27 November 2019

Accountability toolkit

The General Data Protection Regulation (GDPR) introduced an accountability principle, which requires data controllers to demonstrate their compliance with the law through internal data protection measures and practices. These could, and in some circumstances must, include:

- implementing data protection policies;
- recording your processing;
- taking a data protection by design and by default approach;
- having written contracts in place with processors;
- implementing appropriate security measures;
- recording and, where necessary, reporting data breaches;
- appointing a data protection officer;
- establishing processes for handling data subject rights' requests; and
- carrying out data protection impact assessments.

We want to create a toolkit to help organisations to assess whether they have appropriate and effective internal data protection governance arrangements in place and to help them demonstrate their compliance to the ICO, the public, or a business customer.

This is the first stage of our consultation process, where we are looking for a wide range of views from organisations and individuals, across all sectors and organisational sizes. We want to hear from those who have responsibility for data protection and particularly would like to hear about:

- your current practice regarding accountability;
- what might lead to improvements;
- how we can support you in designing your own accountability framework; and
- what scope and structure may be most helpful.

You can respond to this consultation via our online survey or you can download the document and email it to: accountability@ico.org.uk

Alternatively, print off the document and post to:

Accountability toolkit snap survey
Assurance Department
Information Commissioner's Office
Wycliffe House
Water Lane
Wilmslow

Cheshire
SK9 5AF

You can find guidance about accountability in our Guide to the GDPR. If you would like further information about the consultation, please email the accountability@ico.org.uk team.

Please send us your response by Monday 9 December.

Privacy statement

For this survey, we will publish all responses received from organisations but we will remove any personal data before publication. We will not publish responses received from respondents who have indicated that they are an individual acting in a private capacity (e.g. a member of the public). For more information about what we do with personal data see our privacy notice.

Existing practise

NB: Your responses to this survey will be used to help us with our work on accountability only. The information will not be used to consider any regulatory action, and you may respond anonymously should you wish.

Q.1 Please score your understanding of the internal data protection measures and practices you need to put in place to ensure effective compliance with data protection law

Click here to select an option ↓

Q.2 To what extent would you agree with the following statements?

Q2a. My organisation has appropriate and effective internal data protection measures and practices in place to ensure compliance with all aspects of applicable data protection law.

Click here to select an option ↓

Q.2b My organisation could demonstrate its data protection compliance effectively to the ICO, the public or a business customer.

Click here to select an option ↓

Q.3 We want to know how you developed the internal measures and practices that you use to demonstrate compliance.

Please indicate below if you used any of the external sources of information to guide your understanding.

Please click all that apply.

☐ ICO ***Guide to the GDPR***
☐ ICO ***data protection self assessment*** or ***small business owners and sole traders' check list***
☐ A third party privacy management framework
☐ Legal advice
☐ Consultant
☐ Training
☐ I didn't use external sources of information
☐Other - _______________

Q.4 Please highlight the three resources you've found most useful.
One indicates the most useful.

Rank	**Source**	**Why?**
1 (Most useful)	ICO data protection self-assessment or SME and sole traders' check list	*The materials are practical as they enable respondents to answer concrete questions and to assess their level of maturity in real time while identifying areas of improvement. The layered approach enables providing more information to the respondent if needed.*
2	A third party privacy management framework	*The CIPL Accountability Framework complements the ICO assessment framework. The CIPL model enables organisations to design and structure their privacy programs according to the key elements of accountability (Leadership and Oversight, Risk Assessment, Policies and Procedures, Transparency, Training and Awareness, Audit and Monitoring and Response and Enforcement). The CIPL Accountability Framework enables the translation of the GDPR requirements into calibrated, risk-based, verifiable, transparent and enforceable corporate governance, practices and controls, supported by technology tools. The CIPL Accountability Framework also enables continuous improvement of the privacy program.*
3	Choose an item.	

Q.5 Please highlight the three areas you found the most challenging when putting in place and maintaining systems to manage your compliance with data protection.

One indicates the most difficult.

Rank	Source	Why?
1 (Most difficult)	Choose an item.	
2	Choose an item.	
3	Choose an item.	

Improvements

Q.6 Please score the following statements.

Q.6a My organisation could improve the appropriateness and effectiveness of its internal data protection governance arrangements.

Click here to select an option ↓

Please explain:

Q.6b My organisation could improve its readiness to demonstrate its compliance with data protection law to the ICO, the public or business customer.

Click here to select an option ↓

Please explain:

Q.6c There is enough information and support to help people understand the internal data protection measures or practices that they should put in place to achieve data protection compliance.

Click here to select an option ↓

Please explain:

Q.6d There is enough information and support to help people understand how to **evidence** their data protection compliance.

Click here to select an option ↓

Please explain:

Scope

The ICO accountability toolkit would support organisations to implement appropriate and effective data protection measures and practices and to them demonstrate them. The toolkit is not intended to replace a full and proper consideration of the legal requirements for data protection compliance.

It would be more than high-level principles, but it would not go beyond the measures and practices that we may reasonably expect to find in any accountable organisation based on our experience.

It would *not* act as an exhaustive checklist, but as a prompt for organisations to take responsibility for designing their own accountability framework. We would expect organisations to scale the level of data protection according to their circumstances, to take into account the size of their organisation, the nature of their processing and the level of risk. As far as reasonable, we would consider certain adaptations for small to medium enterprises (SMEs).

At this stage, the toolkit would not include sector specific measures or consider specific requirements under part 3 (law enforcement processing) or part 4 (intelligence services processing) of the Data Protection Act 2018.

Q.7 Do you agree with the proposed scope of an ICO accountability toolkit?

Yes

Please explain:

The ICO approach is aligned with CIPL's accountability framework. The ICO toolkit should be limited to providing a general framework containing principles and core elements of accountability as well as examples of accountable practices and should leave organisations with the task of devising their own programs. Effective protection of personal data and sound allocation of resources are better achieved when risk assessments, policies, controls, trainings, audits and responses are aligned to the privacy risk profile, business, culture, and size of the organisation.

Q.8 How do you think we could support small to medium enterprises (SMEs) to demonstrate the extent to which they have effective systems of data protection governance and accountability in place?

Please explain:

The ICO accountability toolkit should provide concrete examples of measures, practices, tools or activities as well as materials that are scalable for smaller organisations. It should also understand from these organisations what specific accountability measures, practices, tools or activities are not scalable and work with them to come up with workable solutions that enable effective data protection and accountability in practice. This is key when these organisations interact with their business partners and data subjects.

Structure

We propose to create an ICO accountability toolkit divided into several main categories. Below are the categories we are currently considering. We have included a brief description of the type of information that each category would cover.

Category	**Description**
1 Management structures	Data protection and information governance responsibilities throughout an organisation including accountability.
2 Policies, procedures and training	Appropriate data protection policies, procedures and training across data protection and information governance.
3 Monitoring and revision	Internal and external auditing of data protection compliance and information governance, regular

	internal monitoring of procedures and practices, and making revisions where required.
4 Contracts and third parties	Contracts including those: with third parties processing personal data; evidencing data transfer mechanisms; and involving data sharing. Policies and procedures regarding contracts involving personal data.
5 Records of processing activities	Procedures and records to support accurate and effective documentation of data processing, in line with GDPR requirements.
6 Lawful basis	Procedures about the lawful basis for processing personal data and special category personal data, and about consent (especially regarding children).
7 Transparency	Procedures are in place to ensure that transparent information is provided in a timely way, using succinct, clear and plain language, and is updated where relevant.
8 Data protection impact assessments	Policies and procedures regarding data protection impact assessments, which are embedded in wider policies and procedures,
9 Data protection by design and by default	Policies, procedures and a privacy culture embedding data protection in all activities involving personal data from beginning to end (such as the design of services or products), and which uphold data minimisation.
10 Security	Policies, procedures and security controls to ensure the security of personal data including evidence of how systems are maintained and updated as required.
11 Data breaches	Policies and procedures regarding the detection, investigation, recording and reporting of breaches, where necessary.
12 Data subjects' rights	Policies and procedures to handle requests for information and other individual rights

Q.9 Are the proposed categories for the accountability toolkit suitable?

Please consider the number of categories, the names of the categories, the scope of the categories, the order of the categories and if there are areas of data protection governance that don't fit into the current categories.

No

Please explain:

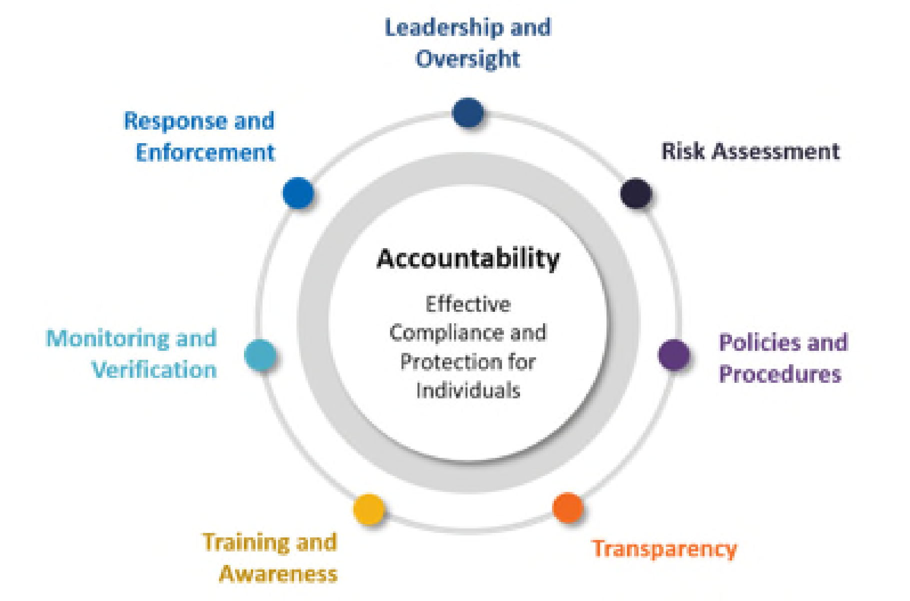
- To be easily understandable and workable, the number of categories should be limited (12 categories may be too much for easy grasp by organisations and their team members in charge of implementing the privacy program).

- There are many categories that relate to the implementation of policies and procedures (data subject rights, data breaches, security, data protection by design and by default, DPIA, lawful basis, record of processing). CIPL would propose to have an overarching category for policies and procedures that contains the policies and procedures an organisation may have to put in place.

- There should be a category on risk assessment to include (1) an overall risk assessment of the organisation on the basis of its core activities; (2) a risk assessment triage to identify the high risk processing within the organisation and; (3) DPIAs in case of high risk processing.

- There should be a specific category on training and awareness - The role of the DPO (or equivalent in case no mandatory DPO is required under GDPR) is key in implementing an accountability framework. It should be clearly mentioned in the toolkit (most likely in the first category on management structures).

- Please see below the CIPL Accountability Framework that could be used as a basis



CIPL "Accountability Wheel" – Universal Elements of Accountability

For each category, we would set out:

1) Our reasonable **expectations** .
These would cover the internal measures and practices we would expect an organisation to use to evidence its accountability - and then for each expectation;

2) **Indicators of effectiveness**
These are how organisations may demonstrate that the expectations are being met.

The expectations and indicators will be informed by our supervisory activity such as audits, investigations, and casework examining organisations' compliance.

As set out earlier, the expectations and indicators are not an exhaustive checklist. Organisations will need to consider how the expectations and indicators apply to their work and what documentation and evidence they would need to have in place given the type of processing they are undertaking.

Where an expectation or indicator relates to a clear requirement set out in the GDPR or the Data Protection Act 2018 this will clearly be indicated.

Here is an indicative example regarding **management structures**:

Expectation 1: Management framework

There is a clear management structure setting out data protection and information governance responsibilities, including accountability, from the highest management level down.

Indicators of effectiveness

- There is an organisational chart showing the reporting lines and flow of information between the highest level of management, audit committee and key committees / groups covering information governance management.
- The framework is clearly outlined in policy documentation.
- Overall responsibility for information governance has been allocated at the highest management level and it can be shown that management is actively engaged.
- Job descriptions for information governance personnel clearly outline their responsibilities and reporting lines.
- Information governance responsibilities are understood by staff in these roles.

Expectation 2. Data Protection Officer (DPO)

Where applicable, you have appointed a Data Protection Officer in accordance with Article 37 GDPR.

Indicators of effectiveness

- The DPO monitors compliance with the GDPR and other data protection laws, data protection policies, awareness-raising, training, and audits.
- There are processes in place to ensure the DPO is involved, in a timely manner, in all issues relating to data protection.
- The DPO is sufficiently well- resourced to be able to perform their tasks.
- There is evidence to confirm that advice and information provided by the DPO is taken into account.
- The DPO has and maintains expert knowledge of data protection law and practices. Records of the DPO’s training and learning are readily available.

- Where an organisation is not required to appoint a DPO, the decision is documented and appropriate.
- Where an organisation is not required to appoint a DPO, responsibility for DP compliance has been assigned appropriately and there are sufficient staff and resources available to enable the organisation to comply with its obligations under the GDPR

Expectation 3. The DPO

The DPO has operational independence and appropriate reporting mechanisms are in place to the highest management level

Indicators of effectiveness

- The DPO has the required independence to perform their tasks.
- The DPO has direct access to give advice to senior managers who are making decisions about personal data processing and they can raise concerns with the highest level of management.
- There is no conflict of interest for any other tasks or duties the organisation has assigned to the DPO.
- There is evidence to confirm that the DPO provides regular updates to the highest level of management on data protection compliance.

Expectation 4. Operational roles and responsibilities

Operational roles and responsibilities have been assigned to support the day to day management of all aspects of data protection.

Indicators of effectiveness

- There are operational roles in place and responsibilities are assigned to ensure the effective management of all records, e.g., in job descriptions and details of how this is operationalised are in place.
- There are operational roles in place and responsibilities are assigned to ensure the effective security of information, e.g., in job descriptions and procedures are in place to make certain these measures are working in practise.
- There are operational roles in place and responsibilities are assigned to assist with compliance with data protection legislation, e.g., in job descriptions. There are procedures in place which ensure those responsible keep their knowledge of data protection legislation up to date.
- There is a network of support, or nominated data protection leads in appropriate departments to help implement and support data protection policies at the local level.

Expectation 5. Information management group

There is a management group in your organisation responsible for the oversight of data protection and information governance.

Indicators of effectiveness

- The group meets and is attended on a regular basis by key information governance personnel.
- The group is chaired by an appropriately senior role e.g. a Senior Information Risk Owner or DPO.
- There are terms of reference in place outlining the aims of the group and records of meeting minutes including actions to be made that are documented upon completion.
- There is a full range of data protection related topics covered by the group including data protection key performance indicators, issues and risks.
- There is a work or action plan in place for the group, which is regularly considered, reviewed and updated with evidence to support such activity readily available.

- Outputs (regarding issues and risks) feed into committees and meetings at the highest management level.

Expectation 6. Operational meetings

There are regular operational meetings to discuss data protection and information governance.

Indicators of effectiveness

- The group(s) meet and are attended regularly by relevant personnel.
- There is evidence of meeting minutes taken and action plans in place that demonstrate when actions have been taken or how they are being progressed.
- The agenda(s) demonstrate appropriate data protection related matters are discussed regularly.
- Outputs (regarding issues and risks) feed into the main information management group.

Q.10 Do you think it is helpful to structure the toolkit in the above way?

First by setting out a high-level general expectation and then setting out what you may use to indicate that the expectation is being met?

Yes

Please explain:

The expectation/indicator model would be very helpful for companies to structure and devise their program and understand the ICO's possible expectations. It is essential however that this model remains flexible: ***First****, the ICO should make it very clear that, absent a clear GDPR obligation (for instance, appointment of a DPO, record of processing, mandatory DPIA), these are just examples that need to be tailored to each organisation's risk, size, geographical scope, activity, sector and culture.* ***Second****, this means that the indicators of effectiveness should not be assessed by application of rigid and one-size-fits-all criteria, but should be assessed flexibly depending on context and the specific risks of the processing. For instance, in expectation 6 "Operational Meetings", the understanding of "regularly" ("The group(s) meet and are attended* ***<u>regularly</u>*** *by relevant personnel" or "The agenda(s) demonstrate appropriate data* *protection related matters are discussed <u>regularly</u>") should differ for high-risk data driven organisations and low risk traditional "brick and mortar" organisations.*

Q.11 Considering the example above for ‘management structures’, what are your views about the level of detail provided?

There is just the right amount of information

Please explain:

The examples of expectations and indicators are very detailed. As long as they are clearly presented as <u>possible non-exhaustive examples</u> that organisations may use to demonstrate accountability, they will be very useful to organisations to devise their own program. Organisations will be able to fully replicate or pick and choose (except for clear GDPR obligations) the solutions adapted to enable effective data protection and will still be able to come up with their own “bespoke” solutions. There should be no presumption of non-compliance if the organisation chooses not to rely on one or several of the ICO examples as long as effective data protection tailored to the risk is in place within the organisation.

Q.12 Do you think that there might be any unintended consequences or challenges as a result of our proposed approach to the accountability toolkit?

Please explain:

The expectations and indicators should be clearly presented as <u>possible non-exhaustive examples</u> to avoid that organisations understand the ICO’s approach as the only possible approach and that all elements should be implemented within organisations in a comprehensive and rigid manner regardless of risk, size, activity and profile. There may also be a risk of “over-implementation” of the requirements for fear of a possible non-compliance and sanction by the ICO.

Q.13 We are looking at a number of different ways of presenting the toolkit, each with slightly different features. To guide our design, please rank the following features from the most important to least important.

Ability to use the toolkit in stages	5

Ability to download the toolkit and use it offline	4
Ability to generate a report of your responses to the toolkit	3
Ability to focus on just the required elements from the accountability toolkit that are applicable to your business. *For example, not everyone has to appoint a DPO under the GDPR*	1 (Most important)
Ability to rate indicators as incomplete, started or complete	2
Ability to suggest further ICO guidance or external information based on your responses.	7 (least important)
Other: *Ability to use the toolkit in the context of an application for BCR, Certification or Code of Conduct with the ICO or another DPA*	6

Q.14 We want to create an accountability toolkit that will support organisations to develop their own accountability frameworks.

Their framework should demonstrate how far they can monitor their compliance through effective systems of governance and accountability.

Ultimately, their framework should be able to prove their compliance to the ICO, the public and/or business customer.

Overall, how helpful do you think our proposed accountability toolkit would be in achieving this aim?

Very helpful

Q.15 If you wish to make any other comments to help us with our work on accountability, including comments about any other means by which we could offer support regarding the accountability principle, please use the box below.

CIPL has worked extensively on developing an Accountability Framework enabling effective data protection. Our latest papers and work are available here:

https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_white_paper_on_organisational_accountability_%E2%80%93_past_present_and_future.pdf

https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_white_paper_-_organizational_accountability_in_light_of_ftc_consent_orders__13_november_2019_.pdf

https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_accountability_q_a__3_july_2019_.pdf

https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/introduction_to_two_new_cipl_papers_on_the_central_role_of_organisational_accountability_in_data_protection.pdf

https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_accountability_paper_1_-_the_case_for_accountability_-_how_it_enables_effective_data_protection_and_trust_in_the_digital_society.pdf

https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_accountability_paper_2_-_incentivising_accountability_-_how_data_protection_authorities_and_law_makers_can_encourage_accountability.pdf

About you

This section is optional – telling us who you are will help us to understand your needs more clearly as we design our guidance products, but you may answer the survey anonymously should you wish.

Q.16 On whose behalf are you responding?
(Please delete as appropriate)

- My own
- On behalf of an organisation (*Center for Information Policy Leadership*)
- On behalf of a sector or group (please specify)

Q.17 What is your role in your organisation?

(Please delete as appropriate)

Other (*Director of Privacy Policy*)

Q.18 What sector do you work in?

Please delete as appropriate

Public

Private

Third/Charity/Voluntary

Combination of the above (Think Tank)

Q.19 How did you find out about this consultation?

ICO blog
Other: _______________

Q.20 As mentioned above, we will be doing further consultation on the accountability toolkit. Please indicate if you would be happy to take part in the next stages of this consultation.

Yes

Q.21 If YES, please let us know how you would like to be contacted.

Q.21A. Name: *Bojana Bellamy or Nathalie Laneret*

Q.21B. Email (optional):*bbellamy@huntonAK.com or nlaneret@huntonAK.com*

Q.21C. Phone (optional): *+44 7876577774 or +32 499516801*