The Privacy 'win-win'
How Can Data Protection be a Differentiator for Businesses and Citizens in a Hyper-connected Age?

Brussels, 18 February 2020
Opening Remarks

Bojana Bellamy, President, CIPL
• 16:00 – 16:10  Opening Remarks  
  Bojana Bellamy, President, CIPL

• 16:10 – 16:40  Keynote by Didier Reynders, European Commissioner for Justice  
  "Valuing Privacy in the Digital Transformation - Setting out the Commission's agenda"

• 16:40 – 17:00  Presenting the Cisco Consumer Privacy Survey and Annual Data Privacy Benchmark Study  
  Lorena Marciano, Director and EMEAR Privacy Officer  
  Chris Gow, Senior Director, EU Public Policy, Cisco

• 17:00 – 18:00  Expert Panel  
  Moderated by Alberto Di Felice – Senior Policy Manager, Digital Europe  
  David Stevens, Chairman of the Belgian Data Protection Authority  
  Caroline Louveaux, Chief Privacy Officer, Mastercard  
  Nathalie Laneret, Director of Privacy Policy, CIPL

• 18:00 – 19:00  Reception
Accountability requires comprehensive privacy programmes that translate legal requirements into risk-based, verifiable and enforceable corporate practices and controls.

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

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

Company values and business ethics shape accountability.

Leadership and Oversight

Effective Compliance and Protection for Individuals

- Risk Assessment
- Policies and Procedures
- Transparency
- Training and Awareness
- Monitoring and Verification
- Response and Enforcement
### Accountability – Examples of Content of Privacy Management Programs

#### 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 program level
- At product or service level
- DPIA for high risk processing
- Risk register
- Risk to organizations
- 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

Organizations must be able to **demonstrate their own implementation** - internally and externally
Benefits of Accountability
For Individuals, Organisations and DPAs

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

Organisations
- Ensures data protection, sustainability and digital trust
- Mitigates legal, commercial and reputational risks
- Enables new business models, digitalisation and data-driven innovation

DPAs
- Reduces enforcement and oversight burden of DPAs
- Promotes constructive engagement with accountable organisations
- Encourages race to the top rather than race to the bottom
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 Papers on Accountability in Data Protection

Organizational Accountability in Light of FTC Consent Orders
13 November 2019
https://bit.ly/3a8PuQ7

Introduction: The Central Role of Organizational Accountability in Data Protection
23 July 2018

CIPL Q&A on Accountability
3 July 2019

The Case for Accountability: How it Enables Effective Data Protection and Trust in the Digital Society
23 July 2018

Accountability’s existence in US Regulatory Compliance and its Relevance for a US Federal Privacy Law
3 July 2019

Incentivising Accountability: How Data Protection Authorities and Law Makers Can Encourage Accountability
23 July 2018
Keynote by Didier Reynders, European Commissioner for Justice

Valuing Privacy in the Digital Transformation
Setting out the Commission's agenda
Presenting the Cisco Consumer Privacy Survey and Annual Data Privacy Benchmark Study

Lorena Marciano, Director and EMEAR Privacy Officer
Chris Gow, Senior Director, EU Public Policy, Cisco
Expert Panel

Alberto Di Felice – Senior Policy Manager, Digital Europe
David Stevens, Chairma, Belgian Data Protection Authority
Caroline Louveaux, Chief Privacy Officer, Mastercard
Nathalie Laneret, Director of Privacy Policy, CIPL
Attractive Return on Privacy Investment

Average Organization

$2.7M Privacy Benefits

$1.2M Privacy Spend

Privacy Benefits Compared to Investments (% of Organizations)

- 47% Benefits at least 2 times investments
- 12% Benefits 1 to 2 times investments
- 33% Benefits roughly the same as investments
- 8% Benefits less than investments
Privacy benefits exceed spending for all company sizes

<table>
<thead>
<tr>
<th>Company size (number of employees)</th>
<th>Privacy Spending</th>
<th>Privacy Benefits</th>
</tr>
</thead>
<tbody>
<tr>
<td>250-499</td>
<td>0.8</td>
<td>1.8</td>
</tr>
<tr>
<td>500-999</td>
<td>1.2</td>
<td>2.3</td>
</tr>
<tr>
<td>1,000-9,999</td>
<td>1.3</td>
<td>2.9</td>
</tr>
<tr>
<td>10,000+</td>
<td>1.9</td>
<td>4.1</td>
</tr>
</tbody>
</table>
Average privacy returns, by country

Global average = 2.7

UK: 3.5
France: 2.5
Spain: 3.2
Germany: 2.6
Italy: 2.4
Business impact of privacy

Percentage of companies getting significant benefits from each area

<table>
<thead>
<tr>
<th>Area</th>
<th>Last Year</th>
<th>This Year</th>
</tr>
</thead>
<tbody>
<tr>
<td>Agility &amp; Innovation</td>
<td>42%</td>
<td>71%</td>
</tr>
<tr>
<td>Operational Efficiency</td>
<td>41%</td>
<td>72%</td>
</tr>
<tr>
<td>Mitigating Breach Losses</td>
<td>39%</td>
<td>71%</td>
</tr>
<tr>
<td>Investor Appeal</td>
<td>36%</td>
<td>73%</td>
</tr>
</tbody>
</table>
Value of Accountability

CIPL Accountability Wheel

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

Accountability
- Effective Compliance and Protection for Individuals

Distribution of Organizations

High Accountability (Above 4.0)
- 33%

Medium Accountability (3.0 to 4.0)
- 42%

Low Accountability (3.0 or less)
- 25%
Value of accountability

Probability of Being Breach-free
- Low: 13%
- Medium: 13%
- High: 28%

Probability Records Impacted (000's)
- Low: 148
- Medium: 108
- High: 106

Average Sales Delay (weeks)
- Low: 5.5 weeks
- Medium: 3.9 weeks
- High: 3.6 weeks

Privacy Returns
- Low: 2.3x
- Medium: 2.7x
- High: 3.1x
Privacy certifications as a buying factor

- ISO 27701
- EU/Swiss-U.S. Privacy Shield
- APEC Cross-Border Privacy Rules
- EU Binding Corporate Rules
• Privacy Actives segment

• Attitudes about GDPR and privacy regulation

• Ongoing Challenges for Consumers
The “Privacy Actives” segment (EU)

I care, I’m willing to act, and I’ve changed providers or companies over data privacy policies / practices

23%

Won’t buy if don’t trust how data is used

<table>
<thead>
<tr>
<th></th>
<th>Privacy Actives</th>
<th>Others</th>
</tr>
</thead>
<tbody>
<tr>
<td>0-20%</td>
<td>56%</td>
<td>20%</td>
</tr>
<tr>
<td>20-40%</td>
<td>91%</td>
<td>56%</td>
</tr>
<tr>
<td>40-60%</td>
<td>91%</td>
<td>56%</td>
</tr>
<tr>
<td>60-80%</td>
<td>91%</td>
<td>56%</td>
</tr>
<tr>
<td>80-100%</td>
<td>91%</td>
<td>56%</td>
</tr>
</tbody>
</table>

How they treat data is how they treat me

<table>
<thead>
<tr>
<th></th>
<th>Privacy Actives</th>
<th>Others</th>
</tr>
</thead>
<tbody>
<tr>
<td>0-20%</td>
<td>83%</td>
<td>62%</td>
</tr>
<tr>
<td>20-40%</td>
<td></td>
<td></td>
</tr>
<tr>
<td>40-60%</td>
<td></td>
<td></td>
</tr>
<tr>
<td>60-80%</td>
<td></td>
<td></td>
</tr>
<tr>
<td>80-100%</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Source: Cisco Consumer Privacy Study - 2019

© 2020 Cisco and/or its affiliates. All rights reserved.
Who should be responsible (EU):

Who should be primarily responsible for protecting data privacy?

- National Government: 50%
- Companies: 18%
- Local Government: 9%
- Associations: 3%
- Individual User: 20%

Source: Cisco Consumer Privacy Study – 2019
GDPR Awareness (EU)

Awareness of GDPR
N=2601

All Respondents

55% Aware
45% Not Aware

By Country

- Italy: 42%
- France: 48%
- Spain: 56%
- Germany: 64%
- UK: 67%

Source: Cisco Consumer Privacy Study – 2019
GDPR Sentiment, by country (EU average)

- Positive: 44%
- Negative: 7%
- Neutral: 49%
Among other things, GDPR has enhanced consumers’ control and rights regarding their data

Impact of GDPR on the individual

<table>
<thead>
<tr>
<th>Statement</th>
<th>Disagree</th>
<th>Neutral</th>
<th>Agree</th>
</tr>
</thead>
<tbody>
<tr>
<td>I have more control over my personal data</td>
<td>22%</td>
<td>36%</td>
<td>42%</td>
</tr>
<tr>
<td>I have greater ability to exercise my rights regarding my data</td>
<td>15%</td>
<td>35%</td>
<td>50%</td>
</tr>
<tr>
<td>I have a great level of trust in companies that use my data</td>
<td>23%</td>
<td>43%</td>
<td>34%</td>
</tr>
<tr>
<td>I receive too many meaningless notifications as a result of GDPR</td>
<td>19%</td>
<td>34%</td>
<td>47%</td>
</tr>
</tbody>
</table>

Source: Cisco Consumer Privacy Study – 2019

© 2020 Cisco and/or its affiliates. All rights reserved.
Many consumers still are unable to effectively protect their data – EU

Are you able to effectively protect your personal data today?

- Yes: 55%
- No: 45%

Reasons why not?

- Too hard to figure out what companies are actually doing with my data: 70%
- If I want the service, I have to accept how my data is used: 45%
- Feel my personal data is already available: 43%
- Don’t trust companies to follow stated policies: 39%
- Don’t understand what service choices are: 37%

Source: Cisco Consumer Privacy Study – 2019