

Centre for Information Policy Leadership Workshop in collaboration with AXA

Accountability under the GDPR: How to Implement, Demonstrate and Incentivise it

5 October 2018, Paris



Centre for
Information
Policy
Leadership
Hunton Andrews Kurth LLP

Opening Remarks

Emmanuel Touzeau, Group Communication and Brand Director - GDPR Sponsor, AXA

Bojana Bellamy, President, CIPL

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

ACTIVE GLOBAL REACH

60+
Member
Companies

We **INFORM** through publications and events

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

5+
Active Projects
& Initiatives

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

We **CREATE** and implement best practices

20+
Events annually

15+
Principals and
Advisors

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://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

The Central Role of Organisational Accountability in Data Protection

- **Paper 1 — The Case for Accountability: How it Enables Effective Data Protection and Trust in the Digital Society**
- **Paper 2 — Incentivising Accountability: How Data Protection Authorities and Law Makers Can Encourage Accountability**

Available at informationpolicycentre.com

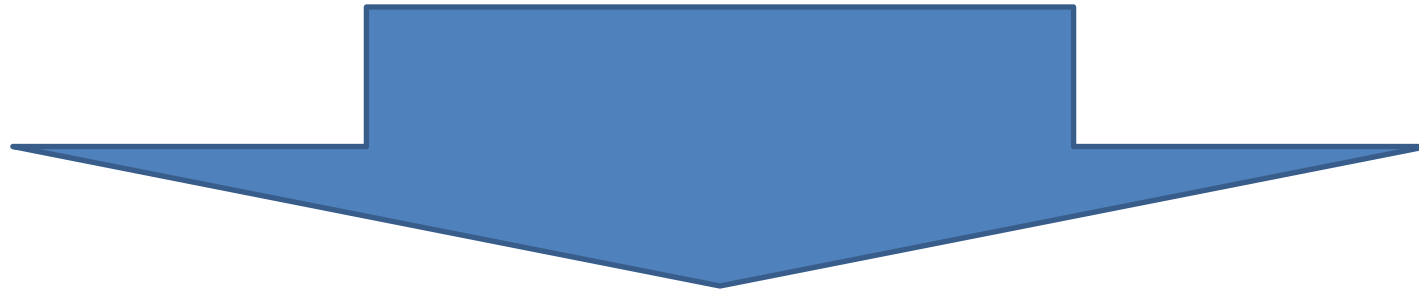
And on your tables!

- **Embark** everybody on the “accountability journey”
- **Reach** consensus on the key elements of accountability
- **Explore** acceptable means to demonstrate accountability
- **Identify** how DPAs can incentivise accountability
- **Present** the potential of accountability as an essential prerequisite of the 4th industrial revolution

Accountability in GDPR: What it is and Why it Matters

Controllers must (Processors, too, in respect of their obligations):

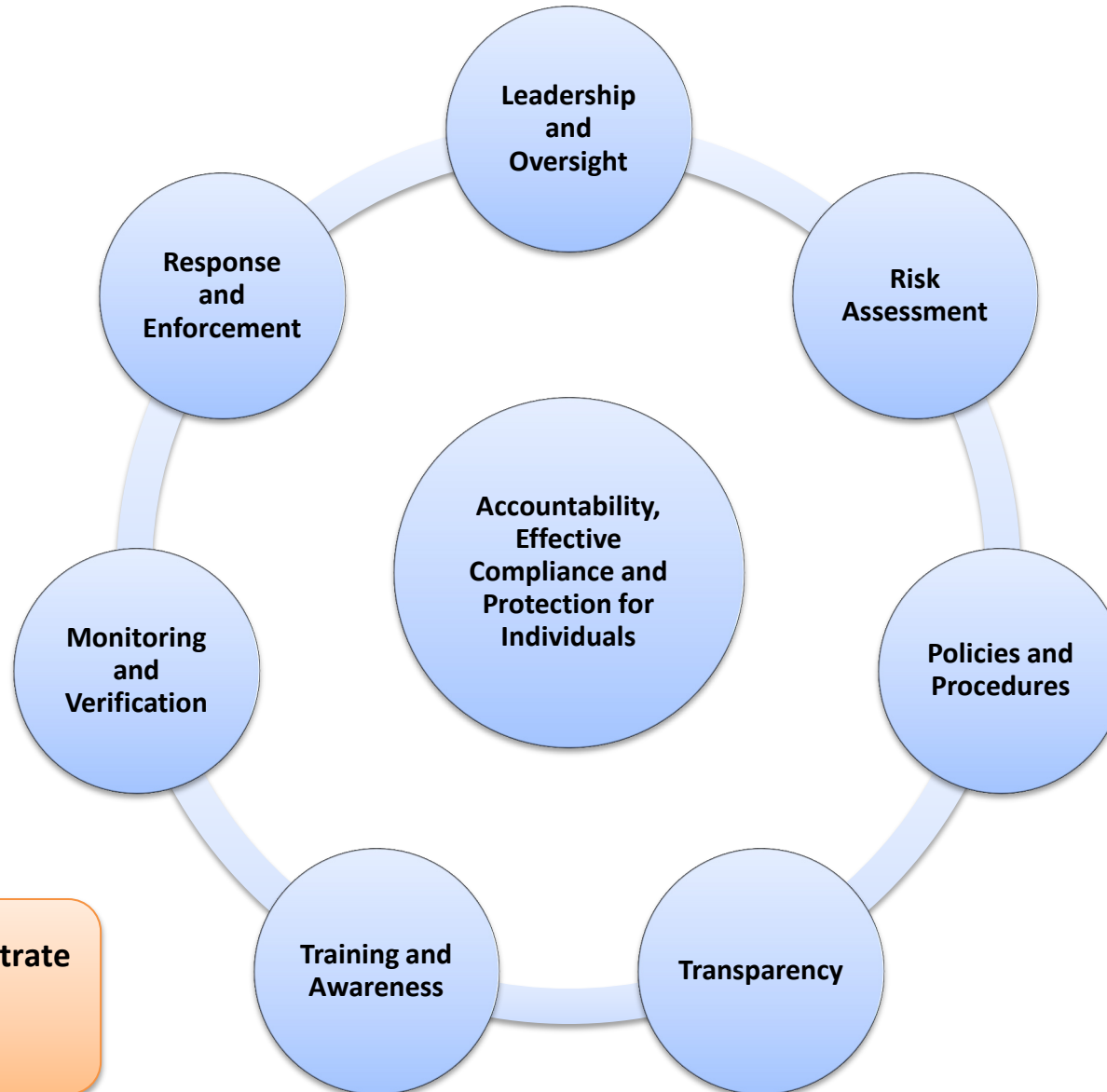
- Be responsible for compliance with the GDPR
- Implement appropriate and effective technical and organisational measures to comply with the GDPR
- Demonstrate compliance & effectiveness of the measures



Taking into account:

- The nature, scope, context and purposes of the data processing
- The risk for individuals — physical, moral, material damages

Universal Elements of Accountability



Organisations must be able to demonstrate accountability – internally and externally

Accountability – Examples of Content of Privacy Management Programmes

- Executive oversight
- Data privacy officer/office of oversight and reporting
- Data privacy governance
- Privacy engineers

Leadership & Oversight



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

Risk Assessment



- Internal privacy rules based on DP principles
- Information security
- Legal basis and fair processing
- Vendor/processor management
- Procedures for response to individual rights

Policies & Procedures



- 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

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

Transparency



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

Training & Awareness



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

Monitoring & Verification



- 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

Response and Enforcement



Organisations must be able to demonstrate - internally and externally

Proactive data management is a business issue; accountability > 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

Accountability – Benefits for DPAs and Individuals

DPAs

Reduces enforcement and oversight burden of DPAs

Promotes constructive engagement with accountable organisations

Enables leverage of peer pressure and “herd” mentality

Individuals

Effective protection and reduced risk/harm

Empowered, able to exercise rights and complaints

Trusting and ready to benefit and participate in digital society

How Can DPAs and Policymakers Incentivise Accountability?

A differentiating or mitigating factor in investigation or enforcement

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

Publicly recognising best in class organisations and showcasing accountable “best practices”

Supporting and guiding organisations (particularly small and emerging companies) on a path towards heightened accountability

Co-funding between DPAs and industry for research into novel accountability tools

Offer to play proactive advisory role to organisations seeking to implement heightened accountability

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



Centre for
Information
Policy
Leadership
Hunton Andrews Kurth LLP

Introductory Scene-Setting Remarks

Peter Hustinx, Former EDPS

An eyewitness account of accountability



Centre for
Information
Policy
Leadership
Hunton Andrews Kurth LLP

Introductory Scene-Setting Remarks

Patrick Rowe, Deputy General Counsel, Accenture

Session I : Accountability under the GDPR

- ❖ **Moderator: Bojana Bellamy**, President, CIPL
- ❖ **John O'Dwyer**, Deputy Commissioner, Irish Office of the Data Protection Commissioner
- ❖ **Elizabeth Denham**, Information Commissioner, UK ICO
- ❖ **Denise Farnsworth**, Deputy DPO, Facebook
- ❖ **William Malcolm**, Director, Privacy Legal, Google
- ❖ **Geff Brown**, Associate General Counsel, Microsoft

Accountability – Examples of Content of Privacy Management Programmes

- Executive oversight
- Data privacy officer/office of oversight and reporting
- Data privacy governance
- Privacy engineers

Leadership & Oversight



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

Risk Assessment



- Internal privacy rules based on DP principles
- Information security
- Legal basis and fair processing
- Vendor/processor management
- Procedures for response to individual rights

Policies & Procedures



- 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

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

Transparency



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

Training & Awareness



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

Monitoring & Verification



- 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

Response and Enforcement



Organisations must be able to demonstrate - internally and externally

Session II : How to Demonstrate Accountability Internally and Externally

- ❖ **Moderator: Nathalie Laneret**, Director of Privacy Policy, CIPL
- ❖ **Sophie Nerbonne**, Director of Compliance and Accountability, CNIL
- ❖ **Piotr Drobek**, Deputy Director, Polish DPA
- ❖ **Alex Cebulsky**, Senior Legal Counsel, Global Data Privacy, Accenture
- ❖ **Igor Babic**, Group Data Protection Officer, AXA Group
- ❖ **Paul Breitbarth**, Director of Strategic Research and Regulator Outreach, Nymity
- ❖ **Mikko Niva**, Group Privacy Officer, Vodafone


CIPL Accountability Wheel and BCR requirements

Key Elements of Accountability



Elements to be found in BCR

- **Binding nature internally and externally**
 - Binding on companies and employees
 - Third party beneficiary rights
 - Breach remediation and compensation
 - Transparency and easy access
- **Effectiveness**
 - Training program
 - Complaint handling process
 - Audit program
 - Network of DPO
- **Cooperation Duty**
 - Duty to cooperate with the DPA
- **Description of processing and data flows**
 - Material scope and geographical scope
- **Mechanism for reporting and recording changes**
 - Process for updating the BCR
- **Data protection safeguards**
 - Compliance with data protection principles including onward transfers
 - Accountability of entities (records, DPIAs, appropriate TOMs)
 - Relationship with national laws

ARTICLE 29 DATA PROTECTION WORKING PARTY	
	
17/EN WP 256	
Working Document setting up a table with the elements and principles to be found in Binding Corporate Rules	
(updated)	
Adopted on 29 November 2017	

Criteria for approval of BCRs	In the BCRs	In the application form	Tests of relevance	Comments	References to application BCRs ⁴
1. BINDING NATURE					
1.1 The duty to respect the BCRs	YES	YES	GDPR Art. 47.1 a and 47.2 c	The BCRs must be legally binding and shall contain a clear duty for each participating member of the Group of undertakings or group of enterprises engaged in a joint economic activity ("BCR member") including their employees to respect the BCRs.	
1.2 An explanation of how the rules are made binding on the BCR members of the group and also the employees	NO	YES	GDPR Art. 47.1 a and 47.2 c	The Group will have to explain in its application form how the rules are made binding : (i) For each participating company/entity in the group by one or more of: - Intra-group agreement, - Unilateral undertakings (this is only possible if the BCR member values responsibility and liability is located in a Member State that recognizes Unilateral undertakings as binding and if this BCR member is legally able to bind the other members subject to BCRs).	

BCR requirements mapped to CIPL Accountability Wheel

Key Elements of Accountability



Elements to be found in BCR



Session III: Best Practices - How are DPAs Incentivising Accountability?

- ❖ **Moderator: Chris Docksey**, Honorary Director General, EDPS
- ❖ **Cecile Schut**, Director System Supervisory, Security and Technology, Dutch DPA
- ❖ **Wojciech Wiewiorowski**, Assistant Supervisor, EDPS
- ❖ **Dieter Kugelman**, State Commissioner, German State Commissioner for Data Protection & Freedom of Information, Rhineland-Palatinate
- ❖ **Emmanuelle Bartoli**, Group Data Protection Officer, Capgemini
- ❖ **Michelle Dennedy**, Vice President and Chief Privacy Officer, Cisco

How Can DPAs and Policymakers Incentivise Accountability?

A differentiating or mitigating factor in investigation or enforcement

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

Publicly recognising best in class organisations and showcasing accountable “best practices”

Supporting and guiding organisations (particularly small and emerging companies) on a path towards heightened accountability

Co-funding between DPAs and industry for research into novel accountability tools

Offer to play proactive advisory role to organisations seeking to implement heightened accountability

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



Centre for
Information
Policy
Leadership
Hunton Andrews Kurth LLP

Closing Remarks

Bojana Bellamy, President, CIPL

Contacts

Bojana Bellamy

President

Centre for Information Policy Leadership

BBellamy@huntonak.com

Markus Heyder

Vice President & Senior Policy Advisor

Centre for Information Policy Leadership

MHeyder@huntonak.com

Nathalie Laneret

Director of Privacy Policy

Centre for Information Policy Leadership

NLaneret@huntonak.com

Sam Grogan

Global Privacy Policy Analyst

Centre for Information Policy Leadership

SGrogan@huntonak.com

Centre for Information Policy Leadership

www.informationpolicycentre.com

Hunton Andrews Kurth Privacy and Information Security Law Blog

www.huntonprivacyblog.com

FOLLOW US ON LINKEDIN

[linkedin.com/company/centre-for-information-policy-leadership](https://www.linkedin.com/company/centre-for-information-policy-leadership)



FOLLOW US ON TWITTER

[@THE_CIPL](https://twitter.com/THE_CIPL)