Preparing for the General Data Protection Regulation: A guide for law firms

GDPR
Are you on track?

APRIL 2018

www.lawsociety.org.uk
CONTENTS

Checklist 1: Awareness .................................................. 3
Checklist 2: Information you hold ................................. 5
Checklist 3: Communicating privacy information .......... 8
Checklist 4: Individuals' rights .................................... 11
Checklist 5: Subject access requests ........................... 16
Checklist 6: Lawful basis for processing personal data .... 18
Checklist 7: Consent .................................................... 21
Checklist 8: Children .................................................. 24
Checklist 9: Data breaches .......................................... 27
Checklist 10: Data protection by design and data protection impact assessments ........................................ 30
Checklist 11: Data protection officers ......................... 33
Checklist 12: International ........................................... 35

USEFUL REFERENCE SOURCES

There are a few source materials that you may find useful to refer to in conjunction with these checklists.

- Preparing for the GDPR: 12 steps to take now, by the Information Commissioner's Office.
- The full text of the GDPR on the EUR-Lex website, to which references to Articles and Recitals in these checklists refer.
- The Law Society's GDPR webpages provide more specific guidance for law firms and collates information from external sources.

Disclaimer

The information is current as of 16 April 2018, however, the contents may be subject to change without notice. Whilst every effort has been made to ensure the accuracy and relevant scope of the information, the Law Society shall not be liable for any actions taken, or decisions made, based on the contents of this guide and you should consider taking appropriate specialist advice before proceeding in this regard.
CHECKLIST 1: AWARENESS

AT A GLANCE

This checklist covers Step 1 of the Information Commissioner’s Office’s (ICO’s) ‘12 Steps to take now’ guidance for preparing for the GDPR. It examines:

- The need for awareness raising and training about the GDPR and its impacts on your firm.

CONTEXT

You should make sure that decision makers and key people in your organisation are aware that the law is changing to the GDPR. They need to appreciate the impact that it is likely to have and identify areas that could cause compliance problems under the GDPR. It would be useful to start by looking at your organisation’s risk register, if you have one.

Implementing the GDPR could have significant resource implications, especially for larger and more complex organisations. You may find compliance difficult if you leave your preparations until the last minute.

POINTS TO CONSIDER

The Law Society’s checklists for preparing for the GDPR are based on the ICO’s already produced – and very useful – ‘12 steps to take now’ for GDPR readiness.

We’re going to assume that your firm is already complying with the Data Protection Act 1998, so we’ll stress what’s different about the GDPR, the issues you need to consider, and the practical steps you need to take to ensure you’re ready for the 25 May when the GDPR becomes law.

Although the ICO stresses that last minute preparations for the GDPR are not ideal, if you have not already done so you should prepare for compliance now.

Who needs to be aware?

Potentially everyone in your firm. The GDPR will impact your whole organisation, and the accountability requirement embedded in it means senior managers should provide leadership. Senior managers also need to understand the risks of non-compliance, both in financial and reputational terms, while anyone with a client focussed role will need to understand the GDPR’s enhanced data subject rights and their implications, and what to do in the event of a data breach.
Who should be responsible?

Whether or not your firm appoints a Data Protection Officer (DPO) [See Checklist 11], you’ll want a suitably qualified and senior person with the necessary resources to act as GDPR lead. One of their roles (and a statutory function of DPOs) should be advising your firm’s employees about their data processing obligations under the GDPR, so they should be in charge of awareness raising and the development of appropriate training.

What kinds of training do we need?

Training should reflect the policies, procedures, internal governance and technology systems used by your firm, and it should explain the GDPR and how it applies to the work staff undertake on a daily basis. It should also emphasise the risks of fines and regulatory action to your firm, and criminal sanction for individuals.

As well as considering the training needs of staff in relation to their roles and responsibilities for processing personal data, your firm’s GDPR lead will also want to consider the specialist training needs of staff in areas including marketing, database management, or human resources.

A particular focus of training should be the identification of data subject access requests [See Checklist 5], and the handling of data breaches [See Checklist 9], possibly including basic cyber awareness training.

Your firm should also consider regularly refreshing cyber and GDPR training and take measures to ensure that new staff receive these as part of their induction training.

CHECKLIST

1. Has your firm identified a GDPR lead to take responsibility for awareness raising?

2. Has your GDPR lead briefed senior managers, associates and partners on the risks associated with the GDPR?

3. Have they developed a programme for awareness raising and training of staff involved in data processing operations?

4. Does this training programme cater to the specialised needs of staff in areas like marketing, database management and human resources?

5. Does your training include how to identify and respond to data subject requests?

6. Does your training include basic cyber security awareness for all staff and what they must do if they become aware of a data breach?

7. Have you put in place procedures to regularly review the content of your cyber and GDPR training and to include it as part of new joiner induction programmes?
CHECKLIST 2: INFORMATION YOU HOLD

AT A GLANCE

This checklist covers Step 2 of the ICO’s ‘12 Steps to take now’ guidance for preparing for the GDPR. It examines:

- Documenting the personal data you hold, and
- Maintaining records of your processing activities.

CONTEXT

You should document what personal data you hold, where it came from and who you share it with. You may need to organise an information audit across the organisation or within particular business areas.

The GDPR requires you to maintain records of your processing activities. It updates rights for a networked world. For example, if you have inaccurate personal data and have shared this with another organisation, you will have to tell the other organisation about the inaccuracy, so it can correct its own records. You won’t be able to do this unless you know what personal data you hold, where it came from and who you share it with. You should document this. Doing this will also help you to comply with the GDPR’s accountability principle, which requires organisations to be able to show how they comply with the data protection principles, for example by having effective policies and procedures in place.

POINTS TO CONSIDER

Your firm is already bound by the Data Protection Act (DPA) and SRA rules about confidentiality and being familiar with the existing data protection rules will give you a good grounding to ensure compliance with the GDPR. You will, however, need to reflect the considerably more prescriptive information provision requirements of the GDPR compared to the DPA. Importantly, these include not only what should be communicated but how. Transparent processing is one of the main principles enshrined in the GDPR and one of the significant rights accorded to data subjects.

What should I do first?

The first step is auditing the information held by your firm. Data mapping in this way (by documenting the data you hold, where it came from and who you share it with) should enable you to carry out a gap analysis to determine the key technical and organisational measures (internal governance and controls) you need to take to comply with your responsibilities for the data you process. The GDPR’s accountability requirement means that you should then take these measures and be able to demonstrate that you have done so (see Article 24).
What information shall I capture in my records?

If you are a controller for the personal data you process, you must document all the information contained in Article 30(1) of the GDPR. This includes:

- the name and contact details of your firm (and, where applicable, of any joint controllers, your representative and your data protection officer)
- the purposes of your processing
- a description of the categories of individuals and categories of personal data
- the categories of recipients of personal data
- where applicable, transfers to third countries, including documenting the transfer mechanism safeguards in place
- where possible, retention schedules
- where possible, a description of your technical and organisational security measures referred to in Article 32(1).

If you are a processor for the personal data you process, you must document all the information contained in Article 30(2) of the GDPR. This includes:

- the name and contact details of the processor or processors and of each controller on behalf of which the processor is acting, and, where applicable, of the controller’s or the processor’s representative, and the data protection officer
- the categories of processing carried out on behalf of each controller
- where applicable, transfers of personal data to third countries, including documenting the transfer mechanism safeguards in place
- where possible, a description of your technical and organisational security measures referred to in Article 32(1).

How do I work out if my firm is a data controller or processor?

If you're unsure about whether you are a controller or processor for the data processing activities, read the ICO's key definitions guidance.

The ICO has also prepared draft templates for firms to capture their data processing activities:

- Template to record activities by data controllers.
- Template to record activities by data processors.

Does this apply to all firms, regardless of size?

In recognition of the challenges this may pose for micro, small and medium-sized businesses, the Regulation introduces a record keeping derogation for organisations with fewer than 250 employees.

Such organisations only need to document processing activities that are:

- not occasional, or
- could result in a risk to the rights and freedoms of individuals, or
- involve the processing of special categories of data or criminal convictions and offence data.

The Article 29 Working Party of EU data protection authorities which adopts guidelines for complying with the GDPR is currently considering the scope of the exemption from documentation for small and medium-sized businesses. The ICO’s webpages on GDPR documentation will be updated to reflect the outcome of these discussions.
CHECKLIST

1. Have you documented your processing activities in writing, with granular and meaningful links between the different pieces of information?

2. Have you considered how you will maintain and regularly review your record keeping obligations? Do you have an organisational process to ensure that this takes place?

3. Have you considered how changes in recipients to whom data will be disclosed, transfers of data to a third country, or technical and organisational security measures will be reflected in your record keeping?

4. Are you able to make your records available to the Information Commissioner’s Office on request?

5. Have you evaluated the extent to which you can claim the record keeping derogation for micro, small and medium-sized businesses?
CHECKLIST 3: COMMUNICATING PRIVACY INFORMATION

AT A GLANCE

This checklist covers Step 3 of the ICO’s ‘12 Steps to take now’ guidance for preparing for the GDPR. It examines:

- Reviewing your privacy notices to comply with the additional information you need to give people when you collect their personal data under the GDPR.

CONTEXT

You should review your current privacy notices and put a plan in place for making any necessary changes in time for GDPR implementation.

When you collect personal data you currently have to give people certain information, such as your identity and how you intend to use their information. This is usually done through a privacy notice. Under the GDPR there are some additional things you will have to tell people. For example, you will need to explain your lawful basis for processing the data, your data retention periods and that individuals have a right to complain to the Information Commissioner’s Office (ICO) if they think there is a problem with the way you are handling their data. The GDPR requires the information to be provided in concise, easy to understand and clear language.

The ICO’s privacy notices code of practice reflects the new requirements of the GDPR.

POINTS TO CONSIDER

What do I need to include in my updated privacy notice to comply with the GDPR?

Where your firm is collecting personal data directly from the data subject, Article 13 sets out the information that must be provided by the controller, at the time the personal data are obtained. This encompasses:

- the controller’s identity and contact details and, if applicable, that of their representative
- the contact details of the data protection officer [See Checklist 11], if applicable
- the legal basis and purposes of processing (where the controller is relying on a basis of ‘legitimate interest’, the interest relied upon must be stated) [See Checklist 6]
- the recipients or categories of recipients of the data
- any intention by the controller to transfer the data to a third country or international organisation must be stated, along with the existence or not of an adequacy notice by the European Commission, and reference to any appropriate safeguards or binding corporate rules relied upon
- the period for which the personal data will be stored or, where that is not possible, the criteria for determining that period
- the existence of the data subject’s right to request access to and rectification or erasure of data, to object to and request the restriction of processing, and to data portability
• the right for the data subject to withdraw their consent at any point where said consent is the lawful basis for processing [See Checklist 7]

• the right to complain to the supervisory authority (the Information Commissioner's Office in the UK)

• information relating to whether the provision of personal data is a statutory or contractual requirement, or required for the purpose of entering into a contract, and the consequences of failure to provide such data

• if applicable, the use of automated decision-making, including profiling, and meaningful information about the logic involved as well as the significance and consequences of such processing for the data subject.

The requirement to provide this information doesn't apply insofar as the data subject already has it.

Similar information transparency requirements are imposed on controllers where personal data have not been obtained directly from data subjects and these are itemised in Article 14. This includes the source of the personal data and whether it came from publicly available sources. Where personal data has been obtained other than directly from data subjects, you must provide the transparency information itemised no later than within one month of collection.

Any old privacy notices will need to be updated to remove any reference to charging for subject access requests. You may also wish to consider including details about how to make a subject access request (SAR) in your privacy notice. This could include a dedicated email address at your firm for the purpose of SARs as well as enquiries about data portability, the right to be forgotten, and other data subject rights. This will not only be helpful for your clients, but it will ensure that enquiries are directed to the right place in your firm.

See Checklist 4 for further information about what you need to do to comply with the data subject rights listed above.

What about legally privileged information?

The Data Protection Bill currently before Parliament will mirror existing provisions in the Data Protection Act 1998 by exempting from the GDPR information provisions, including SARs, personal data in respect of which a claim to LPP could be maintained in legal proceedings.

How do I need to present this information?

In summary, law firms, like other organisations, should publish their privacy notices in easy to understand language on their websites, in contracts and terms of business, and in other communications with clients.

Where possible, data controllers should provide data subjects with direct access to their own data via a secure, remote system, and must take reasonable measures to validate the identity of individuals requesting access to their information. Measures to promote access must not, however, prejudice any rights owed to third parties by the data controller.

Can I use the personal data collected for other purposes?

Personal data must only be used for the purpose for which it is collected. If a firm wants to use the personal data for another purpose, the controller must provide the data subject with information about that further purpose before any further processing taking place.

You should request informed consent from data subjects every six months if you are using their data for marketing purposes, and you will also need to request the consent of former clients if you wish to send them marketing material.
How can I get more information about applying the principles behind communicating privacy information?

The Office of the Information Commissioner has produced guidance on using privacy notices to provide transparent and accessible information to data subjects. This sets out key questions to consider about the effect of your processing on individuals and in demonstrating your fair processing in a privacy notice.

### CHECKLIST

1. Have you reviewed your communications with all the data subjects whose personal data you process to ensure that you meet the significantly more prescriptive transparency provisions of the GDPR?

2. Have you reviewed and revised your online privacy notices?

3. Have you considered how you will ensure that relevant communications with data subjects use clear and plain language? Have you tested this?

4. Have you considered the need for updated training to ensure that your staff are all aware of their transparency and fairness obligations to data subjects?
CHECKLIST 4: INDIVIDUALS’ RIGHTS

AT A GLANCE

This checklist covers Step 4 of the ICO’s ‘12 Steps to take now’ guidance for preparing for the GDPR. It examines:

- The rights that data subject holders have and the procedures you’ll need to have in place to cover them.

CONTEXT

You should check your procedures to ensure they cover all the rights individuals have, including how you would delete personal data or provide data electronically and in a commonly used format.

The GDPR includes the following rights for individuals:

- the right to be informed
- the right of access
- the right to rectification
- the right to erasure
- the right to restrict processing
- the right to data portability
- the right to object, and
- the right not to be subject to automated decision-making including profiling.

On the whole, the rights individuals will enjoy under the GDPR are the same as those under the DPA but with some significant enhancements.

If you are geared up to give individuals their rights now, then the transition to the GDPR should be relatively easy. This is a good time to check your procedures and to work out how you would react if someone asks to have their personal data deleted, for example. Would your systems help you to locate and delete the data? Who will make the decisions about deletion?

The right to data portability is new. It only applies:

- to personal data an individual has provided to a controller
- where the processing is based on the individual’s consent or for the performance of a contract, and
- when processing is carried out by automated means.

You should consider whether you need to revise your procedures and make any changes. You will need to provide the personal data in a structured commonly used and machine-readable form and provide the information free of charge.
POINTS TO CONSIDER

OK, I’ve updated my privacy notice. Is there anything else I need to do to comply with data subjects’ rights?

Yes. In addition to the enhanced transparency obligations set out in Checklist 3, you’ll want to be sure you fully understand the new and existing data subject rights in the GDPR and how your firm will respond to them. There are new rights to data portability, to erasure (‘the right to be forgotten’), and to the restriction of processing and these are summarised below. You’ll need to ensure that your firm’s internal procedures and systems can handle requests by data subjects exercising their rights, and that you can do so without undue delay and within prescribed time limits.

How long do I have to respond to data subjects’ rights?

The GDPR states that requests must be responded to without undue delay and no later than one month from the receipt of requests. For complex or numerous requests, the period may be extended for a further two months, but the controller must inform the data subject of the extension and the reasons for the delay. If the data controller does not take action on the data subject’s request, they must inform them why this is the case, and make them aware of their right to complain to the Office of the Information Commissioner.

What do I need to know about data portability?

This allows a data subject to instruct a data controller to transmit their personal data to another controller, i.e., from one solicitor to another, where it is technically feasible to do so, and the right only applies to processing by automated means on the basis of contract or consent [See Checklist 6]. The aim of this provision is to enhance consumer rights and create opportunities for innovative data sharing between controllers. Data subjects will be entitled to receive the personal data they have provided to a controller in a structured, commonly used and machine-readable format and to have that data transmitted to another controller without hindrance. The right to portability must not adversely affect ‘the rights and freedoms of others’.

You should look at the ICO’s guidance on data portability and the Article 29 Working Party (of EU data protection authorities) guidance and FAQs for more on what to do to comply with these requirements.

How do I comply with the right to erasure?

Data subjects have a right to have their personal data erased when it is no longer required for the purposes for which it was collected, where a data subject has withdrawn his or her consent or objects to the processing of personal data concerning him or her, or where the processing of his or her personal data does not otherwise comply with the GDPR. This does not apply, however, where there is a lawful reason for continued processing, including ‘for the establishment, exercise or defence of legal claims’ (Article 17(3)).

Where erasure is appropriate, data controllers who have disclosed personal data to other controllers need to inform them of erasure requests and their obligation to erase any links or copies of the data. Controllers are also required to erase personal data they have made public, and to inform third parties in receipt of the data of the request for erasure, unless it proves impossible or would involve disproportionate effort.

As this is another new right introduced by the GDPR, it’s worth familiarising yourself with the ICO guidance on erasure.
What about the right to the restriction of processing?

This is another new right. Article 18 sets out the conditions under which a data subject can exercise her right to restrict the processing of her data. These are:

- Where the accuracy of the data held by the controller is contested by the data subject and the controller is verifying its accuracy.
- Where processing is unlawful and the data subject requests restriction of processing rather than erasure.
- Where the data is no longer required by the controller for the purposes of processing for which it was collected, but the data subject requires it for the establishment, exercise or defence of a legal claim.
- Where a data subject has objected to processing (Article 21), any period necessary to determine whether the controller’s legitimate grounds for processing override those of the data subject.

Where a data subject exercises their right to restrict processing, other than for storage, the affected personal data may only be processed:

- with the data subject’s consent
- for establishing, exercising or defending legal claims
- for the protection of another natural or legal person’s rights, or
- for reasons of important public interest of the Union or a Member State.

Controllers must inform data subjects before any restriction of processing is lifted, and must inform any third parties with whom it has shared the relevant data of the restriction, unless doing so proves impossible or would involve disproportionate effort.

There’s useful guidance about how the right to restriction might operate in practice in a GDPR Recital (Recital 67).

What do I need to know about the other data subject rights in the GDPR?

Right to rectification

Data subjects have the right to have any inaccurate personal data held about them corrected by the data controller. They also have the right to have incomplete data completed. Data controllers are also obliged to inform any third parties with whom they’ve shared incorrect personal data that this has been rectified, unless so doing would involve disproportionate effort (Article 19).

Right to object

Data subjects may object to certain types of processing in specific circumstances. These are:

- processing relying on the controller’s legitimate interests or performance of a task carried out in the public interest or the exercise of official authority
- processing for direct marketing
- processing for scientific, historical, or statistical purposes.

Each of these grounds of objection operate differently, but in all cases the controller must respond to a request within one month, with the possibility of a two-month extension for complex or numerous requests.

In summary, objections to processing on the grounds of legitimate interests or the execution of a task in the public interest or in exercising official authority require the controller to stop processing. They may, however, override an objection if they are able to demonstrate that their legitimate interests override those of the data subject, or that processing is necessary for establishing, exercising, or defending legal claims.

Complaints about processing for direct marketing purposes also require the data controller to cease processing, and, in these cases, there are no grounds for refusal to comply.
Similarly, objections to processing for scientific, historical, or statistical purposes must be complied with and processing ended, unless the processing is in the public interest.

In each of these cases, processing includes profiling (see below).

Controllers must make data subjects aware of these rights to object, clearly and separately from other information, at the time they first communicate with them [See Checklist 3].

**Rights relating to automated decision making**

Where individuals are subject to decision making that is based solely on automated processing and has potentially serious effects on them, the data controller must take steps to safeguard their interests. This includes profiling, which is any form of automated processing for evaluating individuals, for example on their performance at work, interests, or financial situation. In these cases, individuals have the right not to be subject to automated processing, including profiling, where the processing results in a legal, or similarly significant effect.

Exemptions to this right exist, however, where:

- the data subject has given their explicit consent to automated processing
- the processing is necessary for entering into, or the performance of, a contract, or
- where the controller is authorised to use automated means for a legal purpose, such as the prevention of fraud or tax evasion.

In these cases, data controllers must safeguard data subjects’ rights and freedoms and provide them with access to human intervention, the opportunity to express their point of view, and to contest any decision made about them by automated means.

Importantly, the exemptions do not apply where:

- the data subject is a child
- the decision is based on special categories of data [See Checklist 6], unless the data subject has given their consent to automated decision making, or
- the processing is for reasons of substantial public interest (Article 22).
CHECKLIST

1. Can you comply with data subjects’ rights without undue delay and within prescribed time limits?

2. Have you considered how you will verify the identity of data subjects requesting access to their data?

3. Have you considered offering remote access to a secure system to provide data subjects with direct access to their personal data?

4. Are you able to rectify inaccuracies in personal data you are processing, and, where possible, notify third parties to whom you have disclosed inaccurate data?

5. Are you familiar with the grounds on which data subjects can request restriction of processing? Are you aware of its implications?

6. Will your systems allow you to fulfil your data portability obligations?

7. Are you familiar with the related information on reviewing your privacy notices [See Checklist 3], and subject access requests [See Checklist 5]?

8. Have you ensured that the key staff in your firm understand their responsibilities regarding individual rights?
CHECKLIST 5: SUBJECT ACCESS REQUESTS

AT A GLANCE

This checklist covers Step 5 of the ICO’s ‘12 Steps to take now’ guidance for preparing for the GDPR. It examines:

- What you need to do to update your procedures to handle subject access requests (SARs).

CONTEXT

You should update your procedures and plan how you will handle requests to take account of the new rules:

- In most cases you will not be able to charge for complying with a request.
- You will have a month to comply, rather than the current 40 days.
- You can refuse or charge for requests that are manifestly unfounded or excessive.
- If you refuse a request, you must tell the individual why and that they have the right to complain to the supervisory authority and to a judicial remedy. You must do this without undue delay and at the latest, within one month.

If your organisation handles a large number of access requests, consider the logistical implications of having to deal with requests more quickly. You could consider whether it is feasible or desirable to develop systems that allow individuals to access their information easily online.

POINTS TO CONSIDER

By now you should have reviewed your privacy notices to comply with changes brought about by the GDPR [See Checklist 3] and familiarised yourself with its enhanced rights for individuals [See Checklist 4]. If so, reviewing your procedures for meeting SARs is the next step.

What are data subjects’ rights on accessing their personal data?

As data subjects, clients should be able to access their personal data easily and in a concise, transparent, and intelligible form. With this in mind, you should review how easy it would be for you to respond to clients’ subject access requests under your firm’s current processes. This will enable you to decide whether existing processes remain fit for purpose, or if your firm needs to amend these. Firms likely to deal with a large volume of requests may wish to offer remote access for clients to their personal data via a secure system.
What are my responsibilities as a data controller?

Data controllers must:

- provide individuals with a copy of their personal data held for processing purposes if requested in a concise, transparent, intelligible and easily accessible form, using clear and plain language and, unless otherwise requested, in a commonly used electronic form
- use all reasonable means to verify the identity of individuals requesting access to their personal data
- comply with SARs free of charge (a reasonable fee, based on administrative costs, may be charged for further copies)
- respond to SARs without undue delay and in any event within one month of receipt of the request, rather than the current 40 days (the period may be extended by two further months for complex or numerous requests, but the controller must inform the data subject of the extension and the reason for the delay)
- not prejudice the rights they owe to any third party in complying with SARs. This means they must not release any third party personal data pursuant to an SAR, even if it is that of a next of kin. Such data should be withheld or redacted.

As a data controller, is there any additional best practice that I should consider?

Where possible, data controllers should consider providing data subjects with direct access to their own data, via a secure, remote system. The Information Commissioner’s Office’s (ICO’s) guidance says that this may not be appropriate for all organisations, and law firms considering this will want to consider the security of their systems carefully.

Do I have to respond to unfounded or excessive requests?

No. You are permitted to either charge a reasonable fee or refuse to comply with such requests, although the burden of proving that the request was excessive or unfounded is yours. Where the data controller does not take any action, it must inform the data subject why this is the case and inform them of their right to lodge a complaint with the ICO.

What’s the relationship between subject access requests and legal professional privilege (LPP)?

The Data Protection Bill currently before Parliament will mirror existing provisions in the Data Protection Act 1998. Personal data in respect of which a claim to LPP could be maintained in legal proceedings will be exempt from the GDPR information provisions (which include SARs).

CHECKLIST

1. Can you comply with data subjects’ rights without undue delay and within the new shorter prescribed time limits?

2. Are you satisfied that your firm’s processes for verifying an individual’s identity are suitable for dealing with these requests?

3. Have you considered whether your existing processes for enabling access to personal information should be updated?

4. Have you ensured that the key staff in your firm understand what they need to know about handling SARs?
CHECKLIST 6: LAWFUL BASIS FOR PROCESSING PERSONAL DATA

AT A GLANCE

This checklist covers Step 6 of the ICO’s ‘12 Steps to take now’ guidance for preparing for the GDPR. It examines:

- Your consideration of the lawful basis for your processing activity, its implications, and what you need to do.

CONTEXT

You should identify the lawful basis for your processing activity in the GDPR, document it and update your privacy notice to explain it.

Many organisations will not have thought about their lawful basis for processing personal data. Under the current law this does not have many practical implications. However, this will be different under the GDPR because some individuals’ rights will be modified depending on your lawful basis for processing their personal data. The most obvious example is that people will have a stronger right to have their data deleted where you use consent as your lawful basis for processing.

You will also have to explain your lawful basis for processing personal data in your privacy notice and when you answer a subject access request. The lawful bases in the GDPR are broadly the same as the conditions for processing in the DPA. It should be possible to review the types of processing activities you carry out and to identify your lawful basis for doing so. You should document your lawful bases in order to help you comply with the GDPR’s ‘accountability’ requirements.

POINTS TO CONSIDER

What are the lawful bases for processing under the GDPR?

There are six lawful bases:

- Consent
- Performance of a contract
- Compliance with a legal obligation
- The vital interests of the data subject
- The legitimate interests of the data controller
- Public interest or exercise of official authority

How are they different from the existing legal bases?

The lawful bases in the GDPR are broadly similar to the processing conditions in existing legislation.

Where processing is necessary for the performance of a contract, you can choose to rely on that basis if the data subject is a party to that contract. You can also undertake processing that is necessary in order to take steps at the request of the data subject prior to entering into a contract.
If the legal basis relied upon is **compliance with a legal obligation** to which the data controller is subject, it must be clear and precise, ‘and its application should be foreseeable to persons subject to it, in accordance with the case-law of the Court of Justice and the European Court of Human Rights (Recital 41). An example of this might include registering a property purchase with HM Land Registry on behalf of a client.

The **vital interests of the data subject** basis allows processing where it is necessary to protect an interest which is essential for the life of the data subject or another natural person.

To rely on the **legitimate interests of the data controller** basis for lawful processing requires careful consideration and evaluation of the data subject’s expectations at the time their personal data was collected. Guidance from the Information Commissioner’s Office reflects the need for controllers to balance their interests against those of their data subjects. If data subjects would not reasonably expect the processing, or if it would cause unjustified harm, data controllers’ interests are unlikely to override those of data subjects. If relied upon, you will also need to include details of your legitimate interests in your privacy information [See Checklist 3]. Specific prohibitions for this basis apply where data subjects are children and for public authorities.

The GDPR provides an example of the legitimate use of this ground by multinationals sharing personal data relating to their employees or customers in the context of a HR system or client management database. Other examples where the legitimate interest basis might be available include ensuring network and information security (Recital 49), and for the prevention of fraud (Recital 47).

The **public interest or exercise of official authority** basis requires processing to have a basis in EU or Member State law though there need not be a specific law for each individual processing activity (Recital 45).

What about consent? Is the standard the same as under current legislation?

The standard required when relying on consent is significantly greater than under existing legislation, and we do not expect most law firms to rely on it. Under the GDPR, consent must be freely given, and be unambiguous and specific. Where there is a clear imbalance of relationship between the data controller and data subject making the granting of freely given consent unlikely, it cannot be relied upon. More information on the use of consent is contained in Checklist 7.

OK, I’ve identified my legal basis for processing, what do I have to do now?

You’ll remember that the legal basis and purposes of the processing are included in the list of information that must be provided to data subjects at the time personal data is obtained [See Checklist 3]. If you haven’t done so already, you’ll need to update your privacy notice to ensure it includes this information.
What about special categories of data?

There is a general prohibition on processing special categories of data, including any of the following types of information about individuals:

- racial or ethnic origin
- political opinions
- religious or philosophical beliefs
- trade union membership
- genetic data
- biometric data for the purpose of uniquely identifying a natural person
- data concerning health, and
- data concerning a natural person’s sex life or sexual orientation.

If your firm does process any of these types of information, Article 9(2) provides a list of circumstances under which the processing of special categories may be lifted.

CHECKLIST

1. Have you reviewed your processing activity and identified the lawful basis or bases for doing so?

2. If you are considering relying on consent, have you read Checklist 7 and carefully considered its implications?

3. Have you included the lawful basis and purposes of your processing in your privacy notice?

4. Have you documented your decision making about the lawful basis of your processing to comply with the GDPR’s accountability principle?
CHECKLIST 7: CONSENT

AT A GLANCE

This checklist covers Step 7 of the ICO’s ‘12 Steps to take now’ guidance for preparing for the GDPR. This checklist does not examine consent in the context of marketing. The ICO has detailed guidance on key differences affecting direct marketers arising from the GDPR on its website. Our checklist examines:

- Whether you should consider consent as a legal basis for the processing of personal data, and, if so, the steps you need to take.

CONTEXT

You should review how you seek, record and manage consent and whether you need to make any changes. Refresh existing consents now if they don’t meet the GDPR standard.

You should read the detailed guidance the ICO has published on consent under the GDPR, and use our consent checklist to review your practices. Consent must be freely given, specific, informed and unambiguous. There must be a positive opt-in – consent cannot be inferred from silence, pre-ticked boxes or inactivity. It must also be separate from other terms and conditions, and you will need to have simple ways for people to withdraw consent. Public authorities and employers will need to take particular care. Consent has to be verifiable and individuals generally have more rights where you rely on consent to process their data.

You are not required to automatically ‘repaper’ or refresh all existing DPA consents in preparation for the GDPR. But if you rely on individuals’ consent to process their data, make sure it will meet the GDPR standard on being specific, granular, clear, prominent, opt-in, properly documented and easily withdrawn. If not, alter your consent mechanisms and seek fresh GDPR-compliant consent, or find an alternative to consent.

POINTS TO CONSIDER

I rely on consent under current legislation. What’s different about consent under the GDPR?

Importantly, data subjects must be able to withdraw their consent at any time and withdrawing consent must be as simple as giving it (Article 7).

If your firm is currently relying on consent as the basis for processing, you shouldn’t overlook the other legal grounds in reviewing your activity for the GDPR [See Checklist 6]. This is because the GDPR makes the criteria for lawful use of consent significantly more stringent. We don’t expect most law firms to rely on consent as the basis for their processing but, if they do, they will need to consider the following changes to existing legislation.

Organisations may no longer:

- rely on pre-ticked boxes
- infer consent from the absence of a data subject’s objection or other inactivity
- rely on one consent to cover a variety of processing activities.
**Under the GDPR, consent must be:**

- freely given
- specific
- informed, and
- unambiguous.

Consent must also cover all processing activities carried out for the same purpose or purposes (remember that the purposes of processing and the legal basis must be included in your privacy notice – See Checklist 3).

The data subject must be able to refuse or withdraw consent without detriment.

To be informed, the data subject must be aware of the identity of the controller and the purposes of processing for which their data are intended.

Firms will also need to ensure that they can demonstrate the consent of their data subjects to the processing of their personal data through appropriate record keeping.

**What else do I need to know about consent?**

Consent won't be valid if there is a clear imbalance between the controller and data subject, meaning the consent can't be freely given. For example, public authorities are unlikely to be able to rely on consent (Recital 43), and the employer/employee relationship was cited as a likely imbalance during the GDPR’s negotiation.

If a data controller obtains consent from a written declaration on another matter (for example within the terms and conditions of a contract), they must ensure that their request for consent is clearly distinguishable from these other matters. This should be a consideration when issuing client care letters.

Children will need to be at least 13 (subject to passage of the Government’s Data Protection Bill) to consent to ‘information society services’. These are services provided electronically for remuneration at the request of the recipient. The full definition of information society services, taken from Directive 2015/1535 is as follows:

‘service’ means any Information Society service, that is to say, any service normally provided for remuneration, at a distance, by electronic means and at the individual request of a recipient of services.

For the purposes of this definition:

(i) ‘at a distance’ means that the service is provided without the parties being simultaneously present;

(ii) ‘by electronic means’ means that the service is sent initially and received at its destination by means of electronic equipment for the processing (including digital compression) and storage of data, and entirely transmitted, conveyed and received by wire, by radio, by optical means or by other electromagnetic means;

(iii) ‘at the individual request of a recipient of services’ means that the service is provided through the transmission of data on individual request

Parental consent will be required for younger children.

ICO guidance indicates that there is no set time limit for consent, and how long it lasts will depend on the context. Your firm should regularly review and refresh its obtained consents to ensure they reflect current relationships.
CHECKLIST

1. Have you considered the significantly enhanced criteria for the lawful use of consent under the GDPR and whether this is an appropriate legal basis for your firm’s processing of personal data?

2. In particular, have you put the processes and resources into place in your firm to comply with the new data subject rights relating to consent?

3. Have you read the ICOs guidance on consent, and taken steps to ensure that your firm’s practices are compliant?

4. Have you considered how you will regularly review and refresh your consents?
CHECKLIST 8: CHILDREN

AT A GLANCE

This checklist covers Step 8 of the ICO’s ‘12 Steps to take now’ guidance for preparing for the GDPR. It examines:

- What you need to do if you offer online services to children and collect their personal data. It also summarises other steps organisations need to take to comply with the GDPR’s protections for children.

CONTEXT

You should start thinking now about whether you need to put systems in place to verify individuals’ ages and to obtain parental or guardian consent for any data processing activity.

For the first time, the GDPR will bring in special protection for children’s personal data, particularly in the context of commercial internet services such as social networking. If your organisation offers online services (‘information society services’) to children and relies on consent to collect information about them, then you may need a parent or guardian’s consent in order to process their personal data lawfully. The GDPR sets the age when a child can give their own consent to this processing at 16 (although this may be lowered to a minimum of 13 in the UK). If a child is younger, then you will need to get consent from a person holding ‘parental responsibility’.

This could have significant implications if your organisation offers online services to children and collects their personal data. Remember that consent has to be verifiable and that when collecting children’s data your privacy notice must be written in language that children will understand.

POINTS TO CONSIDER

The Information Commissioner’s Office guidance on children states:

Children have the same rights as adults over their personal data and can exercise their own rights as long as they are competent to do so. Where a child is not considered to be competent, an adult with parental responsibility may exercise the child’s data protection rights on their behalf.

Children are identified as vulnerable and deserving of ‘special protection’ in the GDPR, and the importance attached to their protection is mentioned several times. If you process children’s data, you should pay particular attention to the need to adopt a data protection by design and by default approach to your processing. This means that data controllers implement appropriate measures to ensure that GDPR principles are an integral part of their processing, and that they have organisational and technical measures in place ensuring that only personal data necessary for their specific processing activity is collected [See Checklist 10]. You need to pay particular attention to the legal basis of processing and privacy notices if you offer online or ‘information society services’ to children.
Can children provide valid consent?

Because they have the same rights as adults over their personal data under the GDPR, you will want to carefully consider the lawful basis of processing if you are offering an online service directly to children. First and foremost, you need to ensure that the child can understand the basis of their consent, otherwise it will not be ‘informed’ and will therefore be invalid. The age of consent proposed in the UK Data Protection Bill currently before Parliament is 13, and, if passed, only children 13 and over will be able to provide their own consent in the UK (organisations offering online services directly to children in other EU member states will need to check the age limit applicable in each).

For children younger than the age of consent you will need to get this from whoever has parental responsibility, unless the online service you are offering is a preventive or counselling service (Recital 38). Data controllers are also required to make ‘reasonable efforts’ to verify that an authorisation has come from a legally responsible source (Article 8(2)). Furthermore, if consent is used as the legal basis of processing, the requirement for the provision of information to data subjects to be in ‘a concise, transparent, intelligible, and easily accessible form’ is to be met ‘in particular’ when addressed to children (Article 12(1)).

What about other bases for processing children’s data?

Data controllers relying on legitimate interests as the basis of their processing need to consider whether such interests are overridden by the interests or rights and freedoms of data subjects ‘in particular’ where the data subject is a child (Article 6(1)). Controllers will want to ensure they keep a record of their consideration of the balance of interests, including an identification of the risks and consequences of processing, if they are relying on legitimate interests.

Controllers relying on contract as the basis for processing need to consider children’s competence to understand what they are agreeing to.

What about privacy notices? Do I need to adapt mine for children?

If services are provided directly to children, privacy notices must be written with their understanding in mind. The ICO advises that this includes why the personal data is required, the processing involved, the risks and safeguards in place, and their data subject rights so that children understand the implications of sharing their data.
CHECKLIST

1. If you process children’s personal data, have you considered the need to **design your processing with children in mind** from the outset?

2. If required, have you drafted your privacy notices directed at children to reflect their level of understanding of the risks, safeguards, and implications of processing, and their rights as subject data holders?

3. If you are providing online services to children, and relying on consent as your legal basis, have you considered how you will verify children are over the age of competence to consent?

4. If you are providing online services to children, and relying on consent as your legal basis, have you considered how you will secure parental authorisation for children under the age of consent, and how you will verify this?

5. Have you put steps in place to **regularly review the measures you are taking to protect children’s personal data** and consider the need for more effective verification mechanisms for obtaining consent?

6. If you are relying on contract as the legal basis for processing children’s data, have you considered the need to draft your communication with them to help them to understand what they are agreeing to?

7. If you are relying on legitimate interests as the legal basis for processing children’s data, have you documented your consideration of why these are not overridden by their data subject rights?
CHECKLIST 9: DATA BREACHES

AT A GLANCE

This checklist covers Step 9 of the ICO’s ‘12 Steps to take now’ guidance for preparing for the GDPR. The definition of a personal data breach is broad, and data controllers must notify the ICO without undue delay on becoming aware of a breach and, where feasible, within 72 hours. Failure to do so could carry serious consequences, and delays in notification must be explained to the ICO. This checklist examines:

- What you need to detect, report and investigate a personal data breach, and appropriate security measures you should take to keep the data you process safe.

CONTEXT

You should make sure you have the right procedures in place to detect, report and investigate a personal data breach.

Some organisations are already required to notify the ICO (and possibly some other bodies) when they suffer a personal data breach. The GDPR introduces a duty on all organisations to report certain types of data breach to the ICO, and in some cases, to individuals. You only have to notify the ICO of a breach where it is likely to result in a risk to the rights and freedoms of individuals – if, for example, it could result in discrimination, damage to reputation, financial loss, loss of confidentiality or any other significant economic or social disadvantage.

Where a breach is likely to result in a high risk to the rights and freedoms of individuals, you will also have to notify those concerned directly in most cases.

You should put procedures in place to effectively detect, report and investigate a personal data breach. You may wish to assess the types of personal data you hold and document where you would be required to notify the ICO or affected individuals if a breach occurred. Larger organisations will need to develop policies and procedures for managing data breaches. Failure to report a breach when required to do so could result in a fine, as well as a fine for the breach itself.
POINTS TO CONSIDER

The GDPR defines a personal data breach as: a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed.

What are my processing security obligations?

As with existing legislation, these are generic rather than specific in nature. Data controllers and processors are obliged to take technical and organisational steps appropriate to the risk from processing an individual’s personal data. Measures should take into account existing technological developments, the cost of implementation, and the nature, scope, context and purposes of processing. It follows therefore that organisations processing special categories of data would be expected to have in place more robust measures than others. The types of risks that firms should consider include accidental or unlawful destruction and unauthorised disclosure (Article 83). Article 32 provides a non-exhaustive list of potentially appropriate measures firms might consider to counter-act these:

- Pseudonymisation (the processing of personal data so that it can no longer be attributed to a specific data subject without the use of additional and separately-held information subject to organisational and technical measures ensuring the anonymity of the data subject).
- Encryption of personal data.
- Procedures to ensure ongoing confidentiality, integrity, availability and resilience of processing systems and services.
- Procedures to ensure timely restoration of availability and access to personal data in the event of a technical incident.
- Processes for regular testing, assessment, and evaluation of measures for ensuring the security of processing.

My firm has had a breach. What do I need to do?

Notifying the ICO

Mandatory breach notification is a major change from existing legislation. The obligation differs depending on whether you are a data controller or processor.

Controllers must notify the supervisory authority (the ICO in the UK) without undue delay and, where feasible, not later than 72 hours after becoming aware unless the personal data breach ‘is unlikely to result in a risk to the rights and freedoms of natural persons’. If a delay beyond 72 hours occurs, the controller must notify the ICO of the reason for the delay. The information required by the ICO when notifying a breach is specified in Article 33 and comprises:

- The nature of the breach, and, where possible, the categories and approximate numbers of data subjects and personal data records concerned.
- The name and contact details of the data protection officer or other contact in your firm where more information can be obtained.
- The likely consequences of the breach.
- The measures you have taken or propose to take to address the breach including, where appropriate, measures to mitigate its effects.

As with most other aspects of GDPR compliance, controllers should document the breach, and the steps they take to remedy its effects. This will be important in demonstrating to the ICO that your firm has responded in a reasonable and proportionate manner in complying with its obligations.

Processors have a duty to notify the controller without undue delay after becoming aware of a personal data breach.
Notifying data subjects

Where a data breach is likely to result in a high risk to the rights and freedoms of a data subject, the data controller must communicate the breach to them without undue delay, describing its nature in clear and plain language, and comprising at least the information required by the ICO from controllers listed above.

Article 34 specifies conditions under which notifying data subjects isn’t mandatory, including where controllers have taken steps to make personal data unintelligible to unauthorised individuals, where they’ve taken steps to ensure any high risk to the rights and freedoms of data subjects don’t materialise, or where notification would involve disproportionate effort. Read the ICO’s detailed guidance on data breaches.

CHECKLIST

1. Have you considered the pseudonymisation and encryption of the personal data you hold?

2. Can you ensure the ongoing confidentiality, integrity, availability and resilience of your processing systems and services?

3. Can you restore the availability of and access to personal data in a timely manner in the event of a physical or technical incident?

4. Do you have a process for regularly testing, assessing and evaluating the effectiveness of your technical and organisational measures for ensuring the security of your processing?

5. Have you identified all data processors acting on your behalf, ensured they have provided guarantees they are implementing appropriate measures to comply with the GDPR and that their processing is governed by a contract?

6. Are you aware of your obligation to notify a personal data breach to the ICO within 72 hours of becoming aware of it?

7. Are you aware of your obligations, in certain circumstances, to notify data subjects in the event of a breach?

8. Are you aware of the guidance, products and services of the National Cyber Security Centre, and the Law Society’s cyber security and scam prevention webpages?
CHECKLIST 10: DATA PROTECTION BY DESIGN AND DATA PROTECTION IMPACT ASSESSMENTS

AT A GLANCE

This checklist covers Step 10 of the ICO’s ‘12 Steps to take now’ guidance for preparing for the GDPR. It examines:

- The principles of data protection by design and when and how to conduct a DPIA.

CONTEXT

It has always been good practice to adopt a privacy by design approach and to carry out a Privacy Impact Assessment (PIA) as part of this. However, the GDPR makes privacy by design an express legal requirement, under the term ‘data protection by design and by default’. It also makes PIAs – referred to as ‘Data Protection Impact Assessments’ or DPIAs – mandatory in certain circumstances.

A DPIA is required in situations where data processing is likely to result in high risk to individuals, for example:

- where a new technology is being deployed
- where a profiling operation is likely to significantly affect individuals, or
- where there is processing on a large scale of the special categories of data.

If a DPIA indicates that the data processing is high risk, and you cannot sufficiently address those risks, you will be required to consult the ICO to seek its opinion as to whether the processing operation complies with the GDPR.

You should therefore start to assess the situations where it will be necessary to conduct a DPIA. Who will do it? Who else needs to be involved? Will the process be run centrally or locally?

You should also familiarise yourself now with the ICO’s guidance on conducting PIAs as well as guidance from the Article 29 Working Party, and work out how to implement them in your organisation. This guidance shows how PIAs can link to other organisational processes such as risk management and project management.
POINTS TO CONSIDER

Although the GDPR applies to certain manual as well as automated processing, it is explicitly a response to the new challenges to data protection brought about by rapid technological developments.

What is ‘data protection by design and by default’?

Data protection by design means that data controllers need to put in place the appropriate organisational and technical measures to implement the six data protection principles of the GDPR:

• lawfulness, fairness and transparency
• purpose limitation
• data minimisation
• accuracy
• storage limitation, and
• integrity and confidentiality.

Following from these principles, data controllers must ensure that the default position for their technical and organisational measures result in:

• the personal data they collect being limited to what is necessary for each specific purpose of the processing they undertake, and
• personal data not being accessible to ‘an indefinite number’ of natural persons without the data subject’s intervention (to address unchecked ‘third party’ data sharing).

The GDPR puts the onus on data controllers to demonstrate compliance with the six data protection principles. One measure of demonstrating compliance is the DPIA.

What is a DPIA and when do I need to do one?

DPIAs aim to identify, evaluate and address the data protection risks to the rights and freedoms of natural persons associated with new activities involving personal data processing. Where there is a high risk to these rights and freedoms, the GDPR requires data controllers to carry out a DPIA. Some firms will already carry out Privacy Impact Assessments (PIAs), and, if this applies to your firm, you will need to review your processes in light of the GDPR’s requirements, noting new, specific requirements for content and process. If you haven’t already got a PIA process, you’ll need to design a new DPIA process, and build this into your firm’s policies and procedures.

The types of activities requiring a DPIA are set out in the GDPR (Article 35) and include:

• automated processing, including profiling, producing legal or similarly significant effects concerning data subjects
• large-scale, systematic monitoring of a publicly accessible area (for example, by camera)
• large-scale processing which aims to process a considerable amount of personal data at a regional, national or supranational level, and which is likely to result in a high risk to a large number of data subjects
• processing activity considered to be high risk by the supervisory authority (the ICO in the UK which is obliged to publish a list of processing operations requiring a DPIA).

Where processing activity concerns personal data from clients or patients by an individual lawyer or health care professional, a DPIA isn’t mandatory (Recital 91).

The Article 29 Working Party of European data protection authorities has stated that the GDPR does not require a DPIA to be carried out for every processing operation involving risks to rights and freedoms, but does suggest that if organisations are uncertain they should consider conducting one. In any event, the data controller should fully document any decision not to conduct a DPIA.
Is there any guidance on what is ‘high risk’?

Yes. The ICO is required to publish a list of the types of processing it considers to be high risk and that therefore requires a DPIA. You can find the ICO’s list of the draft types they recently consulted on at this page on their site, and you should bookmark this page for the outcome of their consultation.

What do I need to include in a DPIA?

As a minimum, a DPIA should include:

- a description of the proposed processing activity, its purposes, and, if applicable, the legitimate interests pursued by the data controller [See Checklist 6]
- an assessment of the necessity and proportionality of the processing in relation to the purpose
- an assessment of the risks to the rights and freedoms of data subjects
- measures proposed to mitigate the risks in compliance with the requirements of the GDPR.

When do I need to contact the ICO?

If your firm is acting as a data controller and your assessment is that processing would result in a high risk to data subjects that cannot be appropriately mitigated, you must consult with the ICO, providing the results of your DPIA (Article 36).

CHECKLIST

1. Do you understand the GDPR’s six data protection principles and your obligation to implement measures to integrate them into your processing activity?

2. Do you understand when a DPIA may be required by your firm, and have you considered the process, and the individuals who will be in charge of conducting it? (You will need to consult your Data Protection Officer, if you have one [See Checklist 11]).

3. Are you remembering to consider GDPR compliance in procuring new IT equipment?

4. Do you have a process or procedures in place to ensure that the principles of data protection by design and default are built into your IT systems and services?

5. If you will have non-GDPR compliant legacy systems in place after 25 May 2018, have you considered the need for organisational measures to ensure compliance, and, in due course, replacement systems?

6. Do you have access to expert advice that will allow you to understand and deal with any GDPR related IT systems and services issues that may arise?

7. Are your internal or external IT systems and services staff or service providers familiar with the GDPR and with your policies and procedures for compliance?

USEFUL REFERENCE SOURCES

- The ICO’s ‘Conducting Privacy Impact Assessments Code of Practice’
- The ICO’s Data Protection Impact Assessment template
CHECKLIST 11: DATA PROTECTION OFFICERS

AT A GLANCE

This checklist covers Step 11 of the ICO’s ‘12 Steps to take now’ guidance for preparing for the GDPR. It examines:

- What you should consider in deciding whether or not to appoint a DPO.

CONTEXT

You should designate someone to take responsibility for data protection compliance and assess where this role will sit within your organisation’s structure and governance arrangements.

You should consider whether you are required to formally designate a Data Protection Officer (DPO). You must designate a DPO if you are:

- a public authority (except for courts acting in their judicial capacity)
- an organisation that carries out the regular and systematic monitoring of individuals on a large scale, or
- an organisation that carries out the large-scale processing of special categories of data, such as health records, or information about criminal records. The Article 29 Working Party has produced guidance on the designation, position and tasks of DPOs.

It is most important that someone in your organisation, or an external data protection advisor, takes proper responsibility for your data protection compliance and has the knowledge, support and authority to carry out their role effectively.

POINTS TO CONSIDER

The Law Society has published advice on the appointment of Data Protection Officers by law firms which you should read. Its key points are:

- Most law firms will not be required to appoint a DPO under the GDPR.
- Some law firms might be obliged to designate a DPO.
- It is good practice for:
  - all firms to evaluate their processing of personal data against the criteria for the mandatory appointment of a DPO
  - firms to document their decision, and
  - firms to continuously review their decision, especially before any substantial change in processing activity or when carrying out a Data Protection Impact Assessment (DPIA).
- Firms should consider voluntary designation of a DPO. You should document the reasons for your decision. If you do not appoint a DPO, you should document your reasons for that and consider other governance arrangements you will put in place to ensure compliance with the GDPR.
- Governance arrangements should always include a suitably senior and qualified person with the necessary resources to lead on data protection compliance.
• Firms should pay careful attention to the characteristics, role and tasks of the DPO in deciding whom to appoint and ensure that the DPO has the appropriate levels of expertise, independence and resource, as well as considering other relevant issues, such as conflict of interest, the statutory duties of the DPO, that person's duties to his or her clients and fellow partners, etc.

• Appointment of a DPO can facilitate data protection compliance, however, DPOs are not personally responsible in a case of non-compliance with the GDPR. The compliance responsibilities will always remain with the firm, whether acting as a controller or a processor under the GDPR.

The advice also covers other areas, including interpretations of key terms and alternative arrangements that your firm might want to consider. We welcome any comments on the advice, please email us at: GDPR@lawsociety.org.uk

CHECKLIST

1. Have you considered **whether you should appoint a DPO** on a mandatory or voluntary basis?

2. Have you carefully considered the **characteristics, role and tasks of the DPO** as part of your deliberation?

3. In the event you decide not to appoint a DPO, **have you made alternative arrangements** to appoint a suitably senior and qualified person with the necessary resources to lead your firm's data protection compliance work?

4. Have you **documented your decision making**?

5. Have you put a procedure in place to **regularly review your DPO decision making**, particularly when you make a significant change to your data processing activity or when you carry out a data protection impact assessment (DPIA) [See Checklist 10].
CHECKLIST 12: INTERNATIONAL

AT A GLANCE

This checklist covers Step 12 of the ICO’s ‘12 Steps to take now’ guidance for preparing for the GDPR. It examines:

- What you need to consider if your firm carries out cross-border processing in more than one EU member state from an establishment in one or more member states, and transfers of personal data from member states to third countries.

CONTEXT

If your organisation operates in more than one EU member state, you should determine your lead data protection supervisory authority and document this.

The lead authority is the supervisory authority in the state where your main establishment is. Your main establishment is the location where your central administration in the EU is or else the location where decisions about the purposes and means of processing are taken and implemented.

This is only relevant where you carry out cross-border processing – i.e., you have establishments in more than one EU member state or you have a single establishment in the EU that carries out processing which substantially affects individuals in other EU states.

If this applies to your organisation, you should map out where your organisation makes its most significant decisions about its processing activities. This will help to determine your ‘main establishment’ and therefore your lead supervisory authority.

The Article 29 Working Party has produced guidance on identifying a controller or processor’s lead supervisory authority.

POINTS TO CONSIDER

What is cross-border processing?

The GDPR defines it as either:

- Processing in multiple member states by a controller or a processor established in more than one member state, or
- Processing by a controller or processor established in one member state, which substantially affects or is likely to substantially affect data subjects in multiple member states.

Importantly, ‘cross-border processing’ does not refer to processing in countries outside the EU.
What does ‘main establishment’ mean?

For data controllers:
- the place of its central administration in the EU, unless decisions about the purposes and means of processing are taken in another establishment of the controller elsewhere in the EU and the latter establishment has the power to have its decisions implemented.

For data processors:
- either the place of its central administration in the EU, or, if it has no such place, where its main processing activities take place in the EU.

What is the ‘one stop shop’?

The ‘one stop shop’ marks a change to existing legislation that makes organisations operating in more than one member state subject to separate supervisory authorities in each jurisdiction. Instead, the GDPR allows multinational firms and others to report to one supervisory authority. The GDPR designates the supervisory authority of the main establishment or single establishment of a data controller or processor as the competent lead authority where an organisation is undertaking cross-border processing which substantially affects, or is likely to substantially affect, data subjects in more than one member state.

What does ‘substantially affect’ mean?

The GDPR doesn’t define this. The Article 29 Working Party of EU data protection authorities states, however, that supervisory authorities will decide it on a case-by-case basis, taking into account factors such as whether the processing:
- is likely to cause damage, loss or distress to individuals
- is likely to have the effect of limiting rights or denying an opportunity
- affects, or is likely to affect, individuals’ health, well-being or peace of mind
- affects, or is likely to affect, individuals’ financial or economic status or circumstances
- leaves individuals open to discrimination or unfair treatment
- involves analysis of special categories of personal data, particularly that of children
- causes, or is likely to cause, individuals to change their behaviour in a significant way
- has unlikely, unanticipated, or unwanted consequences for individuals
- creates embarrassment or other negative outcomes, including reputational damage, or
- involves the processing of a wide range of personal data.
How are complaints about cross-border processing handled?

If you’ve mapped your processing activity and identified your lead supervisory authority, that’s the body that will decide whether or not to handle any complaint about, or possible infringement of, the GDPR by your firm. Chapter 7 of the GDPR sets out the rules for cooperation and consistency in decision making between lead supervisory authorities and others.

The rules about the ‘one stop shop’ mechanism do not apply to public authorities or private bodies acting in the public interest, which are subject only to the competence of the supervisory authority in the member state in which they are established.

Note also that representatives of data controllers without an establishment in the EU will need to deal with the supervisory authorities in every member state they operate in.

What about transfers of data to third countries?

The GDPR only permits transfers of personal data to third countries or international organisations (governed by public international law or an agreement by two or more countries) where the country or organisation ‘ensures an adequate level of protection’ of the data rights of natural persons set out in the Regulation. The criteria set out for the assessment of adequacy in the GDPR include inter alia respect for human rights and fundamental freedoms, as well as enforceable data subject rights and effective redress for data subjects, the existence of independent data supervisory authorities, and participation in international agreements relating to the protection of personal data (Article 45). Under the GDPR, the European Commission will make an adequacy finding subject to review, if successful, at least every four years.

In the absence of an adequacy finding, the GDPR provides for a number of alternative safeguards (Article 46) to enable data controllers and processors to transfer personal data outside the EU/EEA. One of these is binding corporate rules or BCRs. BCRs are defined as:

> [P]ersonal data protection policies which are adhered to by a controller or a processor established on the territory of a member state for transfers or a set of transfers of personal data to a controller or processor in one or more third countries within a group of undertakings, or group of enterprises engaged in a joint economic activity.

Article 47 sets out the list of requirements that BCRs must specify, and stipulates that the competent supervisory authority must approve them if they include these and are:

- legally binding and apply to and are enforced by every member of the group of undertakings, or group of enterprises engaged in a joint economic activity (including employees), and
- expressly confer enforceable rights on the data subjects whose data are processed.

Another method of transferring data to ‘non-adequate’ countries, is model contract clauses. Read the ICO’s guidance about using model contract clauses.

What about Brexit?

When the UK leaves the EU we will become a third country for GDPR purposes and subject to an adequacy determination by the European Commission. The Prime Minister has indicated that agreement on data protection rules for the transitional period and for our longer-term economic relationship is a priority for the UK during negotiations with the EU.
CHECKLIST

1. If your firm operates in more than one EU member state and undertakes cross-border processing, have you mapped your decision making regarding data processing?

2. Have you determined whether your cross-border processing substantially affects individuals in other EU member states?

3. If you’ve answered ‘yes’ to 1 and 2, have you determined your main establishment and lead supervisory authority?

4. If you send personal data to third countries, have you considered whether you will need BCRs in the absence of an adequacy finding by the European Commission?

5. If so, have you considered how you will ensure that data subjects whose data is sent to third countries can enforce their subject access rights?