Accountability and governance

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
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?

Further Reading

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

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’)

Further Reading

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.

Further Reading

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).

Further Reading

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

Further reading

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.

Further Reading
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.

Further Reading

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.

Further Reading

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

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.

Further Reading

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

Further reading – ICO guidance

Security

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.
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.

Further Reading

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

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
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.

**Further Reading**

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

*External link*

*Relevant provisions in the UK GDPR - Recital 97*

*External link*

---

**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.

**Further Reading**

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

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.

Further Reading

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.
Further reading – ICO guidance

Right to be informed

Rights related to automated decision making including profiling

Data protection self assessment

Accountability Framework