where can information be found on how to do this? 13

Client bank details are not stored on the firm's system but they can be recorded on a client's tax return where a tax refund is being claimed. If someone outside the firm (other than the intended recipient) sees these details is there a problem? 13

Lawful bases for processing 14

Do engagement letters need to ask for the new consent under GDPR? 14

Will new engagement letters have to be sent to all clients? 15

Transparency 16

When should privacy policies be updated? 16

Does anything need to be included in policies in relation to the HMRC / agent relationship, such as in relation to provision of information on the client? 16

Records 16

What records need to be kept to be GDPR compliant? 16

Where can further information on documentation required under GDPR be found? 17

Introduction

What is GDPR?

A new EU data protection framework, the *General Data Protection Regulation* (GDPR) takes effect from 25 May 2018.

The GDPR builds on the concepts and principles in the current Data Protection Act (DPA). There are however some significant enhancements and new elements, the most important of which are summarised below.

In addition to the GDPR, the UK will have a new Data Protection Act. This supplements the GDPR in the UK, implements the Law Enforcement Directive and 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.

The Information Commissioners Office (ICO) has a substantial amount of information and guidance on its website and members are encouraged to refer to it: http://www.ico.org.uk

Who does the GDPR apply to?

The GDPR applies to both controllers and processors of personal data. Controllers determine how and why personal data is processed. Processors process personal data under the instruction of controllers.

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.

Like the DPA, the GDPR applies to personal data. The definition of this has however been expanded, and can now include online identifiers such as IP addresses and data which is given a pseudonym (for example key coding, where names etc. are changed into numbers based on a key).

Anyone currently subject to the DPA is very likely to also be subject to the GDPR.

The GDPR can apply to data controllers or processors which:

- 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 Government has indicated it will implement an equivalent or alternative legal mechanism to the GDPR once the UK leaves the EU. The expectation is that this will largely follow the GDPR given the support expressed by the Government to date.

Are tax advisers data controllers or data processors?

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.

Under GDPR they need to be aware of the distinction between data controllers and data processors to determine their full responsibilities under GDPR.

The distinction is not always clear and it is advisable for members to ensure they meet the requirements for both data controllers and processors.

However, 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.

Members who are subcontractors may also be data processors where they are purely processing the information at the direction of the firm contracting with the client.

Refer to the ICO's guidance on data controllers and data processors for further information.

What are the data protection principles which apply under GDPR?

The GDPR includes a number of data protection principles which set out the main responsibilities for organisations. 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 (see below).
- 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 lawful bases are similar to those previously referred to under the DPA as *conditions for processing*, and include consent of the data subject and where processing is necessary for performance of a contract.

Identifying lawful basis has increased focus under the GDPR when compared to the DPA: the basis has to be included in the organisation's privacy notice (i.e. the information given to an individual when the organisation is collecting their data), and can affect the rights which 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 (see below) 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 (e.g. through social networks). Further guidance is available from the 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 eg. 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 Information Commissioner's Office (ICO) within 72 hours of any personal data breach which 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.

A fine of up to 10 million Euros or 2% of global turnover can apply for failure to notify a breach, as well as penalties for the breach itself.

What are the individual's rights under GDPR?

Individuals have new and strengthened rights under the GDPR with regards to their personal data, including:

- The right to be informed: organisations have to be transparent with individuals as to how they use their personal data.
    - This includes providing information on the organisation's data retention policies and the individual's rights under the GDPR.
    - This is normally achieved by providing a privacy notice
    - Requirements under the GDPR are more detailed, so existing privacy notices will need to be reviewed to make sure they are compliant. (Refer to the ICO's Privacy Notices' Code of Practice).
- The right of access – individuals have the right to confirm whether their personal data is being processed, to receive information about that processing and to have a copy provided within one month. Unlike the DPA, organisations cannot normally charge a fee for this.
- The right to rectification – individuals are entitled to have personal data corrected if it is incorrect or incomplete.
- The right to erasure – also known as the right to be forgotten – individuals can request the deletion or removal of personal data in specific circumstances (including where they withdraw consent or where the data is no longer necessary for the purpose for which it was collected).
- The right to restrict processing – individuals can block or suppress processing of personal data.
- A new right to data portability – individuals can request in specified circumstances that their data is supplied to them in a commonly used format so it can be transferred easily to another data controller, or request that the data is transferred directly to another data controller.
- The right to object – individuals can object to their data being used for direct marketing or certain other reasons (including historical or scientific research).
- Rights in relation to automated decision making and profiling – wholly automated decisions are prohibited unless certain conditions apply.

The timescale for complying with many of these rights is one calendar month, which can be extended in certain circumstances. The DPA right of access timeframe is currently 40 days.

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.
- 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

Holding of Data

What is the scope of GDPR? A lot of articles relate to digital records only. Does it also cover paper records?

The definition of personal data in Article 4 is also referenced on the ICO website:

"The GDPR applies to 'personal data' meaning any information relating to an identifiable person who can be directly or indirectly identified in particular by reference to an identifier.

This definition provides for a wide range of personal identifiers to constitute personal data, including name, identification number, location data or online identifier, reflecting changes in technology and the way organisations collect information about people."

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 (i.e. it is not possible to re-identify the individual to whom the data originally related).

Most firms maintain client records electronically but GDPR also applies to manual filing systems in defined cases.

Certain types of personal data are defined as "special categories" of personal data 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".

What client data should members hold?

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*'.

The GDPR applies to both automated personal data and manual filing systems where data is accessible according to specified criteria – this is wider than the DPA, and can include chronologically ordered manual records.

Under the GDPR the data controller has to implement appropriate measures for ensuring that, by default, only personal data which are necessary for each specific purpose of the processing 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.

What should be included in an information audit and is there ICO guidance on what a good audit looks like?

The ICO checklist on preparing for the GDPR 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 have not produced information audit templates but one suggested approach might be to:

a. Note down all the computer systems used by the organisation and understand what personal data is held on those systems.

b. 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 are old files deleted and disposed of.

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 is 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 say 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:

- 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;
- securely delete information that is no longer needed for this purpose or these purposes; and
- update, archive or securely delete information if it goes out of date.

The CIOT / ATT Professional Rules and Practice Guidelines 2011 state that members should implement a policy for retention of documents and records in their files. When deciding the retention period they should consider:

- Periods of retention required by the law;
- 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 ;
- The period of time for which information in the working papers might be required for use in compiling tax returns

Other relevant factors include:

- The current and future use and relevance of the information,
- The costs, risks and liabilities associated with retaining it; and
- The ease or difficulty of making sure it remains accurate and up to date.

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.

How long should members keep information for an advisory client and what about the situation where the client comes and goes for ad hoc advice?

See the details included above on how long members should hold data under 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.

What client data should members retain when a client moves to another agent?

There are no specific limits or guidance on this subject in the GDPR. The answer 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.

There are also anti-money laundering rules to consider, which 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 also 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. Where there is a legal requirements to retain data (distinct from professional best practice) it is unlikely they would be considered to have kept the information for longer than necessary.

As noted above, 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.

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.

What does it mean to delete data?

ICO guidance states that "The word 'deletion' can mean different things in relation to electronic data. We [the ICO] have produced detailed guidance which sets out how organisations can ensure compliance with the DPA, in particular the fifth data protection principle, when archiving or deleting personal information"

Further information on deleting information is available here. 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.

What should be done about deleting copies of claims and elections etc submitted for previous clients? HMRC will not keep copies and clients may need them in the future if HMRC raise enquiries, there are Tribunal cases etc.

As indicated above the ICO's data protection guidance acknowledges that members may not need to delete all personal data when the relationship ends. The ICO also 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 - which may form the basis of a retention schedule. There has to be a justification for retention more than 'just in case'.

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.

What should be done where a firm has been in operation for a very long time and has retained all records since the start of the business?

Members need to review the data they currently hold, consider whether they need to keep it or not, and delete records where appropriate. Following this review members may need to contact clients and agree with them the ongoing retention of records in some cases.

Contacting Clients

What data security is required under GDPR when interacting with clients?

The ICO guidance indicates that "The GDPR requires personal data to be processed in a manner that ensures its security. As well as requiring protection against unauthorised or unlawful processing it also requires protection against accidental loss, destruction or damage".

The ICO is updating guidance for the GDPR but in the meantime existing 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.

With the introduction of GDPR and the significant penalties which can be imposed it is particularly important to review current security arrangements in relation to data.

Do firms have to 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. See https://ico.org.uk/for-organisations/guide-to-data-protection/encryption/scenarios/sharing-personal-data-online/

What if clients refuse to use secure portals for the exchange of information. Can information still be exchanged by email?

A risk-based approach should be adopted when deciding what level of security is needed in relation to information. 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 see https://ico.org.uk/for-organisations/guide-to-data-protection/encryption/scenarios/sending-personal-data-by-email/

Can clients continue to use Dropbox to transfer data?

Members need to take their own view on the security of using programmes like Dropbox.

Is it acceptable under GDPR to send pdf versions of tax returns to clients and do returns have to be password protected?

Please refer to the answer given above in relation to security when using emails. Members need to take their own security measures to ensure there is no loss, destruction or damage to data being received from or sent to clients. The firm's software provider may be able to provide more details about the various security measures that are available, for example, encryption.

Do emails to clients have to be encrypted? If so where can information be found on how to do this?

Encryption is not mandatory under the Data Protection Act or GDPR but it can be one method which organisations can use to protect against accidental loss, destruction or damage of data.

Further guidance on encryption is included on the ICO website https://ico.org.uk/for-organisations/guide-to-data-protection/encryption/.

ICO guidance includes details on accredited products for data encryption https://ico.org.uk/for-organisations/guide-to-data-protection/encryption/implementing-encryption/.

Client bank details are not stored on the firm's system but they can be recorded on a client's tax return where a tax refund is being claimed. If someone outside the firm (other than the intended recipient) sees these details is there a problem?

Members should consider whether their computer systems or processing operations are accessible by anyone external to the firm. For example, if a member of staff accidentally emails a tax return which is not password protected to the wrong client then the information may become available to external individuals.

If data is not secure action needs to be taken. You should bear in mind that GDPR covers paper documents as well as digital records. Consider the security of the data you hold and the way in which it is processed and be aware that complaints can be made to the ICO about the handling of personal information.

Members must consider the breach reporting requirements under the GDPR to the ICO, and in some cases, to affected individuals too.

Lawful bases for processing

Do engagement letters need to ask for the new consent under GDPR?

In general our members will be processing client personal data under the terms of an engagement letter and therefore will be processing data on a contractual basis rather than on the basis of consent.

However some activities may be covered by consent such as marketing. 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 easy for individuals to withdraw consent.

Once the GDPR is in force all consent arrangements will need to reflect these stricter conditions.

Members are not required to automatically refresh all their existing DPA consents in preparation for the GDPR:

- Members can continue to rely on existing consents if they meet the GDPR standards.
- If existing consents don't meet GDPR standards members will need to seek fresh GDPR compliant consents from clients.

It is important to identify the correct lawful basis for processing data:

- If members do not rely on consent there is no need to refresh existing consents under GDPR.
- Individuals also have greater rights over their data under consent.
- 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.

Alternative lawful bases for processing data could include:

- 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.

CIOT and ATT pro forma engagement letters have been updated to reflect guidance in relation to GDPR. They are available here for CIOT members and here for ATT members.

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

Will new engagement letters have to be sent to all clients?

As indicated in the previous question members are not required to automatically refresh all existing Data Protection Act consents in preparation for GDPR. However, if existing consents don't meet GDPR standards members will need to seek fresh GDPR compliant consents.

However, as indicated above, in most circumstances agents 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 i.e. explaining the clients how their personal data will be processed.

As part of the review of the engagement letter guidance legal counsel indicated that "GDPR is unclear as to notification requirements where a controller wishes to continue to process personal data that were collected prior to the entry into force of the GDPR. In our opinion the prudent approach would be to send updated privacy notices and any revised contractual terms to existing clients before the GDPR enters force". It would therefore be prudent for members to consider what is currently in place with clients in relation to privacy notices, contractual terms etc and any updates which they need to issue in the run up to the introduction of GDPR or when next contacting their clients. Members may wish to prioritise the update of their engagement letters on a risk basis. In particular members should refer to paragraphs 31 and 32 of the engagement letters guidance which sets out the fact that contracts between controllers and processors **must** be in writing. The payroll schedules include an appendix which can be used as a sample from which member can prepare their own agreements for payroll or other areas where they are acting as a data processor.

Transparency

When should privacy policies be updated?

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 believe that if the good practice recommendations in their Privacy notices code of practice is followed the adviser will be well placed to comply with the GDPR regime.

Does anything need to be included in policies in relation to the HMRC / agent relationship, such as in relation to provision of information on the client?

HMRC's data protection policy and procedures refer to the way in which they 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.

Records

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 e.g. 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 (i.e. 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 which could result in a risk to the rights and freedoms of an individual,
    - processing which 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 (e.g. 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.

Where can further information on documentation required under GDPR be found?

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