Centre for Information Policy Leadership
HUNTON ANDREWS KURTH

Information Commissioner's Office

Joint CIPL-ICO Roundtable on the

ICO's Accountability Toolkit

London, 11 February 2020

Agenda

- 10:30 – 10:50 **Opening Remarks**
  Ian Hulme, Director of Regulatory Assurance, ICO
  Chris Taylor, Head of Assurance, ICO
  Bojana Bellamy, President, CIPL
- 10:50 – 12:20 **Session 1. Defining Accountability**
  Moderator: Bojana Bellamy, President, CIPL
  Setting ICO expectations: Liz Archer, Principal Policy Adviser and Lorna Cropper, Secondee, ICO
- 12:20 – 13:00 **Lunch**
- 13:00 – 14:30 **Session 2. Measuring and Demonstrating Accountability**
  Moderator: Nathalie Laneret, Director of Privacy Policy, CIPL
  Setting ICO expectations: Elizabeth Arche, Principal Policy Adviser, ICO
- 14:30 – 15:55 **Session 3. "Incentivising" Accountability and the Potential Visual Design of the ICO's Accountability Toolkit**
  Moderator: Bojana Bellamy, President, CIPL
  Setting ICO expectations: Chris Taylor, Head of Assurance, ICO
- 15:55 – 16:00 **Wrap-Up**

Centre for Information Policy Leadership
HUNTON ANDREWS KURTH

Opening Remarks

Ian Hulme, Director of Regulatory Assurance, ICO

Chris Taylor, Head of Assurance, ICO

Bojana Bellamy, President, CIPL

Disclaimer *- These slides have been prepared by CIPL. They are not endorsed by, and do not represent the views of, the Information Commissioner's Office.*

Welcome

CIPL - A Global Privacy and Security Think Tank

BRIDGING REGIONS | BRIDGING INDUSTRY & REGULATORS | BRIDGING PRIVACY AND DATA DRIVEN INNOVATION

ACTIVE GLOBAL REACH

90+ Member Companies

5+ Active Projects & Initiatives

20+ Events annually

15+ Principals and Advisors

We **INFORM** through publications and events

We **NETWORK** with global industry and government leaders

We **SHAPE** privacy policy, law and practice

We **CREATE** and implement best practices

ABOUT US

- The Centre for Information Policy Leadership (CIPL) is a global privacy and security think tank
- Based in Washington, DC, Brussels and London
- Founded in 2001 by leading companies and Hunton Andrews Kurth LLP
- CIPL works with industry leaders, regulatory authorities and policy makers to develop global solutions and best practices for data privacy and responsible use of data to enable the modern information age

Twitter.com/the_cipl

https://www.linkedin.com/company/centre-for-information-policy-leadership

www.informationpolicycentre.com

2200 Pennsylvania Ave NW
Washington, DC 20037

Park Atrium, Rue des Colonies 11
1000 Brussels, Belgium

30 St Mary Axe
London EC3A 8EP

Centre for Information Policy Leadership
HUNTON ANDREWS KURTH

Opening Remarks – ICO's presentation

Ian Hulme, Director of Regulatory Assurance, ICO

Chris Taylor, Head of Assurance, ICO

Disclaimer *- These slides have been prepared by CIPL. They are not endorsed by, and do not represent the views of, the Information Commissioner's Office.*

Introduction

- What is accountability under the GDPR?
- What's new?
- Why is it important? – a little context
- Why do we want to create an ICO Accountability Toolkit?
- How would it be used?
- How could the ICO measure success?

What is accountability under the GDPR?

1) Makes organisations responsible for complying with the GDPR

2) Says that they must be able to demonstrate compliance.

It means putting in place appropriate and effective internal data protection governance arrangements.

Examples

1. Adopting and implementing data protection policies and procedures
2. Taking a DP by design and by default approach
3. Putting written contracts in place for third party processing
4. Maintaining records of processing
5. Recording and where necessary reporting data breaches
6. Carrying out Data Protection Impact Assessments
7. Implementing security measures
8. Appointing a Data Protection Officer when required

What's new?

Accountability is not a new concept – it was already a well-established feature of good governance and many of the GDPR's requirements were either requirements before or good practice BUT

GDPR introduced a specific principle which explicitly places the responsibility at the door of the controller. Controllers must be able to demonstrate their take on compliance.

It aims to ensure that people's rights are better protected. Data protection authorities can take enforcement action in appropriate cases.

Why is it important?

A little context…

- In a 2010 paper called 'The Future of Privacy', the Article 29 Working Party said that data protection requirements are often insufficiently reflected in concrete measures and practices.
- The importance of data protection has increased as a result of: the amount of data that is being handled and transferred; the complexities of technological development; the modern day value of data; and the potentially devastating consequences when something goes wrong.
- Accountability is seen as critical to **minimising the growing risks** and to building and sustaining people's **trust**.

Why do we want to create a toolkit?

PURPOSE

To support organisations to assess whether they have appropriate and effective internal policies, procedures and measures in place to ensure compliance with data protection requirements.

Ultimately, it will help organisations to demonstrate their compliance to us, an individual customer or business partner.

It’s a commitment we made in our Information Rights Strategic Plan and we are clear in our Regulatory Action Policy that a controller’s accountability mechanisms will be taken into account.

Other versions of privacy management frameworks exist but there’s a real opportunity for the ICO to add value and ‘join the dots’ in our regulatory supervision.

What scope is proposed?

Toolkit aimed at as wide a set of organisations as possible while recognising that it will need to be tailored appropriately as part of a risk-based approach.

More than high-level principles but it would not go beyond the practices and measures we would reasonably expect to find in any accountable organisation. It's not intended to be exhaustive.

At this stage – would not include sector-specific measures or requirements under part 3 (law enforcement) or part 4 (intelligence processing) of the DPA 2018.

How would the toolkit be used?

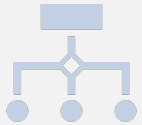
The toolkit would not act as an exhaustive checklist, nor is it intended to replace a full and proper consideration of the legal requirements.

It’s a prompt for organisations to take responsibility for designing their own accountability framework and scaling the level of data protection according to the circumstances such as organisational size; nature of processing; and level of risk.

We’d expect it to be used internally as the basis for investigations, audits and regulatory action in this area.

How could the ICO measure success?

Asking specific, measurable questions in our consultation exercises on likely adoption and utility of the Toolkit and repeating this at later dates;



Use of the Toolkit in case work / investigations; and

Asking data controllers at registration whether they are aware of and consider themselves adherent to the Toolkit and then tracking adoption over time.

Centre for Information Policy Leadership
HUNTON ANDREWS KURTH

Opening Remarks – CIPL's presentation

Bojana Bellamy, President, CIPL

Disclaimer *- These slides have been prepared by CIPL. They are not endorsed by, and do not represent the views of, the Information Commissioner's Office.*

CIPL Accountability Framework

Organisations must be able to demonstrate accountability – internally and externally

Accountability is not static, but dynamic, reiterative and a constant journey

Accountability requires comprehensive privacy programmes that translate legal requirements into risk-based, verifiable and enforceable corporate practices and controls

Company values and business ethics shape accountability

Disclaimer *- These slides have been prepared by CIPL. They are not endorsed by, and do not represent the views of, the Information Commissioner's Office.*

Defining Accountability

Examples of content of privacy management programmes

Leadership and Oversight

- Tone from the top
- Executive oversight
- Data privacy officer/office of oversight and reporting
- Data privacy governance
- Privacy engineers
- Internal/External Ethics Committees

Risk Assessment

- At programme level
- At product or service level
- DPIA for high risk processing
- Risk register
- Risk to organisations
- Risk to individuals
- Records of processing

Policies and Procedures

- Internal privacy rules based on DP principles
- Information security
- Legal basis and fair processing
- Vendor/processor management
- Procedures for response to individual rights
- Other (e.g. Marketing rules, HR rules, M&A due diligence)
- Data transfers mechanisms
- Privacy by design
- Templates and tools for PIA
- Crisis management and incident response

Transparency

- Privacy policies and notices to individuals
- Innovative transparency – dashboards, integrated in products/apps, articulate value exchange and benefits, part of customer relationship
- Information portals
- Notification of data breaches

Training and Awareness

- Mandatory corporate training
- Ad hoc and functional training
- Awareness raising campaigns and communication strategy

Monitoring and Verification

- Documentation and evidence - consent, legitimate interest and other legal bases, notices, PIA, processing agreements, breach response
- Compliance monitoring and testing - verification, self-assessments and audits
- Seals and certifications

Response and Enforcement

- Individual requests and complaints-handling
- Breach reporting, response and rectification procedures
- Managing breach notifications to individuals and regulators
- Implementing response plans to address audit reports
- Internal enforcement of non-compliance subject to local laws
- Engagement/Co-operation with DPAs

Organisations must be able to **demonstrate their own implementation** - internally and externally

Measuring and Demonstrating Accountability

To Whom and How?

To Whom?

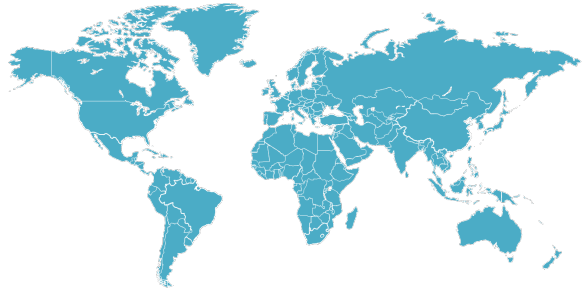
- **Internally** – executives leadership, Board of Directors, shareholders
- **Externally** – business partners, regulators, individuals and civil society

Models of Accountability require:

- Following substantive privacy rules
- Implementation infrastructure
- Verification
- Ability to demonstrate compliance

Global Accountability

- Accountability Elements are present in key laws and regulations around the world.
- Privacy compliance programme based on those elements enable (a) substantial compliance locally and (b) cross border data transfers.



CBPR | GDPR | LGPD | Others

Sample Models of Accountability

- ICO Accountability Toolkit
- Corporate Privacy Programmes
- Binding Corporate Rules (BCR)
- Codes of Conduct
- Certifications & Seals
- APEC Cross Border Privacy Rules (CBPR)
- ISO Standards

“Incentivising” Accountability

How Can DPAs and Law/Policymakers do it?

A **differentiating or mitigating factor** in investigation or enforcement

“Licence to operate” and use data responsibly, based on organizations' evidenced commitment to data privacy

Publicly recognising best in class organizations and **showcasing accountable “best practices”**

A **differentiating or mitigating factor** in investigation or enforcement

Using accountability as **evidence of due diligence** in business processes (outsourcing, IT services, etc.)

Enable **cross-border data transfers** within the company group and to third parties, based on formal accountability schemes

Articulate proactively the elements and levels of accountability to be expected

Business Case for Accountability

Self-Enlightened Interest of Organisations

Proactive data management is a business issue and accountability is beyond legal compliance

- Enable new business models, digitalisation, globalisation and data-driven innovation
- Address increased expectations of individuals for transparency, control and value exchange
- Ensure data protection, sustainability and digital trust
- Address regulatory change, impact and implementation
- Mitigate legal, commercial and reputational risks

CIPL Accountability Mapping Project

Overview

Select CIPL Members are mapping their Privacy Management Programmes to the CIPL Accountability Framework:

- To further promote accountability as **standard market practice**, that is law - and sector - agnostic.
- To build **global consensus and expectations** on accountability with regulators.
- To demonstrate that accountability is a **scalable framework** that works for all size/type of organisations.
- To provide **concrete and diverse evidence and success stories** from companies with mature privacy programmes that accountability is a demonstrable and enforceable framework.

Project Timeline:

- Start: May 2019
- During 2019: interviews and doc review
- Final Report: Estimated Q1 2020
- Socializing Report with DPAs 2020

CIPL Accountability Mapping Project

Preliminary Overall Findings and Top Messages

About organisations

- Organisations and top management are **articulating values and business drivers** in the beginning of, and throughout, their privacy compliance journey
- Organisations consider **privacy as a business strategic topic** that goes beyond mere compliance
- **Processors also take steps to be accountable**, even though certain accountability elements are not always legally required for them
- **Accountability is law-agnostic** – organisations build a one-stop-shop privacy programme

About Accountability

- Accountability is a **flexible and scalable framework** suitable for organisations of all types, sizes, culture, sectors, geographies
- Accountability helps organisations break silos and work more collaboratively **as privacy is a cross-functional topic**
- Accountability **drives global convergence** in data protection
- Data protection grounded on accountability elements is an **enabler of digital trust and innovation**

About the CIPL Accountability Framework

- The Framework is reiterative – a **thoughtful process and an ongoing journey**
- The Framework is familiar to leaders and Boards because it **aligns with other corporate compliance areas** (e.g. anticorruption, AML, export controls, etc.)
- **Risk-based approach** touches upon all elements of the Framework
- The Framework is future proof – it enables organisations to be **more adaptable to change:** regulatory, legal, technological and within business

Centre for Information Policy Leadership
HUNTON ANDREWS KURTH

Session 1. Defining Accountability

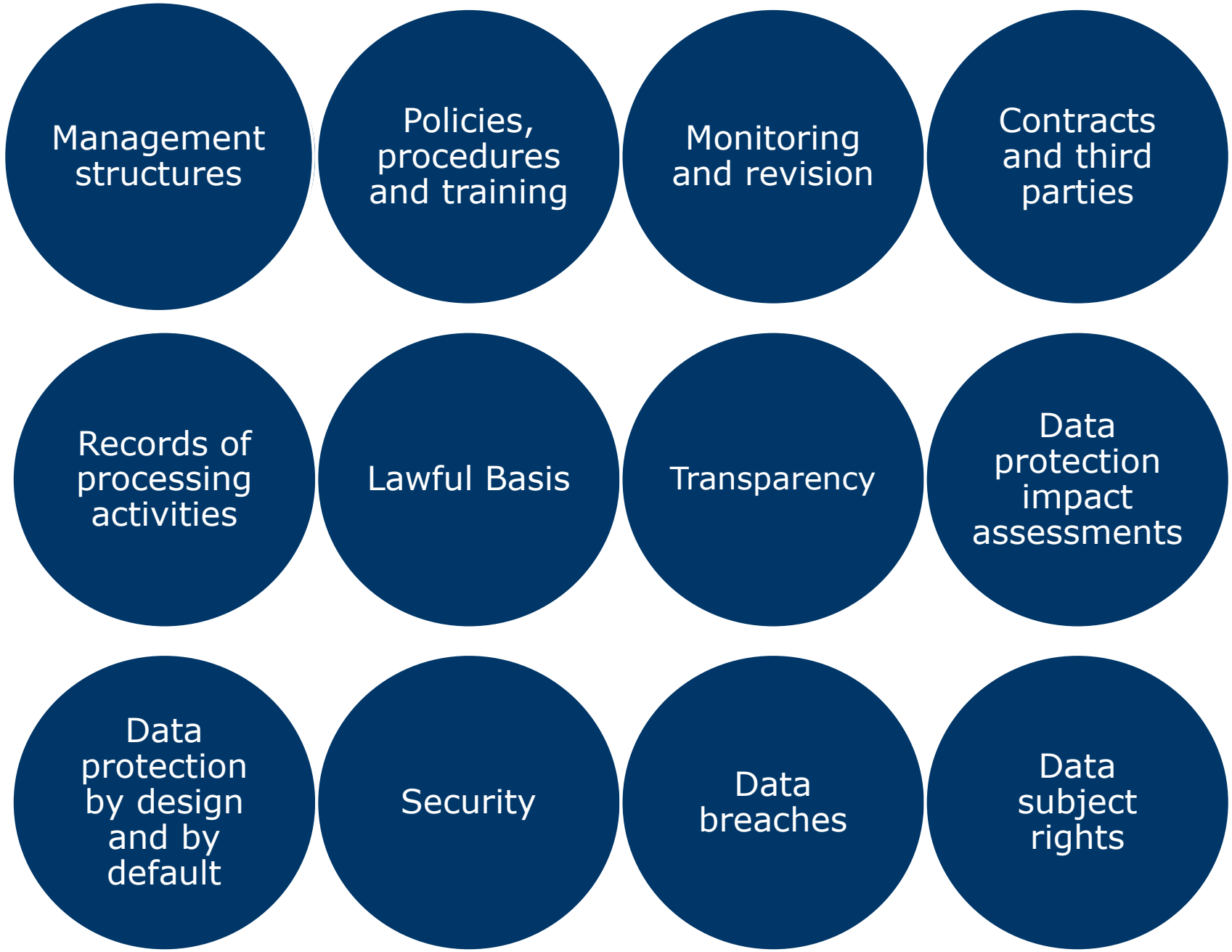
Moderator: **Bojana Bellamy**, President, CIPL

Setting ICO expectations:

Elizabeth Archer, Principal Policy Adviser, ICO and

Lorna Cropper, Secondee, ICO

Toolkit categories



ICO snap survey

Survey published online
28 October 2019

Closed
9 December
2019

Very positive response

163 responses

Wide variety of respondents

We wanted to understand…

1. existing accountability practices
2. what might lead to improvements
3. how the ICO might support organisations designing their own internal accountability programmes
4. what scope and structure would be most helpful

London workshop

Held at Field Fisher Law on 3 February 2020.

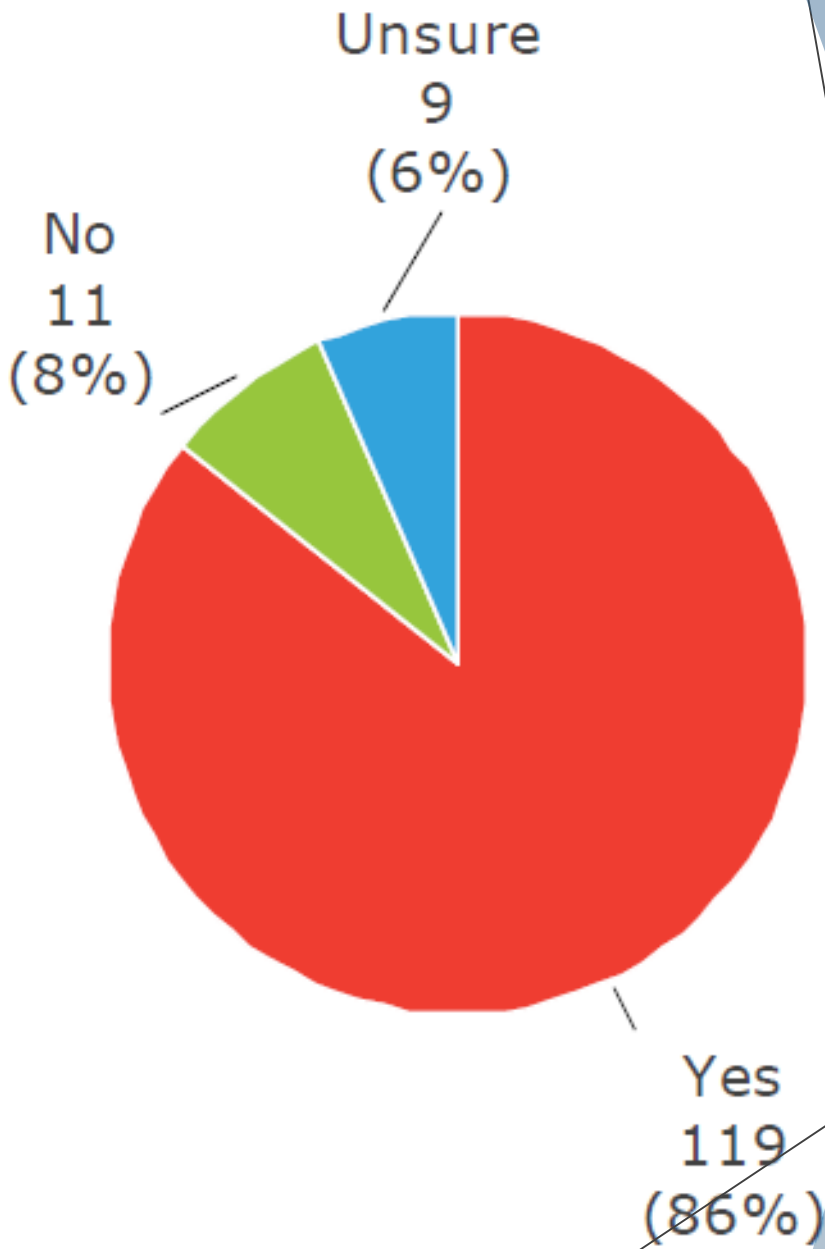
60+ delegates responded to expression of interest survey.

Variety of representatives from across large, medium and small organisations and different sectors: private, public and third.

Focused on exploring key topics arising from survey: category areas; content of the Toolkit in top 3 challenging areas; user experience and design of the Toolkit and ways to create an ‘accountability culture’.

Survey feedback:

Q. Are the proposed Toolkit categories suitable?



Toolkit categories: feedback

Overall number of categories – should be reduced.

Training and awareness should be its own category.

Potential mergers and changes to category names = records of processing and lawful basis; Data protection by design and by default and DPIA

Transparency – should it be a category in its own right?

Missing areas?

Risk

Records management

International transfers

Data sharing

Processors

Monitoring of legal developments

Order of categories…

- A split between ‘governance’ and ‘operational’ areas could be helpful.
- Order could potentially: signal way to approach building a privacy programme, especially for smaller organisations; help to prioritise activities.
- Could align with ‘data cycle’.
- A risk is that order could give impression that some areas are more important than others.

Mapping to CIPL's 'accountability wheel'

Questions for Discussion

Breakout exercise 1

- 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?

Group-wide questions

- 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?

Defining Accountability

Examples of content of privacy management programmes

Leadership and Oversight

- Tone from the top
- Executive oversight
- Data privacy officer/office of oversight and reporting
- Data privacy governance
- Privacy engineers
- Internal/External Ethics Committees

Risk Assessment

- At programme level
- At product or service level
- DPIA for high risk processing
- Risk register
- Risk to organisations
- Risk to individuals
- Records of processing

Policies and Procedures

- Internal privacy rules based on DP principles
- Information security
- Legal basis and fair processing
- Vendor/processor management
- Procedures for response to individual rights
- Other (e.g. Marketing rules, HR rules, M&A due diligence)
- Data transfers mechanisms
- Privacy by design
- Templates and tools for PIA
- Crisis management and incident response

Transparency

- Privacy policies and notices to individuals
- Innovative transparency – dashboards, integrated in products/apps, articulate value exchange and benefits, part of customer relationship
- Information portals
- Notification of data breaches

Training and Awareness

- Mandatory corporate training
- Ad hoc and functional training
- Awareness raising campaigns and communication strategy

Monitoring and Verification

- Documentation and evidence - consent, legitimate interest and other legal bases, notices, PIA, processing agreements, breach response
- Compliance monitoring and testing - verification, self-assessments and audits
- Seals and certifications

Response and Enforcement

- Individual requests and complaints-handling
- Breach reporting, response and rectification procedures
- Managing breach notifications to individuals and regulators
- Implementing response plans to address audit reports
- Internal enforcement of non-compliance subject to local laws
- Engagement/Co-operation with DPAs

Organisations must be able to **demonstrate their own implementation** - internally and externally

Centre for Information Policy Leadership
HUNTON ANDREWS KURTH

Session 2. Measuring and Demonstrating Accountability

Moderator: **Nathalie Laneret**, Director of Privacy Policy, CIPL

Setting ICO expectations:

Elizabeth Archer, Principal Policy Adviser, ICO

Chris Taylor, Head of Assurance, ICO

Expectations and indicators of effectiveness

- For each category, we would set out:
  1) our reasonable expectations about what we would expect to be in place; and
  2) indicators to help organisations understand the types of measures that are likely to indicate that our expectations are being met effectively.
- Will be informed by our supervisory activity such as audits, investigations, and casework.

Expectations

1 Management structures

There is an effective and clearly defined management framework providing oversight of data protection and information governance.

The organisation has considered whether it needs a DPO under Article 37 and if it does, the role satisfies the requirements and responsibilities outlined in the GDPR.

Operational roles and responsibilities have been assigned to support data protection and information governance.

Indicators of effectiveness

1 Management structures

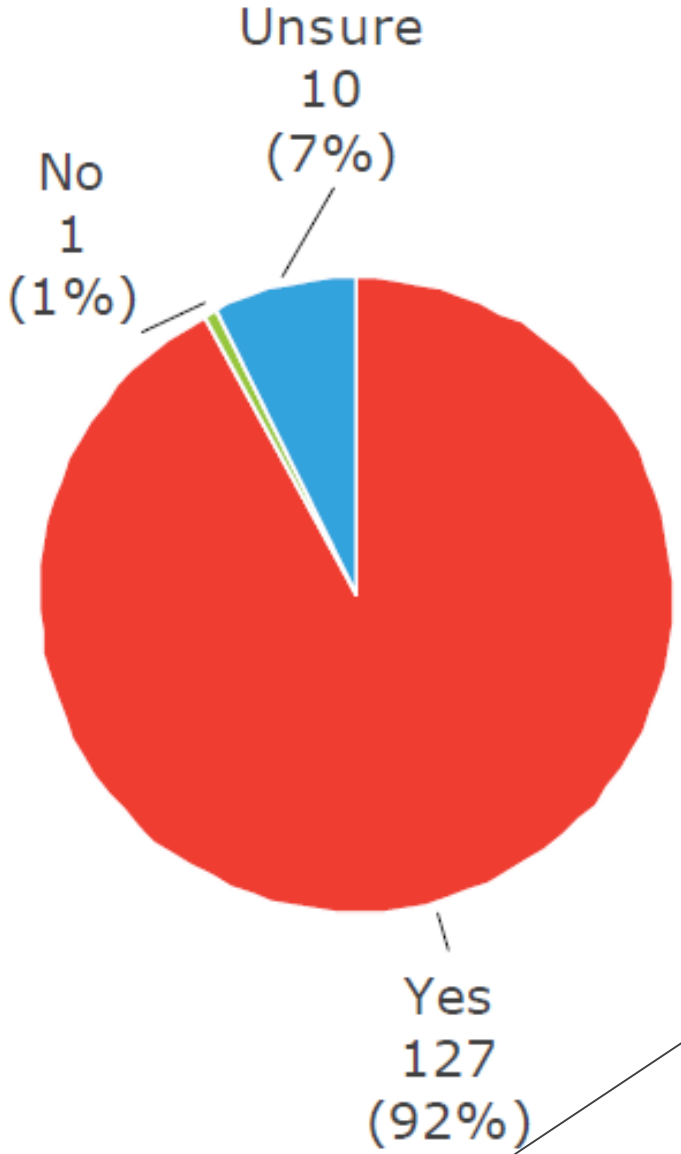
There is an organisation chart showing the reporting lines and flow of information between any relevant committees and groups.

The DPO is tasked with monitoring compliance with the GDPR and other data protection laws, data protection policies, awareness-raising, training and audits.

There are operational roles in place and responsibilities are assigned to ensure the effective management of all records e.g. in job descriptions.

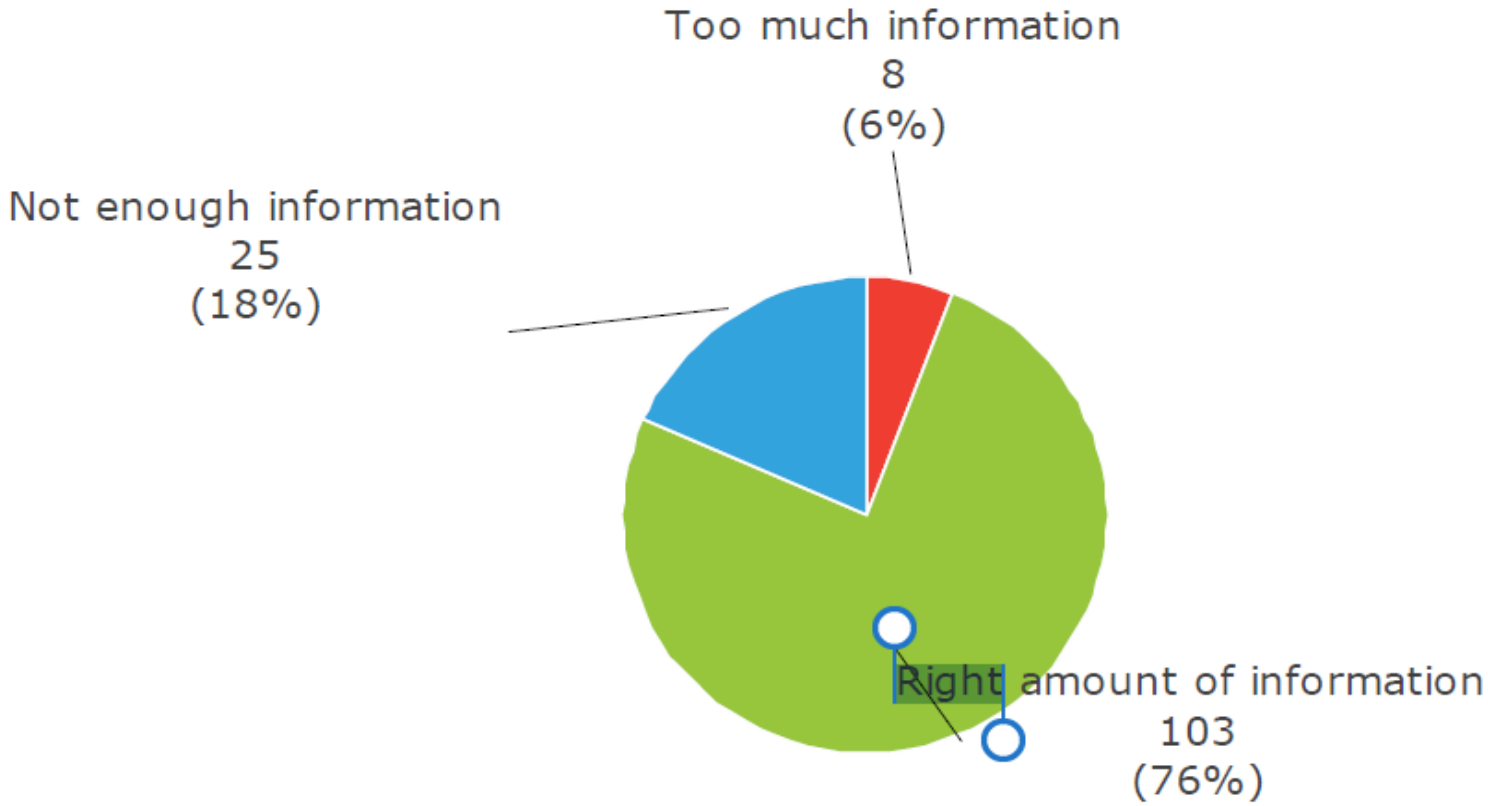
Survey feedback:

Q. Do you think we have proposed a helpful structure?



Survey feedback:

Q. What are your views about the level of detail provided?



Expectations and indicators

Positive response

Could lead to a yes/no or pass/fail response

Possibly too prescriptive

Could be more scalable

Could be written in plainer English

Granularity of detail

- Our ‘management structure’ example looked about right, achieving a fair balance of information that was not too over-bearing
- Concern about suitability for smaller organisations – some details may not be relevant
- Expectations and indicators could be more clearly defined – differences not always obvious
- Could include links to the legislation, fuller explanations, templates or examples

Supporting smaller organisations

- SME support – we are strongly committed to engaging with SMEs and are introducing dedicated resources to build on our more targeted guidance.
- Recognise some may still be undertaking higher risk processing despite size – risk-based approach to Toolkit important.
- Common suggestions for supporting SMEs including checklists, templates, and examples - important to tell this audience not just what we want to see but how we want to see it.
- Key to explain the 'spirit of the law' and why it is important and challenge the 'burden' assumption.
- Possible ways to adapt the Toolkit – support prioritisation when resources are limited. Greater clarity on mandatory requirements and how to scale accountability.

Unintended consequences

- Exacerbating perceptions of DP being an encumbrance
- Generating resistance if toolkit does not align with existing processes or frameworks being used
- Use as a check-list with a simplistic pass/fail outcome
- Limited impact as it does not address fundamental cultural issues

Existing practice and guidance

Top 3 challenging areas

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

Common themes across all these areas:

- Organisational diversity;
- The volume and complexity of information;
- Dealing with internal staff or third parties;
- Uncertainty about level of detail that is required;
- Time-consuming nature and resource impact; and
- Low buy-in from senior staff.

Workshop example 1: Policies, procedures and training

- Templates desirable to see ‘what good looks like’ and more details on key minimum policies.
- Use of terms ‘appropriate’ and ‘relevant’ – what does it mean?
- Importance of being effectively implemented
- Ethical considerations.
- Varying training needs.
- Raising awareness – other effective measures beyond ‘written documents’ e.g. posters, videos etc.
- Reference to testing knowledge required.

Workshop example 2: Contracts and third parties

- Contracts and third parties – Helpful to have more templates e.g. standard contract clauses to help improve consistency.
- More detail and examples on different relationships e.g. joint controllers, processors and sub processors.
- More detail on expectations around ‘due diligence’ and how expectations might vary depending on organisation.
- How to prioritise monitoring of contracts and handle risks.

Workshop example 3: Records of processing activities (ROPA)

- Industry specific examples would be helpful.
- ICO should model a way of doing a ROPA.
- Level of detail a key issue

Accountability mechanisms and interoperability – looking to the future…

Codes of conduct and certification schemes as accountability mechanisms.

Interoperability – to what extent will the Toolkit align with global privacy programmes?

Brexit impact

Questions for Discussion

Breakout exercise 2

- 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)?

Group-wide questions

- 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?

Measuring and Demonstrating Accountability

To Whom and How?

To Whom?

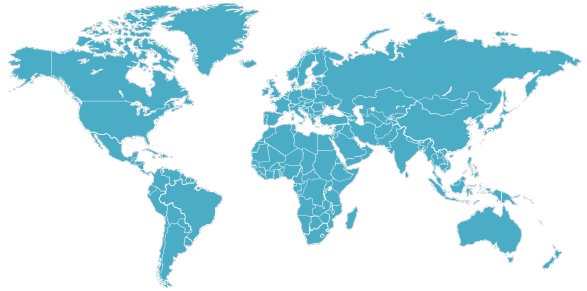
- **Internally** – executives leadership, Board of Directors, shareholders
- **Externally** – business partners, regulators, individuals and civil society

Models of Accountability require:

- Following substantive privacy rules
- Implementation infrastructure
- Verification
- Ability to demonstrate compliance

Global Accountability

- Accountability Elements are present in key laws and regulations around the world.
- Privacy compliance programme based on those elements enable (a) substantial compliance locally and (b) cross border data transfers.



CBPR | GDPR | LGPD | Others

Sample Models of Accountability

- ICO Accountability Toolkit
- Corporate Privacy Programmes
- Binding Corporate Rules (BCR)
- Codes of Conduct
- Certifications & Seals
- APEC Cross Border Privacy Rules (CBPR)
- ISO Standards

Centre for Information Policy Leadership
HUNTON ANDREWS KURTH

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

Moderator: **Bojana Bellamy**, President, CIPL

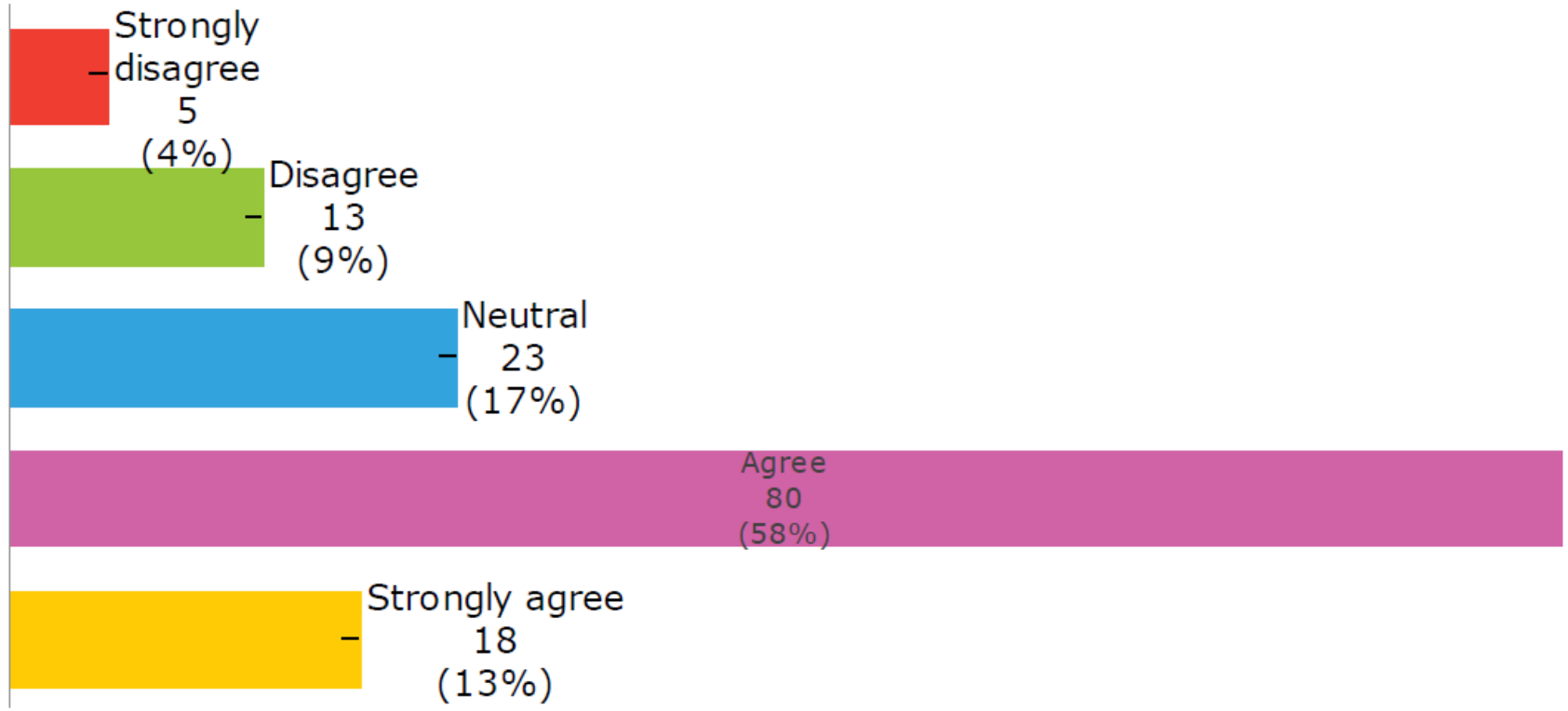
Setting ICO expectations:

Elizabeth Archer, Principal Policy Adviser, ICO and

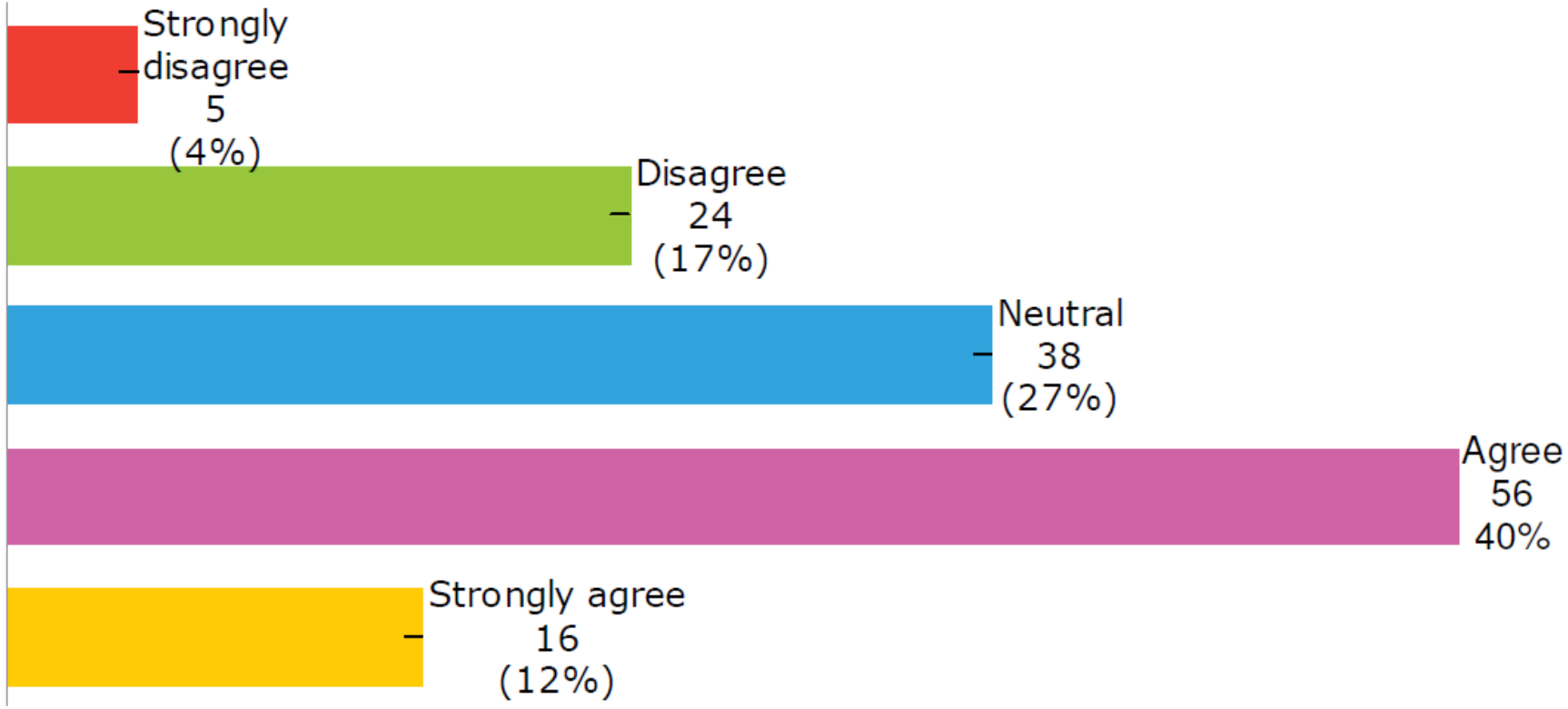
Lorna Cropper, Secondee, ICO

Disclaimer *- These slides have been prepared by CIPL. They are not endorsed by, and do not represent the views of, the Information Commissioner's Office.*

Survey feedback:
Q. My organisation could improve the appropriateness and effectiveness of its internal data protection arrangements.



Snap survey feedback:
Q. My organisation could improve its readiness to demonstrate its compliance.



Survey feedback - improvements

Practice improved since GDPR introduced and a commitment to DP as a process of continuous improvement but there were doubts about the depth of compliance being achieved.

- 1. Embedding a culture of accountability:
  - DP may not be seen as an organisation-wide responsibility.
  - DP may not be prioritised and seen as onerous.
  - Better support from top management seen as key to getting appropriate training and resources.
- 2. Uncertainty about how to demonstrate accountability and what 'good looks like'.

Stakeholder comments…

- "I think businesses in general need to understand the importance of a good governance structure and not just a single over-loaded person or a person in a shared role".
- "There is always room for improvement – I think it all starts with effective policy implementation – we can have a policy which says all the right things, but if it isn't understood and put into practice by your staff base consistently, it is of little value".
- "I would like to see more from the ICO on what they would expect to see…"

Workshop: creating an ‘accountability culture’.

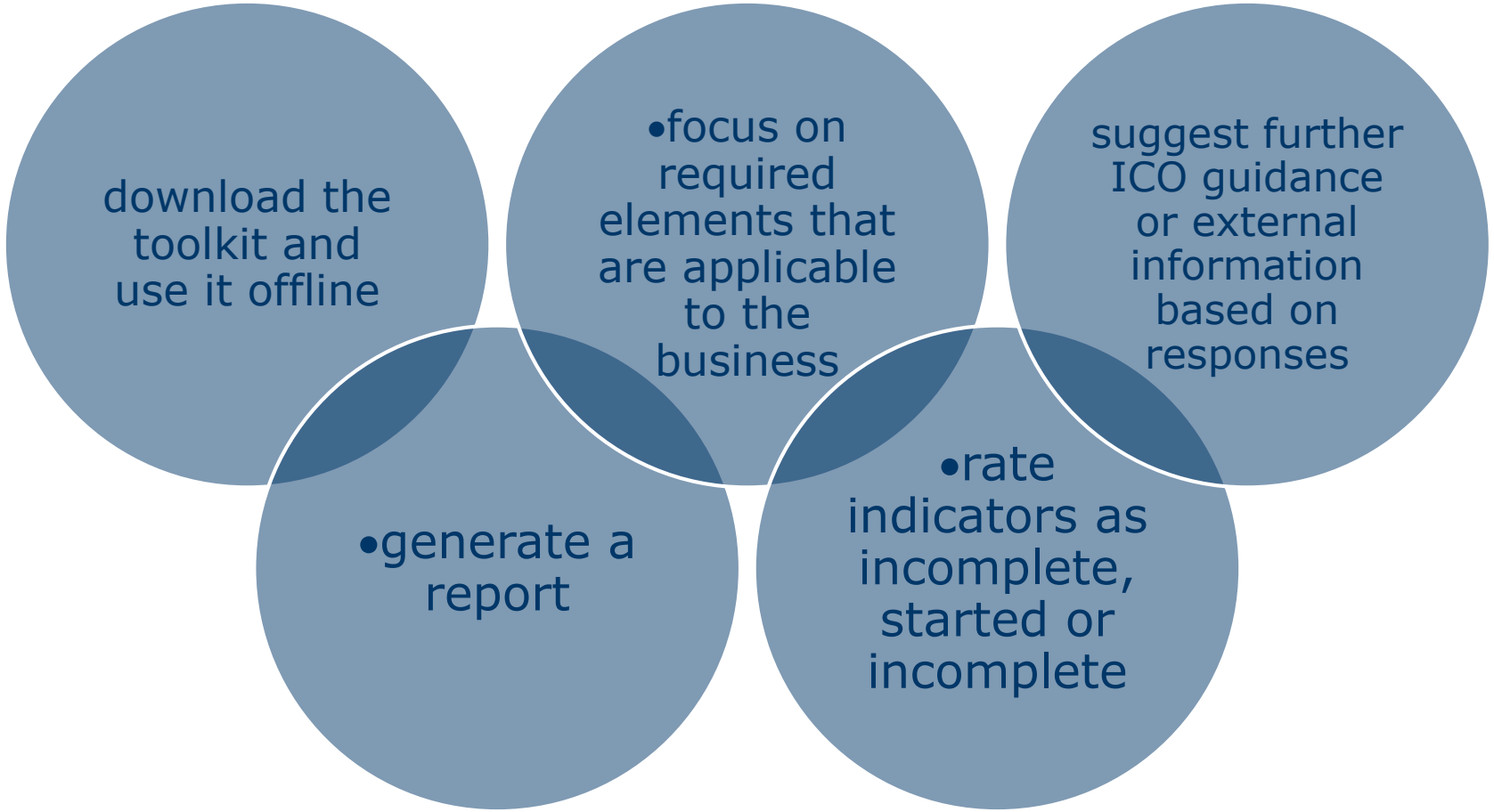
- Who should complete the Toolkit? What level of senior management involvement is expected?
- How could it be used? – to assess current compliance; show how to improve; and act as a maturity measure.
- Desire for a clear ‘output’ - let senior managements know where they benchmark against the baseline. Link to certifications appealing.
- Senior management ‘buy in’ – Toolkit an opportunity to promote and reinforce this.
- Enforcement – costs and consequences powerful motivators.
- Embedding accountability in other processes – making use of other regulators.
- Ongoing marketing campaign on accountability – greater use of social media, writing to CEOs

Promoting accountability through means beyond the Toolkit

- Accountability is a factor to take into account in our Regulatory Action Policy.
- Link between accountability and advanced/digital data uses e.g. sandbox and research.
- Show-casing ‘what good looks like’ – examples and templates of best practice, examples where accountability could have made a difference and avoided consequences/regulatory action, increased support for SMEs, mentoring, accountability and contracts and as an enabler of internal transfers.
- Positive messaging about the considerable benefits.

Functions

Functionality to…



Accountability Toolkit mock up

- What is the Accountability Toolkit?
- What are the benefits?
- How does it work?
- What happens after I complete the Toolkit?

Toolkit categories

Leadership and oversight	Policies, procedures and training	Monitoring and improvement	Processor contracts
Records of processing activities	Lawful basis	Special category data	Transparency
Data protection impact assessments	Personal data breaches	Data protection by design and default	Technical and organisation security
Individual rights	Responding to privacy complaints		

Expectations and indicators

Leadership and oversight

Expectation one of six

There is an effective and clearly defined management framework providing oversight of data protection compliance. *

- ○ Meeting expectation
- ○ Partially meeting expectation
- ○ Not meeting expectation
- ○ Not applicable

☐ CLICK FOR MORE INFORMATION

Expectation two of six

The organisation has considered whether they need a Data Protection Officer (DPO), and if they do the role includes all the requirements and responsibilities for a DPO as outlined in the General Data Protection Regulation (GDPR). *

- ○ Meeting expectation
- ○ Partially meeting expectation
- ○ Not meeting expectation
- ○ Not applicable

☐ CLICK FOR MORE INFORMATION

Toolkit report for each category:

Traffic light report – red, yellow and green

Download and fill in measures to take to meet ICO expectations and measures already taken.

The report below lays out the expectations you identified your organisation is not meeting, those partially met and those already met

9 February 2020

Next steps

1. Download a Word version of the report

2. Fill in the measures you will take to meet those expectations you are not yet meeting or are only partially meeting

3. Fill in the measure you have already taken to meet or partially meet our expectations.

Expectation not being met

Where a DPO is needed, the role has operational independence and appropriate reporting mechanisms are in place to senior management.

List the measures you will take to meet this expectation:

There is a structure (such as a group or committee) which provides overall oversight, direction, and guidance at operational level for DP and information governance compliance through all the organisation. They should act as a channel for communication of information and risks to senior management.

List the measures you will take to meet this expectation:

Workshop feedback:

- Helpful to see indicators of effectiveness without having to click.
- Definition of ‘expectation met’, ‘partially met’ and ‘not met’.
- Scoring method and clear actions – more useful for management communication.
- Outcome report for the whole Toolkit rather than individual categories.
- Want Toolkit to *be* a tool – more interactive, downloadable software with ability to upload documents.
- Useful to be able to save and record progress, owner and dates.
- Greater focus on evidence to demonstrate compliance.

Questions for Discussion

Breakout exercise 3

- 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?

Breakout exercise 4

- 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?

Group-wide questions

- 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?

"Incentivising" Accountability

How Can DPAs and Law/Policymakers do it?

A **differentiating or mitigating factor** in investigation or enforcement

"Licence to operate" and use data responsibly, based on organizations' evidenced commitment to data privacy

Publicly recognising best in class organizations and **showcasing accountable "best practices"**

A **differentiating or mitigating factor** in investigation or enforcement

Using accountability as **evidence of due diligence** in business processes (outsourcing, IT services, etc.)

Enable **cross-border data transfers** within the company group and to third parties, based on formal accountability schemes

Articulate proactively the elements and levels of accountability to be expected

Business Case for Accountability

Self-Enlightened Interest of Organisations

Proactive data management is a business issue and accountability is beyond legal compliance

- Enable new business models, digitalisation, globalisation and data-driven innovation
- Address increased expectations of individuals for transparency, control and value exchange
- Ensure data protection, sustainability and digital trust
- Address regulatory change, impact and implementation
- Mitigate legal, commercial and reputational risks

Centre for Information Policy Leadership
HUNTON ANDREWS KURTH

Wrap-Up

Bojana Bellamy, President, CIPL

Disclaimer *- These slides have been prepared by CIPL. They are not endorsed by, and do not represent the views of, the Information Commissioner's Office.*

Voting Time

Question 1

Would you participate in the ICO's **Beta Phase** of the Accountability Toolkit?

A. Yes

B. No

C. Maybe

Voting Time

Question 2

Would you be interested in providing **case studies** to the ICO?

A. Yes

B. No

C. Maybe

Centre for Information Policy Leadership
HUNTON ANDREWS KURTH

Thank you.

Centre for Information Policy Leadership
HUNTON ANDREWS KURTH

Appendices

Disclaimer *- These slides have been prepared by CIPL. They are not endorsed by, and do not represent the views of, the Information Commissioner's Office.*

Accountability – What it is

Comprehensive

- Comprehensive internal programme giving effect to DP requirements
- Verifiable, demonstrable and enforceable data protection commitment, infrastructure and controls

Relevant

- Relevant and scalable for all organisations
- Private and public sector; large multinationals and SMEs; controllers and processors

Consistent

- Consistent with other areas of corporate law and governance and duty of care
- Anti-bribery; anti-money laundering; export controls; Sarbanes-Oxley; Sustainability; Fiduciary duty

Demonstrable

- Internally: Executive leadership; Board of Directors; shareholders
- Externally: Business partners; regulators; individuals; civil society

Effective

- Corporate Digital Responsibility fit for 21st century
- Delivers effective protection for individuals and data
- Enables responsible use, sharing and flows of data and innovation

Accountability – What it is not

Self-regulation

- Sits on top of and in addition to legal requirements - it does not replace them (co-regulation)
- Accountability operationalises legal rules and delivers legal compliance

Carte blanche to use data

- Requires organisations to implement all applicable DP norms and be able to demonstrate that implementation

Self-serving tool

- Provides also benefits for regulators, individuals and society

An excuse for failure

- Minimises the risks of breaches, and requires organisations to be prepared, responsive and responsible when they occur
- Can be a mitigating factor in enforcement, but it does not give organisations a free pass

Accountability

Systematic Changes Ahead for Organisations

- **Moving from legal compliance to accountability** – sustainable, risk-based and global privacy programme
- **Data privacy = business issue** – impact on organisational data strategy and digital transformation
- **Data privacy = board-level issue** – higher enterprise risk; larger business, legal and compliance impact; security breach notification and management; enforcement and litigation
- **Holistic and joined up approach** between CIO, CISO, CDO, CPO, Legal and communication/media relations
- **CPO/DPO** – More strategic, senior, visible, leadership role with multiple skills
- **Systematic management of external engagement and relationships** – Privacy regulators, individuals, media, privacy advocates

Accountability and Interoperability

Cross-border Data Flows

Accountability

The cornerstone of corporate digital responsibility, sustainable privacy protection for individuals, responsible use of data, and the 4th Industrial Revolution

Enables compliance with local law requirements

Enables compliance with cross-border transfer requirements

Solutions = **Interoperable Accountability Frameworks**

- BCRs
- Certifications
- CBPR & PRP
- Codes of Conduct
- Privacy Shield
- ISO Standard

✓ Accountability **delivers benefits** to organisations, regulators, individuals and society

✓ Regulators, law and policymakers **must incentivise** accountability / accountable organisations

Disclaimer *- These slides have been prepared by CIPL. They are not endorsed by, and do not represent the views of, the Information Commissioner's Office.*

Accountability and Interoperability

A transferrable concept

Existing Regulated Areas

- Anti-corruption
- White collar crime and corporate fraud
- Anti-money laundering
- Healthcare
- Export controls and regulation
- Competition law

Data Privacy

- Codified in GDPR
- GDPR spin-off effect introducing accountability in new laws (e.g. Brazil LGPD, DIFC (Dubai) Bill, India Bill)
- Regulatory guidance (e.g. Hong Kong, Canada, Singapore, Australia, Mexico, Columbia)
- FTC Consent Decrees
- GPEN 2019 Accountability Sweep

New Areas of Digital Responsibility

- Online content and safety
- Information misuse
- Children's data
- AI/Machine Learning
- Healthcare and biotechnology

Benefits of Accountability

For DPAs and Individuals

DPAs

- Reduces enforcement and oversight burden of DPAs
- Promotes constructive engagement with accountable organiaations
- Encourages race to the top rather than race to the bottom

Individuals

- Effective protection and reduced risk/harm
- Empowered, able to exercise rights and complaints
- Trust/ready to benefit from and participate in digital society

Effective and Results-Based Regulators

in the Digital World

Effective regulators have to act in a connected world

Strategic, prioritized, risk-based, transparent regulatory policy

- Prioritised activities (leadership, enforcement, complaint handling, authoriser)
- Innovative regulatory methods (e.g. Regulatory sandbox)

Constructive engagement with regulated organisations

- Maximum consultation, participation and frank exchanges

Incentivize and encourage accountability

- E.g. Showcase best practices and accountability efforts; differentiating factor in enforcement

Act in a connected way with other regulators

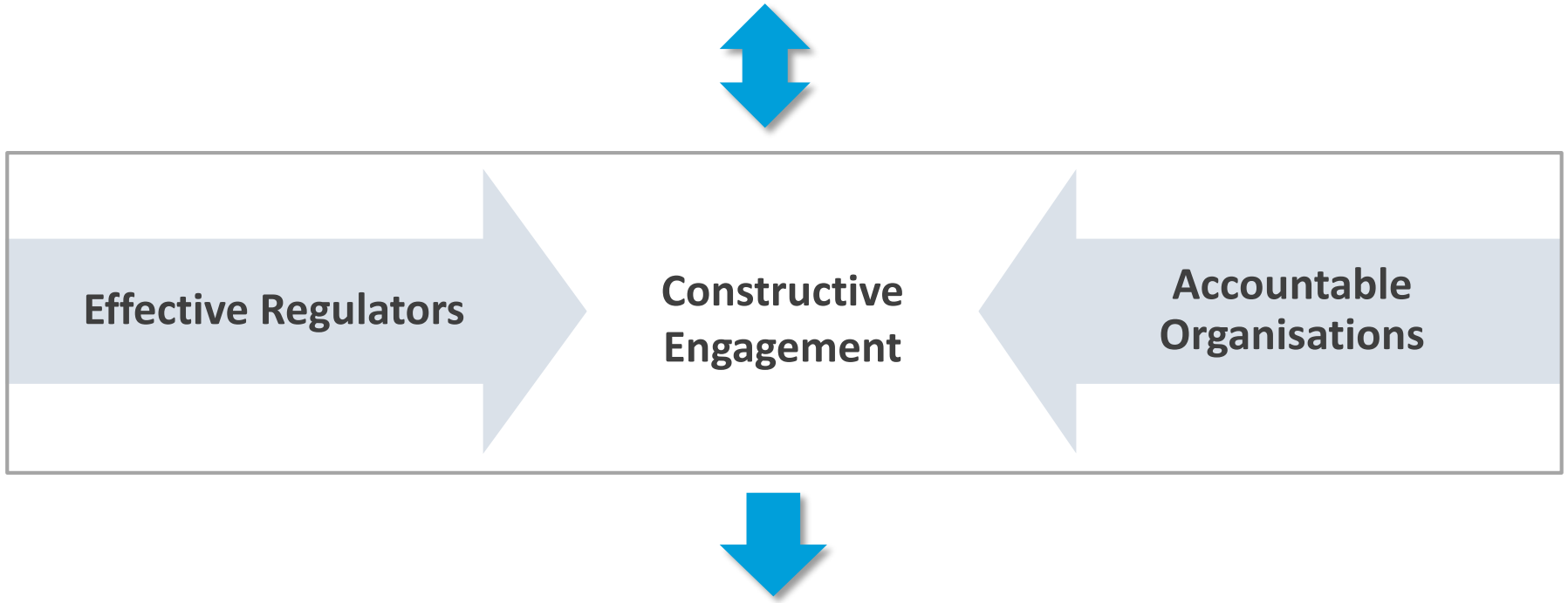
- Regulatory guidance, approaches to enforcement, mutual cooperation

Build bridges with different regimes

- Accountability frameworks (e.g. APEC CBPR and EU BCR)

Framework for Trusted Digital Age

Media | Market forces | Political forces | Civil Society | Certifiers | Redress Schemes



Effective Protection for Individuals and Benefits for Digital Society

Next Steps for Accountability

- ✓ Build **global consensus** on accountability and its universal elements – Organisations, DPAs, Boards, Auditors
- ✓ Promote and **incentivise implementation** of accountability by organisations
- ✓ Drive **alignment of regulatory guidance** on accountability (e.g. Hong Kong, Canada, Australia, Singapore, US, Mexico, Colombia, GDPR, Brazil, etc)
- ✓ **Explore links between accountability** (privacy management programmes) **and certifications**
- ✓ **Learn from the precedent set by other areas of law** and corporate governance (US, UK and other)
- ✓ Use accountability as a **bridge to drive and deliver trusted cross-border data flows**

Centre for Information Policy Leadership
HUNTON ANDREWS KURTH

CIPL Papers

On Accountability and Data Protection

Paper Title	Publication Date	Link
Accountability Mapping Report	Upcoming	Upcoming
Organisational Accountability - Past, Present and Future	30 October 2019	https://bit.ly/2REMkeO
Organisational Accountability in Light of FTC Consent Orders	13 November 2019	https://bit.ly/2GeDZt2
CIPL Q&A on Accountability	3 July 2019	https://bit.ly/33JedYb
Accountability's existence in US Regulatory Compliance and its Relevance for a US Federal Privacy Law	3 July 2019	https://bit.ly/2H93vAH
Introduction: The Central Role of Organisational Accountability in Data Protection	23 July 2018	https://bit.ly/2sWkkqQ
The Case for Accountability: How it Enables Effective Data Protection and Trust in the Digital Society	23 July 2018	https://bit.ly/2BaQOSY
Incentivising Accountability: How Data Protection Authorities and Law Makers Can Encourage Accountability	23 July 2018	https://bit.ly/2GbGPjx