# About this detailed guidance

These pages sit alongside our Guide to the GDPR and provide more detailed guidance for UK organisations about documenting their processing activities under the GDPR.

The GDPR contains explicit provisions that require you to maintain internal records of your processing activities. Among other things, records must be kept on processing purposes, data sharing, and retention. Documenting this information is linked to the principle of accountability and will help you to demonstrate your compliance with the GDPR.

This guidance will help you understand why documenting your processing activities is important, who must maintain such records, what must be recorded, and how to do all these things.

For an introduction to the key themes and provisions of the GDPR, you should refer back to the Guide to the GDPR. You can navigate back to the Guide at any time using the link at the top of this page. Links to other relevant guidance and sources of further information are also provided throughout.

# What's new under the GDPR?

## Is documentation something new?

Yes – documentation is a new requirement under the GDPR. It is mainly about keeping internal records of your processing activities. It reflects the increased importance of accountability and your obligation to ensure (and demonstrate) that what you do with people's personal data is in line with the GDPR. Article 30 sets out the different types of information you need to document including the purposes of processing, categories of personal data and recipients of personal data.

## Further Reading

> Relevant provisions in the GDPR – See Article 30(1)-(2), and Recital 82
> External link

## Don't we do this already?

There are some similarities between documenting your processing activities under the GDPR and the information you had to provide when registering with the ICO under the Data Protection Act 1998 (the 1998 Act). A key difference is that you no longer need to proactively provide this information to the ICO as part of an annual registration process. However, you may have to make it available to the ICO on request; for example, for an investigation.

## Further Reading

> Relevant provisions in the GDPR - See Article 30(4), and Recital 82
> External link

## What should we do now?

You can use your existing register entry for the 1998 Act as a basis from which to create your record of processing activities. You may wish to do an information audit to get a more comprehensive view of the types of personal data you hold and what you do with it. Your processing activities must be documented in writing and you need to ensure this is in place by 25 May 2018.

## Further Reading

> Relevant provisions in the GDPR - See Article 30(1)-(3), and Recital 82
> External link

# What is documentation?

## What does the GDPR say about documentation?

The accountability principle requires you to demonstrate that your organisation processes personal data in line with the GDPR. To help you do this, you can implement several technical and organisational measures. One such measure is contained in Article 30, which says that an organisation shall:

> "…maintain a record of processing activities under its responsibility."

There are several specified areas where records must be maintained, such as the purposes of processing personal data, data sharing and retention. This is what we mean by documentation.

## Further Reading

Relevant provisions in the GDPR – See Articles 5(2) and 30, and Recital 82
External link

**Further reading – ICO guidance**

Principles

Accountability and governance

## Why is documentation important?

Documenting your processing activities is important for several reasons. First, it is a legal requirement. Although you do not need to proactively provide these records to the ICO, you may have to make the information available on request; for example, for an investigation. As a key element of the accountability principle, documenting your processing activities can also help you to ensure (and demonstrate) your compliance with other aspects of the GDPR. For instance, it can help you with the following things:

- *Drafting your privacy notice* – much of the information you have to document is very similar to what you need to tell people in your privacy notice.
- *Responding to access requests* – knowing what personal data is held and where it is will help you to efficiently handle requests from individuals for access to their information.
- *Taking stock of your processing activities* – this will make it much easier for you to address other matters under the GDPR such as ensuring that the personal data you hold is relevant, up to date and secure.

However, it’s not just about legal compliance with the GDPR; documentation will also help you do the following:

- *Improve data governance* – highlighting and addressing data protection matters through documentation will support good practice in data governance. This can give you assurance as to data quality, completeness and provenance.
- *Increase business efficiency* – knowing what personal data you hold, why you hold it and for how long, will help you to develop more effective and streamlined business processes.

## Further Reading

Relevant provisions in the GDPR - See Articles 5 and 13-15, and Recitals 39, 60 and 63
External link

**Further reading – ICO guidance**

Principles

Right to be informed

Right of access

# Who needs to document their processing activities?

## Do all organisations need to document their processing activities?

Most organisations must document their processing activities to some extent. Both controllers and processors have their own documentation obligations, but controllers need to keep more extensive records than processors.

Organisations with 250 or more employees must document all their processing activities.

## Further Reading

Relevant provisions in the GDPR - See Articles 4(7)-(8) and 30(1)-(2), and Recital 82
External link

**Further reading – ICO guidance**

Key definitions

## What about small and medium-sized organisations?

The GDPR provides a limited exemption for small and medium-sized organisations. If you employ fewer than 250 people, you need only document processing activities that:

- are not occasional (e.g., are more than just a one-off occurrence or something you do rarely); or
- are likely to result in a risk to the rights and freedoms of individuals (e.g., something that might be intrusive or adversely affect individuals); or
- involve special category data or criminal conviction and offence data (as defined by Articles 9 and 10 of the GDPR).

**Example – processing that is not occasional**

An insurance company has 100 staff. Among other things, it regularly processes personal data in the context of processing claims, sales and HR. Although the company has fewer than 250 staff, it must still document these types of processing activities because they are not occasional. However, some of the company's processing activities occur less frequently. For instance, it occasionally carries out an internal staff engagement survey. The company doesn't do this particular processing activity very often, so it need not document it as part of its record of processing activities.

**Example – processing that is likely to result in a risk to the rights and freedoms of individuals**

The same company carries out several other processing activities on an infrequent basis. For instance, it occasionally does profiling on its customer database for the purposes of insurance-risk classification. Rare though this is, the company must still document it. This is because creating inferred data through profiling can be intrusive and result in risks to individuals' rights and freedoms.

**Example – processing that involves special category data or criminal conviction and offence data**

From time to time, the insurance company also does recruitment campaigns. For these, it collects information on applicants' health and ethnic origin for equal opportunities monitoring. The campaigns are rare but the company must still document this processing activity because it involves processing special category data.

Even if you need not document some or all of your processing activities, we think it is still good practice to do so. Keeping records on what personal data you hold, why you hold it and who you share it with will help you manage the data more effectively and comply with other aspects of the Regulation.

**Please note**

The Article 29 Working Party (WP29) is currently considering the scope of the exemption from documentation of processing activities for small and medium-sized organisations.

WP29 includes representatives from the data protection authorities of each EU member state. It adopts guidelines for complying with the requirements of the GDPR.

If necessary, we will update this guidance to reflect the outcome of WP29's discussions.

## Further Reading

Relevant provisions in the GDPR - See Articles 9(1), 10 and 30(5), and Recitals 51 and 75-76
External link

**Further reading – ICO guidance**

Key definitions

# What do we need to document under Article 30 of the GDPR?

## What do controllers have to document?

If you are a controller for the personal data you process, you need to document the following:

- Your organisation's name and contact details.
- If applicable, the name and contact details of your data protection officer – a person designated to assist with GDPR compliance under Article 37.
- If applicable, the name and contact details of any joint controllers – any other organisations that decide jointly with you why and how personal data is processed.
- If applicable, the name and contact details of your representative – another organisation that represents you if you are based outside the EU, but you monitor or offer services to people in the EU.
- The purposes of the processing – why you use personal data, e.g. customer management, marketing, recruitment.
- The categories of individuals – the different types of people whose personal data is processed, e.g. employees, customers, members.
- The categories of personal data you process – the different types of information you process about people, e.g. contact details, financial information, health data.
- The categories of recipients of personal data – anyone you share personal data with, e.g. suppliers, credit reference agencies, government departments.
- If applicable, the name of any third countries or international organisations that you transfer personal data to – any country or organisation outside the EU.
- If applicable, the safeguards in place for exceptional transfers of personal data to third countries or international organisations. An exceptional transfer is a non-repetitive transfer of a small number of people's personal data, which is based on a compelling business need, as referred to in the second paragraph of Article 49(1) of the GDPR.
- If possible, the retention schedules for the different categories of personal data – how long you will keep the data for. This may be set by internal policies or based on industry guidelines, for instance.
- If possible, a general description of your technical and organisational security measures – your safeguards for protecting personal data, e.g. encryption, access controls, training.

## Further Reading

Relevant provisions in the GDPR - See Articles 4(7), 4(9), 4(17), 5(1)(e)-(f), 26, 30(1), 32, 37 and 49(1), and Recitals 39, 79, 83, 97 and 113
External link

**Further reading – ICO guidance**

Key definitions

Principles

Data protection officers

International transfers

Security

**Further reading – Article 29**

The Article 29 Working Party (WP29) includes representatives from the data protection authorities of each EU member state. It adopts guidelines for complying with the requirements of the GDPR.

WP29 guidelines on Data Protection Officers

## What do processors have to document?

If you are a processor for the personal data you process, you need to document the following:

- Your organisation's name and contact details.
- If applicable, the name and contact details of your data protection officer – a person designated to assist with GDPR compliance under Article 37.
- The name and contact details of each controller on whose behalf you are acting – the organisation that decides why and how the personal data is processed.
- If applicable, the name and contact details of your representative – another organisation that represents you if you are based outside the EU but you monitor or offer services to people in the EU.
- If applicable, the name and contact details of each controller's representative – another organisation that represents the controller if they are based outside the EU, but monitor or offer services to people in the EU.
- The categories of processing you carry out on behalf of each controller – the types of things you do with the personal data, e.g. marketing, payroll processing, IT services.
- If applicable, the name of any third countries or international organisations that you transfer personal data to – any country or organisation outside the EU.
- If applicable, the safeguards in place for exceptional transfers of personal data to third countries or international organisations. An exceptional transfer is a non-repetitive transfer of a small number of people's personal data, which is based on a compelling business need, as referred to in the second paragraph of Article 49(1) of the GDPR.
- If possible, a general description of your technical and organisational security measures – your safeguards for protecting personal data, e.g. encryption, access controls, training.

# Further Reading

Relevant provisions in the GDPR - See Articles 4(7)-(9), 5(1)(f), 30(2), 32, 37 and 49(1), and Recitals 39, 83, 97 and 113
External link

**Further reading – ICO guidance**

Key definitions

Principles

Data protection officers

International transfers

Security

**Further reading – Article 29**

The Article 29 Working Party (WP29) includes representatives from the data protection authorities of each EU member state. It adopts guidelines for complying with the requirements of the GDPR.

WP29 guidelines on Data Protection Officers

# Should we document anything else?

## Are there other things that need documenting?

There are several other provisions in the GDPR and in the UK's Data Protection Bill where documentation is necessary, especially when you are a controller for the personal data being processed. While it is not always a requirement that such information is recorded alongside (or linked from) the record of your processing activities, we think that doing so makes good business sense. It can also help you demonstrate your compliance with other aspects of the Regulation.

## Should we document anything for our privacy notice?

By keeping good records as part of your documentation process, you will be better able to draft your privacy notice and have a better understanding and more complete oversight of your processing activities.

There are several similarities between what you must document about your processing activities and what you must tell people in a privacy notice. However, there are some additional information requirements for your privacy notice, as follows:

- The lawful basis for the processing – one or more of the bases laid out in Article 6(1) of the GDPR.
- If applicable, the legitimate interests for the processing – these are the interests pursued by your organisation or a third party if you are relying on the lawful basis for processing under Article 6(1)(f) of the GDPR. You could also include a link to the record of your assessment of whether legitimate interests apply to the particular processing purpose.
- The rights available to individuals regarding the processing – e.g. access, rectification, erasure, restriction, data portability, and objection. The rights vary depending on the lawful basis for processing. Your documentation can reflect these differences.
- If applicable, the existence of automated decision-making, including profiling. In certain circumstances you will need to tell people about the logic involved and the envisaged consequences.
- If applicable, the source of the personal data. This is relevant when you didn't obtain personal data directly from an individual.

## Further Reading

Relevant provisions in the GDPR - See Articles 6(1) and 13-22, and Recitals 40, 44-49, 65 and 68-71

External link

**Further reading – ICO guidance**

Lawful basis for processing

Legitimate interests

Individual rights

Right to be informed

Rights related to automated decision making including profiling

**Further reading – Article 29**

The Article 29 Working Party (WP29) includes representatives from the data protection authorities of each EU member state. It adopts guidelines for complying with the requirements of the GDPR.

WP29 has published guidelines on Transparency. These were subject to a consultation process and the final version is due to be adopted in April 2018.

WP29 has also published guidelines on Automated individual decision-making and Profiling. These were subject to a consultation process and the final version is due to be adopted in February 2018.

Other relevant guidelines published by WP29 include:

WP29 guidelines on the right to data portability

## What about consent?

When relying on consent as your lawful basis for processing, you must be able to demonstrate how and when that consent was obtained. It may be impractical to document each individual consent as part of your record of processing activities. But you can use this record to indicate you are relying on consent for a particular processing activity, and to link to where the consent has been documented. This can help to maintain an effective audit trail. It can also enable to you quickly locate and provide evidence of consent if challenged.

## Further Reading

Relevant provisions in the GDPR - See Articles 6(1)(a) and 7(1), and Recital 42
External link

**Further reading – ICO guidance**

Consent

**Further reading – Article 29**

The Article 29 Working Party (WP29) includes representatives from the data protection authorities of each EU member state. It adopts guidelines for complying with the requirements of the GDPR.

WP29 has published guidelines on Consent. These were subject to a consultation process and the final version is due to be adopted in April 2018.

## Is there anything else we should document?

*Controller-processor contracts* – if a controller uses a processor to carry out a particular processing activity, a written contract must be in place. Both controllers and processors can use their record of processing activities to link to the relevant contract documents.

*The location of personal data* – recording where personal data is stored will help you locate information more easily when an individual exercises the right of access to their personal data (e.g. manual records held in HR file, electronic records held on cloud server, electronic records held by data processor).

*Data Protection Impact Assessments (DPIAs)* – you must carry out a DPIA when what you are doing with personal data is likely to result in a high risk to individuals' rights and freedoms, particularly when new technologies are involved. You can use your record of processing activities to help flag when a DPIA is required, to keep a track of its progress, and to link to the completed report.

*Personal data breaches* – one of the requirements regarding personal data breaches is that they must be documented. It is up to you to decide how to do this, but we think it is useful to mark any breaches against your record of processing activities, while also linking to the full breach documentation. This can help you monitor which processing activities the breaches relate to and identify any patterns or potential areas of concern.

*Special category data or criminal conviction and offence data* – in the UK, the Data Protection Bill (which is currently going through Parliament and is subject to amendments) sets out several conditions for the processing of special category or criminal conviction and offence data. To satisfy several of these conditions, you must have a policy document that details your procedures for complying with the principles in Article 5 of the GDPR and sets out your policies for retaining and erasing the special category / criminal conviction and offence data. You must also review and retain the policy document when processing the special category / criminal conviction and offence data, and then for at least 6 months afterwards.

If you process these types of personal data, you must document the following information as part of your record of processing activities:

- The condition for processing you rely on in the Data Protection Bill, as set out in Parts 1-3 of Schedule 1.
- The lawful basis for the processing – one or more of the bases laid out in Article 6(1) of the GDPR.
- Whether the personal data is retained and erased in line with the accompanying policy document you must maintain – if not, you must detail the reasons why.

## Further Reading

Relevant provisions in the GDPR - See Articles 15, 28, 33(5) and 35, and Recitals 63, 81 and 84
External link

Relevant provisions in the Data Protection Bill - See Schedule 1
External link

**Further reading – ICO guidance**

Key definitions

Contracts

Right of access

Data protection impact assessments

Data breaches

**Further reading – Article 29**

The Article 29 Working Party (WP29) includes representatives from the data protection authorities of each EU member state. It adopts guidelines for complying with the requirements of the GDPR.

WP29 has published guidelines on Personal data breach notification. These were subject to a consultation process and the final version is due to be adopted in February 2018.

Other relevant guidelines published by WP29 include:

WP29 guidelines on Data Protection Impact Assessments

# How do we document our processing activities?

## How should we prepare?

A good way to start is by doing an information audit or data-mapping exercise to clarify what personal data your organisation holds and where. It is important that people across your organisation are engaged in the process; this can help ensure nothing is missed when mapping the data your organisation processes. It is equally important to obtain senior management buy-in so that your documentation exercise is supported and well resourced.

## What steps should we take next?

Once you have a basic idea of what personal data you have and where it is held, you will be in good position to begin documenting the information you must record under the GDPR. It is up to you how you do this, but we think these three steps will help you get there:

1. *Devise a questionnaire* – you can distribute this to the areas of the organisation you have identified as processing personal data. Use straightforward (jargon-free) questions that will prompt answers to the areas requiring documentation.

**Example questions**

- Why do you use personal data?
- Who do you hold information about?
- What information do you hold about them?
- Who do you share it with?
- How long do you hold it for?
- How do you keep it safe?

2. *Meet directly with key business functions* – this will help you gain a better understanding of how certain parts of your organisation use data.

**Example business functions**

- *IT staff* can help answer questions about technical security measures.
- *Information governance staff* should be able to provide information on retention periods.
- *Legal and compliance staff* may hold details of any data-sharing arrangements.

3. *Locate and review policies, procedures, contracts and agreements* – as well as feeding directly into the documentation exercise, this can help you compare and contrast intended and actual data processing activities.

**Example documents**

- Privacy policies
- Data protection policies
- Data retention policies
- Data security policies
- System use procedures
- Data processor contracts
- Data sharing agreements

## Further Reading

Relevant provisions in the GDPR - See Article 30(1)-(2)
External link

## How should we document our findings?

The documentation of your processing activities must be in writing; this can be in paper or electronic form. Generally, most organisations will benefit from maintaining their documentation electronically so they can easily add to, remove, and amend it as necessary. Paper documentation may be adequate for very small organisations whose processing activities rarely change.

However you choose to document your organisation's processing activities, it is important that you do it in a granular and meaningful way. For instance, you may have several separate retention periods, each specifically relating to different categories of personal data. Equally it is likely that the organisations you share personal data with differ depending on the type of people you hold information on and your purposes for processing the data. The record of your processing activities needs to reflect these differences. A generic list of pieces of information with no meaningful links between them will not meet the GDPR's documentation requirements.

**Example - would not meet GDPR documentation requirements:**

### Categories of personal data

- Contact details

- Financial details
- Lifestyle information
- Location
- IP address...

### Categories of individuals

- Suppliers
- Employees
- Emergency contacts
- Customers
- Clients...

### Categories of personal data

- Contact details
- Financial details
- Lifestyle information
- Location
- IP address...

**Example - would meet GDPR documentation requirements:**

| Purposes of processing | Categories of individuals | Categories of personal data |
|---|---|---|
| Staff administration | Employees | Contact details |
| | | Financial details... |
| | Emergency contacts... | Contact details... |
| Customer orders | Customers | Contact details |
| | | Financial details |
| | | IP address... |

| | | |
|---|---|---|
| | Suppliers... | Contact details<br>Financial details<br>Location... |
| Marketing | Customers | Contact details |
| | | Lifestyle information |
| | Clients... | Contact details... |

## What should we document first?

Start with the broadest piece of information about a particular processing activity, then gradually narrow the scope as you document each requirement under Article 30:

- *Controllers* – it makes sense for controllers to begin with a business function – e.g. HR, Sales, Customer Services. Although the GDPR does not require you to document this information, focusing on each function of your business, one at a time, will help to give your record of processing activities a logical structure. Each business function is likely to have several different purposes for processing personal data, each purpose will involve several different categories of individuals, and in turn those categories of individuals will have their own categories of personal data and so on.

- *Processors* – although you have less information to document as a processor, it still helps to adopt a 'broad to narrow' approach. Start with the controller you are processing personal data for. There may be several different categories of processing you carry out for each controller, and in turn different types of international transfers, security measures and so on.

Documentation using this type of approach should help you create a complete and comprehensive record of your processing activities within which you document the different types of information in a granular way and meaningfully link them together.

## Is there a template we can use?

Yes, we have created two basic templates to help you document your processing activities; one for controllers and one for processors. Each template contains a section for the information you must document, and extra sections for information you are not obliged to document under Article 30 but that can be useful to maintain alongside your record of processing activities.

Using these templates is not mandatory. You can document your organisation's processing activities in many different ways, ranging from basic templates to specialist software packages. How you choose to maintain your documentation will depend on factors such as the size of your organisation, the volume of personal data processed, and the complexity of the processing operations.

Documentation template for controllers

Documentation template for processors

## What if we have an existing documentation method?

In addition to data protection, organisations are often subject to several other regulations that have their own documentation obligations, particularly in sectors such as insurance and finance. If your organisation is subject to such regulatory requirements, you may already have an established data governance framework in place that supports your existing documentation procedures; it may even overlap with the GDPR's record-keeping requirements. If so, the GDPR does not prohibit you from combining and embedding the documentation of your processing activities with your existing record-keeping practices. But you should be careful to ensure you can deliver all the requirements of Article 30, if necessary by adjusting your data governance framework to account for them.

## Do we need to update our record of processing activities?

Keeping a record of your processing activities is not a one-off exercise; the information you document must reflect the current situation as regards the processing of personal data. So you should treat the record as a living document that you update as and when necessary. This means you should conduct regular reviews of the information you process to ensure your documentation remains accurate and up to date.