Accountability framework self-assessment report

Your [Mvine Ltd] report

You can use this report to help you determine the next steps your organisation needs to take in order to comply with the accountability principle and to track your progress over time.

It can also work as a communications tool to help you to inform the appropriate individuals in your organisation, such as senior managers, of your current levels of compliance and what further action is needed to improve.

How to use this report

You can download this report as a Word document using the button on the top right corner of the page. The report contains a template for an action plan, which we suggest you complete. If you have an problem downloading the report into a word document please let us know.

You may find it easier to complete the report if you change the page orientation to landscape and turn on table gridlines (for more information, please see the help section of your word processing program).

Alternatively, we have created the Accountability Tracker, which is an excel document for you to complete. This consists of a list of the expectations and a drop down menu where you can reflect the ratings. We have added additional columns for you to populate that we think will help you make an actionable plan for improvement.

When devising improvement actions, we recommend you involve decision makers and people who will implement the actions. Your action plan should be agreed at a sufficient level of seniority with assigned responsibility for its delivery.

- 77: I am likely to be meeting this expectation
- 0: I am likely to be partially meeting this expectation
- 0: I am not likely to be meeting this expectation
- 0: This is not relevant to my organisation

Based on your answers you are meeting more than 75% of our expectations

---

The table below reflects your answers to the self assessment.

Where you have indicated you are likely meeting or partially meeting our expectations we suggested that you record how you doing so.

Where you have indicated you are partially meeting or not meeting our expectation we suggest you record the actions you are taking to meet the expectation and the actions you need to take in order to fully meet it.

There are examples of ways you can meet our expectations in the Accountability Framework

Leadership and oversight

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.

Expectations	Status	Action plan
There is an organisational structure for managing data protection and information governance, which provides strong leadership and oversight, clear	**Meeting expectation**	

reporting lines and responsibilities, and effective information flows.

Meeting expectation

Your organisation makes sure that the DPO’s role is adequately supported and covers all the requirements and responsibilities.

Yes

Is your organisation required to appoint a Data Protection Officer under Article 37 of the General Data Protection Regulations (GDPR)?

Meeting expectation

Your organisation makes sure that the DPO’s role is adequately supported and covers all the requirements and responsibilities.

Meeting expectation

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

Meeting expectation

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

An oversight group provides direction and guidance across your organisation for data protection and information governance activities.	Meeting expectation	
In your organisation, operational level groups meet to discuss and coordinate data protection and information governance activities.	Meeting expectation	

Policies and procedures

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.

Expectations	Status	Action plan
Your organisation's policies and procedures provide your staff with enough direction to understand their roles and responsibilities regarding data protection and information governance.	Meeting expectation	

Meeting expectation

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

Meeting expectation

Staff are fully aware of the data protection and information governance policies and procedures that are relevant to their role.

Meeting expectation

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

Training and awareness

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.

Expectations	**Status**	**Action plan**
You have an all-staff data protection and information governance training programme	**Meeting expectation**	
Your training programme includes induction and refresher training for all staff on data protection and information governance.	**Meeting expectation**	
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.	**Meeting expectation**	
Your organisation can demonstrate that staff understand the training. You verify their understanding and monitor it appropriately	**Meeting expectation**	

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.	Meeting expectation	

Individuals’ rights

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.

Expectations	Status	Action plan
You inform individuals about their rights and all staff are aware of how to identify and deal with both verbal and written requests.	Meeting expectation	
You have appropriate resources in place to handle requests from individuals about their personal data.	Meeting expectation	

Your organisation logs receipt of all verbal and written requests from individuals and updates the log to track the handling of each request.	Meeting expectation
You deal with requests from individuals in a timely manner that meets individual expectations and statutory timescales.	Meeting expectation
Your organisation monitors how your staff handle requests and you use that information to make improvements.	Meeting expectation
Your organisation has appropriate systems and procedures to change inaccurate information, add additional information to incomplete records or add a supplementary statement where necessary.	Meeting expectation
You have appropriate methods and procedures in place within your organisation to erase, suppress or otherwise stop processing personal data if required.	Meeting expectation

Your organisation has appropriate methods and procedures in place to restrict the processing of personal data if required.	**Meeting expectation**
Individuals are able to move, copy or transfer their personal data from your organisation to another securely, without affecting the data.	**Meeting expectation**
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.	**Meeting expectation**
Your organisation has procedures to recognise and respond to individuals' complaints about data protection, and individuals are made aware of their right to complain.	**Meeting expectation**

Transparency

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.

Expectations	Status	Action plan
Your organisation's privacy information or notice includes all the information required under Articles 13 and 14 of the GDPR.	**Meeting expectation**	
You have a recorded procedure to make sure that privacy information is provided to individuals at the right time, unless an exemption applies.	**Meeting expectation**	
Your organisation provides privacy information to individuals that is: • concise; • transparent; • intelligible; • clear; • uses plain language; and • communicated in a way that is effective for the target audience.	**Meeting expectation**	

Meeting expectation

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

Meeting expectation

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

Meeting expectation

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

Meeting expectation

You are open about how you use personal data, and offer tools to support transparency and control, especially when processing children’s personal data.

Records of processing and lawful basis

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.

Expectations	Status	Action plan
Your organisation frequently carries out comprehensive data mapping exercises, providing a clear understanding of what information is held and where.	Meeting expectation	
Your organisation has a formal, documented, comprehensive and accurate Record of Processing Activities (ROPA) based on a data mapping exercise, that is reviewed regularly.	Meeting expectation	
Your ROPA contains all the relevant requirements set out in Article 30 of the GDPR.	Meeting expectation	
Your organisation's ROPA includes links to other relevant documentation as a matter of good practice.	Meeting expectation	

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).	**Meeting expectation**
You make information about the purpose of the processing and the lawful basis publicly available. This is easy to locate, access and read.	**Meeting expectation**
You comply with the GDPR’s consent requirements.	**Meeting expectation**
You proactively review records of previously gathered consent, which demonstrates a commitment to confirming and refreshing the consents.	**Meeting expectation**
Your organisation has effective systems in place to conduct risk-based age checks and,	**Meeting expectation**

where required, to obtain and record parental or guardian consent.	Meeting expectation	
Does your organisation rely on legitimate interest for the processing of personal data?	This does not apply to my organisation.	

Contracts and data sharing

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.

Expectations	Status	Action plan
Your organisation's policies and procedures make sure that you appropriately manage data sharing decisions.	Meeting expectation	

You arrange and regularly review appropriate data sharing agreements with parties with whom you regularly share personal data.	**Meeting expectation**
Your organisation has procedures in place to make sure that restricted transfers are made appropriately.	**Meeting expectation**
You have appropriate procedures in place regarding the work that processors do on your behalf.	**Meeting expectation**
All of your controller-processor contracts cover the terms and clauses necessary to comply with data protection law.	**Meeting expectation**
You carry out due diligence checks to guarantee that processors will implement appropriate technical and organisational measures to meet GDPR requirements.	**Meeting expectation**

Your organisation reviews data processors' compliance with their contracts.	**Meeting expectation**
Your organisation considers 'data protection by design' when selecting services and products to use in data processing activities.	**Meeting expectation**
Your organisation proactively takes steps to only share necessary personal data with processors or other third parties.	**Meeting expectation**

Risks and data protection impact assessments

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.

Expectations	Status	Action plan
Your organisation has appropriate policies, procedures and measures to identify, record and manage information risks.	Meeting expectation	
You take a 'data protection by design and by default' approach to managing risks, and, as appropriate, you build Data Protection Impact Asessment (DPIA) requirements into policies and procedures.	Meeting expectation	
You understand whether a DPIA is required, or where it would be good practice to do one. There is a clear DPIA policy and procedure.	Meeting expectation	
DPIAs always include the appropriate information and are comprehensively documented.	Meeting expectation	

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

Records management and security

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.

Expectations	Status	Action plan
You have minimum standards for the creation of records and effective mechanisms to locate and retrieve them.	Meeting expectation	
You have appropriate security measures in place to protect data that is in transit, data you receive or transfer to another organisation.	Meeting expectation	

You have procedures in place to make sure that records containing personal data are accurate, adequate and not excessive.	Meeting expectation
You have an appropriate retention schedule outlining storage periods for all personal data, which you review regularly.	Meeting expectation
You cover methods of destruction in a policy and they are appropriate to prevent disclosure of personal data prior to, during or after disposal.	Meeting expectation
You have an asset register that records assets, systems and applications used for processing or storing personal data across your organisation.	Meeting expectation
You identify, document and implement rules for the acceptable use of software (systems or applications) processing or storing information.	Meeting expectation

You limit access to personal data to authorised staff only and regularly review users’ access rights.	**Meeting expectation**
You prevent unauthorised access to systems and applications.	**Meeting expectation**
You have appropriate mechanisms in place to manage the security risks of using mobile devices, home or remote working and removable media.	**Meeting expectation**
You secure physical business locations to prevent unauthorised access, damage and interference to personal data.	**Meeting expectation**

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

Breach response and monitoring

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.

Expectations	Status	Action plan
You have procedures in place to make sure that you detect, manage and appropriately record personal data incidents and breaches.	Meeting expectation	
You have procedures to assess all security incidents and then report relevant breaches to the ICO within the statutory time frame.	Meeting expectation	

You have procedures to notify affected individuals where the breach is likely to result in a high risk to their rights and freedoms.	**Meeting expectation**
You review and monitor personal data breaches.	**Meeting expectation**
Your organisation has undertaken an external data protection and information governance audit or other compliance checking procedure.	**Meeting expectation**
Your internal audit programme covers data protection and information governance (for example security and records management) in sufficient detail.	**Meeting expectation**
Your organisation has business targets relating to data protection compliance and information governance, and you can access the relevant information to assess against them.	**Meeting expectation**

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.	**Meeting expectation**