Guide to accountability and governance

0.0.6 | 19 May 2023

Guide to accountability and governance 5
At a glance 5
Checklist 5
In brief 6
What is accountability? 7
Why is accountability important? 7
What do we need to do? 8
Should we implement data protection policies? 9
Should we adopt a 'data protection by design and default' approach? 10
Do we need to use contracts? 10
What documentation should we maintain? 11
What security measures should we put in place? 12
How do we record and report personal data breaches? 12
Should we carry out data protection impact assessments (DPIAs)? 13
Should we assign a data protection officer (DPO)? 14
Should we adhere to codes of conduct and certification schemes? 15
What else should we consider? 16
Documentation 18
At a glance 18
Checklists 18
In brief 20
What is documentation? 20
Who needs to document their processing activities? 20
What do we need to document under Article 30 of the UK GDPR? 21
Should we document anything else? 21
How do we document our processing activities? 22
Data protection by design and default 24
At a glance 24
Checklists 24
In brief 25
What does the UK GDPR say about data protection by design and by default? 26
What is data protection by design? 27
What is data protection by default? 28

Who is responsible for complying with data protection by design and by default? 28
What are we required to do? 30
When should we do this? 31
What are the underlying concepts of data protection by design and by default? 32
How do we do this in practice? 33
How does data protection by design and by default link to data protection impact assessments (DPIAs)? 35
What is the role of privacy-enhancing technologies (PETs)? 36
What about international transfers? 36
What is the role of certification? 37
What additional guidance is available? 37
Data protection impact assessments 39
At a glance 39
Checklists 40
DPIA awareness checklist 40
DPIA screening checklist 40
DPIA process checklist 42
Have we written a good DPIA? 43
In brief 44
What is a DPIA? 45
When do we need a DPIA? 45
How do we carry out a DPIA? 46
Do we need to consult the ICO? 47
Data protection officers 49
At a glance 49
Checklists 49
Appointing a DPO 49
Position of the DPO 50
Tasks of the DPO 50
Accessibility of the DPO 51
In brief 51
Do we need to appoint a Data Protection Officer? 51
What is the definition of a public authority? 52

What are ‘core activities’? 52
What does ‘regular and systematic monitoring of data subjects on a large scale’ mean? 53
What does processing special category data and personal data relating to criminal convictions and offences on a large scale mean? 54
What professional qualities should the DPO have? 54
What are the tasks of the DPO? 55
Can we assign other tasks to the DPO? 55
Can the DPO be an existing employee? 56
Can we contract out the role of the DPO? 56
Can we share a DPO with other organisations? 57
Can we have more than one DPO? 57
What do we have to do to support the DPO? 57
What details do we have to publish about the DPO? 58
Is the DPO responsible for compliance? 59
Contracts 60
At a glance 60
Checklists 60
What to include in the contract 60
In brief 61
When is a contract needed and why is it important? 61
What needs to be included in the contract? 62
What responsibilities and liabilities do controllers have when using a processor? 62
What responsibilities and liabilities do processors have in their own right? 63

Guide to accountability and governance

> **19 May 2023** - we have broken the Guide to the UK GDPR down into smaller guides. All the content stays the same.

At a glance

- Accountability is one of the data protection principles - it makes you responsible for complying with the UK GDPR and says that you must be able to demonstrate your compliance.
- You need to put in place appropriate technical and organisational measures to meet the requirements of accountability.
- There are a number of measures that you can, and in some cases must, take including:
    - adopting and implementing data protection policies;
    - taking a 'data protection by design and default' approach;
    - putting written contracts in place with organisations that process personal data on your behalf;
    - maintaining documentation of your processing activities;
    - implementing appropriate security measures;
    - recording and, where necessary, reporting personal data breaches;
    - carrying out data protection impact assessments for uses of personal data that are likely to result in high risk to individuals' interests;
    - appointing a data protection officer; and
    - adhering to relevant codes of conduct and signing up to certification schemes.
- Accountability obligations are ongoing. You must review and, where necessary, update the measures you put in place.
- If you implement a privacy management framework this can help you embed your accountability measures and create a culture of privacy across your organisation.
- Being accountable can help you to build trust with individuals and may help you mitigate enforcement action.

Checklist

☐ We take responsibility for complying with the UK GDPR, at the highest management level and throughout our organisation.

☐ We keep evidence of the steps we take to comply with the UK GDPR.

We put in place appropriate technical and organisational measures, such as:

☐ adopting and implementing data protection policies (where proportionate);

☐ taking a 'data protection by design and default' approach - putting appropriate data protection measures in place throughout the entire lifecycle of our processing operations;

☐ putting written contracts in place with organisations that process personal data on our behalf;

☐ maintaining documentation of our processing activities;

☐ implementing appropriate security measures;

☐ recording and, where necessary, reporting personal data breaches;

☐ carrying out data protection impact assessments for uses of personal data that are likely to result in high risk to individuals' interests;

☐ appointing a data protection officer (where necessary); and

☐ adhering to relevant codes of conduct and signing up to certification schemes (where possible).

☐ We review and update our accountability measures at appropriate intervals.

In brief

- What is accountability?
- Why is accountability important?

- What do we need to do?
- Should we implement data protection policies?
- Should we adopt a 'data protection by design and default' approach?
- Do we need to use contracts?
- What documentation should we maintain?
- What security measures should we put in place?
- How do we record and report personal data breaches?
- Should we carry out data protection impact assessments (DPIAs)?
- Should we assign a data protection officer (DPO)?
- Should we adhere to codes of conduct and certification schemes?
- What else should we consider?

Relevant provisions in the UK GDPR - See Articles 5 and 24, and Recitals 39 and 74

https://www.legislation.gov.uk/eur/2016/679/contents

What is accountability?

There are two key elements. First, the accountability principle makes it clear that you are **responsible** for complying with the GDPR. Second, you must be able to **demonstrate** your compliance.

Article 5(2) of the GDPR says:

> "The controller shall be responsible for, and be able to demonstrate compliance with, paragraph 1 ('accountability')

Relevant provisions in the UK GDPR - See Article 5 and Recitals 39 and 74

https://www.legislation.gov.uk/eur/2016/679/contents

Further reading – ICO guidance

Principles

Why is accountability important?

Taking responsibility for what you do with personal data, and demonstrating the steps you have taken to protect people's rights not only results in better

legal compliance, it also offers you a competitive edge. Accountability is a real opportunity for you to show, and prove, how you respect people's privacy. This can help you to develop and sustain people's trust.

Furthermore, if something does go wrong, then being able to show that you actively considered the risks and put in place measures and safeguards can help you provide mitigation against any potential enforcement action. On the other hand, if you can't show good data protection practices, it may leave you open to fines and reputational damage.

Relevant provisions in the UK GDPR - See Article 83

https://www.legislation.gov.uk/eur/2016/679/contents

What do we need to do?

Accountability is not a box-ticking exercise. Being **responsible** for compliance with the UK GDPR means that you need to be proactive and organised about your approach to data protection, while **demonstrating** your compliance means that you must be able to evidence the steps you take to comply.

To achieve this, if you are a larger organisation you may choose to put in place a privacy management framework. This can help you create a culture of commitment to data protection, by embedding systematic and demonstrable compliance across your organisation. Amongst other things, your framework should include:

- robust program controls informed by the requirements of the UK GDPR;
- appropriate reporting structures; and
- assessment and evaluation procedures.

If you are a smaller organisation you will most likely benefit from a smaller scale approach to accountability. Amongst other things you should:

- ensure a good level of understanding and awareness of data protection amongst your staff;
- implement comprehensive but proportionate policies and procedures for handling personal data; and
- keep records of what you do and why.

Article 24(1) of the UK GDPR says that:

- you must implement technical and organisational measures to ensure, and demonstrate, compliance with the UK GDPR;
- the measures should be risk-based and proportionate; and
- you need to review and update the measures as necessary.

While the UK GDPR does not specify an exhaustive list of things you need to do to be accountable, it does set out several different measures you can take that will help you get there. These are summarised under the headings below, with links to the relevant parts of the guide. Some measures you are obliged to take and some are voluntary. It will differ depending on what personal data you have and what you do with it. These measures can form the basis of your programme controls if you opt to put in place a privacy management framework across your organisation.

Should we implement data protection policies?

For many organisations, putting in place relevant policies is a fundamental part of their approach to data protection compliance. The UK GDPR explicitly says that, where proportionate, implementing data protection policies is one of the measures you can take to ensure, and demonstrate, compliance.

What you have policies for, and their level of detail, depends on what you do with personal data. If, for instance, you handle large volumes of personal data, or particularly sensitive information such as special category data, then you should take greater care to ensure that your policies are robust and comprehensive.

As well as drafting data protection policies, you should also be able to show that you have implemented and adhered to them. This could include awareness raising, training, monitoring and audits – all tasks that your data protection officer can undertake (see below for more on data protection officers).

Relevant provisions in the UK GDPR - See Articles 24(2) and Recital 78

https://www.legislation.gov.uk/eur/2016/679/contents

Relevant provisions in the UK GDPR - See Recital 78

https://www.legislation.gov.uk/eur/2016/679/introduction

Should we adopt a 'data protection by design and default' approach?

Privacy by design has long been seen as a good practice approach when designing new products, processes and systems that use personal data. Under the heading 'data protection by design and by default', the UK GDPR legally requires you to take this approach.

Data protection by design and default is an integral element of being accountable. It is about embedding data protection into everything you do, throughout all your processing operations. The UK GDPR suggests measures that may be appropriate such as minimising the data you collect, applying pseudonymisation techniques, and improving security features.

Integrating data protection considerations into your operations helps you to comply with your obligations, while documenting the decisions you take (often in data protection impact assessments – see below) demonstrates this.

Relevant provisions in the UK GDPR - See Article 25

https://www.legislation.gov.uk/eur/2016/679/article/25

Relevant provisions in the UK GDPR - See Recital 78

Recitals:https://www.legislation.gov.uk/eur/2016/679/introduction

Further reading – ICO guidance

- Data protection by design and default
- Anonymisation

Do we need to use contracts?

Whenever a controller uses a processor to handle personal data on their behalf, it needs to put in place a written contract that sets out each party's responsibilities and liabilities.

Contracts must include certain specific terms as a minimum, such as requiring the processor to take appropriate measures to ensure the security of processing and obliging it to assist the controller in allowing individuals to exercise their rights under the UK GDPR.

Using clear and comprehensive contracts with your processors helps to ensure that everyone understands their data protection obligations and is a good way to demonstrate this formally.

Relevant provisions in the UK GDPR - See Article 28

https://www.legislation.gov.uk/eur/2016/679/article/28

Relevant provisions in the UK GDPR - See Recital 81

https://www.legislation.gov.uk/eur/2016/679/introduction

Further reading – ICO guidance

- Contracts

What documentation should we maintain?

Under Article 30 of the UK GDPR, most organisations are required to maintain a record of their processing activities, covering areas such as processing purposes, data sharing and retention.

Documenting this information is a great way to take stock of what you do with personal data. Knowing what information you have, where it is and what you do with it makes it much easier for you to comply with other aspects of the UK GDPR such as making sure that the information you hold about people is accurate and secure.

As well as your record of processing activities under Article 30, you also need to document other things to show your compliance with the UK GDPR. For instance, you need to keep records of consent and any personal data breaches.

Relevant provisions in the UK GDPR - See Articles 7(1), 30 and 33(5), and Recitals 42 and 82

https://www.legislation.gov.uk/eur/2016/679/contents

Further reading – ICO guidance

- Documentation

- Consent
- Personal data breaches

What security measures should we put in place?

The UK GDPR repeats the requirement to implement technical and organisational measures to comply with the UK GDPR in the context of security. It says that these measures should ensure a level of security appropriate to the risk.

You need to implement security measures if you are handling any type of personal data, but what you put in place depends on your particular circumstances. You need to ensure the confidentiality, integrity and availability of the systems and services you use to process personal data.

Amongst other things, this may include information security policies, access controls, security monitoring, and recovery plans.

Relevant provisions in the UK GDPR - See Articles 5(f) and 32, and Recitals 39 and 83

https://www.legislation.gov.uk/eur/2016/679/contents

Further reading – ICO guidance

- Security

How do we record and report personal data breaches?

You must report certain types of personal data breach to the Information Commissioner's Office (ICO), and in some circumstances, to the affected individuals as well.

Additionally, the UK GDPR says that you must keep a record of any personal data breaches, regardless of whether you need to report them or not.

You need to be able to detect, investigate, report (both internally and externally) and document any breaches. Having robust policies, procedures and reporting structures helps you do this.

Relevant provisions in the UK GDPR - See Articles 33-34 and Recitals 85-88

https://www.legislation.gov.uk/eur/2016/679/contents

Further reading – ICO guidance

- Personal data breaches

Further reading – European Data Protection Board

The European Data Protection Board (EDPB), which has replaced 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 EU version of the GDPR.

WP29 adopted guidelines on Personal data breach notification, which have been adopted by the EDPB.

EDPB guidelines are no longer directly relevant to the UK regime and are not binding under the UK regime. However, they may still provide helpful guidance on certain issues.

Should we carry out data protection impact assessments (DPIAs)?

A DPIA is an essential accountability tool and a key part of taking a data protection by design approach to what you do. It helps you to identify and minimise the data protection risks of any new projects you undertake.

A DPIA is a legal requirement before carrying out processing likely to result in high risk to individuals' interests.

When done properly, a DPIA helps you assess how to comply with the requirements of the UK GDPR, while also acting as documented evidence of your decision-making and the steps you took.

Relevant provisions in the UK GDPR - See Articles 35-36, and Recitals 84 and 89-95

https://www.legislation.gov.uk/eur/2016/679/contents

Further reading – ICO guidance

- Data protection impact assessments

Further reading – European Data Protection Board

The European Data Protection Board (EDPB), which has replaced 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 adopted guidelines on data protection impact assessments, which have been endorsed by the EDPB.

EDPB guidelines are no longer directly relevant to the UK regime and are not binding under the UK regime. However, they may still provide helpful guidance on certain issues".

Should we assign a data protection officer (DPO)?

Some organisations are required to appoint a DPO. A DPO's tasks include advising you about the UK GDPR, monitoring compliance and training staff.

Your DPO must report to your highest level of management, operate independently, and have adequate resources to carry out their tasks.

Even if you're not obliged to appoint a DPO, it is very important that you have sufficient staff, skills, and appropriate reporting structures in place to meet your obligations under the UK GDPR.

Relevant provisions in the UK GDPR - See Articles 37-39

https://www.legislation.gov.uk/eur/2016/679

Relevant provisions in the UK GDPR - Recital 97

https://www.legislation.gov.uk/eur/2016/679/introduction

Further reading – ICO guidance

- Data protection officers

Further reading – European Data Protection Board

The European Data Protection Board (EDPB), which has replaced 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 adopted guidelines on data protection officers, which have been endorsed by the EDPB.

EDPB guidelines are no longer directly relevant to the UK regime and are not binding under the UK regime. However, they may still provide helpful guidance on certain issues".

Should we adhere to codes of conduct and certification schemes?

Under the UK GDPR, trade associations and representative bodies may draw up codes of conduct covering topics such as fair and transparent processing, pseudonymisation, and the exercise of people's rights.

In addition, the ICO or accredited certification bodies can issue certification of the data protection compliance of products and services.

Both codes of conduct and certification are voluntary, but they are an excellent way of verifying and demonstrating that you comply with the GDPR.

Relevant provisions in the UK GDPR - See Articles 40-43, and Recitals 98 and 100

https://www.legislation.gov.uk/eur/2016/679

Further reading – ICO guidance

- Codes of conduct and certification

What else should we consider?

The above measures can help to support an accountable approach to data protection, but it is not limited to these. You need to be able to prove what steps you have taken to comply. In practice this means keeping records of what you do and justifying your decisions.

Example

A company wants to use the personal data it holds for a new purpose. It carries out an assessment in line with Article 6(4) of the UK GDPR, and determines that the new purpose is compatible with the original purpose for which it collected the personal data. Although this provision of the UK GDPR does not specify that the company must document its compatibility assessment, it knows that to be accountable, it needs to be able to prove that their handling of personal data is compliant with the UK GDPR. The company therefore keeps a record of the compatibility assessment, including its rationale for the decision and the appropriate safeguards it put in place.

Accountability is not just about being answerable to the regulator; you must also demonstrate your compliance to individuals. Amongst other things, individuals have the right to be informed about what personal data you collect, why you use it and who you share it with. Additionally, if you use techniques such as artificial intelligence and machine learning to make decisions about people, in certain cases individuals have the right to hold you to account by requesting explanations of those decisions and contesting them. You therefore need to find effective ways to provide information to people about what you do with their personal data, and explain and review automated decisions.

The obligations that accountability places on you are ongoing – you cannot simply sign off a particular processing operation as 'accountable' and move on. You must review the measures you implement at appropriate intervals to ensure that they remain effective. You should update measures that are no longer fit for purpose. If you regularly change what you do with personal data, or the types of information that you collect, you should review and update your measures frequently, remembering to document what you do and why.

Relevant provisions in the UK GDPR - See Articles 12-14, 22 and 24(1), and Recitals 39, 58-61 and 71

https://www.legislation.gov.uk/eur/2016/679/contents

Further reading – ICO guidance

- Right to be informed
- Rights related to automated decision making including profiling
- Data protection self assessment
- Accountability Framework

Documentation

> **19 May 2023** - we have broken the Guide to the UK GDPR down into smaller guides. All the content stays the same.

At a glance

- The UK GDPR contains explicit provisions about documenting your processing activities.
- You must maintain records on several things such as processing purposes, data sharing and retention.
- You may be required to make the records available to the ICO on request.
- Documentation can help you comply with other aspects of the UK GDPR and improve your data governance.
- Controllers and processors both have documentation obligations.
- For small and medium-sized organisations, documentation requirements are limited to certain types of processing activities.
- Information audits or data-mapping exercises can feed into the documentation of your processing activities.
- Records must be kept in writing.
- Most organisations will benefit from maintaining their records electronically.
- Records must be kept up to date and reflect your current processing activities.
- We have produced some basic templates to help you document your processing activities.

Checklists

Documentation of processing activities – requirements

☐ If we are a controller for the personal data we process, we document all the applicable information under Article 30(1) of the UK GDPR.

☐ If we are a processor for the personal data we process, we document all the applicable information under Article 30(2) of the UK GDPR.

If we process special category or criminal conviction and offence data, we document:

☐ the condition for processing we rely on in the Data Protection Act 2018 (DPA 2018);

☐ the lawful basis for our processing; and

☐ whether we retain and erase the personal data in accordance with our policy document.

where required in schedule 1 of the DPA 2018.

☐ We document our processing activities in writing.

☐ We document our processing activities in a granular way with meaningful links between the different pieces of information.

☐ We conduct regular reviews of the personal data we process and update our documentation accordingly.

Documentation of processing activities – best practice

When preparing to document our processing activities we:

☐ do information audits to find out what personal data our organisation holds;

☐ distribute questionnaires and talk to staff across the organisation to get a more complete picture of our processing activities; and

☐ review our policies, procedures, contracts and agreements to address areas such as retention, security and data sharing.

As part of our record of processing activities we document, or link to documentation, on:

☐ information required for privacy notices;

☐ records of consent;

☐ controller-processor contracts;

☐ the location of personal data;

☐ Data Protection Impact Assessment reports; and

☐ records of personal data breaches.

☐ We document our processing activities in electronic form so we can add, remove and amend information easily.

In brief

- What is documentation?
- Who needs to document their processing activities?
- What do we need to document under Article 30 of the GDPR?
- Should we document anything else?
- How do we document our processing activities?
- In detail

What is documentation?

- Most organisations are required to maintain a record of their processing activities, covering areas such as processing purposes, data sharing and retention; we call this **documentation**.
- Documenting your processing activities is important, not only because it is itself a legal requirement, but also because it can support good data governance and help you demonstrate your compliance with other aspects of the UK GDPR.

Who needs to document their processing activities?

- Controllers and processors each have their own documentation obligations.

- If you have 250 or more employees, you must document all your processing activities.
- There is a limited exemption for small and medium-sized organisations. If you have fewer than 250 employees, you 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 conviction and offence data.

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

You must document the following information:

- The name and contact details of your organisation (and where applicable, of other 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.
- Details of your transfers to third countries including documenting the transfer mechanism safeguards in place.
- Retention schedules.
- A description of your technical and organisational security measures.

Should we document anything else?

As part of your record of processing activities, it can be useful to document (or link to documentation of) other aspects of your compliance with the UK GDPR and the UK's Data Protection Act 2018. Such documentation may include:

- information required for privacy notices, such as:
    - the lawful basis for the processing
    - the legitimate interests for the processing
    - individuals' rights
    - the existence of automated decision-making, including profiling
    - the source of the personal data;
- records of consent;
- controller-processor contracts;
- the location of personal data;

- Data Protection Impact Assessment reports;
- records of personal data breaches;
- information required for processing special category data or criminal conviction and offence data under the Data Protection Act 2018, covering:
    - the condition for processing in the Data Protection Act;
    - the lawful basis for the processing in the UK GDPR; and
    - your retention and erasure policy document.

How do we document our processing activities?

- Doing an information audit or data-mapping exercise can help you find out what personal data your organisation holds and where it is.

- You can find out why personal data is used, who it is shared with and how long it is kept by distributing questionnaires to relevant areas of your organisation, meeting directly with key business functions, and reviewing policies, procedures, contracts and agreements.

- When documenting your findings, the records you keep must be in writing. The information must be documented in a granular and meaningful way.

We have developed basic templates to help you document your processing activities.

Documentation template for controllers

https://ico.org.uk/media2/migrated/2172937/gdpr-documentation-controller-template.xlsx

Documentation template for processors

https://ico.org.uk/media2/migrated/2172936/gdpr-documentation-processor-template.xlsx

Relevant provisions in the UK GDPR – See Article 30 and Recital 82

https://www.legislation.gov.uk/eur/2016/679/contents

Relevant provisions in the Data Protection Act 2018 – See Schedule 1

https://services.parliament.uk/bills/2017-19/dataprotection.html

In more detail – ICO guidance

We have produced more detailed guidance on documentation.

The Accountability Framework looks at the ICO's expectations in relation to records of processing.

In more detail - European Data Protection Board

The European Data Protection Board (EDPB), which has replaced 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 published a position paper on Article 30(5) (the exemption for small and medium-sized organisations), which has been endorsed by the EDPB.

EDPB guidelines are no longer be directly relevant to the UK regime and are not binding under the UK regime. However, they may still provide helpful guidance on certain issues

Data protection by design and default

> **19 May 2023** - we have broken the Guide to the UK GDPR down into smaller guides. All the content stays the same.

At a glance

- The UK GDPR requires you to put in place appropriate technical and organisational measures to implement the data protection principles effectively and safeguard individual rights. This is 'data protection by design and by default'.
- In essence, this means you have to integrate or 'bake in' data protection into your processing activities and business practices, from the design stage right through the lifecycle.
- This concept is not new. Previously known as 'privacy by design', it has always been part of data protection law. The key change with the UK GDPR is that it is now a legal requirement.
- Data protection by design is about considering data protection and privacy issues upfront in everything you do. It can help you ensure that you comply with the UK GDPR's fundamental principles and requirements, and forms part of the focus on accountability.

Checklists

☐ We consider data protection issues as part of the design and implementation of systems, services, products and business practices.

☐ We make data protection an essential component of the core functionality of our processing systems and services.

☐ We anticipate risks and privacy-invasive events before they occur, and take steps to prevent harm to individuals.

☐ We only process the personal data that we need for our purposes(s), and that we only use the data for those purposes.

☐ We ensure that personal data is automatically protected in any IT system, service, product, and/or business practice, so that individuals should not have to take any specific action to protect their privacy.

☐ We provide the identity and contact information of those responsible for data protection both within our organisation and to individuals.

☐ We adopt a 'plain language' policy for any public documents so that individuals easily understand what we are doing with their personal data.

☐ We provide individuals with tools so they can determine how we are using their personal data, and whether our policies are being properly enforced.

☐ We offer strong privacy defaults, user-friendly options and controls, and respect user preferences.

☐ We only use data processors that provide sufficient guarantees of their technical and organisational measures for data protection by design.

☐ When we use other systems, services or products in our processing activities, we make sure that we only use those whose designers and manufacturers take data protection issues into account.

☐ We use privacy-enhancing technologies (PETs) to assist us in complying with our data protection by design obligations.

In brief

- What does the UK GDPR say about data protection by design and by default?
- What is data protection by design?
- What is data protection by default?
- Who is responsible for complying with data protection by design and by default?
- What are we required to do?
- When should we do this?
- What are the underlying concepts of data protection by design and by default?
- How do we do this in practice?
- How does data protection by design and by default link to data protection impact assessments (DPIAs)?
- What is the role of privacy-enhancing technologies (PETs)?
- What about international transfers?
- What is the role of certification?

- What additional guidance is available?

What does the UK GDPR say about data protection by design and by default?

The UK GDPR requires you to integrate data protection concerns into every aspect of your processing activities. This approach is 'data protection by design and by default'. It is a key element of the UK GDPR's risk-based approach and its focus on accountability, ie your ability to demonstrate how you are complying with its requirements.

Some organisations already adopt a 'privacy by design approach' as a matter of good practice. If this is the case for you, then you are well-placed to meet the requirements of data protection by design and by default. However, you may still need to review your processes and procedures to ensure that you are meeting your obligations.

Articles 25(1) and 25(2) of the GDPR outline your obligations concerning data protection by design and by default.

Article 25(1) specifies the requirements for data protection by design:

> 'Taking into account the state of the art, the cost of implementation and the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for rights and freedoms of natural persons posed by the processing, the controller shall, both at the time of the determination of the means for processing and at the time of the processing itself, implement appropriate technical and organisational measures, such as pseudonymisation, which are designed to implement data-protection principles, such as data minimisation, in an effective manner and to integrate the necessary safeguards into the processing in order to meet the requirements of this Regulation and protect the rights of data subjects.'

Article 25(2) specifies the requirements for data protection by default:

> 'The controller shall implement appropriate technical and organisational measures for ensuring that, by default, only personal data which are

> necessary for each specific purpose of the processing are processed. That obligation applies to the amount of personal data collected, the extent of their processing, the period of their storage and their accessibility. In particular, such measures shall ensure that by default personal data are not made accessible without the individual's intervention to an indefinite number of natural persons.'

Article 25(3) states that if you adhere to an approved certification under Article 42, you can use this as one way of demonstrating your compliance with these requirements.

Relevant provisions in the UK GDPR - Article 25 and Recital 78

https://www.legislation.gov.uk/eur/2016/679/contents

What is data protection by design?

Data protection by design is ultimately an approach that ensures you consider privacy and data protection issues at the design phase of any system, service, product or process and then throughout the lifecycle.

As expressed by the UK GDPR, it requires you to:

- put in place appropriate technical and organisational measures designed to implement the data protection principles effectively; and
- integrate safeguards into your processing so that you meet the UK GDPR's requirements and protect individual rights.

In essence this means you have to integrate or 'bake in' data protection into your processing activities and business practices.

Data protection by design has broad application. Examples include:

- developing new IT systems, services, products and processes that involve processing personal data;
- developing organisational policies, processes, business practices and/or strategies that have privacy implications;
- physical design;
- embarking on data sharing initiatives; or
- using personal data for new purposes.

The underlying concepts of data protection by design are not new. Under the name 'privacy by design' they have existed for many years.

What is data protection by default?

Data protection by default requires you to ensure that you only process the data that is necessary to achieve your specific purpose. It links to the fundamental data protection principles of data minimisation and purpose limitation.

You have to process some personal data to achieve your purpose(s). Data protection by default means you need to specify this data before the processing starts, appropriately inform individuals and only process the data you need for your purpose. It does **not** require you to adopt a 'default to off' solution. What you need to do depends on the circumstances of your processing and the risks posed to individuals.

Nevertheless, you must consider things like:

- adopting a 'privacy-first' approach with any default settings of systems and applications;
- ensuring you do not provide an illusory choice to individuals relating to the data you will process;
- not processing additional data unless the individual decides you can;
- ensuring that personal data is not automatically made publicly available to others unless the individual decides to make it so; and
- providing individuals with sufficient controls and options to exercise their rights.

Who is responsible for complying with data protection by design and by default?

Article 25 specifies that, as the controller, you have responsibility for complying with data protection by design and by default. Depending on your circumstances, you may have different requirements for different areas within your organisation. For example:

- your senior management, eg developing a culture of 'privacy awareness' and ensuring you develop policies and procedures with data protection in mind;
- your software engineers, system architects and application developers, eg those who design systems, products and services should take account of data protection requirements and assist you in complying with your obligations; and

- your business practices, eg you should ensure that you embed data protection by design in all your internal processes and procedures.

This may not apply to all organisations, of course. However, data protection by design is about adopting an organisation-wide approach to data protection, and 'baking in' privacy considerations into any processing activity you undertake. It doesn't apply only if you are the type of organisation that has your own software developers and systems architects.

In considering whether to impose a penalty, the ICO will take into account the technical and organisational measures you have put in place in respect of data protection by design. Additionally, under the Data Protection Act 2018 (DPA 2018) we can issue an Enforcement Notice against you for any failings in respect of Article 25.

What about data processors?

If you use another organisation to process personal data on your behalf, then that organisation is a data processor under the UK GDPR.

Article 25 does not mention data processors specifically. However, Article 28 specifies the considerations you must take whenever you are selecting a processor. For example, you must only use processors that provide:

> 'sufficient guarantees to implement appropriate technical and organisational measures in such a manner that the processing will meet the requirements of this Regulation and ensure the protection of the rights of the data subject'

This requirement covers both data protection by design in Article 25 as well as other aspects (eg your security obligations under Article 32). Your processor cannot necessarily assist you with your data protection by design obligations (unlike with security measures), however you must only use processors that provide sufficient guarantees to meet the UK GDPR's requirements.

What about other parties?

Data protection by design and by default can also impact organisations other than controllers and processors. Depending on your processing activity, other

parties may be involved, even if this is just where you purchase a product or service that you then use in your processing. Examples include manufacturers, product developers, application developers and service providers.

Recital 78 extends the concepts of data protection by design to other organisations, although it does not place a requirement on them to comply – that remains with you as the controller. It says:

> 'When developing, designing, selecting and using applications, services and products that are based on the processing of personal data or process personal data to fulfil their task, producers of the products, services and applications should be encouraged to take into account the right to data protection when developing and designing such products, services and applications and, with regard to the state of the art, to make sure that controllers and processors are able to fulfil their data protection obligations.'

Therefore, when considering what products and services you need for your processing, you should look to choose those where the designers and developers have taken data protection into account. This can help to ensure that your processing adheres to the data protection by design requirements.

If you are a developer or designer of products, services and applications, the UK GDPR places no specific obligations on you about how you design and build these products. (You may have specific obligations as a controller in your own right, eg for any employee data.) However, you should note that controllers are required to consider data protection by design when selecting services and products for use in their data processing activities – therefore if you design these products with data protection in mind, you may be in a better position.

Relevant provisions in the UK GDPR - Articles 25 and 28, and Recitals 78, 79, 81 and 82

https://www.legislation.gov.uk/eur/2016/679/contents

What are we required to do?

You must put in place appropriate technical and organisational measures designed to implement the data protection principles effectively and safeguard individual rights.

There is no 'one size fits all' method to do this, and no one set of measures that you should put in place. It depends on your circumstances.

The key is that you consider data protection issues from the start of any processing activity, and adopt appropriate policies and measures that meet the requirements of data protection by design and by default.

Some examples of how you can do this include:

- minimising the processing of personal data;
- pseudonymising personal data as soon as possible;
- ensuring transparency in respect of the functions and processing of personal data;
- enabling individuals to monitor the processing; and
- creating (and improving) security features.

This is not an exhaustive list. Complying with data protection by design and by default may require you to do much more than the above.

However, we cannot provide a complete guide to all aspects of data protection by design and by default in all circumstances. This guidance identifies the main points for you to consider. Depending on the processing you are doing, you may need to obtain specialist advice that goes beyond the scope of this guidance.

Relevant provisions in the UK GDPR - Recital 78

https://www.legislation.gov.uk/eur/2016/679/contents

When should we do this?

Data protection by design starts at the initial phase of any system, service, product, or process. You should begin by considering your intended processing activities, the risks that these may pose to individuals, and the possible measures available to ensure that you comply with the data protection principles and protect individual rights. These considerations must cover:

- the state of the art and costs of implementation of any measures;
- the nature, scope, context and purposes of your processing; and

- the risks that your processing poses to the rights and freedoms of individuals.

This is similar to the information risk assessment you should do when considering your security measures.

These considerations lead into the second step, where you put in place actual technical and organisational measures to implement the data protection principles and integrate safeguards into your processing.

This is why there is no single solution or process that applies to every organisation or every processing activity, although there are a number of commonalities that may apply to your specific circumstances as described below.

The UK GDPR requires you to take these actions:

- 'at the time of the determination of the means of the processing' – in other words, when you are at the design phase of any processing activity; and
- 'at the time of the processing itself' – ie during the lifecycle of your processing activity.

What are the underlying concepts of data protection by design and by default?

The underlying concepts are essentially expressed in the seven 'foundational principles' of privacy by design, as developed by the Information and Privacy Commissioner of Ontario.

Although privacy by design is not necessarily equivalent to data protection by design, these foundational principles can nevertheless underpin any approach you take.

'Proactive not reactive; preventative not remedial'

You should take a proactive approach to data protection and anticipate privacy issues and risks before they happen, instead of waiting until after the fact. This doesn't just apply in the context of systems design – it involves developing a culture of 'privacy awareness' across your organisation.

'Privacy as the default setting'

You should design any system, service, product, and/or business practice to protect personal data automatically. With privacy built into the system, the individual does not have to take any steps to protect their data – their privacy remains intact without them having to do anything.

‘Privacy embedded into design’

Embed data protection into the design of any systems, services, products and business practices. You should ensure data protection forms part of the core functions of any system or service – essentially, it becomes integral to these systems and services.

‘Full functionality – positive sum, not zero sum’

Also referred to as ‘win-win’, this principle is essentially about avoiding trade-offs, such as the belief that in any system or service it is only possible to have privacy **or** security, not privacy **and** security. Instead, you should look to incorporate all legitimate objectives whilst ensuring you comply with your obligations.

‘End-to-end security – full lifecycle protection’

Put in place strong security measures from the beginning, and extend this security throughout the ‘data lifecycle’ – ie process the data securely and then destroy it securely when you no longer need it.

‘Visibility and transparency – keep it open’

Ensure that whatever business practice or technology you use operates according to its premises and objectives, and is independently verifiable. It is also about ensuring visibility and transparency to individuals, such as making sure they know what data you process and for what purpose(s) you process it.

‘Respect for user privacy – keep it user-centric’

Keep the interest of individuals paramount in the design and implementation of any system or service, eg by offering strong privacy defaults, providing individuals with controls, and ensuring appropriate notice is given.

How do we do this in practice?

One means of putting these concepts into practice is to develop a set of practical, actionable guidelines that you can use in your organisation, framed by your assessment of the risks posed and the measures available to you. You could base these upon the seven foundational principles.

However, how you go about doing this depends on your circumstances – who you are, what you are doing, the resources you have available, and the nature of the data you process. You may not need to have a set of documents and organisational controls in place, although in some situations you will be required to have certain documents available concerning your processing.

The key is to take an organisational approach that achieves certain outcomes, such as ensuring that:

- you consider data protection issues as part of the design and implementation of systems, services, products and business practices;
- you make data protection an essential component of the core functionality of your processing systems and services;
- you only process the personal data that you need in relation to your purposes(s), and that you only use the data for those purposes;
- personal data is automatically protected in any IT system, service, product, and/or business practice, so that individuals should not have to take any specific action to protect their privacy;
- the identity and contact information of those responsible for data protection are available both within your organisation and to individuals;
- you adopt a 'plain language' policy for any public documents so that individuals easily understand what you are doing with their personal data;
- you provide individuals with tools so they can determine how you are using their personal data, and whether you are properly enforcing your policies; and
- you offer strong privacy defaults, user-friendly options and controls, and respect user preferences.

Many of these relate to other obligations in the UK GDPR, such as transparency requirements, documentation, Data Protection Officers and DPIAs. This shows the broad nature of data protection by design and how it applies to all aspects of your processing. Our guidance on these topics will help you when you consider the measures you need to put in place for data protection by design and by default.

In more detail – ICO guidance

Read our sections on the data protection principles, individual rights, accountability and governance, documentation, data protection impact assessments, data protection officers and security.

The Accountability Framework looks at the ICO's expectations in relation to data protection by design.

In more detail – European Data Protection Board

The European Data Protection Board (EDPB) adopts guidelines for complying with the requirements of the EU GDPR.

The EDPB has adopted guidelines on Data Protection by Design and Default.

EDPB guidelines are no longer directly relevant to the UK regime and are not binding under the UK regime. However, they may still provide helpful guidance on certain issues.

Further reading

We will produce further guidance on how you can implement data protection by design soon. However, the Information and Privacy Commissioner of Ontario has published guidance on how organisations can 'operationalise' privacy by design, which may assist you.

How does data protection by design and by default link to data protection impact assessments (DPIAs)?

A DPIA is a tool that you can use to identify and reduce the data protection risks of your processing activities. They can also help you to design more efficient and effective processes for handling personal data.

DPIAs are an integral part of data protection by design and by default. For example, they can determine the type of technical and organisational measures you need in order to ensure your processing complies with the data protection principles.

However, a DPIA is only required in certain circumstances, such as where the processing is likely to result in a risk to rights and freedoms, though it is good practice to undertake a DPIA anyway. In contrast, data protection by design is a broader concept, as it applies organisationally and requires you to take certain considerations even before you decide whether your processing is likely to result in a high risk or not.

What is the role of privacy-enhancing technologies (PETs)?

Privacy-enhancing technologies or PETs are technologies that embody fundamental data protection principles by minimising personal data use, maximising data security, and empowering individuals. A useful definition from the European Union Agency for Cybersecurity (ENISA) refers to PETs as:

> 'software and hardware solutions, ie systems encompassing technical processes, methods or knowledge to achieve specific privacy or data protection functionality or to protect against risks of privacy of an individual or a group of natural persons.'

PETs link closely to the concept of privacy by design, and therefore apply to the technical measures you can put in place. They can assist you in complying with the data protection principles and are a means of implementing data protection by design within your organisation on a technical level.

Further reading

We have published guidance on PETs.

What about international transfers?

Data protection by design also applies in the context of international transfers in cases where you intend to transfer personal data overseas to a third country that does not have an adequacy decision.

You need to ensure that, whatever mechanism you use, appropriate safeguards are in place for these transfers. As detailed in Recital 108, these safeguards need to include compliance with data protection by design and by default.

Relevant provisions in the UK GDPR - Article 47 and Recital 108

https://www.legislation.gov.uk/eur/2016/679/contents

In more detail – ICO guidance

Read our guidance on international transfers.

What is the role of certification?

Article 25(3) says that:

> 'An approved certification mechanism pursuant to Article 42 may be used as an element to demonstrate compliance with the requirements set out in paragraphs 1 and 2 of this Article.'

This means that being certified through an ICO approved certification scheme can assist you in showing how you are complying with, and implementing, data protection by design and by default.

What additional guidance is available?

The ICO will publish more detailed guidance about data protection by design and privacy enhancing technologies soon, as well as how these concepts apply in the context of the code of practice on age appropriate design in the DPA 2018 section 123.

In the meantime, there are a number of publications about the privacy by design approach. We have summarised some of these below.

Further reading

The **Information and Privacy Commissioner of Ontario** (IPC) originated the concept of privacy by design in the 1990s. The IPC has a number of relevant publications about the concept and how you can implement it in your organisation, including:

- the original seven foundational principles of privacy by design (external link, PDF); and
- a primer on privacy by design, published in 2013 (external link, PDF); and
- guidance on Operationalizing privacy by design, published in 2012 (external link, PDF)

The **European Union Agency for Cybersecurity** (ENISA) has also published research and guidance on privacy by design, including:

- a research report on privacy and data protection by design (external link);
- a research report on privacy by design and big data (external link); and
- a subsection on privacy-enhancing technologies (external link)

The **Norwegian data protection authority** (Datatilsynet) has produced guidancee on how software developers can implement data protection by design and by default.

Data protection impact assessments

The Brexit transition period ended on 31 December 2020. The GDPR has been retained in UK law as the UK GDPR, and will continue to be read alongside the Data Protection Act 2018, with technical amendments to ensure it can function in UK law. If you transfer or receive data from overseas please visit our End of Transition and International Transfers pages. You should make sure you can identify any data you collected before the end of 2020 about people outside the UK, for further information, see our Q&A on Legacy Data.

On 01 January, there will not be any significant change to the UK data protection regime, or to the criteria that compel DPIAs. This guidance draws on European resources which we still consider to be relevant, and so these resources remain part of our DPIA guidance.

We will keep this guidance under review and update it as and when any aspect of your obligations or our approach changes. Please continue to monitor our website for updates.

> **19 May 2023** - we have broken the Guide to the UK GDPR down into smaller guides. All the content stays the same.

- Click here for a sample DPIA Template
- Click here to contact the ICO about your DPIA

At a glance

- A Data Protection Impact Assessment (DPIA) is a process to help you identify and minimise the data protection risks of a project.
- You must do a DPIA for processing that is **likely to result in a high risk** to individuals. This includes some specified types of processing. You can use our screening checklists to help you decide when to do a DPIA.
- It is also good practice to do a DPIA for any other major project which requires the processing of personal data.
- Your DPIA must:

    - describe the nature, scope, context and purposes of the processing;
    - assess necessity, proportionality and compliance measures;
    - identify and assess risks to individuals; and
    - identify any additional measures to mitigate those risks.
- To assess the level of risk, you must consider both the likelihood and the severity of any impact on individuals. High risk could result from either a high probability of some harm, or a lower possibility of serious harm.
- You should consult your data protection officer (if you have one) and, where appropriate, individuals and relevant experts. Any processors may also need to assist you.
- If you identify a high risk that you cannot mitigate, you must consult the ICO before starting the processing.
- If you are processing for law-enforcement purposes, you should read this alongside the Guide to Law Enforcement Processing.
- The ICO will give written advice within eight weeks, or 14 weeks in complex cases. If appropriate, we may issue a formal warning not to process the data, or ban the processing altogether.

Checklists

DPIA awareness checklist

☐ We provide training so that our staff understand the need to consider a DPIA at the early stages of any plan involving personal data.

☐ Our existing policies, processes and procedures include references to DPIA requirements.

☐ We understand the types of processing that require a DPIA, and use the screening checklist to identify the need for a DPIA, where necessary.

☐ We have created and documented a DPIA process.

☐ We provide training for relevant staff on how to carry out a DPIA.

DPIA screening checklist

☐ We consider carrying out a DPIA in any major project involving the use of personal data.

☐ We consider whether to do a DPIA if we plan to carry out any other:

☐ evaluation or scoring;

☐ automated decision-making with significant effects;

☐ systematic monitoring;

☐ processing of sensitive data or data of a highly personal nature;

☐ processing on a large scale;

☐ processing of data concerning vulnerable data subjects;

☐ innovative technological or organisational solutions;

☐ processing that involves preventing data subjects from exercising a right or using a service or contract.

☐ We always carry out a DPIA if we plan to:

☐ use systematic and extensive profiling or automated decision-making to make significant decisions about people;

☐ process special-category data or criminal-offence data on a large scale;

☐ systematically monitor a publicly accessible place on a large scale;

☐ use innovative technology in combination with any of the criteria in the European guidelines;

☐ use profiling, automated decision-making or special category data to help make decisions on someone’s access to a service, opportunity or benefit;

☐ carry out profiling on a large scale;

☐ process biometric or genetic data in combination with any of the criteria in the European guidelines;

☐ combine, compare or match data from multiple sources;

☐ process personal data without providing a privacy notice directly to the individual in combination with any of the criteria in the European guidelines;

☐ process personal data in a way that involves tracking individuals' online or offline location or behaviour, in combination with any of the criteria in the European guidelines;

☐ process children's personal data for profiling or automated decision-making or for marketing purposes, or offer online services directly to them;

☐ process personal data that could result in a risk of physical harm in the event of a security breach.

☐ We carry out a new DPIA if there is a change to the nature, scope, context or purposes of our processing.

☐ If we decide not to carry out a DPIA, we document our reasons.

DPIA process checklist

☐ We describe the nature, scope, context and purposes of the processing.

☐ We ask our data processors to help us understand and document their processing activities and identify any associated risks.

☐ We consider how best to consult individuals (or their representatives) and other relevant stakeholders.

☐ We ask for the advice of our data protection officer.

☐ We check that the processing is necessary for and proportionate to our purposes, and describe how we will ensure compliance with data protection principles.

☐ We do an objective assessment of the likelihood and severity of any risks to individuals' rights and interests.

☐ We identify measures we can put in place to eliminate or reduce high risks.

☐ We record our decision-making in the outcome of the DPIA, including any difference of opinion with our DPO or individuals consulted.

☐ We implement the measures we identified, and integrate them into our project plan.

☐ We consult the ICO before processing, if we cannot mitigate high risks.

☐ We keep our DPIAs under review and revisit them when necessary.

Have we written a good DPIA?

A good DPIA helps you to evidence that:

- you have considered the risks related to your intended processing; and
- you have met your broader data protection obligations.

This checklist will help ensure you have written a good DPIA.

We have:

☐ confirmed whether the DPIA is a review of pre-GDPR processing or covers intended processing, including timelines in either case;

☐ explained why we needed a DPIA, detailing the types of intended processing that made it a requirement;

☐ structured the document clearly, systematically and logically;

☐ written the DPIA in plain English, with a non-specialist audience in mind, explaining any technical terms and acronyms we have used;

☐ set out clearly the relationships between controllers, processors, data subjects and systems, using both text and data-flow diagrams where appropriate;

☐ ensured that the specifics of any flows of personal data between people, systems, organisations and countries have been clearly explained and presented;

☐ explicitly stated how we are complying with each of the Data Protection Principles under GDPR and clearly explained our lawful basis for processing (and special category conditions if relevant);

☐ explained how we plan to support the relevant information rights of our data subjects;

☐ identified all relevant risks to individuals' rights and freedoms, assessed their likelihood and severity, and detailed all relevant mitigations;

☐ explained sufficiently how any proposed mitigation reduces the identified risk in question;

☐ evidenced our consideration of any less risky alternatives to achieving the same purposes of the processing, and why we didn't choose them;

☐ given details of stakeholder consultation (e.g. data subjects, representative bodies) and included summaries of findings;

☐ attached any relevant additional documents we reference in our DPIA, e.g. Privacy Notices, consent documents;

☐ recorded the advice and recommendations of our DPO (where relevant) and ensured the DPIA is signed off by the appropriate people;

☐ agreed and documented a schedule for reviewing the DPIA regularly or when we change the nature, scope, context or purposes of the processing;

☐ consulted the ICO if there are residual high risks we cannot mitigate.

In brief

- What is a DPIA?

- When do we need a DPIA?
- How do we carry out a DPIA?
- Do we need to consult the ICO?
- In more detail

What is a DPIA?

A DPIA is a way for you to systematically and comprehensively analyse your processing and help you identify and minimise data protection risks.

DPIAs should consider compliance risks, but also broader risks to the rights and freedoms of individuals, including the potential for any significant social or economic disadvantage. The focus is on the potential for harm – to individuals or to society at large, whether it is physical, material or non-material.

To assess the level of risk, a DPIA must consider both the likelihood and the severity of any impact on individuals.

A DPIA does not have to indicate that all risks have been eradicated. But it should help you document them and assess whether or not any remaining risks are justified.

DPIAs are a legal requirement for processing that is likely to be high risk. But an effective DPIA can also bring broader compliance, financial and reputational benefits, helping you demonstrate accountability and building trust and engagement with individuals.

A DPIA may cover a single processing operation or a group of similar processing operations. A group of controllers can do a joint DPIA.

It’s important to embed DPIAs into your organisational processes and ensure the outcome can influence your plans. A DPIA is not a one-off exercise. You should see it as an ongoing process that is subject to regular review.

When do we need a DPIA?

You must do a DPIA before you begin any type of processing that is “likely to result in a high risk”. This means that although you have not yet assessed the actual level of risk, you need to screen for factors that point to the potential for a widespread or serious impact on individuals.

In particular, the UK GDPR says you must do a DPIA if you plan to:

- use systematic and extensive profiling with significant effects;
- process special category or criminal offence data on a large scale; or
- systematically monitor publicly accessible places on a large scale.

When considering if your processing is likely to result in high risk, you should consider the relevant European guidelines. These define nine criteria of processing operations likely to result in high risk. While the guidelines suggest that, in most cases, any processing operation involving two or more of these criteria requires a DPIA, you may consider in your case that just meeting one criterion could require a DPIA.

The ICO also requires you to do a DPIA if you plan to:

- use innovative technology (in combination with any of the criteria from the European guidelines);
- use profiling or special category data to decide on access to services;
- profile individuals on a large scale;
- process biometric data (in combination with any of the criteria from the European guidelines);
- process genetic data (in combination with any of the criteria from the European guidelines);
- match data or combine datasets from different sources;
- collect personal data from a source other than the individual without providing them with a privacy notice ('invisible processing') (in combination with any of the criteria from the European guidelines);
- track individuals' location or behaviour (in combination with any of the criteria from the European guidelines);
- profile children or target marketing or online services at them; or
- process data that might endanger the individual's physical health or safety in the event of a security breach.

You should also think carefully about doing a DPIA for any other processing that is large scale, involves profiling or monitoring, decides on access to services or opportunities, or involves sensitive data or vulnerable individuals.

Even if there is no specific indication of likely high risk, it is good practice to do a DPIA for any major new project involving the use of personal data. You can use or adapt the checklists to help you carry out this screening exercise.

How do we carry out a DPIA?

A DPIA should begin early in the life of a project, before you start your processing, and run alongside the planning and development process. It should include these steps:

You must seek the advice of your data protection officer (if you have one). You should also consult with individuals and other stakeholders throughout this process.

The process is designed to be flexible and scalable. You can use or adapt our sample DPIA template, or create your own. If you want to create your own, you may want to refer to the European guidelines which set out Criteria for an acceptable DPIA

Although publishing a DPIA is not a requirement of UK GDPR, you should actively consider the benefits of publication. As well as demonstrating compliance, publication can help engender trust and confidence. We would therefore recommend that you publish your DPIAs, where possible, removing sensitive details if necessary.

Do we need to consult the ICO?

You don’t need to send every DPIA to the ICO and we expect the percentage sent to us to be small. But you must consult the ICO if your DPIA identifies a high risk and you cannot take measures to reduce that risk. You cannot begin the processing until you have consulted us.

If you want your project to proceed effectively then investing time in producing a comprehensive DPIA may prevent any delays later, if you have to consult with the ICO.

You need to send us a copy of your DPIA.

Once we have the information we need, we will generally respond within eight weeks (although we can extend this by a further six weeks in complex cases).

We will provide you with a written response advising you whether the risks are acceptable, or whether you need to take further action. In some cases we may advise you not to carry out the processing because we consider it would be in breach of the GDPR. In appropriate cases we may issue a formal warning or take action to ban the processing altogether.

Relevant provisions in the UK GDPR - See Articles 35 and 36 and Recitals 74-77, 84, 89-92, 94 and 95

https://www.legislation.gov.uk/eur/2016/679/contents

Joint Surveillance Camera Commissioner /ICO guidance on Data protection impact assessments for surveillance camera systems

https://www.gov.uk/government/publications/data-protection-impact-assessments-for-surveillance-cameras

In more detail – ICO guidance

We have published more detailed guidance on DPIAs.

The Accountability Framework looks at the ICO's expectations in relation to DPIAs.

In more detail – European Data Protection Board

- WP29 produced guidelines on data protection impact assessments, which have been endorsed by the EDPB.
- Other relevant guidelines include:
- Guidelines on Data Protection Officers ('DPOs') (WP243)
- Guidelines on automated individual decision-making and profiling for the purposes of Regulation 2016/679 (WP251)

Data protection officers

> **18 September 2023** - We have made updates the section 'What are the tasks of the DPO?'. The guidance now makes clear that while the DPO may be contacted by people whose personal data is being processed, in many large organisations, communication with the DPO is overseen by an office of the DPO or other support staff. This can help the DPO to discharge their responsibilities in an effective and efficient manner.
>
> **19 May 2023** - we have broken the Guide to the UK GDPR down into smaller guides. All the content stays the same.

At a glance

- The UK GDPR introduces a duty for you to appoint a data protection officer (DPO) if you are a public authority or body, or if you carry out certain types of processing activities.
- DPOs assist you to monitor internal compliance, inform and advise on your data protection obligations, provide advice regarding Data Protection Impact Assessments (DPIAs) and act as a contact point for data subjects and the Information Commissioner's Office (ICO).
- The DPO must be independent, an expert in data protection, adequately resourced, and report to the highest management level.
- A DPO can be an existing employee or externally appointed.
- In some cases several organisations can appoint a single DPO between them.
- DPOs can help you demonstrate compliance and are part of the enhanced focus on accountability.

Checklists

Appointing a DPO

☐ We are a public authority or body and have appointed a DPO (except if we are a court acting in our judicial capacity).

☐ We are not a public authority or body, but we know whether the nature of our processing activities requires the appointment of a DPO.

☐ We have appointed a DPO based on their professional qualities and expert knowledge of data protection law and practices.

☐ We aren't required to appoint a DPO under the UK GDPR but we have decided to do so voluntarily. We understand that the same duties and responsibilities apply had we been required to appoint a DPO. We support our DPO to the same standards.

Position of the DPO

☐ Our DPO reports directly to our highest level of management and is given the required independence to perform their tasks.

☐ We involve our DPO, in a timely manner, in all issues relating to the protection of personal data.

☐ Our DPO is sufficiently well resourced to be able to perform their tasks.

☐ We do not penalise the DPO for performing their duties.

☐ We ensure that any other tasks or duties we assign our DPO do not result in a conflict of interests with their role as a DPO.

Tasks of the DPO

☐ Our DPO is tasked with monitoring compliance with the UK GDPR and other data protection laws, our data protection policies, awareness-raising, training, and audits.

☐ We will take account of our DPO's advice and the information they provide on our data protection obligations.

☐ When carrying out a DPIA, we seek the advice of our DPO who also monitors the process.

☐ Our DPO acts as a contact point for the ICO. They co-operate with the ICO, including during prior consultations under Article 36, and will consult on any other matter.

☐ When performing their tasks, our DPO has due regard to the risk associated with processing operations, and takes into account the nature, scope, context and purposes of processing.

Accessibility of the DPO

☐ Our DPO is easily accessible as a point of contact for our employees, individuals and the ICO.

☐ We have published the contact details of the DPO and communicated them to the ICO.

In brief

- Do we need to appoint a Data Protection Officer?
- What is the definition of a public authority?
- What are 'core activities'?
- What does 'regular and systematic monitoring of data subjects on a large scale' mean?
- What does processing special category data and personal data relating to criminal convictions and offences on a large scale mean?
- What professional qualities should the DPO have?
- What are the tasks of the DPO?
- Can we assign other tasks to the DPO?
- Can the DPO be an existing employee?
- Can we contract out the role of the DPO?
- Can we share a DPO with other organisations?
- Can we have more than one DPO?
- What do we have to do to support the DPO?
- What details do we have to publish about the DPO?
- Is the DPO responsible for compliance?

Do we need to appoint a Data Protection Officer?

Under the UK GDPR, you **must** appoint a DPO if:

- you are a public authority or body (except for courts acting in their judicial capacity);
- your core activities require large scale, regular and systematic monitoring of individuals (for example, online behaviour tracking); or
- your core activities consist of large scale processing of special categories of data or data relating to criminal convictions and offences.

This applies to both controllers and processors. You can appoint a DPO if you wish, even if you aren't required to. If you decide to voluntarily appoint a

DPO you should be aware that the same requirements of the position and tasks apply had the appointment been mandatory.

Regardless of whether the UK GDPR obliges you to appoint a DPO, you must ensure that your organisation has sufficient staff and resources to discharge your obligations under the UK GDPR. However, a DPO can help you operate within the law by advising and helping to monitor compliance. In this way, a DPO can be seen to play a key role in your organisation's data protection governance structure and to help improve accountability.

If you decide that you don't need to appoint a DPO, either voluntarily or because you don't meet the above criteria, it's a good idea to record this decision to help demonstrate compliance with the accountability principle.

Does my organisation need a data protection officer (DPO)?

https://ico.org.uk/for-organisations/data-protection-fee/does-my-organisation-need-a-data-protection-officer-dpo/

What is the definition of a public authority?

Section 7 of the Data Protection Act 2018 defines what a 'public authority' and a 'public body' are for the purposes of the UK GDPR.

What are 'core activities'?

The other two conditions that require you to appoint a DPO only apply when:

- your core activities consist of processing activities, which, by virtue of their nature, scope and / or their purposes, require the regular and systematic monitoring of individuals on a large scale; or
- your core activities consist of processing on a large scale of special category data, or data relating to criminal convictions and offences.

Your core activities are the primary business activities of your organisation. So, if you need to process personal data to achieve your key objectives, this is a core activity. This is different to processing personal data for other secondary purposes, which may be something you do all the time (eg payroll or HR information), but which is not part of carrying out your primary objectives.

Example

For most organisations, processing personal data for HR purposes will be a secondary function to their main business activities and so will not be part of their core activities.

However, a HR service provider necessarily processes personal data as part of its core activities to provide HR functions for its client organisations. At the same time, it will also process HR information for its own employees, which will be regarded as an ancillary function and not part of its core activities.

What does 'regular and systematic monitoring of data subjects on a large scale' mean?

There are two key elements to this condition requiring you to appoint a DPO. Although the UK GDPR does not define 'regular and systematic monitoring' or 'large scale', the Article 29 Working Party (WP29) provided some guidance on these terms in its guidelines on DPOs. WP29 has been replaced by the European Data Protection Board (EDPB) which has endorsed these guidelines. Although these guidelines relate to the EU version of the GDPR, they are also a useful resource for understanding the requirements of the UK GDPR.

'Regular and systematic' monitoring of data subjects includes all forms of tracking and profiling, both online and offline. An example of this is for the purposes of behavioural advertising.

When determining if processing is on a large scale, the guidelines say you should take the following factors into consideration:

- the numbers of data subjects concerned;
- the volume of personal data being processed;
- the range of different data items being processed;
- the geographical extent of the activity; and
- the duration or permanence of the processing activity.

Example

A large retail website uses algorithms to monitor the searches and purchases of its users and, based on this information, it offers

recommendations to them. As this takes place continuously and according to predefined criteria, it can be considered as regular and systematic monitoring of data subjects on a large scale.

What does processing special category data and personal data relating to criminal convictions and offences on a large scale mean?

Processing special category data or criminal conviction or offences data carries more risk than other personal data. So when you process this type of data on a large scale you are required to appoint a DPO, who can provide more oversight. Again, the factors relevant to large-scale processing can include:

- the numbers of data subjects;
- the volume of personal data being processed;
- the range of different data items being processed;
- the geographical extent of the activity; and
- the duration or permanence of the activity.

Example

A health insurance company processes a wide range of personal data about a large number of individuals, including medical conditions and other health information. This can be considered as processing special category data on a large scale.

What professional qualities should the DPO have?

- The UK GDPR says that you should appoint a DPO on the basis of their professional qualities, and in particular, experience and expert knowledge of data protection law.
- It doesn’t specify the precise credentials they are expected to have, but it does say that this should be proportionate to the type of processing you carry out, taking into consideration the level of protection the personal data requires.
- So, where the processing of personal data is particularly complex or risky, the knowledge and abilities of the DPO should be correspondingly advanced enough to provide effective oversight.

- It would be an advantage for your DPO to also have a good knowledge of your industry or sector, as well as your data protection needs and processing activities.

What are the tasks of the DPO?

The DPO's tasks are defined in Article 39 as:

- to inform and advise you and your employees about your obligations to comply with the UK GDPR and other data protection laws;
- to monitor compliance with the UK GDPR and other data protection laws, and with your data protection polices, including managing internal data protection activities; raising awareness of data protection issues, training staff and conducting internal audits;
- to advise on, and to monitor, data protection impact assessments;
- to cooperate with the ICO; and
- to be the first point of contact for the ICO.

Article 38 of the UK GDPR also establishes that DPOs may be contacted by people whose personal information is being processed (employees, customers etc.). In many large organisations, communication with the DPO is overseen by an office of the DPO or other support staff. This can help the DPO to discharge their responsibilities in an effective and efficient manner.

It's important to remember that the DPO's tasks cover all personal data processing activities, not just those that require their appointment under Article 37(1).

- When carrying out their tasks the DPO is required to take into account the risk associated with the processing you are undertaking. They must have regard to the nature, scope, context and purposes of the processing.
- The DPO should prioritise and focus on the more risky activities, for example where special category data is being processed, or where the potential impact on individuals could be damaging. Therefore, DPOs should provide risk-based advice to your organisation.
- If you decide not to follow the advice given by your DPO, you should document your reasons to help demonstrate your accountability.

Can we assign other tasks to the DPO?

The UK GDPR says that you can assign further tasks and duties, so long as they don't result in a conflict of interests with the DPO's primary tasks.

Example

As an example of assigning other tasks, Article 30 requires that organisations must maintain records of processing operations. There is nothing preventing this task being allocated to the DPO.

Basically this means the DPO cannot hold a position within your organisation that leads him or her to determine the purposes and the means of the processing of personal data. At the same time, the DPO shouldn't be expected to manage competing objectives that could result in data protection taking a secondary role to business interests.

Examples

A company's head of marketing plans an advertising campaign, including which of the company's customers to target, what method of communication and the personal details to use. This person cannot also be the company's DPO, as the decision-making is likely to lead to a conflict of interests between the campaign's aims and the company's data protection obligations.

On the other hand, a public authority could appoint its existing FOI officer / records manager as its DPO. There is no conflict of interests here as these roles are about ensuring information rights compliance, rather than making decisions about the purposes of processing.

Can the DPO be an existing employee?

Yes. As long as the professional duties of the employee are compatible with the duties of the DPO and do not lead to a conflict of interests, you can appoint an existing employee as your DPO, rather than you having to create a new post.

Can we contract out the role of the DPO?

You can contract out the role of DPO externally, based on a service contract with an individual or an organisation. It's important to be aware that an

externally-appointed DPO should have the same position, tasks and duties as an internally-appointed one.

Can we share a DPO with other organisations?

- You may appoint a single DPO to act for a group of companies or public authorities.
- If your DPO covers several organisations, they must still be able to perform their tasks effectively, taking into account the structure and size of those organisations. This means you should consider if one DPO can realistically cover a large or complex collection of organisations. You need to ensure they have the necessary resources to carry out their role and be supported with a team, if this is appropriate.
- Your DPO must be easily accessible, so their contact details should be readily available to your employees, to the ICO, and people whose personal data you process.

Can we have more than one DPO?

- The UK GDPR clearly provides that an organisation must appoint a single DPO to carry out the tasks required in Article 39, but this doesn't prevent it appointing other data protection specialists as part of a team to help support the DPO.
- You need to determine the best way to set up your organisation's DPO function and whether this necessitates a data protection team. However, there must be an individual designated as the DPO for the purposes of the UK GDPR who meets the requirements set out in Articles 37-39.
- If you have a team, you should clearly set out the roles and responsibilities of its members and how it relates to the DPO.
- If you hire data protection specialists other than a DPO, it's important that they are not referred to as your DPO, which is a specific role with particular requirements under the UK GDPR.

What do we have to do to support the DPO?

You must ensure that:

- the DPO is involved, closely and in a timely manner, in all data protection matters;
- the DPO reports to the highest management level of your organisation, ie board level;

- the DPO operates independently and is not dismissed or penalised for performing their tasks;
- you provide adequate resources (sufficient time, financial, infrastructure, and, where appropriate, staff) to enable the DPO to meet their UK GDPR obligations, and to maintain their expert level of knowledge;
- you give the DPO appropriate access to personal data and processing activities;
- you give the DPO appropriate access to other services within your organisation so that they can receive essential support, input or information;
- you seek the advice of your DPO when carrying out a DPIA; and
- you record the details of your DPO as part of your records of processing activities.

This shows the importance of the DPO to your organisation and that you must provide sufficient support so they can carry out their role independently. Part of this is the requirement for your DPO to report to the highest level of management. This doesn't mean the DPO has to be line managed at this level but they must have direct access to give advice to senior managers who are making decisions about personal data processing.

What details do we have to publish about the DPO?

The UK GDPR requires you to:

- publish the contact details of your DPO; and
- provide them to the ICO.

This is to enable individuals, your employees and the ICO to contact the DPO as needed. You aren't required to include the name of the DPO when publishing their contact details but you can choose to provide this if you think it's necessary or helpful.

You're also required to provide your DPO's contact details in the following circumstances:

- when consulting the ICO under Article 36 about a DPIA; and
- when providing privacy information to individuals under Articles 13 and 14.

However, remember you do have to provide your DPO's name if you report a personal data breach to the ICO and to those individuals affected by it.

Is the DPO responsible for compliance?

The DPO isn't personally liable for data protection compliance. As the controller or processor it remains your responsibility to comply with the UK GDPR. Nevertheless, the DPO clearly plays a crucial role in helping you to fulfil your organisation's data protection obligations.

Relevant provisions in the UK GDPR - See Articles 35-36, 37-39, 83 and Recital 97

https://www.legislation.gov.uk/eur/2016/679/contents

In more detail - ICO guidance

- See the following section of the Guide to UK GDPR: Accountability and governance
- See our Guide to freedom of information
- The Accountability Framework looks at the ICO's expectations in relation to leadership and oversight.

In more detail – European Data Protection Board

The European Data Protection Board (EDPB), which has replaced 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 EU version of the GDPR.

WP29 published guidelines on DPOs and DPO FAQs, which have been endorsed by the EDPB.

EDPB guidelines are no longer directly relevant to the UK regime and are not binding under the UK regime. However, they may still provide helpful guidance on certain issue

Contracts

> **19 May 2023** - we have broken the Guide to the UK GDPR down into smaller guides. All the content stays the same.

At a glance

- Whenever a controller uses a processor, there must be a written contract (or other legal act) in place.
- The contract is important so that both parties understand their responsibilities and liabilities.
- The UK GDPR sets out what needs to be included in the contract.
- If a processor uses another organisation (ie a sub-processor) to assist in its processing of personal data for a controller, it needs to have a written contract in place with that sub-processor.

Checklists

What to include in the contract

The contract (or other legal act) sets out details of the processing including:

☐ the subject matter of the processing;

☐ the duration of the processing;

☐ the nature and purpose of the processing;

☐ the type of personal data involved;

☐ the categories of data subject;

☐ the controller's obligations and rights.

The contract or other legal act includes terms or clauses stating that:

☐ the processor must only act on the controller's documented instructions, unless required by law to act without such instructions;

☐ the processor must ensure that people processing the data are subject to a duty of confidence;

☐ the processor must take appropriate measures to ensure the security of processing;

☐ the processor must only engage a sub-processor with the controller's prior authorisation and under a written contract;

☐ the processor must take appropriate measures to help the controller respond to requests from individuals to exercise their rights;

☐ taking into account the nature of processing and the information available, the processor must assist the controller in meeting its UK GDPR obligations in relation to the security of processing, the notification of personal data breaches and data protection impact assessments;

☐ the processor must delete or return all personal data to the controller (at the controller's choice) at the end of the contract, and the processor must also delete existing personal data unless the law requires its storage; and

☐ the processor must submit to audits and inspections. The processor must also give the controller whatever information it needs to ensure they are both meeting their Article 28 obligations.

In brief

- When is a contract needed and why is it important?
- What needs to be included in the contract?
- What responsibilities and liabilities do controllers have when using a processor?
- What responsibilities and liabilities do processors have in their own right?
- In more detail

When is a contract needed and why is it important?

Whenever a controller uses a processor to process personal data on their behalf, a written contract needs to be in place between the parties.

Similarly, if a processor uses another organisation (ie a sub-processor) to help it process personal data for a controller, it needs to have a written contract in place with that sub-processor.

Contracts between controllers and processors ensure they both understand their obligations, responsibilities and liabilities. Contracts also help them comply with the UK GDPR, and assist controllers in demonstrating to individuals and regulators their compliance as required by the accountability principle.

What needs to be included in the contract?

Contracts must set out:

- the subject matter and duration of the processing;
- the nature and purpose of the processing;
- the type of personal data and categories of data subject; and
- the controller's obligations and rights.

Contracts must also include specific terms or clauses regarding:

- processing only on the controller's documented instructions;
- the duty of confidence;
- appropriate security measures;
- using sub-processors;
- data subjects' rights;
- assisting the controller;
- end-of-contract provisions; and
- audits and inspections.

What responsibilities and liabilities do controllers have when using a processor?

Controllers must only use processors that can give sufficient guarantees they will implement appropriate technical and organisational measures to ensure their processing will meet UK GDPR requirements and protect data subjects' rights.

Controllers are primarily responsible for overall compliance with the UK GDPR, and for demonstrating that compliance. If this isn't achieved, they may be liable to pay damages in legal proceedings or be subject to fines or other penalties or corrective measures.

What responsibilities and liabilities do processors have in their own right?

In addition to its contractual obligations to the controller, a processor has some direct responsibilities under the UK GDPR. If a processor fails to meet its obligations, or acts outside or against the controller's instructions, it may be liable to pay damages in legal proceedings or be subject to fines or other penalties or corrective measures.

A processor may not engage a sub-processor's services without the controller's prior specific or general written authorisation. If authorisation is given, the processor must put in place a contract with the sub-processor. The terms of the contract that relate to Article 28(3) must offer an equivalent level of protection for the personal data as those in the contract between the controller and processor. Processors remain liable to the controller for the compliance of any sub-processors they engage.

Relevant provisions in the UK GDPR - See Articles 28, 29, 30, 31, 32, 33, 34, 35 and 36 and Recitals 81, 82 and 83

https://www.legislation.gov.uk/eur/2016/679/contents

In more detail – ICO guidance

We have produced more detailed guidance on contracts and liabilities between controllers and processors.

The Accountability Framework looks at the ICO's expectations in relation to contracts.