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

5 October 2018, Paris
Opening Remarks

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

Bojana Bellamy, President, CIPL
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
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!
Objectives of the Workshop

- **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
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
Organisations must be able to demonstrate accountability – internally and externally
Organisations must be able to demonstrate - internally and externally.
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

Proactive data management is a business issue; accountability > legal compliance
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?

<table>
<thead>
<tr>
<th>A differentiating or mitigating factor in investigation or enforcement</th>
<th>“Licence to operate” and use data responsibly, based on organisations’ evidenced commitment to data privacy</th>
<th>Publicly recognising best in class organisations and showcasing accountable “best practices”</th>
</tr>
</thead>
<tbody>
<tr>
<td>Supporting and guiding organisations (particularly small and emerging companies) on a path towards heightened accountability</td>
<td>Co-funding between DPAs and industry for research into novel accountability tools</td>
<td>Offer to play proactive advisory role to organisations seeking to implement heightened accountability</td>
</tr>
<tr>
<td>Using accountability as evidence of due diligence in business processes (outsourcing, IT services etc)</td>
<td>Enable cross-border data transfers within the company group and to third parties, based on formal accountability schemes</td>
<td>Articulate proactively the elements and levels of accountability to be expected</td>
</tr>
</tbody>
</table>
Introductory Scene-Setting Remarks

Peter Hustinx, Former EDPS
An eyewitness account of accountability
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

## Leadership & Oversight
- Executive oversight
- Data privacy officer/office of oversight and reporting
- Data privacy governance
- Privacy engineers

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

## Policies & 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
- Access to information portals
- Notification of data breaches

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

## Monitoring & Verification
- 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

## 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 - 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

- **Leadership and Oversight**
- **Risk Assessment**
- **Policies and Procedures**
- **Monitoring and Verification**
- **Response and Enforcement**
- **Training and Awareness**
- **Transparency**

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
BCR requirements mapped to CIPL Accountability Wheel

Key Elements of Accountability

- Leadership and Oversight
- Response and Enforcement
- Risk Assessment
- Accountability, Effective Compliance and Protection for Individuals
- Policies and Procedures
- Transparency
- Training and Awareness

Elements to be found in BCR

- Third party beneficiary rights
- Breach remediation & compensation
- Binding on company and employees
- Complaint Handling Process
- Audit Program
- Network of DPOs
- Material & geographical scope
- Process for updating the BCR
- Duty to cooperate with the DPA
- Accountability
- National Laws
- Transparency & easy access
- Training Program
- Compliance with Data Protection Pples
- Monitoring and Verification
- Response and Enforcement
- Leadership and Oversight
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 Kugelmann,** 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
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

FOLLOW US ON TWITTER
@THE_CIPL