Accountability Framework – demonstrate your data protection compliance

Introduction to the Accountability Framework

At a glance

Accountability is one of the key principles in data protection law – it makes you responsible for complying with the legislation and says that you must be able to demonstrate your compliance.

The Accountability Framework can help any organisation, whether small or large, with their obligations.

The framework is divided into 10 categories and contains expectations and examples of how your organisation can demonstrate your accountability.

As a starting point, we'd advise reading the Guide to the GDPR section on accountability first.

Provide feedback

The Accountability Framework has launched as a 'beta' product – we're keen to hear what you think and develop the tool and guidance based on your feedback. You can feedback here or you can register to take part in future events related to the Framework.

Introduction to the Accountability Framework

This section introduces the Framework, who it's for and how it can help your organisation.

Categories

- Leadership and oversight
- Policies and procedures
- Training and awareness
- Individuals' rights
- Transparency
- Records of processing and lawful basis
- Contracts and data sharing
- Risks and data protection impact assessments
- Records management and security
- Breach response and monitoring

Take a self-assessment

The accountability self-assessment will help you to assess the extent to which your organisation is currently meeting the ICO's expectations in relation to accountability.

Introduction to the Accountability Framework

What is accountability?

Accountability is one of the key principles in data protection law – it makes you responsible for complying with the legislation and says that you must be able to demonstrate your compliance.

It's a real opportunity to show that you set high standards for privacy and lead by example to promote a positive attitude to data protection across your organisation.

Accountability enables you to minimise the risks of what you do with personal data by putting in place appropriate and effective policies, procedures and measures. These must be proportionate to the risks, which can vary depending on the amount of data being handled or transferred, its sensitivity and the technology you use.

Regulators, business partners and individuals need to see that you are managing personal data risks if you want to secure their trust and confidence. This can enhance your reputation and give you a competitive edge, helping your business to thrive and grow.

For more information about accountability, please read our guidance on accountability and governance.

Who can use the framework?

You will find the Accountability Framework useful if you are responsible for putting appropriate measures in place to make sure that your organisation complies with data protection. You could be senior management, the data protection officer (DPO) or have records management or information security responsibilities.

The Accountability Framework can help to support any organisation, whether small or large, with their obligations. The key is that the measures you put in place must be **appropriate**, **risk-based** and **proportionate**. This depends on your organisation and what you are doing with personal data.

If you work for a smaller organisation you will most likely benefit, in the first instance, from the resources available on our SME hub, in particular the Assessment for small business owners and sole traders, and our Data protection self-assessment toolkit which has been created with smaller organisations in mind.

What is the scope of the framework?

This framework supports the foundations of an effective privacy management programme. It is not exhaustive and does not replace the need for you to comply with all applicable aspects of data protection, exercise your own judgement, and use other relevant guidance and materials such as the Guide to the General Data Protection Regulation (GDPR).

The framework is not sector-specific because we want it to be relevant to as broad an audience as possible. In time, we will include case studies to highlight practical experience across different sectors and differently sized organisations.

How can I use the framework?

The framework is an opportunity for you to assess your organisation's accountability. Depending on your circumstances, you may use it in different ways. For example, you may want to:

- create a comprehensive privacy management programme;
- check your existing practices against the ICO's expectations;
- consider whether you could improve existing practices, perhaps in specific areas;
- understand ways to demonstrate compliance;
- record, track and report on progress; or
- increase senior management engagement and privacy awareness across your organisation.

The framework is divided into 10 categories, for example 'Leadership and oversight'. Selecting a category will display our key expectations and a bullet-pointed list of ways you can meet our expectations. This list is based on our experiences when working with organisations. It is not exhaustive, and organisations may meet our expectations in slightly different or unique ways.

You can demonstrate the ways you are meeting our expectations with documentation, but accountability is also about what you actually do in practice so you should also review how effective the measures are.

Accountability is **not about ticking boxes**. While there are some accountability measures that you must take, such as conducting a data protection impact assessment for high-risk processing, there isn't a 'one size fits all' approach.

You will need to consider your organisation and what you are doing with personal data in order to manage personal data risks appropriately. As a general rule, the greater the risk, the more robust and comprehensive the measures in place should be.

To help you assess, report and improve your data protection compliance, you can complete our accountability self-assessment.

You can also use our accountability tracker if you want to record more detail and create an action plan to track your progress over time.

Leadership and oversight

Why is this important?

A fundamental building block of accountability is strong leadership and oversight. This includes making sure that staff have clear responsibilities for data protection-related activities at a strategic and operational level. Some organisations legally require a DPO; but everyone must allocate sufficient resources and make sure that data protection is a shared responsibility, rather than solely the task of someone working directly in a data protection role. You make senior management and the board accountable, and they must lead by example to promote the organised, proactive and positive approach to data protection that underpins everything else.

At a glance – what we expect from you

- Organisational structure
- Whether to appoint a DPO
- Appropriate reporting
- Operational roles
- Group to provide oversight and direction
- Operational group meetings

Further reading

ICO guidance:

- Accountability and Governance
- Data Protection Officers

ICO interactive tool:

- Does my organisation need a data protection officer?

External guidance:

- The National Archives: Organisational arrangements to support records management
- Centre for the Protection of National Infrastructure: Good security governance and Leadership in security
- National Cyber Security Centre: 10 Steps to Cyber Security – A Board-level responsibility
- Get Safe Online: Governance

Organisational structure

Organisational structure

There is an organisational structure for managing data protection and information governance, which provides strong leadership, clear reporting lines and responsibilities, and effective information flows. This could mean clear management roles and responsibilities for staff in the information security or records management departments.

Ways to meet our expectations:

- The board, or highest senior management level, has overall responsibility for data protection and information governance.
- Decision-makers lead by example and promote a proactive, positive culture of data protection compliance.
- You have clear reporting lines and information flows between relevant groups; such as from a management board to an audit committee, or from an executive team to an information governance steering group.
- Policies clearly set out the organisational structure for managing data protection and information governance.
- Job descriptions clearly set out responsibilities and reporting lines to management.
- Job descriptions are up-to-date, fit for purpose and reviewed regularly.
- Data protection and information governance staff understand the organisational structure and their responsibilities.

Can you answer yes to the following questions?

- Do staff report that your organisational structure is effective?
- Is there a positive and proactive culture of data protection compliance across your organisation?
- Are staff aware of their responsibilities and those of others within the structure?

Whether to appoint a DPO

Whether to appoint a DPO

If it is necessary to appoint a DPO under Article 37 of the GDPR, your organisation makes sure that the DPO's role is adequately supported and covers all the requirements and responsibilities.

Ways to meet our expectations:

- The DPO has specific responsibilities in line with Article 39 of the GDPR for data protection compliance, data protection policies, awareness raising, training and audits.
- The DPO has expert knowledge of data protection law and practices.
- The DPO has the authority, support and resources to do their job effectively.
- If your organisation is not required to appoint a DPO, you record the decision.
- If your organisation is not required to appoint a DPO, you appropriately assign responsibility for data protection compliance and you have enough staff and resources to manage your obligations under data protection law.

Can you answer yes to the following questions?

- Could your DPO explain their responsibilities and how to carry them out effectively?
- Does your DPO feel supported in their role?

Appropriate reporting

Appropriate reporting

The DPO is independent and unbiased. They must report to the highest management level and staff must be clear about how to contact them.

Ways to meet our expectations:

- Staff know who the DPO is, what their role is and how to contact them.
- All data protection issues involve the DPO in a timely manner.
- Your organisation follows the DPO’s advice and takes account of their knowledge about data protection obligations.
- The DPO performs their tasks independently, without any conflicts of interest, and does not take any direct operational decisions about the manner and purposes of processing personal data within your organisation.
- The DPO directly advises senior decision-makers and raises concerns with the highest management level.
- The DPO provides senior management with regular updates about data protection compliance.

Can you answer yes to the following questions?

- Could your DPO explain their responsibilities and how they carry them out effectively?
- Does your DPO feel supported in their role?
- Is it easy for your DPO to get access to the highest level management?
- Can your staff explain what the DPO does and how to get in touch with them?

Operational roles

Operational roles

Your organisation’s operational roles support the practical implementation of data protection and information governance.

Ways to meet our expectations:

- Data protection and information governance staff have clear responsibilities for making sure that your organisation is data protection compliant.
- Your staff manage all records effectively and they keep information secure.
- A network of support or nominated data protection leads help implement and maintain data protection policies at a local level.
- Data protection and information governance staff have the authority, support and resources to carry out their responsibilities effectively.

Can you answer yes to the following questions?

- Are staff job descriptions accurate and up to date?
- Could staff explain their role and responsibilities in detail and how these are achieved in practice?
- Do they feel supported?

Oversight groups

Oversight groups

An oversight group provides direction and guidance across your organisation for data protection and information governance activities.

Ways to meet our expectations:

- Key staff, eg the DPO, regularly attend the oversight group meetings.
- An appropriately senior staff member chairs the group, eg the DPO or senior information risk owner (SIRO).
- Clear terms of reference set out the group's aims.
- The group's meeting minutes record what takes place.
- The group covers a full range of data protection-related topics including key performance indicators (KPIs), issues and risks.
- The group has a work or action plan that is monitored regularly.
- The board or highest management level considers data protection and information governance issues and risks reported by the oversight group.

Can you answer yes to the following questions?

- Do group members report that the meetings are effective?
- Do they meet frequently enough and cover appropriate topics?
- Are senior management aware of the issues and risks?

Operational group meetings

Operational group meetings

In your organisation, operational level groups meet to discuss and coordinate data protection and information governance activities.

Ways to meet our expectations:

- The groups meet and are attended by relevant staff regularly.
- The groups produce minutes of the meetings and action plans.
- The agenda shows the groups discuss appropriate data protection and information governance issues regularly.
- Any data protection and information governance issues and risks that arise are report to the oversight group.

Can you answer yes to the following questions?

- Would the group members say that the meetings are effective?
- Do they meet frequently enough and cover appropriate topics?
- Is the oversight group aware of the issues and risks?

Policies and procedures

Why is this important?

Policies and procedures provide clarity and consistency, by communicating what people need to do and why. Policies can also communicate goals, values and a positive tone. Data protection law specifically requires you to put in place data protection policies where proportionate. What you have policies for and their level of detail varies, but effective data protection policies and procedures can help your organisation to take the practical steps to comply with your legal obligations.

At a glance - What we expect from you

- Direction and support
- Review and approval
- Staff awareness
- Data Protection by design and by default

Further reading

ICO guidance:

- Accountability and Governance
- Principles
- Data Protection by design and by default
- Children
- Age Appropriate Design Code of Practice

Further resources:

- Awareness-raising materials

External guidance:

- The National Archives: Records management policy
- National Cyber Security Centre: Security advice
- Get Safe Online: Rules, Guidelines and Procedures

Direction and support

Direction and support

Your organisation’s policies and procedures provide your staff with enough direction to understand their roles and responsibilities regarding data protection and information governance.

Ways to meet our expectations:

- The policy framework stems from strategic business planning for data protection and information governance, which the highest level of management endorses.
- Policies cover data protection, records management and information security.
- You make operational procedures, guidance and manuals readily available to support data protection policies and provide direction to operational staff.
- Policies and procedures clearly outline roles and responsibilities.

Can you answer yes to the following questions?

- Do staff know where to find relevant policies and are they easy to find?
- Could your staff explain their role and responsibilities and how the policies and procedures help them?

Review and approval

Review and approval

You have a review and approval process in place to make sure that policies and procedures are consistent and effective.

Ways to meet our expectations:

- All policies and procedures follow an agreed format and style.
- An appropriately senior staff member reviews and approves all new and existing policies and procedures.
- Existing policies and procedures are reviewed in line with documented review dates, are up-to-date and fit for purpose.
- You update policies and procedures without undue delay when they require changes, eg because of operational change, court or regulatory decisions or changes in regulatory guidance.
- All policies, procedures and guidelines show document control information, including version number, owner, review date and change history.

Can you answer yes to the following questions?

- Is the highest level of management aware of the strategic business plan for information governance?
- Are policies consistent?
- Is the approval process appropriate?

Staff awareness about the policies and procedures

Staff awareness

Staff are fully aware of the policies and procedures that are relevant to their role.

Ways to meet our expectations:

- Your staff read and understand the policies and procedures, including why they are important to implement and comply with.
- You tell staff about updated policies and procedures.
- You make policies and procedures readily available for all staff on your organisation’s intranet site (or equivalent shared area) or provide them in other formats.
- Guidelines, posters or publications help to emphasise key messages and raise staff awareness of policies and procedures.

Can you answer yes to the following questions?

- Could your staff easily find policies on the intranet or equivalent shared area?
- Are they aware of the main content?
- Would we see any data protection awareness-raising materials available or on display around your office, such as posters?

Data protection by design and by default

Data protection by design and by default

Your policies and procedures foster a ‘data protection by design and by default’ approach across your organisation.

Ways to meet our expectations:

- Where relevant, you consider policies and procedures across your organisation with data protection in mind.
- You have policies and procedures to ensure data protection issues are considered when systems, services, products and business practices involving personal data are designed and implemented, and that personal data is protected by default.
- Your organisation’s approach to implementing the data protection principles and safeguarding individuals’ rights, such as data minimisation, pseudonymisation and purpose limitation, is set out in policies and procedures.
- The personal data of vulnerable groups, eg children, is given extra protection in policies and procedures.

Can you answer yes to the following questions?

- Could your staff easily find policies on the intranet or equivalent shared area?
- Are they aware of the main content?
- Would we see any data protection awareness-raising materials available or on display around your office, such as posters?

Training and awareness

Why is this important?

This makes sure that all employees receive appropriate training about your privacy programme, including what its goals are, what it requires people to do and what responsibilities they have. The training must be relevant, accurate and up to date. Training and awareness is key to actually putting into practice your policies, procedures and measures by:

- integrating data protection across your entire organisation so it is second nature;
- making sure you are compliant; and
- being able to prove what you are doing.

At a glance – what we expect from you

- All staff training programme
- Induction and refresher training
- Specialised roles
- Monitoring
- Awareness-raising

Further reading

ICO guidance:

- Awareness raising resources
- ICO training videos

External guidance:

- National Cyber Security Centre: 10 Steps to Cyber Security – User education and awareness

All-staff training programme

All-staff training programme

You have an all-staff data protection and information governance training programme.

Ways to meet our expectations:

- Your programme incorporates national and sector-specific requirements.
- Your programme is comprehensive and includes training for all staff on key areas of data protection such as handling requests, data sharing, information security, personal data breaches and records management.
- You consider the training needs of all staff and use this information to compile the training programme.
- You assign responsibilities for managing information governance and data protection training across your organisation and you have training plans or strategies in place to meet training needs within agreed time-scales.
- You have dedicated and trained resources available to deliver training to all staff.
- You regularly review your programme to ensure that it remains accurate and up to date.
- Senior management sign off your programme.

Can you answer yes to the following questions?

- Are you meeting staff training needs effectively?
- Have your trainers received appropriate training?
- Are their responsibilities clear and could they explain how you implement their responsibilities in practice?

Induction and refresher training

Induction and refresher training

Your training programme includes induction and refresher training for all staff on data protection and information governance.

Ways to meet our expectations:

- Appropriate staff, such as the DPO or an information governance manager, oversee or approve induction training.
- Your staff receive induction and refresher training, regardless of how long they will be working for your organisation, their contractual status or grade.
- Your staff receive induction training prior to accessing personal data and within one month of their start date.
- Your staff complete refresher training at appropriate intervals.

Can you answer yes to the following questions?

- Could we observe your training delivery methods?
- Is it effective?
- Do you follow up on ‘no shows’?
- Could staff explain their training records?

Specialised roles

Specialised roles

Specialised roles or functions with key data protection responsibilities (such as DPOs, subject access and records management teams) receive additional training and professional development beyond the basic level provided to all staff.

Ways to meet our expectations:

- You complete a training needs analysis for information governance and data protection staff to inform the training plan and to ensure it is specific to the individual's responsibilities.
- You detail training and skills requirements in job descriptions.
- You have evidence to confirm that key roles complete up-to-date and appropriate specialised training and professional development, and they are subject to proportionate refresher training.
- You keep on record copies of the training material provided as well as details of who receives the training.

Can you answer yes to the following questions?

- Do staff consider that you identify their training needs specifically?
- Are there appropriate plans to meet those needs?
- Are the training materials effective?

Monitoring

Monitoring

Your organisation can demonstrate that staff understand the training. You verify their understanding and monitor it appropriately eg through assessments or surveys.

Ways to meet our expectations:

- You conduct an assessment at the end of the training to test staff understanding and make sure that it is effective, which could include a minimum pass mark.
- You keep copies of the training material provided on record as well as details of who receives the training.
- You monitor training completion in line with organisational requirements at all levels of the organisation, and you follow up with staff who do not complete the training.
- Staff are able to provide feedback on the training they receive.

Can you answer yes to the following questions?

- Do staff react positively to the training?
- Is there an easy way to provide feedback?
- Does that process result in changes?
- Are senior managers aware of training monitoring outcomes?

Awareness raising

Awareness raising

You regularly raise awareness across your organisation of data protection, information governance and associated policies and procedures in meetings or staff forums. You make it easy for staff to access relevant material.

Ways to meet our expectations:

- You have evidence that your organisation regularly uses a variety of appropriate methods to raise staff awareness and the profile of data protection and information governance, for example by emails, team briefings and meetings, posters, handouts and blogs.
- You make it easy for staff to access relevant material, and find out who to contact if they have any queries relating to data protection and information governance.

Can you answer yes to the following questions?

- Could we observe awareness-raising materials around your office?
- Would staff know who to contact?
- Do you make it easy for them to find and access relevant information?

Individuals' rights

Why is this important?

Data protection law aims to empower individuals and give them greater control over their personal data through several rights, which you need to facilitate effectively. Compliance with individual rights minimises the privacy risks to individuals as well as to organisations. It will help you to comply with other data protection requirements, such as the principles. Good data protection compliance enhances your reputation and gives you a competitive edge because it increases the trust and confidence that people have in how you handle personal data.

At a glance – what we expect from you

- Informing individuals and identifying requests
- Resources
- Logging and tracking requests
- Timely responses
- Monitoring and evaluating performance
- Inaccurate or incomplete information
- Erasure
- Restriction
- Data portability
- Rights relating to automated decision-making and profiling
- Individual complaints

Further reading

ICO guidance:

- Individual rights
- Right to rectification
- Right to erasure
- Right to restrict processing
- Data portability
- Rights related to automated decision making including profiling
- Children
- Guidance on the AI Auditing Framework (draft)

Informing individuals and identifying requests

Informing individuals and identifying requests

You inform individuals about their rights and all staff are aware of how to identify and deal with both verbal and written requests.

Ways to meet our expectations:

- You give individuals clear and relevant information about their rights and how to exercise them.
- Your policies and procedures set out processes for dealing with requests from individuals about their rights.
- All staff receive training and guidance about how to recognise a request and where to send them.

Can you answer yes to the following questions?

- Do all staff understand how to recognise a request and where to send them?
- Would individuals say that you provided useful materials to help them to exercise their rights?

Resources

Resources

You have appropriate resources in place to handle requests from individuals about their data.

Ways to meet our expectations:

- A specific person/s or team are responsible for managing and responding to requests.
- Staff receive specialised training to handle requests, including regular refresher training.
- You have sufficient resources to deal with requests.
- If a staff member is absent, you train other staff to carry out key tasks.
- Your organisation can deal with any increase in requests or reduction in staffing levels.

Can you answer yes to the following questions?

- Are staff aware of their key responsibilities and how to deliver them in practice?
- Would your staff say that you have appropriate resources to deal with the volume of requests?
- In the case of staff absences, could key tasks in the request process be covered by more than one individual?

Logging and tracking requests

Logging and tracking requests

Your organisation logs receipt of all verbal and written requests from individuals and updates the log to track the handling of each request.

Ways to meet our expectations:

- You have processes in place to ensure the log is accurate and updated as appropriate.
- The log shows the due date for requests, the actual date of the final response and the action taken.
- A checklist records the key stages in the request handling process, eg which systems or departments have been searched. This is either part of the log or a separate document.
- You have records of your organisation's request responses, and any disclosed or withheld information from subject access requests.

Can you answer yes to the following questions?

- Could you locate relevant records easily?
- Are the records correct?
- Would a small sample of requests show that your staff follow the policies and procedures?

Timely responses

Timely responses

You deal with requests from individuals in a timely manner that meets individual expectations and statutory timescales.

Ways to meet our expectations:

- You action all requests within statutory timescales.
- The staff responsible for managing requests meet regularly to discuss any issues and investigate, prioritise or escalate any delayed cases.
- If you need an extension, you update individuals on the progress of their request and keep them informed.
- If a request is refused, you have records about the reasons why and you inform individuals about the reasons for any refusals or exemptions.

Can you answer yes to the following questions?

- Would staff say that the process in place to deal with issues is regular and effective?
- Would requesters say they were kept well-informed about the progress of their request?
- Did requesters receive clear information?

Monitoring and evaluating performance

Monitoring and evaluating performance

Your organisation monitors how your staff handle requests and you use that information to make improvements.

Ways to meet our expectations:

- The staff responsible for managing requests meet regularly to discuss any issues.
- You produce regular reports on performance and case quality assessments to ensure that requests are handled appropriately.
- You share reports with senior management, that they review and action at appropriate meetings.
- Your organisation analyses any trends in the nature or cause of requests to improve performance or reduce volumes.

Can you answer yes to the following questions?

- Are the management reports easy to understand?
- Does senior management know about current performance?
- Are the actions clear and are they followed up?

Inaccurate or incomplete information

Inaccurate or incomplete information

Your organisation has appropriate systems and procedures to change inaccurate information, add additional information to incomplete records or add a supplementary statement where necessary.

Ways to meet our expectations:

- Your organisation takes proportionate and reasonable steps to check the accuracy of the personal data held and, if necessary, is able to rectify it.
- If your organisation is satisfied that the data is accurate, you have a procedure to explain this to the individual. You need to inform the individual of their right to complain, and as a matter of good practice, record on the system the fact that the individual disputes the accuracy of the information.
- If personal data has been disclosed to others, your organisation contacts each recipient to inform them about the rectification, unless this is impossible or involves disproportionate effort.
- If asked, the organisation tells the data subject which third parties have received the personal data.

Can you answer yes to the following questions?

- Would staff say there are effective processes in place to rectify inaccurate or incomplete personal data?
- Would requesters say they were given clear information about the steps you took?

Erasure

Erasure

You have appropriate methods and procedures in place within your organisation to delete, suppress or otherwise stop processing personal data if required.

Ways to meet our expectations:

- You erase personal data from back-up systems as well as live systems where necessary, and you clearly tell the individual what will happen to their data.
- If the personal data is disclosed to others, your organisation contacts each recipient to inform them about the erasure, unless this is impossible or involves disproportionate effort.
- If asked to, your organisation tells the data subject which third parties have received the personal data.
- If personal data has been made public in an online environment, you take reasonable steps to tell other controllers, if they are processing it, to erase links to, copies or replication of that data.
- Your organisation gives particular weight to a request for erasure where the processing is or was based on a child's consent, especially when processing any personal data on the internet.

Can you answer yes to the following questions?

- Would staff say there are effective processes in place to erase personal data?
- Would requesters say they were given clear information about the steps you took?

Restriction

Restriction

Your organisation has appropriate methods and procedures in place to restrict the processing of personal data if required.

Ways to meet our expectations:

- Your organisation restricts personal data in a way appropriate for the type of processing and the system, for example temporarily moving the data to another system or removing it from a website.
- If the personal data has been disclosed to others, your organisation contacts each recipient to tell them about the restriction, unless this is impossible or involves disproportionate effort.
- If asked to, your organisation tells the data subject which third parties have received the personal data.

Can you answer yes to the following questions?

- Would staff say you have effective processes in place to restrict personal data?
- Would requesters say you gave them clear information about the steps you took?

Data portability

Data portability

Individuals are able to move, copy or transfer their personal data from your organisation to another securely, without affecting the data.

Ways to meet our expectations:

- When requested, you provide personal data in a structured, commonly used and machine readable format.
- Where possible and if an individual requests it, your organisation can directly transmit the information to another organisation.

Can you answer yes to the following questions?

- Would staff say you have effective data portability processes in place?
- Would requesters say you gave them clear information?

Rights related to automated decision-making and profiling

Rights related to automated decision-making and profiling

Your organisation can protect individual rights related to automated decision-making and profiling, particularly where the processing is solely automated with legal or similarly significant effects.

Ways to meet our expectations:

- You complete additional checks for vulnerable groups, such as children, for all automated decision-making and profiling..
- Your organisation only collects the minimum data needed and has a clear retention policy for the profiles created.
- If your organisation uses solely automated decisions that have legal or similarly significant effects on individuals, you have a recorded process to ensure these decisions only occur in accordance with Article 22 of the GDPR. If this applies, your organisation must also carry out a data protection impact assessment (DPIA).
- Where the decision is solely automated and has legal or similarly significant effects on individuals, a recorded process allows simple ways for individuals to request human intervention, express their opinion and challenge a decision.
- You conduct regular checks for accuracy and bias to ensure that systems are working as intended, and you feed this back into the design process.

Can you answer yes to the following questions?

- Do staff and customers find your retention policy clear?
- Do staff say you have effective processes to protect rights relating to automated decision-making and profiling?
- Would individuals say you made it easy to request human intervention, express their opinion and challenge a decision?

Individual complaints

Individual complaints

Your organisation has procedures to recognise and respond to individuals' complaints about data protection, and individuals are made aware of their right to complain, eg through a complaints page on your website.

Ways to meet our expectations:

- You have procedures to handle data protection complaints raised by individuals and you report their resolution to senior management.
- The DPO’s contact details or alternative contact points are publicly available if individuals wish to raise a complaint about the use of their data.
- You tell individuals about their right to make a complaint to the ICO in your privacy information.

Can you answer yes to the following questions?

- Would complainants say that they were clear about how to make complaints and how it would be handled?

Transparency

Why is this important?

Transparency is a key data protection principle which is fundamental to a 'data protection by design and by default' approach. It facilitates the exercise of individuals' rights and gives people greater control. This is particularly important if the processing is complex or if it relates to a child. Proactively respecting people's privacy can give you a competitive advantage by increasing the confidence of the public, regulators and business partners. Being open and honest about what you do with personal data will support contracting and data sharing with third parties.

At a glance – what we expect from you

- Privacy notice content
- Timely privacy information
- Effective privacy information
- Automated decision-making and profiling
- Staff awareness
- Privacy information review
- Tools supporting transparency and control

Further reading

ICO guidance:

- Guidance on Explaining decisions made with AI
- Right to be informed
- Children
- Draft Guidance on explaining
  - AI Part 1 The basics of explaining AI,
  - Part 2 Explaining AI in practice,
  - Part 3 What explaining AI means for your organisation
- Age Appropriate Design Code of Practice

ICO template:

- Privacy notice and a simplified privacy notice template appropriate for community and voluntary groups

Privacy notice content

Privacy notice content

Your organisation's privacy information or notice includes all the required information under Article 13 and 14 of the GDPR.

Ways to meet our expectations:

- Privacy information includes all relevant contact information, eg the name and contact details of your organisation (and your representative if applicable) and the DPO’s contact details.
- Privacy information includes the purposes of the processing and the lawful bases (and, if applicable, the legitimate interests for the processing).
- Privacy information includes the categories of personal data you obtain and the data source, if this isn’t the individual the data relates to.
- Privacy information includes details of all personal data that you share with other organisations and, if applicable, details of transfers to any third countries or international organisations.
- Privacy information includes retention periods for the personal data, or if that is not possible, the criteria used to determine the period.
- Privacy information includes details about individuals' rights including, if applicable, the right to withdraw consent and the right to make a complaint.
- Privacy information includes details of whether individuals are under a statutory or contractual obligation to provide the personal data (if applicable, and if you collect the personal data from the individual it relates to).
- You provide individuals with privacy information regarding the source of the processed personal data if you don’t obtain it from the individual concerned, eg if the data is from publicly accessible sources such as social media, the open electoral register or Companies House.

Can you answer yes to the following questions?

- Do your staff understand what privacy information is and what must be provided?
- Are individuals provided with clear information about the source of personal data, if you don’t obtain it from the individual concerned?

Timely privacy information

Timely privacy information

You have a recorded procedure to make sure that individuals receive privacy information at the right time, unless an exemption applies.

Ways to meet our expectations:

- Individuals receive privacy information when their data is collected (eg when they fill in a form) or by observation (eg when using CCTV or people are tracked online).
- If you obtain personal data from a source other than the individual it relates to, you provide privacy information to individuals, no later than one month of obtaining the data.

Can you answer yes to the following questions?

- Do your staff understand when and how privacy information should be provided?

Effective privacy information

Effective privacy information

Your organisation provides privacy information that is:

- concise;
- transparent;
- intelligible;
- clear
- in plain language; and
- communicated in a way that is effective for the target audience.

Ways to meet our expectations:

- You proactively make individuals aware of privacy information and have a free, easy way to access it.
- You provide privacy information to individuals in electronic and hard-copy form, using a combination of appropriate techniques, such as a layered approach, icons and mobile and smart device functionalities.
- You write privacy information in clear and plain language that the intended audience can understand, and offer it in accessible formats if required.
- Your organisation takes particular care to ensure that you write privacy information for children in clear and plain language, that it's age appropriate, and explains the risks involved in the processing and the safeguards you have put in place.

Can you answer yes to the following questions?

- Would customers say you proactively made them aware of privacy information?
- Did you use an appropriate form of communication?
- Was it easy to understand?

Automated decision-making and profiling

Automated decision-making and profiling

Your organisation is transparent about any processing relating to automated decision-making and profiling.

Ways to meet our expectations:

- You have procedures for individuals to access the personal data you use to create profiles, so they can review for accuracy and edit it if needed.
- If the decision is solely automated and has legal or similarly significant effects, your organisation tells individuals about the processing - including what information you are using, why and what the impact is likely to be.
- If the purpose is initially unclear, you give individuals an indication of what your organisation is going to do with their data, and you proactively update your privacy information as this becomes clearer.
- If the decision is solely automated and has legal or similarly significant effects, your organisation explains the processing in a meaningful way that enables individuals to exercise their rights including obtaining human intervention, expressing their point of view and contesting the decision.

Can you answer yes to the following questions?

- Would individuals say that you explained the processing to them in a meaningful way that helped them to exercise their rights?
- Is it easy for them to access the personal data you used to create profiles?

Staff awareness

Staff awareness

Your organisation can demonstrate that any member of front-line staff is able to explain the necessary privacy information to data subjects and provide guidance.

Ways to meet our expectations:

- You arrange organisation-wide staff training about privacy information.
- Front-line staff receive more specialised or specific training.
- Staff are aware of the various ways in which the organisation provides privacy information.

Can you answer yes to the following questions?

- Do your staff have good general knowledge about privacy information and the ways it is provided?
- Do front-line staff have more detailed knowledge?

Privacy information review

Privacy information review

Your organisation has procedures to review the privacy information provided to data subjects regularly to make sure that it is accurate, up to date and effective.

Ways to meet our expectations:

- You review privacy information against the records of processing activities, to ensure it remains up to date and that it accurately explains what happens with individuals' personal data.
- You maintain a log of historical privacy notices, including the dates you made any changes, in order to allow a review of what privacy information you provided to data subjects and when.
- Your organisation carries out user testing to evaluate the privacy information's effectiveness.
- Your organisation analyses complaints from the public about how you use their personal data, and in particular, any complaints about how you explain that use.
- If your organisation plans to use personal data for a new purpose, you have a procedure to update the privacy information and communicate the changes to individuals before starting any new processing.

Can you answer yes to the following questions?

- Is there an effective review process?
- Would individuals say that you provide effective privacy information?

Tools supporting transparency and control

Tools supporting transparency and control

Your organisation is open about how personal data is used, especially when processing children's personal data, and you offer tools which support transparency and control.

Ways to meet our expectations:

- Privacy policies are clear and easy for members of the public to access.
- You provide individuals with tools, such as secure self-service systems, dashboards and just-in-time notices, so they can access, determine and manage how your organisation uses their personal data.
- Your organisation offers strong privacy defaults and user-friendly options and controls.
- Where relevant, you have processes in place to help children exercise their data protection rights in an easily accessible way that they understand.
- You implement appropriate measures to protect children using digital services.

Can you answer yes to the following questions?

- Would the public say that your policies are clear, easy to find and access?
- Do they feel appropriately supported in accessing, determining and managing how their data is used?
- Would children say the same?

Records of processing and lawful basis

Why is this important?

It's a legal requirement to document your processing activities. Taking stock of what information you have, where it is and what you do with it makes it much easier for you to improve your information governance and comply with other aspects of data protection law (such as creating a privacy notice and keeping personal data secure). It is a clear way to show what you are doing in line with the accountability principle and we may require you to provide these records to us. Your processing won't be lawful without a valid lawful basis so you must justify your choice appropriately.

At a glance – what we expect from you

- Data-mapping
- Records of processing activities (ROPA)
- ROPA requirements
- Good practice for ROPAs
- Documenting your lawful basis
- Lawful basis transparency
- Consent requirements
- Reviewing consent
- Risk-based age checks and parental/guardian consent
- Legitimate Interest Assessment (LIA)

Further reading

ICO guidance:

- Documentation
- Lawful basis for processing
- Lawful basis for processing - consent
- Lawful basis for processing – Legitimate interests
- Special category data
- Criminal offence data
- Children
- Age Appropriate Design Code of Practice
- ICO template: Appropriate Policy Document
- ICO tool: Lawful basis interactive guidance tool

External guidance:

- The National Archives: Find out what information you have

Data mapping

Data mapping

Your organisation frequently carries out comprehensive data mapping exercises, providing a clear understanding of what information is held and where.

Ways to meet our expectations:

- Your organisation carries out information audits (or data mapping exercises) to find out what personal data is held and to understand how the information flows through your organisation.
- You keep the data map up to date and you clearly assign the responsibilities for maintaining and amending it.
- You consult your staff to make sure that there is an accurate picture of processing activities, for example by using questionnaires and staff surveys.

Can you answer yes to the following questions?

- Would staff say that there was an effective process in place to identify what personal data is held across the organisation?
- Could staff explain their responsibilities and how they are carried out in practice?
- Would the record match what people were currently doing?

Record of processing activities (ROPA)

Record of processing activities (ROPA)

Your organisation has a formal, documented, comprehensive and accurate ROPA based on a data mapping exercise that is reviewed regularly.

Ways to meet our expectations:

- You record processing activities in electronic form so you can add, remove and amend information easily.
- Your organisation regularly reviews the record against processing activities, policies and procedures to ensure that it remains accurate and up to date, and you clearly assign responsibilities for doing this.
- You regularly review the processing activities and types of data you process for data minimisation purposes.

Can you answer yes to the following questions?

- Would staff say that you have effective processes in place to keep the record up to date, accurate and make sure that the data is minimised?
- Could staff explain their responsibilities and how they carry them out in practice?

ROPA requirements

ROPA requirements

Your ROPA contains all the relevant requirements set out in Article 30 of the GDPR.

Ways to meet our expectations:

- The ROPA includes (as a minimum):
  - your organisation's name and contact details, whether it is a controller or a processor (and where applicable, the joint controller, their representative and the DPO);
  - the purposes of the processing;
  - a description of the categories of individuals and of personal data;
  - the categories of recipients of personal data;
  - details of transfers to third countries, including a record of the transfer mechanism safeguards in place;
  - retention schedules; and
  - a description of the technical and organisational security measures in place.
- You have an internal record of all processing activities carried out by any processors on behalf of your organisation.

Can you answer yes to the following questions?

- Would staff say that you have effective processes in place to keep the record up to date, accurate and make sure that the data is minimised?
- Could staff explain their responsibilities and how they carry them out in practice?

Good practice for ROPAs

Good practice for ROPAs

Your organisation’s ROPA includes links to other relevant documentation, such as contracts or records as a matter of good practice.

Ways to meet our expectations:

- The ROPA also includes, or links to, documentation covering:
  - information required for privacy notices, such as the lawful basis for the processing and the source of the personal data;
  - records of consent;
  - controller-processor contracts;
  - the location of personal data;
  - DPIA 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 (DPA 2018); and
  - retention and erasure policy documents.

Can you answer yes to the following questions?

- Are staff aware of the need to identify a lawful basis for processing personal data?
- Can they identify an appropriate lawful basis?
- Are they aware of the additional requirements to protect special category and criminal offence data?

Documenting your lawful basis

Documenting your lawful basis

You document and appropriately justify your organisation's lawful basis for processing personal data in line with Article 6 of the GDPR (and Articles 9 and 10, if the processing involves special category or criminal offence data).

Ways to meet our expectations:

- Your organisation selects the most appropriate lawful basis (or bases) for each activity following a review of the processing purposes.
- You document the lawful basis (or bases) relied upon and the reasons why.
- If your organisation processes special category or criminal offence data, you identify and document a lawful basis for general processing and an additional condition for processing this type of data (or in the case of criminal offence data, you identify the official authority to process).
- In the case of special category or criminal offence data, you document consideration of the requirements of Article 9 or 10 of the GDPR and Schedule 1 of the DPA 2018 where relevant.
- Where Schedule 1 requires it, you have an appropriate policy document including:
  - which Schedule 1 conditions you are relying upon;
  - what procedures you have in place to ensure compliance with the data protection principle;
  - how you will treat special category or criminal offence data for retention and erasure purposes;
  - a review date; and
  - details of an individual assigned responsibility for the processing.
- You identify the lawful basis before starting any new processing.

Can you answer yes to the following questions?

- Would customers agree that your privacy notice is easy to find, access and understand?

Lawful basis transparency

Lawful basis transparency

You make information about the purpose of the processing and the lawful basis publicly available. This is easy to locate, access and read.

Ways to meet our expectations:

- You make information about the purposes of the processing, your lawful basis and relevant conditions for processing any special category or criminal offence data publicly available in your organisation's privacy notice(s).
- You provide information in an easily understandable format.
- If there is a genuine change in circumstances, or if your lawful basis must change due to a new and unanticipated purpose, you inform individuals in a timely manner and record the changes.

Consent requirements

Consent requirements

If your organisation relies on consent for the processing of personal data, you comply with the GDPR's consent requirements of being:

- specific;
- granular;
- prominent;
- opt-in;
- documented; and
- easily withdrawn.

Ways to meet our expectations:

- Consent requests:
  - are kept separate from other terms and conditions;
  - require a positive opt-in and do not use pre-ticked boxes;
  - are clear and specific (not a pre-condition of signing up to a service);
  - inform individuals how to withdraw consent in an easy way; and
  - give your organisation's name as well as any third parties relying on consent.
- You have records of what an individual has consented to, including what they were told and when and how they consented. The records are thorough and easy for relevant staff to access, review and withdraw if required.
- You have evidence and examples of how consent is sought from individuals, for example online forms or notices, opt-in tick boxes or paper-based forms.

Can you answer yes to the following questions?

- Do staff agree that the records of consent are easy to access, understand and review?
- Do customers say that you make it easy to understand and manage consent?

Reviewing consent

Reviewing consent

You proactively review records of previously gathered consent, which demonstrates a commitment to confirming and refreshing the consents.

Ways to meet our expectations:

- You have a procedure to review consents to check that the relationship, the processing and the purposes have not changed and to record any changes.
- Your organisation has a procedure to refresh consent at appropriate intervals.
- Your organisation uses privacy dashboards or other preference management tools to help people manage their consent.

Can you answer yes to the following questions?

- Are staff aware of the process to review consents?
- Is the procedure easy to find, access and understand?
- Do individuals say it was easy to manage their consent preferences?

Risk-based age checks and parental or guardian consent

Risk-based age checks and parental or guardian consent

Your organisation has effective systems in place to conduct risk-based age checks and, where required, to obtain and record parental or guardian consent.

Ways to meet our expectations:

- Your organisation makes reasonable efforts to check the age of those giving consent, particularly where the individual is a child.
- You have a reasonable and effective procedure to determine whether the individual in question can provide their own consent, and if not, an effective way to gain and record parental or guardian consent.
- When providing online services to children, your organisation has risk-based age checking systems in place to establish age, with an appropriate level of certainty based on the risks to children's rights and freedoms.
- When providing online services to children, if the child is under 13, you have records of parental or guardian consent which are regularly reviewed, and you make reasonable efforts to verify that the person giving consent has parental responsibility. You give particular consideration when a child reaches the age of 13 and is able to provide their own consent.

Can you answer yes to the following questions?

- Do staff and individuals agree that you have a reasonable and effective way to conduct risk-based age checks, gain parental or guardian consent and review what’s in place?

Legitimate interest assessment (LIA)

Legitimate interest assessment (LIA)

If your organisation’s lawful basis is legitimate interests, you have completed an appropriate LIA prior to starting the processing.

Ways to meet our expectations:

- The LIA identifies the legitimate interest, the benefits of the processing and whether it is necessary.
- The LIA includes a 'balancing test' to show how your organisation determines that its legitimate interests override the individuals’ and considers the following issues:
  - Not using people's data in intrusive ways or in ways which could cause harm, unless there is a very good reason.
  - Protecting the interests of vulnerable groups such as people with learning disabilities or children.
  - Whether you could introduce safeguards to reduce any potentially negative impact.
  - Whether you can offer an opt-out.
  - Whether you require a DPIA.
- You clearly document the decision and the assessment.
- You complete the LIA prior to the start of the processing.
- You keep the LIA under review and refresh it if changes affect the outcome.

Can you answer yes to the following questions?

- Do staff say that the LIAs are clear and comprehensive?
- Is the review process effective?

Contracts and data sharing

Why is this important?

It is good practice for you to have written data sharing agreements when controllers share personal data. This helps everyone to understand the purpose for the sharing, what will happen at each stage and what responsibilities they have. It also helps you to demonstrate compliance in a clear and formal way. Similarly, written contracts help controllers and processors to demonstrate compliance and understand their obligations, responsibilities and liabilities.

At a glance – what we expect from you

- Data sharing policies and procedures
- Data sharing agreements
- Restricted transfers
- Processors
- Controller-processor contract requirements
- Processor due diligence checks
- Processor compliance reviews
- Third-party products and services
- Purpose limitation

Further reading

ICO guidance:

- International transfers
- Contracts
- Draft data sharing code of practice
- Data protection at the end of the transition period
- Data protection by design and by default
- Principles – purpose limitation
- Principles – data minimisation
- ICO template: Controller to controller contract and Controller to processor contract
- ICO tool: Keep data flowing from the EEA to the UK – interactive tool

External guidance:

- Wales Accord on the Sharing of Personal Information (Welsh organisations only)

Data sharing policies and procedures

Data sharing policies and procedures

Your organisation’s policies and procedures make sure that you appropriately manage data sharing decisions, eg through a DPIA.

Ways to meet our expectations:

- You have a review process, through a DPIA or a similar exercise, to assess the legality, benefits and risks of the data sharing.
- You document all sharing decisions for audit, monitoring and investigation purposes and regularly review them.
- Your organisation has clear policies, procedures and guidance about data sharing, including who has the authority to make decisions about systematic data sharing or one-off disclosures, and when it is appropriate to do so.
- Your organisation adequately trains all staff likely to make decisions about sharing and makes them aware of their responsibilities. You refresh this training periodically as appropriate.

Can you answer yes to the following questions?

- Are staff aware of their responsibilities and how to carry them out effectively?
- Would staff say they have a clear process to follow?
- Is your organisation meeting their training needs?

Data sharing agreements

Data sharing agreements

You arrange and regularly review appropriate data sharing agreements with parties with whom you routinely share personal data.

Ways to meet our expectations:

- You agree data sharing agreements with all the relevant parties and senior management sign them off.
- The data sharing agreement includes details about:
  - the parties' roles;
  - the purpose of the data sharing;
  - what is going to happen to the data at each stage; and
  - the standards set (with a high privacy default for children).
- Where necessary, procedures and guidance covering each organisation’s day-to-day operations support the agreements..
- If your organisation is acting as a joint controller (within the meaning of Article 26 of the GDPR), you set out responsibilities under an arrangement or a data sharing agreement and you provide appropriate privacy information to individuals.
- You have a regular review process to make sure that the information remains accurate and up to date, and to examine how the agreement is working.
- You keep a central log of the current sharing agreements.

Can you answer yes to the following questions?

- Are staff with sharing responsibilities aware of the process?
- Is there contingency built into the process if something goes wrong or if people aren’t available to perform their role?
- Would staff say the decision-making is maintained or appropriately delegated?

Restricted transfers

Restricted transfers

Your organisation has procedures in place to make sure that restricted transfers are made appropriately.

Ways to meet our expectations:

- You consider whether the restricted transfer is covered by an adequacy decision or by 'appropriate safeguards' listed in data protection law, such as contracts incorporating standard contractual data protection clauses adopted by the Commission or Binding Corporate Rules (BCRs).
- If a restricted transfer is not covered by either of the above options, you consider whether the transfer is covered by an exemption set out in Article 49 of the GDPR.

Can you answer yes to the following questions?

- Are staff aware of the process and their responsibilities?
- Are you meeting their training needs?
- Do staff adhere to the policies and procedures?

Processors

Processors

You have appropriate procedures in place regarding the work that processors do on your behalf.

Ways to meet our expectations:

- You have written contracts with all processors.
- If using a processor, you assess the risk to data subjects and make sure to effectively mitigate these risks.
- An appropriate level of management approves the contracts and both parties sign. The level of management required for approval is proportionate to the value and risk of the contract.
- Each contract (or other legal act) sets out details of the processing, including the:
  - subject matter of the processing;
  - duration of the processing;
  - nature and purpose of the processing;
  - type of personal data involved;
  - categories of data subject; and
  - controller's obligations and rights, in accordance with the list set out in Article 28(3) of the GDPR.
- You keep a record or log of all current processor contracts, which you update when processors change.
- You review contracts periodically to make sure they remain up to date.
- If a processor uses a sub-processor to help with the processing it is doing on your behalf, they have written authorisation from your organisation and a written contract with that sub-processor.

Can you answer yes to the following questions?

- Are staff aware of the need for a written contract when using a processor?
- How do they make sure the contracts are kept up to date?
- Are the risks of using a processor mitigated effectively?
- Do you have an appropriate approval process for contracts?
- Is it easy for staff to find existing contracts where appropriate?

Controller-processor contract requirements

Controller-processor contract requirements

All of your controller-processor contracts cover the terms and clauses necessary to comply with data protection law.

Ways to meet our expectations:

- 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;
  - ensure that people processing the data are subject to a duty of confidence;
  - help the controller respond to requests from individuals to exercise their rights; and
  - submit to audits and inspections.
- Contracts include the technical and organisational security measures that the processor must adopt (including encryption, pseudonymisation, resilience of processing systems and backing up personal data in order to be able to reinstate the system).
- The contract includes clauses to make sure that the processor either deletes or returns all personal data to the controller at the end of the contract. The processor must also delete existing personal data unless the law requires its storage.
- The contract includes clauses to make sure that the processor assists the controller in meeting its GDPR obligations regarding the security of processing, the notification of personal data breaches and DPIAs.

Can you answer yes to the following questions?

- Was the International Organisation for Standardization (ISO) consulted on the appropriateness of security measures detailed within contracts?

Processor due diligence checks

Processor due diligence checks

You have due diligence checks to guarantee that data processors will implement appropriate technical and organisational measures to meet GDPR requirements.

Ways to meet our expectations:

- The procurement process builds in due diligence checks proportionate to the risk of the processing before you agree a contract with a processor.
- The due diligence process includes data security checks, eg site visits, system testing and audit requests.
- The due diligence process includes checks to confirm a potential processor will protect data subjects' rights.

Can you answer yes to the following questions?

- Are staff aware of what they need to do?
- Is there a clear and effective process?
- Are due diligence checks proportionate to the risks?

Processor compliance reviews

Processor compliance reviews

Your organisation reviews data processors’ compliance with their contracts.

Ways to meet our expectations:

- Contracts include clauses to allow your organisation to conduct audits or checks, to confirm the processor is complying with all contractual terms and conditions.
- You carry out routine compliance checks, proportionate to the processing risks, to test that processors are complying with contractual agreements.

Can you answer yes to the following questions?

- Is there any follow-up where you identify non-compliance to contract terms or a Service Level Agreement?
- Are the checks proportionate to the risks?

Third-party products and services

Third-party products and services

Your organisation considers ‘data protection by design’ when selecting services and products to use in data processing activities.

Ways to meet our expectations:

- When you use third-party products or services to process personal data, you make sure to choose suppliers that design their products or services with data protection in mind.

Can you answer yes to the following questions?

- Do staff consider suppliers’ approach to data protection when using third-party products or services to process personal data?
- Is there a clear way for them to do this?

Purpose limitation

Purpose limitation

Your organisation proactively takes steps to only share necessary personal data with processors or other third parties.

Ways to meet our expectations:

- Your organisation only shares the personal data necessary to achieve its specific purpose.
- When information is shared, it is pseudonymised or minimised wherever possible. You also consider anonymisation so that the information is no longer personal data.

Can you answer yes to the following questions?

- Do staff understand what they should consider when sharing data to make sure it is limited appropriately?

Risks and data protection impact assessments (DPIAs)

Why is this important?

The need to identify, assess and manage privacy risks is an integral part of accountability. Understanding the risks of the way you use personal data specifically is central to creating an appropriate and proportionate privacy management framework. A DPIA is a key risk management tool, and an important part of integrating 'data protection by design and by default' across your organisation. It helps you to identify, record and minimise the data protection risks of projects. DPIAs are mandatory in some cases and there are specific legal requirements for content and process. If you cannot mitigate a high risk, you must have a process for reporting this to the ICO.

At a glance – what we expect from you

- Identifying, recording and managing risks
- Data protection by design and by default
- DPIA policy and procedures
- DPIA content
- DPIA risk mitigation and review

Further reading

ICO guidance:

- Data protection impact assessments
- Data protection by design and by default
- ICO template: DPIA template

External guidance:

- The National Archives: Information Assurance
- The National Archives: Managing information risks
- National Cyber Security Centre: 10 Steps to Cyber Security – Risk Management Regime

Identifying, recording and managing risks

Identifying, recording and managing risks

Your organisation has appropriate policies, procedures and measures to identify, record and manage information risks.

Ways to meet our expectations:

- An information risk policy (either a separate document or part of a wider corporate risk policy) sets out how your organisation and its data processors manage information risk, and how you monitor compliance with the information risk policy.
- You have a process to help staff report and escalate information governance or data protection concerns and risks to a central point, for example staff forums.
- You identify and manage information risks in an appropriate risk register, which includes clear links between corporate and departmental risk registers and the risk assessment of information assets.
- You have formal procedures to identify, record and manage risks associated with information assets in an information asset register.
- If you identify information risks, you have appropriate action plans, progress reports and a consideration of the lessons learnt to avoid future risk.
- You put in place measures to mitigate the risks identified within risk categories and you test these regularly to maintain effectiveness.

Can you answer yes to the following questions?

- Do staff know how to report and escalate concerns and risks?
- Could staff explain the links between the information risk register, the risk assessment of information assets, departmental risk registers and the corporate risk register?

Data protection by design and by default approach to managing risks

Data protection by design and by default

You take a data protection by design and by default approach to managing risks, and, as appropriate, you build DPIA requirements into policies and procedures.

Ways to meet our expectations:

- You reference DPIA requirements in all risk, project and change management policies and procedures, with links to DPIA policies and procedures.
- Your procedures state that, if required, a DPIA must begin at the project's outset, before processing starts, and that the DPIA must run alongside the planning and development process.
- You anticipate risks and privacy-invasive events before they occur, making sure that at the initial design phase of any system, product or process and throughout, you consider the:
  - intended processing activities;
  - risks that these may pose to the rights and freedoms of individuals; and
  - possible measures available to mitigate the risks.

Can you answer yes to the following questions?

- Would staff working on personal data processing projects be able to explain how they manage the risks as part of the project?

DPIA policy and procedures

DPIA policy and procedures

You understand whether a DPIA is required, or where it would be good practice to complete one. There is a clear DPIA policy and procedure.

Ways to meet our expectations:

- You have a DPIA policy which includes:
  - clear procedures to decide whether you conduct a DPIA;
  - what the DPIA should cover;
  - who will authorise it; and
  - how you will incorporate it into the overall planning.
- You have a screening checklist to consider if you need a DPIA, including all the relevant considerations on the scope, type and manner of the proposed processing.
- If the screening checklist indicates that you do not need a DPIA, you document this.
- Your procedure includes the requirement to seek advice from the DPO and other internal staff as appropriate.
- Your procedure includes consultation with controllers, data processors, individuals, their representatives and any other relevant stakeholders as appropriate.
- Staff training includes the need to consider a DPIA at the early stages of any plan involving personal data and, where relevant, you train staff in how to carry out a DPIA.
- You assign responsibility for completing DPIAs to a member of staff, who has enough authority over a project to effect change, eg a project lead or manager.

Can you answer yes to the following questions?

- Are your policies and procedures easy to locate?
- Are staff aware of the process?
- Do they consider it effective?
- Have they had adequate training?
- Are DPIAs conducted by those with appropriate authority to effect change?

DPIA content

DPIA content

DPIAs always include the appropriate information and are comprehensively documented.

Ways to meet our expectations:

- Your organisation has a standard, well-structured DPIA template which is written in plain English.
- DPIAs:
  - include 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.
- DPIAs clearly set out the relationships and data flows between controllers, processors, data subjects and systems.
- DPIAs identify measures that eliminate, mitigate or reduce high risks.
- You have a documented process, with appropriate document controls, that you review periodically to ensure it remains up to date.
- You record your DPO’s advice and recommendations and the details of any other consultations.
- Appropriate people sign off DPIAs, such as a project lead or senior manager.

Can you answer yes to the following questions?

- Do staff use the DPIA template and find it easy to understand?
- Is the process effective?
- Is the DPO satisfied that their advice is taken into account?
- Are they satisfied with any consultation that has taken place and how that you reflect any feedback in the outcome?

DPIA risk mitigation and review

DPIA risk mitigation and review

You take appropriate and effective action to mitigate or manage any risks a DPIA identifies, and you have a DPIA review process.

Ways to meet our expectations:

- You have a procedure to consult the ICO if you cannot mitigate residual high risks.
- You integrate outcomes from DPIAs into relevant work plans, project action plans and risk registers.
- You do not start high risk processing until mitigating measures are in place following the DPIA.
- You have a procedure to communicate the outcomes of DPIAs to appropriate stakeholders, eg through a formal summarised report.
- You consider actively publishing DPIAs where possible, removing sensitive details if necessary.
- You agree and document a schedule for reviewing the DPIA regularly or when the nature, scope, context or purposes of the processing changes.

Can you answer yes to the following questions?

- Do staff understand when to consult the ICO?
- Do you effectively integrate outcomes from DPIAs into projects?
- Are appropriate stakeholders aware of the outcomes of DPIAs?

Records management and security

Why is this important?

Good records management supports good data governance and data protection. Wider benefits include supporting information access, making sure that you can find information about past activities, and enabling the more effective use of resources. Some of the consequences of poor records management include poor decisions, failure to handle information securely and inefficiencies. Information security also supports good data governance, and is itself a legal data protection requirement. Poor information security leaves your systems and services at risk and may cause real harm and distress to individuals – it may even endanger lives in some extreme cases.

At a glance – what we expect from you

- Creating, locating and retrieving records
- Security for transfers
- Data quality
- Retention schedule
- Destruction
- Information Asset Register
- Rules for acceptable software use
- Access control
- Unauthorised access
- Mobile devices, home or remote working and removable media
- Secure areas
- Business continuity, disaster recovery and back-ups

Further reading

ICO guidance:

- Principles – storage limitation
- Documentation
- Security
- Encryption
- Passwords in online services
- Data security: a guide to the basics
- Working from home guidance
- ICO video – Cyber Security – balancing cost benefit decisions

External guidance:

The National Archives:

- Records management implementation guides
- Keeping records to meet corporate requirements
- How to manage your information
- Tracking records
- Information Asset Register factsheet
- Identifying information assets
- Template Information Asset Register
- Business continuity management toolkit
- Protecting archives and manuscripts against disaster

National Cyber Security Centre:

- Security advice
- 10 Steps to Cyber Security
- Cyber Essentials
- Centre for the Protection of National Infrastructure Security advice
- Get Safe Online – Security advice for businesses and template Acceptable Usage Policy
- Privacy Sense: Creating a clear desk policy
- Surveillance Camera Commissioner: Surveillance Camera Code of Practice

Creating, locating and retrieving records

Creating, locating and retrieving records

You have minimum standards for the creation of records and effective mechanisms to locate and retrieve records.

Ways to meet our expectations:

- You have policies and procedures to ensure that you appropriately classify, title and index new records in a way that facilitates management, retrieval and disposal.
- You identify where you use manual and electronic record-keeping systems and maintain a central log or information asset register.
- You know the whereabouts of records at all times, you track their movements, and you make attempts to trace records that are missing or not returned.
- You index records stored off-site with unique references to enable accurate retrieval and subsequent tracking.

Can you answer yes to the following questions?

- Do staff know how to classify and structure records appropriately?
- Is the asset register kept up to date?
- Have there been any issues locating records?

Security for transfers

Security for transfers

You have appropriate security measures in place to protect data that is in transit, data you receive or data you transfer to another organisation.

Ways to meet our expectations:

- You document rules to protect the internal and external transfer of records by post, fax and electronically, for example in a transfer policy or guidance.
- You minimise data transferred off-site and keep it secure in transit.
- When you transfer data off site, you use an appropriate form of transport (for example secure courier, encryption, secure file transfer protocol (SFTP) or Virtual Private Network (VPN)) and you make checks to ensure the information has been received.
- You have agreements in place with any third parties used to transfer business information between your organisation and third parties.

Can you answer yes to the following questions?

- Are staff aware of the policies and procedures and do they follow them?
- Do staff know how to send emails or information by post or fax securely?
- Have they been using appropriate forms of transport?

Data quality

Data quality

You have procedures in place to make sure that records containing personal data are accurate, adequate and not excessive.

Ways to meet our expectations:

- You conduct regular data quality reviews of records containing personal data to make sure they are accurate, adequate and not excessive.
- You make staff aware of data quality issues following data quality checks or audits to prevent recurrence.
- Records containing personal data (whether active or archived) are 'weeded' periodically to reduce the risks of inaccuracies and excessive retention.

Can you answer yes to the following questions?

- Could staff demonstrate the process for conducting data quality reviews?
- Do staff understand their responsibilities and do they know what to do if they identify issues?

Retention schedule

Retention schedule

You have an appropriate retention schedule outlining storage periods for all personal data, which you review regularly.

Ways to meet our expectations:

- You have a retention schedule based on business need with reference to statutory requirements and other principles (for example the National Archives).
- The schedule provides sufficient information to identify all records and to implement disposal decisions in line with the schedule.
- You assign responsibilities to make sure that staff adhere to the schedule and you review it regularly.
- You regularly review retained data to identify opportunities for minimisation, pseudonymisation or anonymisation and you document this in the schedule.

Can you answer yes to the following questions?

- Are staff aware of the retention schedule?
- Do they adhere to it?
- Could staff explain what their responsibilities are and how they carry them out effectively?

Destruction

Destruction

You cover methods of destruction in a policy and they are appropriate to prevent disclosure of personal data prior to, during or after disposal.

Ways to meet our expectations:

- For paper documents, you use locked waste bins for records containing personal data, and either in-house or third party cross shredding or incineration is in place.
- For information held on electronic devices, wiping, degaussing or secure destruction of hardware (shredding) is in place.
- You either hold, collect or send away securely confidential waste awaiting destruction.
- You have appropriate contracts in place with third parties to dispose of personal data, and they provide you with appropriate assurance that they have securely disposed of the data, for example through audit checks and destruction certificates.
- You have a log of all equipment and confidential waste sent for disposal or destruction.

Can you answer yes to the following questions?

- Is there a secured location for waste collected daily until collected for disposal internally or by a third party?
- Is there a secure storage area for equipment awaiting disposal?

Information asset register

Information asset register

You have an asset register that records assets, systems and applications used for processing or storing personal data across the organisation.

Ways to meet our expectations:

- Your organisation has an asset register which holds details of all information assets (software and hardware) including:
- asset owners;
  - asset location;
  - retention periods; and
  - security measures deployed.
- You review the register periodically to make sure it remains up to date and accurate.
- You periodically risk-assess assets within the register and you have physical checks to make sure that the hardware asset inventory remains accurate.

Can you answer yes to the following questions?

- Is the register accurate – could you use it to find equipment around your office?
- If we selected a sample of software, could you demonstrate that the details in the register are correct?

Rules for acceptable software use

Rules for acceptable software use

You identify, document and implement rules for the acceptable use of software (systems or applications) processing or storing information.

Ways to meet our expectations:

- You have Acceptable Use or terms and conditions of use procedures in place.
- You have system operating procedures which document the security arrangements and measures in place to protect the data held within systems or applications.
- Your organisation monitors compliance with acceptable use rules and makes sure that staff are aware of any monitoring.

Can you answer yes to the following questions?

- Are staff aware of the policies and procedures?
- Are they well understood?

Access control

Access control

You limit access to personal data to authorised staff only and regularly review users’ access rights.

Ways to meet our expectations:

- You have an Access Control policy which specifies that users must follow your organisation's practices in the use of secret authentication information, for example passwords or tokens.
- You implement a formal user access provisioning procedure to assign access rights for staff (including temporary staff) and third-party contractors to all relevant systems and services required to fulfil their role, for example 'new starter process'.
- You restrict and control the allocation and use of privileged access rights.
- You keep a log of user access to systems holding personal data.
- You regularly review users’ access rights and adjust or remove rights where appropriate, for example when an employee changes role or leaves the organisation.

Can you answer yes to the following questions?

- Are staff aware of the policies and procedures?
- Are third-party access rights assigned appropriately given what is required in a contract?
- Are access rights correct and up to date?
- Would a sample of new starters, movers and leavers show adherence to the policies and procedures?

Unauthorised access

Unauthorised access

You prevent unauthorised access to systems and applications, for example by passwords, technical vulnerability management and malware prevention tools.

Ways to meet our expectations:

- You restrict access to systems or applications processing personal data to the absolute minimum in accordance with the principle of least privilege (for example read/write/delete/execute access rules are applied).
- You apply minimum password complexity rules and limited log on attempts to systems or applications processing personal data.
- You have password management controls in place, including default password changing, controlled use of any shared passwords and secure password storage (not in plain text).
- Email content and attachment security solutions (encryption) appropriately protect emails containing sensitive personal data.
- You log and monitor user and system activity to detect anything unusual.
- You implement anti-malware and anti-virus (AV) protection across the network and on critical or sensitive information systems if appropriate.
- Anti-malware and anti-virus protection is kept up-to-date and you configure it to perform regular scans.
- Your organisation has access to and acts upon any updates on technical vulnerabilities to systems or software, for example vendor’s alerts or patches.
- You regularly run vulnerability scans.
- You deploy URL or web content filtering to block specific websites or entire categories.
- You strictly control or prohibit the use of social media, or messaging apps such as WhatsApp to share personal data.
- You have external and internal firewalls and intrusion detection systems in place as appropriate to ensure the security of information in networks and systems from unauthorised access or attack, for example denial of service attacks.
- You do not have unsupported operating systems in use, for example Windows XP or Windows Server 2003.
- You establish special controls to safeguard the confidentiality and integrity of data passing over public networks or over wireless networks and to protect the connected systems and applications.

Can you answer yes to the following questions?

- Would a sample of systems access at various job levels confirm that you apply access levels appropriately?

- Are the passwords complex?
- Could staff demonstrate that anti-virus and anti-malware has been implemented on key information systems?
- Do you install vendor updates in a timely manner?
- Could we access a black-listed site or an unsupported operating system on-site?

Mobile devices, home or remote working and removable media

Mobile devices, home or remote working and removable media

You have appropriate mechanisms in place to manage the security risks of using mobile devices, home or remote working and removable media.

Ways to meet our expectations:

- You have a mobile device and a home/remote working policy that demonstrates how your organisation will manage the associated security risks.
- You have protections in place to avoid the unauthorised access to or disclosure of the information processed by mobile devices, for example, encryption and remote wiping capabilities.
- You implement security measures to protect information processed when home or remote working, for example VPN and two-factor authentication.
- Where you have a business need to store personal data on removable media, you minimise personal data and your organisation implements a software solution that can set permissions or restrictions for individual devices as well as an entire class of devices.
- You do not allow equipment, information or software to be taken off-site without prior authorisation and you have a log of all mobile devices and removable media used and who they are allocated to.

Can you answer yes to the following questions?

- Can staff find the policies and procedures?
- Are they aware of the main contents?
- Would a sample of devices have appropriate encryption?
- Could you demonstrate appropriate access arrangements for home or remote working?
- Are staff working from home or remotely aware of the authorisation requirements?

Secure areas

Secure areas

You secure physical business locations to prevent unauthorised access, damage and interference to personal data.

Ways to meet our expectations:

- You protect secure areas (areas that contain either sensitive or critical information) by appropriate entry controls such as doors and locks, alarms, security lighting or CCTV.
- You have visitor protocols in place such as signing-in procedures, name badges and escorted access.
- You implement additional protection against external and environmental threats in secure areas such as server rooms.
- Office equipment is appropriately placed and protected to reduce the risks from environmental threats and opportunities for unauthorised access.
- You securely store paper records and control access to them.
- You operate a clear desk policy across your organisation where personal data is processed.
- You have regular clear desk 'sweeps' or checks and issues are fed back appropriately
- You operate a 'clear screen' policy across your organisation where personal data is processed.

Can you answer yes to the following questions?

- Are printer/fax areas secure?
- Do staff follow protocols and are they clearly communicated?
- Would we see appropriate environmental controls in your secure areas?
- Would a tour of your offices reveal an effective clear desk policy?
- Are screens left unlocked?

Business continuity, disaster recovery and back-ups

Business continuity, disaster recovery and back-ups

You have plans to deal with serious disruption, and you back up key systems, applications and data to protect against loss of personal data.

Ways to meet our expectations:

- You have a risk-based Business Continuity Plan to manage disruption and a Disaster Recovery Plan to manage disasters, which identify records that are critical to the continued functioning of the organisation.
- You take back-up copies of electronic information, software and systems (and ideally store them off-site).
- The frequency of backups reflects the sensitivity and importance of the data.
- You regularly test back-ups and recovery processes to ensure they remain fit for purpose.

Can you answer yes to the following questions?

- Are staff aware of the plans and are they easy to access?
- Could staff explain the effectiveness of the plans and how to test them?

Breach response and monitoring

Why is this important?

You need to be able to detect, investigate, risk-assess and record any breaches. You must report them as appropriate. Having effective processes in place helps you to do this. A personal data breach can have a range of adverse effects on individuals. There can be serious repercussions for organisations, their employees and customers, such as financial penalties (failure to notify a breach when required can result in a fine up to 10 million Euros or 2% of your global turnover), reputational damage, loss of business and disciplinary action.

At a glance – what we expect from you

- Detecting, managing and recording incidents and breaches
- Assessing and reporting breaches
- Notifying individuals
- Reviewing and monitoring
- External audit or compliance check
- Internal audit programme
- Performance and compliance information
- Use of management information

Further reading

ICO guidance:

- Personal data breaches
- ICO Webinar: Personal data breaches: Assessing the risk and Personal data breach reporting

External guidance:

- National Cyber Security Centre: 10 Steps to Cyber Security - Incident management

Detecting, managing and recording incidents and breaches

Detecting, managing and recording incidents and breaches

You have procedures in place to make sure that you detect, manage and appropriately record personal data incidents and breaches.

Ways to meet our expectations:

- You have appropriate training in place so that staff are able to recognise a security incident and a personal data breach.
- A dedicated person or team manages security incidents and personal data breaches.
- Staff know how to escalate a security incident promptly to the appropriate person or team to determine whether a breach has occurred.
- Procedures and systems facilitate the reporting of security incidents and breaches.
- Your organisation has a response plan for promptly addressing any security incidents and personal data breaches that occur.
- You centrally log/record/document both actual breaches and near misses (even if they do not need to be reported to the ICO or individuals).
- The log documents the facts relating to the near miss or breach including:
  - its causes;
  - what happened;
  - the personal data affected;
  - the effects of the breach; and
  - any remedial action taken and rationale.

Can you answer yes to the following questions?

- Could staff explain what constitutes a personal data breach?
- Do they know how to report incidents?
- Would a sample of how you manage incidents demonstrate adherence to the policy and procedures?

Assessing and reporting breaches

Assessing and reporting breaches

You have procedures to assess all security incidents and then report relevant breaches to the ICO within the statutory time frame.

Ways to meet our expectations:

- You have a procedure to assess the likelihood and severity of the risk to individuals as a result of a personal data breach.
- You have a procedure to notify the ICO of a breach within 72 hours of becoming aware of it (even when all the information is not yet available) and you notify the ICO on time.
- The procedure includes details of what information must be given to the ICO about the breach.
- If you consider it unnecessary to report a breach, you document the reasons why your organisation considers the breach unlikely to result in a risk to the rights and freedoms of individuals.

Can you answer yes to the following questions?

- Are staff aware of the policies and procedures and are they easy to find?
- Do staff understand how to conduct the risk assessment?
- Do they know when a breach needs to be reported to the ICO?

Notifying individuals

Notifying individuals

You have procedures to notify affected individuals where the breach is likely to result in a high risk to their rights and freedoms.

Ways to meet our expectations:

- You have a procedure setting out how you will tell affected individuals about a breach when it is likely to result in a high risk to their rights and freedoms.
- You tell individuals about personal data breaches in clear, plain language without undue delay
- The information you provide to individuals includes the DPO’s details, a description of the likely consequences of the breach and the measures taken (including mitigating actions and any possible adverse effects).
- You provide individuals with advice to protect themselves from any effects of the breach.

Can you answer yes to the following questions?

- Would individuals say that they were told about personal data breaches in a helpful and timely way?
- Did they get the information they needed?
- Were they satisfied with the steps you took to mitigate the impact?

Reviewing and monitoring

Reviewing and monitoring

You review and monitor personal data breaches.

Ways to meet our expectations:

- You analyse all personal data breach reports to prevent a recurrence.
- Your organisation monitors the type, volume and cost of incidents.
- You undertake trend analysis on breach reports over time to understand themes or issues.
- Groups with oversight for data protection and information governance review the outputs.

Can you answer yes to the following questions?

- Could we see an example of how you handled an incident that required lessons to be learned?
- Were the steps you took to prevent a recurrence of the incident effective?

External audit or compliance check

External audit or compliance check

Your organisation arranges an external data protection and information governance audit or other compliance checking procedure.

Ways to meet our expectations:

- Your organisation completes externally-provided self-assessment tools to provide assurances on data protection and information security compliance.
- Your organisation is subject to or employs the services of an external auditor to provide independent assurances (or certification) on data protection and information security compliance.
- Your organisation adheres to an appropriate code of conduct or practice for your sector (if one exists).
- You produce audit reports to document the findings.
- You have a central action plan in place to take forward the outputs from data protection and information governance audits.

Can you answer yes to the following questions?

- Do staff adhere to the external standards as claimed?
- Are they aware of a range of suitable external tools?
- Are senior managers aware?

Internal audit programme

Internal audit programme

If your organisation has an internal audit programme, it covers data protection and related information governance (for example security and records management) in sufficient detail.

Ways to meet our expectations:

- You monitor your own data protection compliance and you regularly test the effectiveness of the measures you have in place.
- Your organisation regularly tests staff adherence to data protection and information governance policies and procedures.
- You routinely conduct informal ad-hoc monitoring and spot checks.
- You ensure your monitoring of policy compliance is unbiased by keeping it separate from those who implement the policies.
- You have a central audit plan/schedule in place to show the planning of data protection and information governance internal audits.
- You produce audit reports to document the findings.
- You have a central action plan in place to take forward the outputs from data protection and information governance audits.

Can you answer yes to the following questions?

- Could staff explain a sample of actions from the action plan including how they were identified, progressed and closed?
- Do senior management have oversight of the Action Plan?
- Are there appropriate links to a risk management process and register?

Performance and compliance information

Performance and compliance information

My organisation has business targets relating to data protection compliance and information governance and we can access the relevant information to assess against them.

Ways to meet our expectations:

- You have KPIs regarding subject access request (SAR) performance (the volume of requests and the percentage completed within statutory timescales).
- You have KPIs regarding the completion of data protection and information governance training, including a report showing the percentage of staff who complete training.
- You have KPIs regarding information security, including the number of security breaches, incidents and near misses.
- You have KPIs regarding records management, including the use of metrics such as file retrieval statistics, adherence to disposal schedules and the performance of the system in place to index and track paper files containing personal data.

Can you answer yes to the following questions?

- Could staff explain any instances of non-compliance to statutory timescales highlighted in the reports and the actions taken to address the issue?

Use of management information

Use of management information

All relevant management information and the outcomes of monitoring and review activity are communicated to relevant internal stakeholders, including senior management as appropriate. This information informs discussions and actions.

Ways to meet our expectations:

- You have a dashboard giving a high-level summary of all key data protection and information governance KPIs.
- The group(s) providing oversight of data protection and information governance regularly discuss KPIs and the outcomes of monitoring and reviews.
- Data protection and information governance KPIs and the outcomes of monitoring and reviews are discussed regularly by groups at operational level, for example in team meetings.

Can you answer yes to the following questions?

- Could you give examples of information flowing between operational levels and senior management?
- Are staff given appropriate information?
- Do they understand it and are the actions taken clear?