CIPL
Centre for Information Policy Leadership
HUNTON ANDREWS KURTH

ico.
Information Commissioner's Office

Centre for Information Policy Leadership (CIPL) and Information Commissioner's Office (UK ICO)

Joint Roundtable on the ICO's Accountability Toolkit

- Under Chatham House Rule -

Hunton Andrews Kurth, Meeting Rooms 3 & 4
30 St Mary Axe
London EC3A 8EP

Tuesday, 11 February 2020 | 10:30 AM – 4:00 PM (lunch provided)

AGENDA

The UK ICO is currently developing an Accountability Toolkit that aims to help organisations assess whether they have appropriate and effective internal data protection governance arrangements in place, and to help them demonstrate their GDPR compliance to the UK ICO, the public, or a business customer. This toolkit is going through a public consultation process, which is currently being supplemented by this roundtable.

10:00 **Registration and coffee**

10:30 **Opening Remarks**

The UK ICO and CIPL present their work on accountability, namely the UK ICO Accountability Toolkit, the CIPL Accountability Framework and Accountability Mapping Project.

- **Ian Hulme**, Director of Regulatory Assurance, ICO
- **Chris Taylor**, Head of Assurance, ICO
- **Bojana Bellamy**, President, CIPL

10:50 **Session 1. Defining Accountability**

Roundtable participants will explore the meaning, structure and key elements of accountability, drawing upon the previous presentation about the CIPL Accountability Framework and the UK ICO Accountability Toolkit.

Breakout session – Exercise 1: see Appendix for description and discussion questions. This will be followed by group-wide discussions on:

- *What are the core elements of accountability?*
- *Should the core elements of accountability be applied to all organisations, in all cases? Consider the concept of scalability in the context of data processors, public sector and SMEs, also.*
- *What is the relation between the ICO Accountability Toolkit and the CIPL Accountability Framework?*

- Moderator: **Bojana Bellamy**, President, CIPL
- Setting ICO expectations**:**
  Elizabeth Archer, Principal Policy Adviser, ICO
  Lorna Cropper, Secondee, ICO

12:20 **Lunch**

13:00 **Session 2. Measuring and Demonstrating Accountability**

CIPL will present the preliminary results of its Accountability Mapping project. ICO will talk about the outline of its structure for the Accountability Toolkit: categories; expectations and indications of effectiveness.

Breakout session – Exercise 2: see Appendix for description and discussion questions. This will be followed by group-wide discussions on:

- *How can organisations measure that their privacy programme is effective? Are there any indicators of effectiveness of KPIs of accountability that organisations could use? (e.g. time to respond to a DSR or to handle data breach, number of complaints)*
- *How can organisations use the reporting function of the ICO Accountability Toolkit and/or the CIPL Accountability Framework internally and externally (to their Board, internal Risk and Audit Committees, shareholders, investors, DPAs, business partners, joint-controllers, JVs, data subjects, general public, etc.)?*
- *What is the role of the ICO Accountability Toolkit and of the CIPL Accountability Framework for global organisations when they need to demonstrate compliance and accountability with various laws and regulations of different countries?*
- *What is the link between privacy programmes (including the ICO Accountability Toolkit and of the CIPL Accountability Framework), BCR and other certifications (e.g. CBPR, ISO standards, etc.) in their efforts to demonstrate accountability internally and externally?*
- *How much and how far should organisations be documenting their decisions and data processing activities?*

- Moderator: **Nathalie Laneret**, Director of Privacy Policy, CIPL
- Setting ICO expectations**:**
  Elizabeth Archer, Principal Policy Adviser, ICO
  Chris Taylor, Head of Assurance, ICO

14:30 **Session 3. "Incentivising" Accountability and the Potential Visual Design of the ICO's Accountability Toolkit**

Participants will discuss how organisations can build a culture of accountability and encourage their highest level of management to give sufficient resources to data protection. They will also discuss how regulators should incentivise accountability and ensure that it becomes a market standard and enabler of interoperability between different jurisdictional rules.

Breakout session – Exercises 3 and 4: see Appendix for description and discussion questions. This will be followed by group-wide discussions on:

- *How can the ICO promote its Accountability Toolkit outside of the UK? How can regulators promote interoperability between different privacy regimes globally?*
- *How can the ICO and other DPAs incentivise and encourage accountability? Can the ICO show-case also good practices for accountability?*
- *Should regulators take a different approach to incentivising accountability depending on the size and type of organisations?*
- *What are innovative ways that industry can use to share best accountability practices among peers? Are there any challenges?*

❖ Moderator: **Bojana Bellamy**, President, CIPL
❖ Setting ICO expectations**:**
Elizabeth Archer Principal Policy Adviser, ICO
Lorna Cropper, Secondee, ICO

15:55 **Wrap up, next steps and voting on ICO accountability pilot and best practice show-case**

❖ **Bojana Bellamy**, President, CIPL

16:00 **End of roundtable**

Appendix - Description of exercises undertaken during the breakout sessions

All breakout sessions will be followed by regrouping participants for 10 min feedback.

Break out - Exercise 1: Category Scope

In your group you have a copy of the main category areas the ICO is proposing to cover in the toolkit, and a brief description of the expected content.

In our consultation exercise many organisations fed back that these seemed about right – however there were plenty of suggestions of other ways to 'cut it'.

We'd like to explore this in more depth with you. For example:

- Are any major categories missing from the ICO Accountability Toolkit?
- Do we need to streamline or rearrange the categories to make it easier to digest or use?
- Should Data Protection Impact Assessments be part of data protection by design and by default?
- Should lawful basis sit within records of processing?
- Should transparency stand alone or be integrated into other areas?

Break out - Exercise 2: Challenging Areas

Our consultation exercise told us that three of the main areas that controllers find challenging in demonstrating their accountability are:

- Contracts and third parties
- Records of processing
- Policies, procedures and training

In your groups you have working draft content of what expectations and indicators might look like in the above areas - that address the governance, management and accountability arrangements. These are work in progress – for example, at present the contracts category area is focussed on 'processor contracts' only and may well need to be broadened to include transfers and data sharing.

Remember that the toolkit is aimed at as wide a set of organisations as possible recognising that all organisations of all sizes may well need to take it and adapt how they implement.

Please take some time to look through draft content in your groups and answer the following questions**:**

- What is considered acceptable evidence of compliance within each category of the ICO Accountability Toolkit?
- Are there any fundamental areas missing?
- Is the general scope of the areas right?
- Does the level of detail in the expectations and indicators seem about right?

- What other guidance products might be most helpful in these areas? (e.g. case studies, worked scenarios, other products)?

Remember: we are seeking to identify the common key practical steps that enable organisations to demonstrate their accountability and manage these areas NOT every item that may need to be in place in any context.

Break out - Exercise 3: Supporting an accountability culture

We'd like to explore with you in more detail the role that a toolkit like this might play in creating the culture of accountability the ICO wants to see. And we know that getting there is about more than just the creation of a toolkit like this: how your internal culture, governance structures, management processes and day to day operational challenges play out are all factors that we need to consider.

- How might organisations use this toolkit in creating a culture of accountability?
- Does the toolkit strike the balance between encouraging organisations to take ownership and consider accountability within the context of their own organisation and the ways they are using personal data vs telling people what to?
- Will the toolkit be useful in discussion with 'top management'? How can the ICO help DPOs get management buy-in for accountability?
- How can privacy compliance frameworks (including the ICO Accountability Toolkit) support organisations with corporate sustainability and making decisions concerning corporate investments?
- How would you integrate this toolkit into your existing practices?
- How might the ICO enhance the toolkit over time to further support a culture of accountability?
- What other actions might ICO consider taking in this area?

Exercise 4: Visual Design and Presentation of the UK ICO's Accountability Toolkit

Reflecting on the information you have heard this morning about what may be possible for an initial release of the toolkit, how do you think the information can best be presented and made available?

- How well did the option presented meet your expectations and why?
- Do you think any important features are missing?
- Which features do you think will be most helpful?
- What wouldn't be helpful?