

Federal Trade Commission  
Via Online Submission  
Competition and Consumer Protection in the 21<sup>st</sup> Century Hearings, Project Number P181201

16 August 2018

**RE: The Commission’s remedial authority to deter unfair and deceptive conduct in privacy and data security matters — the identification of any additional tools or authorities the Commission may need to adequately deter unfair and deceptive conduct related to privacy and data security**

The Centre for Information Policy Leadership (CIPL) welcomes this opportunity to respond to the Federal Trade Commission’s request for comments on the Commission’s remedial authority to deter unfair and deceptive conduct in privacy and data security matters and, in particular, on the identification of any additional tools or authorities the Commission may need in that connection.

CIPL recently published two white papers on the central role of organizational accountability in data protection which are directly relevant to this topic. Accountability, as a concept in data protection, comprises a whole range of tools which enable scalable compliance and foster corporate digital responsibility beyond pure legal compliance. Data protection authorities (DPAs) (such as the FTC) have a crucial role to play in proactively incentivizing organizational accountability.

Organizational accountability preemptively addresses unfair and deceptive conduct related to privacy and data security matters by ensuring that organizations have an accountable and comprehensive internal privacy management program in place or participate in certified or verified accountability schemes such as APEC CBPR, EU BCR, GDPR certifications or codes of conduct. Furthermore, by incentivizing accountability, organizations are more likely to implement it at a level above and beyond mere compliance with laws. They will have the necessary motivation to make the required investments in upper end or heightened accountability. Organizations that are incentivized to achieve gold plate corporate digital responsibility are focused on getting it right which is contrary to engaging in unfair or deceptive conduct related to privacy and data security.

The first CIPL white paper on this topic, entitled, *“The Case for Accountability: How it Enables Effective Data Protection and Trust in Digital Society”* explains how accountability provides the necessary framework and tools for scalable compliance, fosters corporate digital responsibility beyond pure legal compliance, and empowers and protects individuals. It also details the benefits of implementing accountability to individuals, regulators and organizations.

The second CIPL white paper on this topic, entitled, *“Incentivizing Accountability: How Data Protection Authorities and Law Makers Can Encourage Accountability”* explains why and how accountability should be specifically incentivized, particularly by DPAs and law makers. It argues that given the many benefits of accountability for all stakeholders, DPAs and law makers should encourage and incentivize organizations to implement accountability. They should not merely rely on the threat of sanctions to ensure legally required accountability, nor should they leave the implementation of heightened accountability (i.e., accountability beyond what is legally required) to various “internal” incentives of the organizations, such as improved customer trust and competitive advantage. Instead, DPAs and law makers should proactively provide additional external incentives, including on the grounds that accountability provides broader benefits to all stakeholders beyond just the organization itself and specifically helps DPAs carry out their many regulatory tasks.

CIPL believes that finding ways to further support, encourage and incentivize organizational accountability can serve as a relevant additional tool that the FTC could utilize to adequately address unfair and deceptive conduct related to privacy and data security.

I attach a copy of the introductory overview of CIPL’s white papers and the two recently published papers as an annex to this letter.

Thank you for the opportunity to comment and I hope that these materials are useful to the FTC. If you would like to discuss this paper further or require additional information, please contact Bojana Bellamy at [bbellamy@huntonak.com](mailto:bbellamy@huntonak.com) or Markus Heyder at [mheyder@huntonak.com](mailto:mheyder@huntonak.com).

Sincerely,



Markus Heyder

Vice President and Senior Policy Counselor,  
Centre for Information Policy Leadership



## **Introducing Two New CIPL Papers on The Central Role of Organisational Accountability in Data Protection**

Accountability has become a key building block of data protection through legislation, regulatory guidance, global standards, privacy enforcement outcomes, as well as through general adoption by enlightened global organisations that have made it the basis of their corporate privacy and information management programs. The European Union has incorporated the concept of accountability into the General Data Protection Regulation (GDPR), which went into effect on 25 May 2018.<sup>1</sup> There is opportunity for accountability to become the bridge that connects different legal regimes, regardless of the legal frameworks involved. It is, however, essential that accountability is properly understood and applied consistently according to a well-established global meaning to ensure such interoperability between regions.

The Centre for Information Policy Leadership<sup>2</sup> (CIPL) has issued two new papers on the topic of organisational accountability. Collectively, the goal of these two papers is to show that:

- Organisational accountability is central to effective data protection. It places the principal responsibility for protecting personal data and privacy where it belongs — on organisations that collect or handle personal data. Accountability is also essential for the digital transformation of our society and economy in the fourth industrial revolution (4IR). It is the only antidote to the current trust deficit in the digital economy and complex information ecosystem.
- The concept of accountability is already well established and understood globally. To ensure global coherence and further convergence with respect to this concept, “GDPR accountability” must be interpreted and applied consistently in line with this generally accepted understanding. This includes taking into account the earlier Opinion on accountability by the Article 29 Data Protection Working Party (WP29).<sup>3</sup>
- The many benefits of organisational accountability to all stakeholders warrant incentivising the implementation of accountability, particularly where such accountability goes above and beyond what is strictly required by law.

Both papers can be accessed on CIPL’s website at:

**The Case for Accountability: How it Enables Effective Data Protection and Trust in the Digital Society**  
[http://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl\\_accountability\\_paper\\_1\\_-\\_the\\_case\\_for\\_accountability\\_-\\_how\\_it\\_enables\\_effective\\_data\\_protection\\_and\\_trust\\_in\\_the\\_digital\\_society.pdf](http://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_accountability_paper_1_-_the_case_for_accountability_-_how_it_enables_effective_data_protection_and_trust_in_the_digital_society.pdf)

**Incentivising Accountability: How Data Protection Authorities and Law Makers Can Encourage Accountability**  
[http://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl\\_accountability\\_paper\\_2\\_-\\_incentivising\\_accountability\\_-\\_how\\_data\\_protection\\_authorities\\_and\\_law\\_makers\\_can\\_encourage\\_accountability.pdf](http://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_accountability_paper_2_-_incentivising_accountability_-_how_data_protection_authorities_and_law_makers_can_encourage_accountability.pdf)

### CIPL Paper One

The first of the two papers is entitled “**The Case for Accountability: How it Enables Effective Data Protection and Trust in the Digital Society.**” It explains the following:

- The concept of organisational accountability and how it is reflected in the GDPR;
- The essential elements of accountability and how the requirements of the GDPR (and of other normative frameworks) map to these elements;
- Global acceptance and adoption of accountability;
- How organisations can implement accountability (including by and between controllers and processors) through comprehensive internal privacy programs that implement external rules or the organisation’s own data protection policies and goals, or through verified or certified accountability mechanisms, such as Binding Corporate Rules (BCR), APEC Cross-Border Privacy Rules (CBPR), APEC Privacy Recognition for Processors (PRP), other seals and certifications, including future GDPR certifications and codes of conduct; and
- The benefits that accountability can deliver to each stakeholder group.

The following diagram shows the essential elements of accountability:



The objective of the paper is to promote a general understanding of how, through its essential elements, accountability provides the necessary framework and tools for scalable legal compliance by controllers and processors; how it empowers and protects individuals with respect to the use of their personal data and fosters corporate digital responsibility that goes beyond what is strictly required by law; and how it provides significant benefits to all stakeholders and ultimately enables trust in the digital economy and society.

Accountability places primary responsibility for protecting individuals on the organisation rather than the individual. This is important in an increasingly complex information ecosystem in which individuals are frequently not in a position to carry that responsibility themselves. Through its core elements such as risk-assessment, consideration of fairness and ethics, appropriate oversight, training and ongoing internal monitoring, accountability enables appropriate, context-specific mitigations and controls for risks associated with the technologies and business practices deployed by organisations. Accountability also involves maximum transparency, which enables regulatory oversight, as well as consumer trust and informed choices. Organisations can implement accountability both through independent, organisation-specific internal privacy programs and through participation in privacy certifications, seals, codes of conduct and other formal accountability schemes. Accountability can be implemented with reference to a law, other external standard or framework, or based on internal policies.

Accountability shapes not only the relationship between organisations, individuals and regulators but also the relationship between different organisations in the ecosystem, including controllers and processors. Indeed, the more organisations demonstrate a commitment to accountability and responsible data use, the more individuals, regulators and business partners will trust them to use data productively for the benefit of all. If implemented appropriately, accountability will deliver substantial benefits to all stakeholders and the digital society at large, including “bridge building” between privacy regimes. It will also promote more constructive engagement between organisations, individuals, society and data protection authorities (DPAs), which is essential for the success of the 4IR.

### **Benefits of Organisational Accountability by Stakeholder**

<b>Benefits for Organisations</b>
<ul style="list-style-type: none"> <li>• Enables more effective privacy protections by requiring risk-based prioritisation of such protections.</li> </ul>
<ul style="list-style-type: none"> <li>• Assists organisations in ensuring and demonstrating legal compliance to business partners and regulators.</li> </ul>
<ul style="list-style-type: none"> <li>• Fosters a culture of internal privacy compliance and constructive engagement with DPAs.</li> </ul>
<ul style="list-style-type: none"> <li>• Fosters good data hygiene and good data management and helps to support the strategic objectives of organisations around data.</li> </ul>
<ul style="list-style-type: none"> <li>• Enables greater harmonisation of organisations’ privacy policies and practices with the various requirements of the different jurisdictions in which they do business.</li> </ul>
<ul style="list-style-type: none"> <li>• Generates trust among the public and regulators that the organisation is processing personal data responsibly, potentially enhancing the reputation and goodwill of the organisation and adding value to its brand (trust advantage<sup>4</sup>).</li> </ul>
<ul style="list-style-type: none"> <li>• Enables organisations to engage in broader beneficial uses of personal data, including data for social good, research and responsible AI and machine learning by minimising the risks of new data uses (e.g., through incorporating privacy by design, transparency, risk assessment, etc.) and demonstrating responsible data use to regulators.</li> </ul>

- Assists SMEs with implementing scalable privacy tools and controls within their organisations, appropriate to their size and type of operation.
- Provides legal certainty for organisations with regard to cross-border data protection compliance through participation in recognised accountability frameworks, such as BCR and CBPR.
- Enables cross-border data transfers through recognised mechanisms such as BCR and CBPR.
- Furthers the creation of interoperability between different accountability frameworks and thus global solutions to data transfers for organisations.
- Helps differentiate between organisations and provides a competitive edge to those who choose to invest in accountability relative to those who do not (accountability advantage).
- Improves overall level of privacy behaviours of organisations which in turn improves the health of the data ecosystem in general and benefits all stakeholders in the digital economy in the long run.
- Serves as a due diligence tool for controllers in identifying qualified and accountable processors.

#### **Benefits for Individuals**

- Delivers real and more effective protection of individuals and their data.
- Ensures that the protection follows personal data transferred across borders.
- Assures individuals that compliance with local legal requirements are met and increases individuals' trust in organisations' processing of their data.
- Enhances privacy protections for individuals beyond minimum requirements and empowers individuals in the management of their data (e.g., through the extension of individual rights or voluntary security breach reporting by organisations).
- Shifts the burden of protecting individuals more explicitly to organisations.
- Provides individuals with a benchmark for deciding whether to allow their data to be processed by certain organisations.
- Provides individuals' rights and interests heightened consideration and protection through required risk assessments and balancing processes.
- Permits individuals to reap the benefits of participation in the digital society.
- Enables more effective domestic and cross-border enforcement.

#### **Benefits for Regulators**

- Provides assurance to DPAs that organisations are identifying and prioritising high-risk data processing.
- Reduces the oversight, complaint-handling and enforcement burdens of DPAs through the involvement of third-party certifiers, Accountability Agents and third-party dispute resolution bodies.
- Allows DPAs to be more selective and strategic with their often limited resources in pursuing their overall mission.
- Promotes constructive engagement with accountable organisations.
- Improves cross-border privacy enforcement cooperation through the creation of mutually recognised requirements and processes, such as in BCR and CBPR.
- Assists DPAs in carrying out investigations and enforcement actions by bridging together different legal regimes and providing a more uniform data protection environment.
- Simplifies investigations and enforcement actions and enables companies to demonstrate compliance to DPAs by requiring organisations to maintain records of processing.
- Keeps organisations honest in terms of claims made to the public by facilitating exposure of false claims.

## CIPL Paper Two

The second of the two papers is entitled “**Incentivising Accountability: How Data Protection Authorities and Law Makers Can Encourage Accountability.**” It explains why and how accountability should be specifically incentivised, particularly by DPAs and law makers.

Accountability not only enables compliance with the law but may also include measures that go above and beyond pure legal compliance and encourages the development of a privacy sensitive culture. It demonstrates that an organisation, often as a matter of “enlightened self-interest,” wants to “get it right” and is trying to do so. This paper argues that, given the many benefits of accountability for all stakeholders, DPAs and law makers should encourage and incentivise organisations to implement accountability, and should not leave incentivising legally required accountability to the threat of sanctions, or the implementation of accountability beyond purely legal compliance to various “internal” incentives of the organisation, such as increased consumer trust and a competitive advantage. Instead, DPAs and law makers should provide additional external incentives on the grounds that accountability provides broader benefits to stakeholders beyond the organisation itself, including serving as an important signal for DPAs to identify and differentiate responsible organisations and helping them to target their limited enforcement resources where they are most needed and effective.

Examples of accountability that exceed basic legal requirements include organisations implementing risk mitigations and controls or undertaking other protective measures that are not specifically required by law and organisations participating in non-mandatory privacy certifications and codes of conduct or similar formal privacy accountability schemes, such as BCR, APEC CBPR and PRP, other seals and certifications, including future GDPR certifications and codes of conduct. Accountability also provides specific and tangible benefits directly to DPAs, because it facilitates the exercise of their duties, thereby providing further justification for encouraging and incentivising it.

There is a broad range of incentives that DPAs and/or law makers should provide to encourage accountability, as shown in this table<sup>5</sup>:

### **Incentives for Implementing Accountability**

Using demonstrated accountability<sup>6</sup> as a differentiating or mitigating factor in investigation or enforcement contexts

For example:

- As one of the discretionary factors in considering whether to initiate an investigation or enforcement action.
- As a mitigating factor in assessing the type of penalties and levels of fines.
- As a mitigating factor in case of an individual failure/human error, where the organisation is able to demonstrate that it took the reasonable precautions to prevent the failure or error.

DPAs should communicate this policy regularly and refer to it in specific enforcement cases.

Using demonstrated accountability as a “licence to operate” and use data responsibly, based on organisations’ evidenced commitment to data protection

As one of the bases for:

- Facilitating responsible AI, machine learning, automated decision-making and other big data applications because of the risk assessment, mitigations and other controls in the accountability program.
- Allowing broader use of data for social good and research.
- Participation in relevant “regulatory sandbox” initiatives.

Publicly recognising best in class organisations and showcasing accountable “best practices” (including those that may be an aggregation of such best practices compiled and generalised by regulators)

- To promote reputation and trust of accountable organisations.
- To promote healthy peer pressure and competition in the marketplace.

Supporting and guiding organisations (particularly small and emerging companies) on a path towards accountability, either individually or through association bodies

For example:

- Compliance Agreements used by the Canadian Office of the Privacy Commissioner.

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

- Similar to proposals contained in the Privacy Bridges Report of 37<sup>th</sup> International Privacy Conference, Amsterdam 2015<sup>7</sup> (See Bridge 10 on Collaborating on and Funding for Privacy Research Programs).
- Specific grants by regulators such as the UK ICO and Canadian Federal and Provincial regulators to fund research projects in accountability.

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

- In context of novel technology or business models.
- Offer specific resources, including documentation and dedicated contact persons, to support the implementation of heightened accountability.

Using accountability as evidence of due diligence

For example:

- In a selection process of processors and other vendors.
- In M&A transactions.

Using formal accountability schemes as evidence of uniform and high level privacy protection to enable cross-border data transfers within the company group and to third parties

- APEC CBPR and PRP; EU BCR; GDPR certifications.

Articulate proactively the elements and levels of accountability to be expected

- For instance, at what point would expecting accountability measures constitute undue hardship to organisations?<sup>8</sup>
- Based on the concept of proportionality and a risk-based approach to accountability measures.

Indeed, providing such incentives would be a core component of a results-based approach to data protection oversight and enforcement that relies on constructive engagement with industry as further described in CIPL’s 2017 discussion paper on “Regulating for Results — Strategies and Priorities for Leadership and Engagement.”<sup>9</sup>

CIPL believes that taking accountability seriously and proactively incentivising it is essential to creating trust in the digital economy and society and, in fact, will be game-changing in that respect.

## References

---

<sup>1</sup> Prior to the GDPR, the concept of “accountability” arguably was already implicit in the Data Protection Directive (Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data) as well as case law and the Article 29 Working Party’s Opinion on accountability (WP29 Opinion 3/2010 on the principle of accountability, adopted 13 July 2010, available at [http://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2010/wp173\\_en.pdf](http://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2010/wp173_en.pdf)).

<sup>2</sup> CIPL is a global data privacy and cybersecurity think tank in the law firm of Hunton Andrews Kurth and is financially supported by the law firm and 61 member companies that are leaders in key sectors of the global economy. CIPL’s mission is to engage in thought leadership and develop best practices that ensure both effective privacy protections and the responsible use of personal information in the modern information age. CIPL’s work facilitates constructive engagement between business leaders, privacy and security professionals, regulators and policymakers around the world. For more information, please see CIPL’s website at <http://www.informationpolicycentre.com/>. Nothing in this paper should be construed as representing the views of any individual CIPL member company or of the law firm of Hunton Andrews Kurth.

<sup>3</sup> The European Data Protection Board (EDPB) might consider re-issuing the WP29 Opinion on accountability.

<sup>4</sup> See The Trust Advantage: How to Win with Big Data, Boston Consulting Group, November 2013, available at <https://www.bcg.com/publications/2013/marketing-sales-trust-advantage-win-with-big-data.aspx>.

<sup>5</sup> Some of these incentives may already be promoted today. For example, using formal accountability schemes as evidence of uniform and high-level privacy protection to enable cross-border data transfers within the company group and to third parties is a typical incentive of implementing BCRs. Where an incentive is already actively promoted, efforts should be made for its continued provision.

<sup>6</sup> “Demonstrated accountability” includes all the essential elements of accountability (i.e., leadership and oversight, risk assessment, policies and procedures, transparency, training and awareness, monitoring and verification, and response and enforcement). Thus, the degree to which each of the accountability elements are demonstrably implemented within an organisation will impact the degree to which such implementation can serve as a mitigating factor.

<sup>7</sup> Privacy Bridges: EU and US Privacy Experts in Search of Transatlantic Privacy Solutions, 37<sup>th</sup> International Privacy Conference, Amsterdam, 2015, at page 40, available at <https://privacybridges.mit.edu/sites/default/files/documents/PrivacyBridges-FINAL.pdf>.

<sup>8</sup> Some regulators, as a matter of their statutory duty, already consider the impact on organisations of adopting regulator recommendations as to best practices. Making these determinations for more of their recommendations and suggested best practices will include conducting more detailed impact assessments to measure the costs and benefits to organisations of adopting such practices.

<sup>9</sup> “Regulating for Results — Strategies and Priorities for Leadership and Engagement”, 10 October 2017, available at [https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl\\_final\\_draft\\_-\\_regulating\\_for\\_results\\_-\\_strategies\\_and\\_priorities\\_for\\_leadership\\_and\\_engagement\\_2\\_.pdf](https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_final_draft_-_regulating_for_results_-_strategies_and_priorities_for_leadership_and_engagement_2_.pdf).



## **The Central Role of Organisational Accountability in Data Protection**

**Discussion Paper 1 (of 2)**

# **The Case for Accountability: How it Enables Effective Data Protection and Trust in the Digital Society**

Centre for Information Policy Leadership

**23 July 2018**

## Table of Contents

<b>I. Objectives of this Paper</b> .....	3
<b>II. Background on Organisational Accountability</b> .....	4
A. The Elements of Accountability .....	5
B. Approaches to Implementing Accountability .....	8
C. Accountability under the GDPR.....	10
1. Controllers.....	10
2. Processors .....	11
3. Elements of Accountability in the GDPR and in General .....	12
D. Implementing and Demonstrating Accountability within an Organisation.....	13
1. Comprehensive Internal Privacy Programs.....	14
2. Co-regulatory Frameworks, Certifications, Codes of Conduct or Similar Schemes.....	14
E. Which Organisations are Expected to be “Accountable”?.....	15
1. Controllers and Processors .....	15
a. The Impact of Accountability on Contractual Provisions and Negotiations.....	16
2. Public Sector Organisations .....	18
<b>III. The Benefits of Accountability</b> .....	19
A. Accountability Benefits to Stakeholders.....	20
B. Types and Categories of Accountability Benefits.....	21
<b>IV. Conclusion</b> .....	26

## I. Objectives of this Paper

Accountability now has broad international support and has been adopted in many laws, including in the EU General Data Protection Regulation (GDPR), regulatory policies and organisational practices. It is essential that there is consensus and clarity on the precise meaning and application of organisational accountability among all stakeholders, including organisations implementing accountability and data protection authorities (DPAs) overseeing accountability. Without such consensus, organisations will not know what DPAs expect of them and DPAs will not know how to assess organisations' accountability-based privacy programs with any degree of consistency and predictability. Thus, drawing from the global experience with accountability to date and from the Centre for Information Policy Leadership's (CIPL)<sup>1</sup> own extensive prior work on accountability, this paper seeks to explain the following issues:

- The concept of organisational accountability and how it is reflected in the GDPR;
- The essential elements of accountability and how the requirements of the GDPR (and of other normative frameworks) map to these elements;
- Global acceptance and adoption of accountability;
- How organisations can implement accountability (including by and between controllers and processors) through comprehensive internal privacy programs that implement external rules or the organisation's own data protection policies and goals, or through verified or certified accountability mechanisms, such as Binding Corporate Rules (BCR), APEC Cross-Border Privacy Rules (CBPR), APEC Privacy Recognition for Processors (PRP), other seals and certifications, including future GDPR certifications and codes of conduct; and
- The benefits that accountability can deliver to each stakeholder group.

In addition, the paper argues that accountability exists along a spectrum, ranging from basic accountability requirements required by law (such as under the GDPR) to stronger and more granular accountability measures that may not be required by law but that organisations may nevertheless want to implement because they convey substantial benefits.

Indeed, in its earlier Opinion on accountability,<sup>2</sup> the Article 29 Data Protection Working Party (WP29) specifically recognised and supported implementing accountability through voluntary accountability schemes, characterising them as a "second tier" of accountability beyond what may be strictly required by law:

[T]he 'legal architecture' of the accountability mechanisms would envisage two levels: the first tier would consist of a basic statutory requirement binding upon *all* data

controllers. The content of the requirement would include two elements: the implementation of measures/procedures, and the maintenance of evidence thereto. Specific requirements could complement this first tier. A second tier would include voluntary accountability systems that go above and beyond the minimum legal requirements, as far as the underlying data protection principles (providing higher safeguards than those required under the applicable rules) and/or in terms of how they implement or ensure the effectiveness of the measures (implement requirements that go beyond the minimum level).<sup>3</sup>

Of course, such heightened and voluntary accountability is not limited to formal accountability systems (such as BCR, codes of conduct and certifications) — organisations can also implement accountability through their own internal privacy programs. Regardless of how such heightened accountability is implemented, however, it should be encouraged and incentivised.

Thus, while in this paper we focus on the concept of accountability, issues relating to its implementation and the benefits of accountability to various stakeholders, the second paper in this series addresses the specific issue of incentivising accountability, especially where it goes above the minimum legal requirements.<sup>4</sup> The second paper explains:

- How and why accountability measures, ideally, should exceed the minimum legal requirements;
- The many benefits of accountability to all stakeholders, including DPAs, particularly as it moves up along the accountability spectrum from the required basics to “heightened accountability”; and
- Why DPAs and legislators should incentivise accountability and what the incentives might be?

## II. Background on Organisational Accountability

In a nutshell, the concept of “accountability” requires organisations to take necessary steps to:

- a) Implement applicable data protection requirements or goals; and
- b) Be able to demonstrate such implementation.

In its 2010 Opinion on accountability, the WP29 defined accountability as follows: “a statutory accountability principle would explicitly require data controllers to implement appropriate and effective measures to put into effect the principles and obligations [of the applicable law] and demonstrate this on request.”<sup>5</sup> Similarly, in its earlier work on this topic, CIPL explained that accountability “involves setting privacy protection goals for companies based on criteria established in law, self-regulation and best practices, and vesting the organisation with both

the ability and the responsibility to determine appropriate, effective measures to reach those goals,” complemented by the “organisation’s ability to demonstrate its capacity to achieve specified privacy objectives.”<sup>6</sup>

The understanding of accountability set forth in the previous paragraph has become a cornerstone of effective data protection and a dominant trend in global data privacy law, policy and organisational practices. Indeed, the term encapsulates what most regulators now expect of responsible organisations that handle personal data and what many privacy frameworks and data protection laws have incorporated as a matter of basic obligation or best practice. As recommended by the WP29 in its 2010 Opinion on accountability, the GDPR has now explicitly incorporated accountability into EU data protection law.<sup>7</sup> The OECD Privacy Guidelines<sup>8</sup> and the APEC Privacy Framework<sup>9</sup> have long since explicitly incorporated accountability as a core data protection concept, and data privacy regulators in numerous jurisdictions have issued regulatory guidance or enforcement orders encouraging or requiring accountability including, Canada, Mexico, Hong Kong, Singapore, Australia, Colombia and the United States.<sup>10</sup> Also, the revised Council of Europe Convention 108 makes explicit that accountability is a key concept.<sup>11</sup>

#### **A. The Elements of Accountability**

Accountability-based data privacy and governance programs typically encompass and address each individual element of accountability. The “Accountability Wheel” in *Figure 1* below identifies the essential elements of organisational accountability (which are further explained in *Table 1* below). They include:

- 1) Leadership and Oversight
- 2) Risk Assessment (including DPIA)
- 3) Policies and Procedures (including Fairness and Ethics)
- 4) Transparency
- 5) Training and Awareness
- 6) Monitoring and Verification
- 7) Response and Enforcement

These elements have already been developed and promoted by global organisations,<sup>12</sup> as well as in CIPL’s previous work on accountability.<sup>13</sup> They are consistent also with regulatory guidance, for example, privacy management program guidance from both the Hong Kong and Canadian Privacy Commissioners<sup>14</sup> and the WP29’s 2010 Opinion on accountability. Furthermore, these elements are consistent with other areas of corporate law and compliance,

including anti-bribery, anti-money laundering (AML), export control and competition.<sup>15</sup> They have been used by organisations, regulators and courts to determine if an organisation has maintained an effective and comprehensive compliance program in any given regulatory area.

With accountability firmly part of the GDPR and widely adopted in other global laws and regimes, many organisations will be investing in comprehensive data privacy and governance programs. Not all organisations will have to begin this process from scratch. Many organisations already have comprehensive privacy programs or will have already implemented non-privacy accountability-based compliance frameworks and can leverage and mutualise their existing efforts to create, streamline and merge accountability for data protection into their broader corporate accountability programs. Thus, it is critical that there is a uniform understanding of the concept of accountability and a harmonised interpretation of how to deliver accountability in practice for all stakeholders:

- For the organisations implementing accountability;
- For the regulators that are enforcing it; and
- For individuals who are the focus of privacy law and compliance and who will ultimately benefit from accountability, as it is designed to deliver more effective protection for individuals and their data.

This paper seeks to promote consensus in understanding the elements of accountability, to ensure that organisations implement them consistently and that DPAs assess and respond to such implementation consistently and predictably.

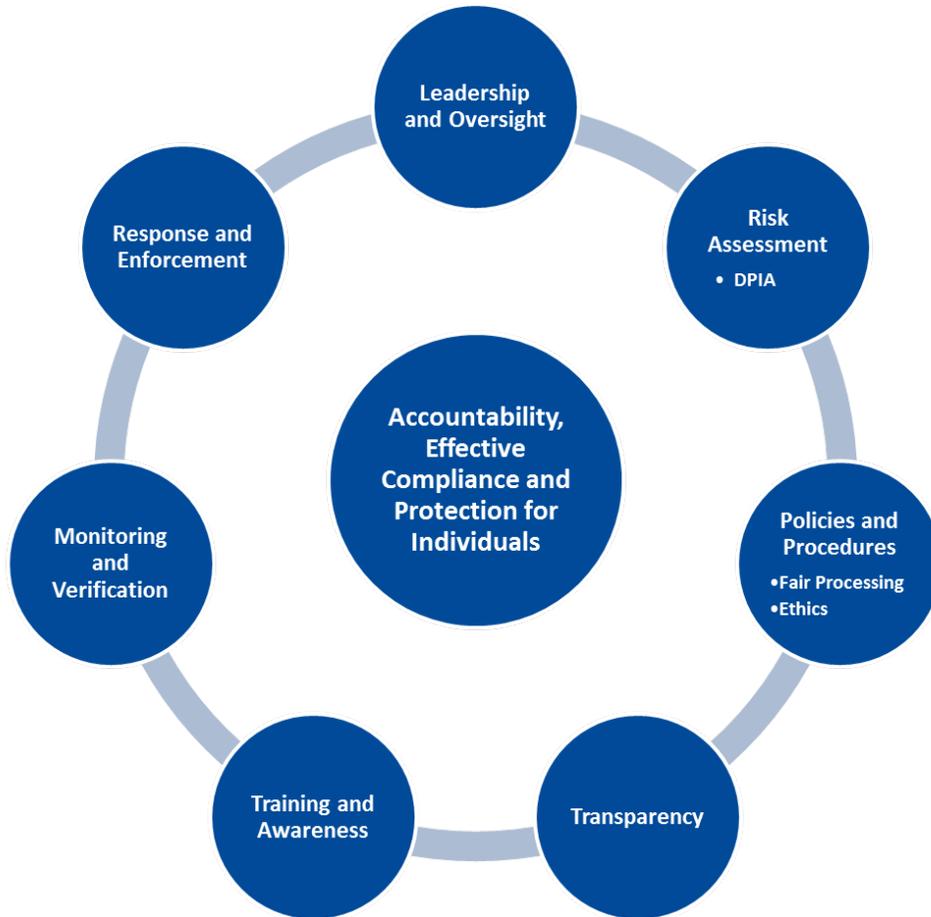


Figure 1 – CIPL “Accountability Wheel” – Universal Elements of Accountability

Accountability Element:	The Accountable Organisation...
<b>Leadership and Oversight</b>	Ensures appropriate data privacy governance, accountability, oversight, reporting, and buy-in from mid-level and top-level management, including appointing appropriate personnel (e.g., DPO or DPO Team, senior level privacy executives and data governance staff) to oversee the organisation’s privacy and accountability program and report to senior management and the board.
<b>Risk Assessment</b>	At program level, periodically assesses its privacy program and its relevance in light of changes in business models, risk, law, technology and other external and internal factors. At product, service and project level, implements controls to identify, understand and mitigate risks to individuals and organisations. In case of a data breach incident, assesses the potential risks to the rights and freedoms of individuals to mitigate the risks and perform the relevant notifications to the DPA and the data subjects.

<b>Policies and Procedures</b>	Builds and maintains written data privacy policies and procedures that reflect applicable laws, regulations, industry standards and organisational values and goals and implements mechanisms to operationalise them throughout the organisation. This includes policies and procedures to ensure fair processing and ethical considerations.
<b>Transparency</b>	Communicates to individuals critical information about its data privacy program, procedures and protections, as well as the benefits and/or potential risks of data processing and information about individual rights through easily accessible means (e.g., privacy notices, policies and transparency tools such as dashboards and portals). Communicates and engages with relevant data privacy regulators about its privacy program.
<b>Training and Awareness</b>	Ensures ongoing training and communication to employees, contractors and others who handle data processed by the organisation about the privacy program, its objectives and controls.
<b>Monitoring and Verification</b>	Monitors ongoing internal compliance with the program, policies and procedures and establishes procedures for regular self-assessments, internal audits and in some instances external audit or certifications.
<b>Response and Enforcement</b>	Puts in place appropriate procedures for responding to inquiries, complaints, data protection breaches and internal non-compliance. Enforces against internal non-compliance with the program, rules and controls. Cooperates with third-party certification bodies, Accountability Agents, and data privacy regulators in investigations and enforcement actions.

*Table 1 – Organisational measures to implement the elements of accountability*

On page 13, *Table 2* illustrates how many of the GDPR requirements map to the above elements of accountability. It is not an exhaustive list but an example of how various legal requirements fit within the accountability framework. It is intended to aid organisations in structuring their compliance efforts and relating their compliance activities under a given law to the universal elements of accountability. Importantly, based on risk assessments and in accordance with the risk-based approach of the GDPR, organisations can set priorities in terms of measures to implement the elements of accountability based on where there is the biggest risk to the organisation and to individuals. Finally, other data privacy laws, standards or frameworks can similarly be mapped to these essential elements of accountability.

## **B. Approaches to Implementing Accountability**

Organisations can implement accountability through various means. They include:

- a) Internal organisational privacy and information management programs;
- b) Regulated frameworks such as EU Binding Corporate Rules (BCR)<sup>16</sup> and the EU-US Privacy Shield;<sup>17</sup>

- c) Industry codes of conduct, such as the FEDMA European Code of Practice for the Use of Personal Data in Direct Marketing<sup>18</sup> or the CISPE Code of Conduct<sup>19</sup> and as envisaged in the GDPR;<sup>20</sup>
- d) Third-party certifications and seals, such as APEC Cross-Border Privacy Rules (CBPR) and the APEC Privacy Recognition for Processors (PRP),<sup>21</sup> various national privacy marks, for example, Japan's JIPDEC Privacy Mark System<sup>22</sup> and certifications envisaged in Article 42 of the GDPR;
- e) International standards, such as ISO 27018 (Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors) (hereinafter, Cloud Privacy and Security standard).<sup>23</sup>

Although each of these mechanisms differ in nature and scope, each of them requires organisations to

1. Build and implement comprehensive internal data privacy and governance programs (including policies and procedures) that implement and operationalise data privacy protections that govern the organisations' use of data. These protections can be based on:
  - legal obligations in laws such as the GDPR or other data privacy laws;
  - requirements established by accountability schemes (e.g., Privacy Shield, BCR or CBPR);
  - requirements established by internal company policies, goals or internal codes of business ethics;
  - requirements of external third-party certification schemes, seals or codes of conduct; or
  - requirements of international standards, such as the ISO Cloud Privacy and Security Standard.
2. Be able to verify the implementation of such programs internally through different assessments, controls and internal audits and, in some cases externally, through external audits or certifications.
3. Be able to demonstrate the existence and effectiveness of such programs, both internally to their corporate boards, and externally to individuals, business partners, shareholders and civil society bodies representing individuals and, upon demand, to DPAs in an investigation or enforcement context, or to a third-party certifier in the context of certified accountability frameworks.

It is important to note that due to the variety of potential external and internal sources for the privacy standards that will be operationalised through an organisation's privacy management program, this paper does not argue that accountability must be mandated or informed by a law. However, in most cases, some external standard will provide the substantive requirements that must be implemented through a privacy program or other accountability mechanism. For example, participating APEC economies in the CBPR system are required to enforce the APEC CBPR program requirements through their domestic laws but it is not a requirement that a participating economy have a dedicated data protection law in place. For instance, the US is a participating economy in the APEC CBPR system with no general law on data protection, but enforces the APEC CBPR program requirements through the US Federal Trade Commission Act.<sup>24</sup>

Further, as is evident from the above list, accountability can often be implemented through or accompanied by some form of external certification and validation, which ensures both verification and demonstration. Examples include BCR, CBPR, PRP, or certifications under ISO standards such as the ISO 27018 Cloud Privacy and Security standard and ISO 27001 (Information Security Management Systems)<sup>25</sup> and, perhaps, any future certifications under the GDPR.

### **C. Accountability under the GDPR**

As mentioned, the GDPR expressly incorporates accountability as a requirement. Although this requirement is stated explicitly with respect to controllers, the GDPR also includes increased statutory and contractual processor obligations that imply accountability obligations for processors.

#### **1. Controllers**

The following provisions of the GDPR spell out the accountability requirements for controllers:

- Article 5(2): Accountability is now explicitly a data protection principle — “The controller shall be responsible for, and be able to demonstrate compliance with paragraph 1 (accountability)”, i.e. the basic data protection principles contained in GDPR Article 5, such as fair processing, lawful basis for processing, purpose specification and limitation, data quality, etc.<sup>26</sup>
- Article 24(1): This provision concretises the concept of accountability and incorporates the risk-based approach into the GDPR.<sup>27</sup> Organisations must implement, review and keep up-to-date appropriate technical and organisational measures, including policies, procedures, rules and tools, to:
  - a) Ensure compliance with the GDPR; and

b) Be able to demonstrate compliance.

Such measures must be based on and proportionate to, among other factors, the likelihood and severity of risks for individuals. In other words, accountability and privacy management programs must be risk-based.<sup>28</sup>

Arguably, all GDPR requirements require some accountability on the part of the controller and operational policies and procedures to give effect to the legal obligations. Some of the more new and/or notable accountability measures envisaged in the GDPR include:

- Article 6: The choice of, and evidence for a legal basis, in particular legitimate interest processing in Article 6(1)(f)
- Article 12-14: Transparency and privacy notices
- Articles 15-22: Procedures to respond to individual rights
- Article 25: Data protection by design and by default
- Article 28: Processor due diligence, contracting and management
- Article 30: Maintaining records of processing
- Article 31: Cooperation with the supervisory authority
- Article 32: Security policies and procedures
- Articles 33-34: Data breach notification
- Article 35-36: Data Protection Impact Assessments
- Articles 37-39: Appointment of a data protection officer
- Articles 44-49: Appropriate data transfers mechanisms

## **2. Processors**

As to processor accountability, the GDPR imposes new legislative obligations and liabilities for processors, as well as contractual obligations between controllers and processors in Article 28. In order to comply with the enhanced contractual requirements and new legislative obligations, processors, just like controllers, will likely be expected to implement internal policies and procedures for their processing activities. Based on Article 28(1) of the GDPR, the processor shall “implement appropriate technical measures and organisational measures in such a manner that processing will meet the requirements” of the GDPR. Organisational measures

have to be interpreted in the larger sense of overall measures for governing the processor duties including having policies and procedures as well as the ability to review the processes with monitoring, auditing and response mechanisms. In other words, accountability and the implementation of privacy management programs are equally relevant for processors as for controllers, even if there are differences in the responsibilities.

Specific obligations on processors introduced by the GDPR include:

- Article 28: Processor (due diligence, contracting and management in case of sub-processing, assistance to the controller, confidentiality, data deletion or returning data to the controller, notification of illegal instructions to the controller)
- Article 30: Maintaining records of processing
- Article 31: Cooperation with the supervisory authority
- Article 32: Security policies and procedures
- Article 33: Data breach notification to the controller
- Article 37-39: Appointment of a data protection officer
- Articles 44-49: Appropriate data transfer mechanisms

All of these reflect elements of accountability, as further discussed below.

### 3. Elements of accountability in the GDPR and in general

Below are some of the examples of GDPR requirements that map to the elements of accountability, as well as general controls and measures that organisations should implement to ensure accountability under the GDPR and other national data protection laws. Organisations must be able to demonstrate (internally and externally) these controls and measures:

Accountability Element:	Examples of controls/measures mapped to accountability elements:
<b>Leadership and Oversight</b>	<ul style="list-style-type: none"> <li>• Executive oversight</li> <li>• Data privacy officer/Office of oversight and reporting</li> <li>• Data privacy governance</li> <li>• Privacy engineers</li> </ul>
<b>Risk Assessment</b>	<ul style="list-style-type: none"> <li>• At program level</li> <li>• At product or service level</li> <li>• In case of data breach incident</li> <li>• DPIA for high-risk processing</li> <li>• Risk to organisations</li> <li>• Risk to individuals</li> </ul>

<b>Policies and Procedures</b>	<ul style="list-style-type: none"> <li>• Internal privacy rules based on data protection principles</li> <li>• Information security</li> <li>• Legal basis and fair processing</li> <li>• Vendor/Processor management</li> <li>• Procedures for response to individual rights</li> <li>• Other procedures (e.g., Marketing rules, HR rules, M&amp;A due diligence)</li> <li>• Data transfer mechanisms</li> <li>• Privacy by design</li> <li>• Privacy by default</li> <li>• Templates and tools for privacy impact assessments</li> <li>• Crisis management and incident response</li> </ul>
<b>Transparency</b>	<ul style="list-style-type: none"> <li>• Privacy policies and notices to individuals</li> <li>• Innovative transparency – dashboards, integrated in products/apps, articulate value exchange and benefits, part of the customer relationship</li> <li>• Access to information portals</li> <li>• Notification of data breaches</li> </ul>
<b>Training and Awareness</b>	<ul style="list-style-type: none"> <li>• Mandatory corporate training</li> <li>• Ad hoc and functional training</li> <li>• Awareness raising campaigns and communication strategy</li> </ul>
<b>Monitoring and Verification</b>	<ul style="list-style-type: none"> <li>• Internal records of processing</li> <li>• Documentation and evidence – consent, legitimate interest and other legal bases, notices, PIA, processing agreements, breach response</li> <li>• Compliance monitoring as appropriate, such as verification, self-assessments and audits</li> <li>• Seals and certifications</li> </ul>
<b>Response and Enforcement</b>	<ul style="list-style-type: none"> <li>• Individual requests and complaint-handling</li> <li>• Breach reporting, response and rectification procedures</li> <li>• Managing breach notifications to individuals and regulators</li> <li>• Implementing response plans to address audit reports</li> <li>• Internal enforcement of non-compliance subject to local laws</li> <li>• Engagement/Co-operation with DPAs</li> </ul>

*Table 2 – Organisational Accountability Elements Mapped to GDPR Requirements and General Measures*

#### **D. Implementing and Demonstrating Accountability within an Organisation**

There is no “one-size-fits-all” formula for implementing and demonstrating accountability. Each organisation, both controllers and processors, must find its own way to implement and communicate its approach to organisational accountability and responsible use of data based on the applicable legal requirements, its internal policies and goals as well as the risks to individuals that may be associated with the relevant processing operations. To effectively implement and demonstrate accountability, each organisation must make it an integral part of its culture, brand and reputation with an eye on how it wants to be perceived by its customers, business clients, vendors, employees, investors and regulators.

As mentioned earlier, there are different ways in which accountability may be implemented and demonstrated, bearing in mind (1) that they can overlap in practice and (2) that they enable the entire range of possible accountability — starting from what is legally required to any level of accountability beyond what is required.

### **1. Comprehensive internal privacy programs**

One way to implement and demonstrate accountability is through comprehensive internal privacy and information management programs. These programs implement and operationalise applicable legal requirements and/or internal rules and goals and are based on the elements of accountability as set forth in *Figure 1* above. Such comprehensive internal programs ensure that organisations actually comply effectively with all relevant legal requirements or any additional goals they have set for themselves. It also allows organisations to demonstrate their accountability:

- a) Internally — to their corporate boards; and
- b) Externally — to individuals, business partners, shareholders and civil society bodies representing individuals and, upon demand, to DPAs in an investigation or enforcement context, or to a third-party certifier in the context of certified accountability frameworks.

This is consistent with the WP29’s 2010 Opinion on accountability, which notes that the “expected effects of [a legislative accountability] provision would include the implementation of internal measures and procedures putting into effect existing data protection principles, ensuring their effectiveness and the obligation to prove this should data protection authorities request it.”<sup>29</sup> Indeed, as discussed above, the GDPR has made the WP29’s “expectation” a reality. Moreover, as also mentioned above, the DPAs in Hong Kong, Canada, Singapore, Australia, Mexico and Colombia have incorporated and described accountability measures through regulatory guidance.<sup>30</sup> Also, research and consulting organisations are engaged in projects to develop smart operational tools to help privacy officers implement and demonstrate accountability and internal privacy programs, all of which help broaden the uptake of accountability by industry. Importantly, there is now a wealth of experience in leading global organisations in building and implementing first-rate accountable privacy programs.

### **2. Co-regulatory frameworks, certifications, codes of conduct or similar schemes**

Another way to implement accountability is for an organisation to participate in a co-regulatory framework, recognised privacy certification, code of conduct or similar accountability scheme, which typically is voluntary<sup>31</sup> and often goes above and beyond what is minimally required by law. This corresponds to what the WP29 has referred to as “second tier” accountability in its 2010 Opinion on accountability<sup>32</sup> — they help implement “first tier” required accountability but also go above what is required. Of course, participation in such frameworks and schemes also requires the kind of comprehensive internal privacy programs within an organisation described above that effectuate the requirements of these schemes. Examples of such schemes include

EU BCR for controllers or processors, Privacy Shield, APEC CBPR and PRP, and similar mechanisms, including any yet to be developed GDPR certifications and codes of conduct. They could also include programs implementing international standards, such as the relevant ISO standards.

A noteworthy characteristic of such schemes is that they often incorporate (or could be made to incorporate) third-party certification, verification and front-line enforcement, such as through an “Accountability Agent” — a term used in the CBPR and PRP contexts. The benefits of this feature are discussed in Section III. A. below.

## **E. Which Organisations are Expected to be “Accountable”?**

### **1. Controllers and processors**

Under the GDPR and many other data privacy laws and the APEC CBPR and PRP systems, data protection is a shared responsibility of controllers and processors. This shared responsibility must be reflected in the controller-processor contract and throughout the course of delivery of the services. Hence, both controllers and processors should implement accountability based on:

- a) Their respective legal obligations under the GDPR (or other applicable law or binding instruments such as the APEC CBPR or PRP, or other certifications and codes of conduct); and
- b) Contractual requirements and terms of the controller-processor agreement.

As discussed above, the general requirements on accountability in Article 5(2) and Article 24 of the GDPR are addressed only to controllers.<sup>33</sup> However, processors have accountability for their responsibilities as detailed in Section II. C. 2. above. As every processor will also have controller obligations, it would be very artificial for companies to not have accountability requirements that also cover their processor duties. A privacy compliance program will have to focus on companies processors’ duties too, which in most cases will be a very significant way in which a company is able to show accountability to earn trust in the marketplace. Therefore, an argument can be made that similar accountability obligations should also be applied to processors for the following reasons:

- The GDPR imposes increased legislative obligations on processors<sup>34</sup> and also provides for enhanced contractual stipulations for them.<sup>35</sup> It is inconceivable that processors would be able to comply with these without having a comprehensive data privacy program in place based on the elements of accountability, as discussed above.<sup>36</sup> It is in processors’ interest to implement accountability and thus minimise any risks of regulatory or contractual non-compliance and liabilities.
- Processors will be faced with situations where they will have to demonstrate accountability to their clients (controllers), to DPAs, and even to individuals (due to joint

liability).<sup>37</sup> These situations will typically arise in cases of audits, investigations, breach notifications, or enforcement.

- Processors will likely want to demonstrate accountability proactively, as this will help strengthen their reputation in the information ecosystem and make them a trusted business partner. It may also provide them with a competitive edge vis-à-vis other processors. The GDPR provides that controllers must choose processors that are able to provide sufficient guarantees to protect controllers' data. The APEC CBPR require controllers to have mechanisms in place that ensure that their processors comply with the controller's data protection obligations. A processor that is able to show its commitment to data protection based on accountability will be able to drive more clients to its services.
- Processor certifications under the GDPR will be one way in which a processor may be able to gain external recognition for its accountability and data privacy program. GDPR certifications will also serve as sufficient guarantees that an organisation has implemented appropriate technical and organisational measures that meet the requirements of the GDPR. Similarly, the BCR for Processors are widely used by processors to demonstrate accountability, both to regulators and clients. The use of all these mechanisms is likely to increase even further under the GDPR and in general. In the APEC context, the APEC PRP fulfil similar functions of providing external recognition for processors of their accountability as well as providing proof of due diligence by controllers in the selection of their processors.
- Under Article 37(1) of the GDPR, processors (like controllers) have an obligation to designate a data protection officer (DPO) in specified circumstances requiring heightened internal oversight and accountability with respect to data processing activities.

Having accountability for the processor responsibilities however, doesn't mean that controller duties will be merged with processor duties. A good framework of accountability is able to differentiate between different duties and different levels of responsibility. This could, for example, be having specific processor compliance programs in addition to controller compliance programs or policies. BCR also have to be developed separately for controllers and processor activities with variances in the substantive requirements. However, the underlying accountability framework and elements will be the same.

#### **a. The impact of accountability on contractual provisions and negotiations**

Historically, pre-GDPR, in contracting negotiations with processors, controllers often approached data privacy issues from the perspective that the controller was the one that would be held accountable by individuals and regulators. Hence, it was important to make sure the processor clearly committed to complying with specific data protection and security requirements in the contract. Controllers have typically been hesitant to include their own data protection and security obligations in the contract on the grounds that a controller's

compliance or non-compliance was irrelevant from a contractual perspective and due to a concern that any controllers' failure to meet a contract obligation would form the basis of an excuse for any subsequent service failure by the provider.

However, as mentioned, there are a few novelties in the GDPR that are likely to change that overall approach:

- Processors now have their own direct obligations and accountability to individuals and regulators under the GDPR.<sup>38</sup> As such, processors will be concerned about managing this direct statutory liability risk to individuals and regulators in addition to any liability that the controller may try to impose contractually. It would be natural for processors to push back in contractual negotiations with controllers and say, "now that I have this direct statutory liability risk, I can no longer take on the same level of contractual risk."
- It is conceivable that a processor could end up directly liable to third parties and/or regulators for a breach that was caused (in whole or in part) by the controller. Hence, it would also be natural for the processor to require the controller to sign up to certain data protection and security obligations in the processing agreement and accept some level of liability and/or responsibility to indemnify for claims or penalties incurred by the processor to the extent they were caused by the controller. The GDPR appears to expressly contemplate that the controller's obligations would be set out in the processing agreement. GDPR Article 28(3) provides that "Processing by a processor shall be governed by a contract or other legal act [...] that sets out the subject-matter and duration of the processing, the nature and purpose of the processing, the type of personal data and categories of data subjects and the obligations and rights of the controller" (emphasis added).

The GDPR is focused on protecting the rights and freedoms of the individual and now recognises that all parties involved in the processing of an individual's personal data in the ecosystem have some level of responsibility and accountability to ensure those rights and freedoms are protected. The DPAs also have an expectation that all processing parties maintain certain standards and practices throughout their organisations with respect to the protection of personal data. Since the protection of personal data is clearly a shared responsibility, it would be a natural extension for the DPAs to also set an expectation that the data protection obligations and commitments of each contracting party with respect to the personal data being processed are clearly set out in the processing agreement.

This is consistent with the long-standing principle that data protection compliance and accountability cannot be shifted contractually from one party to another. Each party must remain responsible for its own compliance and risk management. It is not only a shared responsibility of controllers and processors to deliver accountability and protection for individuals and their data, but one that has to be maintained across the ever more complex ecosystem of controllers, processors and sub-processors, i.e. along the entire digital supply chain. Furthermore, if it were recognised as an acceptable practice that controllers could entirely shift their compliance, risk management and accountability obligations to processors

then processors, and in particular SMEs, would be impacted financially and this may in turn stifle innovation.

Given the increased responsibilities and liability of processors, as well as accountability obligations and expectations on controllers and processors, it will be important that controllers and processors properly identify their respective responsibilities under the law and their contracts and that they implement their respective accountability measures accordingly. This will result in better alignment between and allocation of their respective roles and responsibilities, both contractually and operationally.

Thus, it is expected that the changes brought by the GDPR to controller and processor responsibilities will bring profound changes to their contracting practices and have significant commercial implications. The impact of the respective responsibilities of controllers and processors on contracting terms and practices, including those relating to liability, and any associated commercial implications, may be discussed in a separate CIPL paper on controller and processor implications of the GDPR.

## **2. Public sector organisations**

It is also important to note that, save for a few specific exceptions, the GDPR does not distinguish between the private sector and public sector organisations. Articles 4(7) and 4(8) of the GDPR specifically include “public authorities” in the definition of a controller and processor. Therefore, the GDPR accountability requirements apply equally to public sector organisations as they do to the private sector. Furthermore, Article 37(1)(a) on the requirement to designate a DPO, which falls under the accountability element of leadership and oversight, specifically states that a controller or processor shall designate a DPO where processing is carried out by a public authority or body, except for courts acting in their judicial capacity. Another example is the requirement to carry out a DPIA. Public sector organisations often process large volumes of personal information about individuals, both sensitive and non-sensitive. Like private sector organisations, public authorities may use new technologies to more efficiently process the data they hold. If such processing is likely to result in a high-risk to individuals, public authorities are required to carry out a DPIA, just like private sector organisations.

Accountability in public sector organisations is even more important given that data often “travels” between the public and private sectors. Because of the increased interest by the public sector in the use of private sector data (for example, in cases of medical research) it is essential that the public sector is subjected to the same accountability requirement as private sector organisations. Thus, it is important that there be a continued effort to promote accountability and the implementation of comprehensive privacy management programs in public sector organisations. This will require ensuring enhanced resources and budget for data protection compliance within public sector organisations.

In some countries, there are indications that accountability is becoming integral in many respects to the public sector. For instance, the UK Security Policy Framework of May 2018,<sup>39</sup> includes a section on accountability and notes that “UK governmental organisations are

responsible for the information they handle under appropriate governance structures, including at Board level lead. A SIRO [Senior Information Risk Owner] is accountable and responsible for information risk across the organisation...” Additionally, the UK Government’s Data Ethics Framework<sup>40</sup> “sets out clear principles for how data should be used in the public sector. It will help [public sector organisations] maximise the value of data whilst also setting the highest standards for transparency and accountability when building or buying new data technology”.

In addition, given the statutory and administrative frameworks in which public bodies operate, there may be a need to explore in future work, whether there are differences in the ways public sector organisations deliver accountability compared to their private sector counterparts. These differences may prove to be limited in practice as even where public sector organisations process data on the basis of statutory requirements, they still have a duty to process such data in line with relevant data protection principles, security measures and controls and in a way that does not cause harm to individuals.

### **III. The Benefits of Accountability**

The benefits of organisational accountability cannot be overstated. Accountability gives organisations the tools for compliance with applicable legal requirements, for protecting individuals from privacy harms and for engendering trust in organisations’ ability to engage in responsible data use. Importantly, accountability provides an approach to data protection that is transparent, risk-based, technology-neutral and future-proof. These are essential prerequisites for trust in technology, systems and the digital market place. Indeed, these prerequisites ensure that organisations are equipped to handle new challenges to data protection law and practice, regardless of advances in technology or changes in the behaviours or expectations of individuals. They provide organisations with the necessary flexibility and agility to customise their data privacy management programs to adequately address the identified risks and avoid the need for constant and time-consuming law reform to keep pace with new and ever changing advances to the digital ecosystem.<sup>41</sup>

Risk assessment, one of accountability’s core elements, facilitates context-appropriate and risk-based privacy protections regardless of the specific technology or practice that is being assessed. Risk assessment requires organisations to assess the risks of a specific data processing initiative or technology, balance the interests of the organisation and society against the possible harms to individuals, and mitigate risk in ways that are appropriate to the context.

Organisations that have implemented the elements of accountability through their internal comprehensive privacy programs and/or through participation in relevant codes of conduct or certifications, including BCR, CBPR, PRP and the Privacy Shield should derive numerous benefits. These benefits include an increase in the trust of individuals, business partners, society and regulators that personal data will be used and managed responsibly and for the benefit of the organisation’s customers and society. Adopting and demonstrating a commitment to accountability not only benefits the organisation itself but also delivers tangible benefits to individuals, business partners, society and regulators.

## A. Accountability Benefits to Stakeholders

One way to look at the benefits of accountability is to consider them from the perspective of the different stakeholders — organisations, individuals, DPAs and governments. The benefits of accountability can be direct or indirect to different stakeholders. Regardless, it is certain that organisations who have adopted accountability will be more likely to deliver to individuals and regulators, and to reap for themselves, the following benefits as summarised in the table below:

<b>Benefits for Organisations</b>
<ul style="list-style-type: none"> <li>• Enables more effective privacy protections by requiring risk-based prioritisation of such protections.</li> </ul>
<ul style="list-style-type: none"> <li>• Assists organisations in ensuring and demonstrating legal compliance to business partners and regulators.</li> </ul>
<ul style="list-style-type: none"> <li>• Fosters a culture of internal privacy compliance and constructive engagement with DPAs.</li> </ul>
<ul style="list-style-type: none"> <li>• Fosters good data hygiene and good data management and helps to support the strategic objectives of organisations around data.</li> </ul>
<ul style="list-style-type: none"> <li>• Enables greater harmonisation of organisations' privacy policies and practices with the various requirements of the different jurisdictions in which they do business.</li> </ul>
<ul style="list-style-type: none"> <li>• Generates trust among the public and regulators that the organisation is processing personal data responsibly, potentially enhancing the reputation and goodwill of the organisation and adding value to its brand (trust advantage<sup>42</sup>).</li> </ul>
<ul style="list-style-type: none"> <li>• Enables organisations to engage in broader beneficial uses of personal data, including data for social good, research and responsible AI and machine learning by minimising the risks of new data uses (e.g., through incorporating privacy by design, transparency, risk assessment, etc.) and demonstrating responsible data use to regulators.</li> </ul>
<ul style="list-style-type: none"> <li>• Assists SMEs with implementing scalable privacy tools and controls within their organisations, appropriate to their size and type of operation.</li> </ul>
<ul style="list-style-type: none"> <li>• Provides legal certainty for organisations with regard to cross-border data protection compliance through participation in recognised accountability frameworks, such as BCR and CBPR.</li> </ul>
<ul style="list-style-type: none"> <li>• Enables cross-border data transfers through recognised mechanisms such as BCR and CBPR.</li> </ul>
<ul style="list-style-type: none"> <li>• Furthers the creation of interoperability between different accountability frameworks and thus global solutions to data transfers for organisations.</li> </ul>
<ul style="list-style-type: none"> <li>• Helps differentiate between organisations and provides a competitive edge to those who choose to invest in accountability relative to those who do not (accountability advantage).</li> </ul>
<ul style="list-style-type: none"> <li>• Improves overall level of privacy behaviours of organisations which in turn improves the health of the data ecosystem in general and benefits all stakeholders in the digital economy in the long run.</li> </ul>
<ul style="list-style-type: none"> <li>• Serves as a due diligence tool for controllers in identifying qualified and accountable processors.</li> </ul>
<b>Benefits for Individuals</b>
<ul style="list-style-type: none"> <li>• Delivers real and more effective protection of individuals and their data.</li> </ul>
<ul style="list-style-type: none"> <li>• Ensures that the protection follows personal data transferred across borders.</li> </ul>
<ul style="list-style-type: none"> <li>• Assures individuals that compliance with local legal requirements are met and increases individuals' trust in organisations' processing of their data.</li> </ul>
<ul style="list-style-type: none"> <li>• Enhances privacy protections for individuals beyond minimum requirements and empowers individuals in the management of their data (e.g., through the extension of individual rights or voluntary security breach reporting by organisations).</li> </ul>

<ul style="list-style-type: none"> <li>• Shifts the burden of protecting individuals more explicitly to organisations.</li> </ul>
<ul style="list-style-type: none"> <li>• Provides individuals with a benchmark for deciding whether to allow their data to be processed by certain organisations.</li> </ul>
<ul style="list-style-type: none"> <li>• Provides individuals' rights and interests heightened consideration and protection through required risk assessments and balancing processes.</li> </ul>
<ul style="list-style-type: none"> <li>• Permits individuals to reap the benefits of participation in the digital society.</li> </ul>
<ul style="list-style-type: none"> <li>• Enables more effective domestic and cross-border enforcement.</li> </ul>

<b>Benefits for Regulators</b>
<ul style="list-style-type: none"> <li>• Provides assurance to DPAs that organisations are identifying and prioritising high-risk data processing.</li> </ul>
<ul style="list-style-type: none"> <li>• Reduces the oversight, complaint-handling and enforcement burdens of DPAs through the involvement of third-party certifiers, Accountability Agents and third-party dispute resolution bodies.</li> </ul>
<ul style="list-style-type: none"> <li>• Allows DPAs to be more selective and strategic with their often limited resources in pursuing their overall mission.</li> </ul>
<ul style="list-style-type: none"> <li>• Promotes constructive engagement with accountable organisations.</li> </ul>
<ul style="list-style-type: none"> <li>• Improves cross-border privacy enforcement cooperation through the creation of mutually recognised requirements and processes, such as in BCR and CBPR.</li> </ul>
<ul style="list-style-type: none"> <li>• Assists DPAs in carrying out investigations and enforcement actions by bridging together different legal regimes and providing a more uniform data protection environment.</li> </ul>
<ul style="list-style-type: none"> <li>• Simplifies investigations and enforcement actions and enables companies to demonstrate compliance to DPAs by requiring organisations to maintain records of processing.</li> </ul>
<ul style="list-style-type: none"> <li>• Keeps organisations honest in terms of claims made to the public by facilitating exposure of false claims.</li> </ul>

*Table 3 – Benefits of Organisational Accountability to Stakeholders*

## **B. Types and Categories of Accountability Benefits**

Another way to look at the benefits of accountability is to look at them by type or category, which may benefit multiple or all stakeholders:

### ***Accountability as a driver towards global intra-company harmonisation***

A multinational organisation's internal privacy program, based on the elements, of accountability allows it to align its privacy policies and practices with the various requirements of the different jurisdictions in which it does business and to harmonise them as much as possible. The internal privacy program of the organisation, in effect, creates a practical bridge between different legal requirements. It sets uniform and high level privacy policies, procedures and operational controls for the company and can foster a company-wide privacy culture across multiple jurisdictions, if the company so chooses.

### ***Accountability as an interoperability bridge and enabler of cross-border data flows***

Certified and enforceable accountability schemes, such as BCR, CBPR, PRP, Privacy Shield and future GDPR certifications or codes of conduct, enable responsible cross-border data transfers. They are (or can be) designed to meet an agreed privacy standard of multiple jurisdictions and to serve as a recognised cross-border transfer mechanism in jurisdictions that impose data transfer restrictions in their privacy laws.<sup>43</sup> Indeed, as discussed, the GDPR specifically recognises the role of BCR, certifications and codes of conduct for this purpose. As such, and in light of the importance of ensuring responsible and protected global data flows, these mechanisms must be further developed and implemented as a matter of priority.

At this stage there is clearly an enormous untapped potential for accountability-based schemes to serve as a bridge between different legal regimes. For example, BCR, CBPR, PRP, future GDPR certifications and similar schemes could be made interoperable with each other<sup>44</sup> and serve as a model for creating a truly global accountability-based data transfer mechanism. Certainly, global organisations are interested in such mechanisms. The more it is possible to address local compliance issues and cross-border transfer restrictions through a single accountability-based system or a set of coordinated and interconnected systems, the better for organisations and for their customers, individuals and regulators.

### ***Accountability as an enabler of legal compliance***

Implementing an accountability-based program, whether certified or not, is a powerful tool for organisations to ensure and demonstrate that they comply with applicable national law (or, in the EU, the GDPR). This is because such programs implement local legal requirements or some formally recognised certification, code of conduct or similar scheme that is recognised by multiple countries on the basis that it is substantially consistent with the respective legal requirements (e.g., the CBPR). As a result, implementing such programs improves legal certainty for organisations.<sup>45</sup>

### ***Accountability as a compliance tool for SMEs***

Formal accountability schemes such as, CBPR, PRP, and future GDPR certifications can be particularly beneficial for SMEs that may not have the resources to independently devise full-fledged internal privacy programs without the assistance of a third-party. Such formal accountability programs should be designed to be scalable to the size and nature of the organisation to be certified, which is essential to making such mechanisms a viable compliance tool for SMEs. Indeed, the GDPR requires such scalability under Articles 40 and 42.

Furthermore, some DPAs are starting to create and adopt specific SME toolkits, for instance, the CNIL,<sup>46</sup> the UK ICO<sup>47</sup>, the Spanish AEPD<sup>48</sup> and the Hong Kong PCPD.<sup>49</sup> These toolkits can provide a starting roadmap for SMEs implementing accountability into their organisations. For some SMEs these toolkits, either alone or accompanied by some form of certification, might be

enough to demonstrate that they have implemented a measurable accountability/privacy management framework, appropriate to their size and type of operation.

***Accountability as a due diligence tool and a tool for competitive advantage***

Formal, verified or certified accountability schemes may be used as a due diligence tool by controllers that are seeking qualified and accountable processors. Thus, certifying a processor under such a scheme benefits both the processor (because it is demonstrably accountable) and the controller (because it needs to contract with accountable processors). Indeed, the GDPR provides that participation in an approved code of conduct or certification is an element by which to demonstrate “sufficient guarantees” that a processor has implemented appropriate measures under the GDPR.<sup>50</sup>

This benefit of accountability is grounded in the fact that accountability-based schemes require a verified internal compliance infrastructure, including written policies and other documentation, which enable the organisation to demonstrate its accountability and compliance not only to regulators but to potential business partners. Naturally, its role as proof of due diligence also makes verified or certified accountability a mechanism to achieve a competitive advantage over organisations that are not certified.

***Accountability as an enabler of proactive privacy protections***

Accountability-based privacy programs also create an infrastructure for organisations to proactively implement strong and effective privacy protections for individuals that in some instances go above and beyond applicable legal requirements for the benefit of individuals and society, including in contexts in which no privacy laws exist at all. For example:

- Many accountable organisations voluntarily apply internal security breach reporting and response practices even in countries where there is no legal requirement to notify the breaches;
- Some organisations voluntarily extend the right of access to all of their customers and employees, even when there is no strict legal obligation to do so;
- Organisations that participate in voluntary data protection and privacy certifications, codes of conduct or similar accountability schemes benefit individuals and other stakeholders by going above and beyond what is required by law. Indeed, to reap the benefits of a CBPR certification, for example, some organisations might certify to the CBPR even in countries where the requirements of the CBPR exceed those found in any domestic laws; and
- Where legislative accountability requirements may not technically apply to processors, accountability schemes may nevertheless provide additional proactive data protection measures that benefit both the processors and all other stakeholders (As explained

above, a data processor might distinguish itself from its competitors by participating in BCR for Processors or the APEC PRP).

### ***Accountability as an enabler of interoperability of privacy norms***

Accountability programs, particularly those of the formal and verified or certified variety, contribute to the international convergence of privacy protections and norms. Such convergence will benefit businesses and regulators alike.<sup>51</sup> For individuals, global convergence would help to ensure a more consistent and high-level of protection and enable their trust in a global market.

### ***Accountability as an enabler of societal trust in modern data uses***

Today's technology causes much data processing to increasingly occur outside the knowledge and awareness of data subjects. This is especially true in recent years with the rise of social media, big data, Internet of Things devices and artificial intelligence. These technologies created a fundamental shift in the generation and collection of personal data and along with changes in organisational and consumer dynamics and behaviours, increased stress has been placed on data protection principles that were first articulated in a pre-Internet era.<sup>52</sup> This reality challenges traditional expectations that notice and consent can effectively protect the individual and requires additional means of protecting and empowering the individual. Accountability provides such other means primarily by placing the burden of protecting individuals on organisations. When organisations discharge this responsibility effectively, they will create trust among the public and regulators that they are processing personal data responsibly, even in the absence of direct individual involvement.

Indeed, without the tools and mechanisms to earn public trust, legitimate uses of information and the ability to innovate may fall victim to unnecessary opposition and restrictions even in instances where there is no risk of harm to individuals. At a time when more and more organisations, as well as society at large, are discovering the enormous economic and societal value of personal data and are searching for new ways to use it legitimately, it is essential that they employ tools that ensure they do so in a responsible, transparent and ethical manner and subject to appropriate privacy controls. Accountability provides these tools. It enables a clear understanding of both the risks and benefits of particular data uses, including novel and innovative data uses, as well as effective communication to the public of the intended benefits and possible trade-offs of such uses, so that the public is fully aware and in a position to accept the value exchange that takes place between businesses and individuals.

### ***Accountability as an enabler of calibrated and risk-based data protection***

Risk assessment is a core element of accountability. It enables organisations to understand the potential risks and harms to individuals that may be associated with their processing operations. It also requires them to implement appropriate mitigations for such risks and harms, taking into account the desired benefits of the processing and rights and interests of

individuals. Risk assessment allows organisations to prioritise their privacy and data protection measures and focus them on where they are needed the most based on the likelihood and severity of risk to individuals. In a world of limited resources, this risk-based approach to privacy protection will result in greater and more effective protections for individuals. Accountability thus ensures that organisations apply privacy requirements and deploy their mitigation resources flexibly and contextually depending on the involved risk while also effectuating the fundamental goals of data protection and complying with all legal requirements.

***Accountability as an enabler of constructive engagement and regulatory oversight***

In the same way that accountability enables a more risk-based and effective approach to privacy protections by organisations, it also enables the same for DPAs. Indeed, the WP29 has noted that accountability “would help them to be more selective and strategic, enabling them to invest their resources in a way as to generate the largest possible scale of compliance.”<sup>53</sup>

However, to reap the full benefits of accountability, including through its core elements of risk assessment and considerations of fairness and ethics, organisations and DPAs must have common and coordinated approaches with respect to its essential elements. Arriving at such common and coordinated approaches will require constructive engagement on these issues between DPAs and accountable organisations. CIPL has previously argued that DPAs’ principal responsibility is leadership on data protection matters and that they should carry out this leadership through “constructive engagement” with organisations.<sup>54</sup> The concept of accountability is uniquely able to both foster such constructive engagement and greatly benefit the DPAs own effectiveness.

For example, DPAs are typically charged with enforcing privacy laws with limited budgets and personnel resources. Accountability is likely to alleviate some of the pressures on DPA resources and it will also allow them to prioritise the allocation of their resources and to adopt a risk-based approach. The various elements of accountability as implemented in comprehensive privacy programs as well as the requirement of having to be able to demonstrate this implementation, will result in the simplification and streamlining of privacy enforcement. Indeed, the nature and extent of an organisation’s accountability acts as a differentiator. All other things being equal, accountability as a differentiator helps DPAs to target their attention to the most demanding and high-risk situations, concentrating less on those who are willing and demonstrably striving for compliance. In investigations of factually complex matters, it also helps both the organisation and the DPA if the organisation is able to provide clear and understandable documentation of the conduct under investigation.<sup>55</sup>

Moreover, in the context of formal and certified accountability schemes, such as BCR, the CBPR and PRP, Privacy Shield, or future GDPR certifications, third-party certifying organisations have front-line oversight, “enforcement” and complaint-handling responsibilities. These certifiers may further be tied into a transnational network of other third-party certifiers that can assist in matters involving cross-border violations. In addition, these schemes may also be supported by

a backstop enforcement cooperation arrangement between international DPAs.<sup>56</sup> Each of these features greatly augments the oversight capacity and enforcement reach of individual DPAs.<sup>57</sup>

Further, the WP29 has previously highlighted the potential of certified accountability to support DPAs:

The use of BCR as legal grounds for international data transfers require that data controllers show that they have put in place adequate safeguards, in which case data protection authorities may authorise the transfers. This in an area where certification services could be helpful. Such services would analyse the assurances provided by the data controller and, if appropriate, issue the relevant seal. A data protection authority could use the certification provided by a given certification program in its analysis of BCR of whether a data controller has provided sufficient safeguards for the purposes of international data transfers. Thus, contributing to streamlining the process for authorisation of international transfers.<sup>58</sup>

Both the number and significance of the above benefits of accountability raise the question of how the uptake of accountability can be specifically encouraged and incentivised. As explained, this is the topic of the second paper in this series.<sup>59</sup>

#### **IV. Conclusion**

As stakeholders continue to codify, expect, encourage, explain, implement and demonstrate organisational accountability, it is important that they do so in a way that is consistent with the global consensus on what accountability means. To reap the full range of accountability's benefits to all stakeholders — organisations, individuals, society and DPAs — it is crucial to maintain as much global coherence as possible. As demonstrated, the benefits of accountability are significant. Many of these benefits are "self-incentivising" for organisations. Others may be less so, particularly where accountability measures would exceed what is legally required. Thus, given the tremendous potential of accountability to place data protection on a sound and sustainable footing going forward, and indeed, to solve the current trust deficit in the digital economy, external incentives to encourage broad implementation of accountability beyond what is required by law are warranted. The case for such "external incentives" is laid out in the second paper of this series.

If you would like to discuss this paper further or require additional information, please contact Bojana Bellamy, [bbellamy@HuntonAK.com](mailto:bbellamy@HuntonAK.com), Markus Heyder, [mheyder@HuntonAK.com](mailto:mheyder@HuntonAK.com), Nathalie Laneret, [nlaneret@HuntonAK.com](mailto:nlaneret@HuntonAK.com) or Sam Grogan, [sgrogan@HuntonAK.com](mailto:sgrogan@HuntonAK.com).

## References

---

<sup>1</sup> CIPL is a global data privacy and cybersecurity think tank in the law firm of Hunton Andrews Kurth and is financially supported by the law firm and 63 member companies that are leaders in key sectors of the global economy. CIPL's mission is to engage in thought leadership and develop best practices that ensure both effective privacy protections and the responsible use of personal information in the modern information age. CIPL's work facilitates constructive engagement between business leaders, privacy and security professionals, regulators and policymakers around the world. For more information, please see CIPL's website at <http://www.informationpolicycentre.com/>. Nothing in this paper should be construed as representing the views of any individual CIPL member company or of the law firm of Hunton Andrews Kurth.

<sup>2</sup> WP29 Opinion 3/2010 on the principle of accountability, adopted 13 July 2010, available at [http://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2010/wp173\\_en.pdf](http://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2010/wp173_en.pdf).

<sup>3</sup> *Id.* at page 6, paragraph 15.

<sup>4</sup> CIPL Discussion paper on "Incentivising Accountability: How Data Protection Authorities and Law Makers Can Encourage Accountability," 23 July 2018, available at [http://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl\\_accountability\\_paper\\_2\\_-\\_incentivising\\_accountability\\_-\\_how\\_data\\_protection\\_authorities\\_and\\_law\\_makers\\_can\\_encourage\\_accountability.pdf](http://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_accountability_paper_2_-_incentivising_accountability_-_how_data_protection_authorities_and_law_makers_can_encourage_accountability.pdf)

<sup>5</sup> *Supra* note 2, at page 3.

<sup>6</sup> The Centre for Information Policy Leadership, "Accountability: A Compendium for Stakeholders," March 2011, at page 3, available at [https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/accountability-a\\_compendium\\_for\\_stakeholders\\_march\\_2011\\_.pdf](https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/accountability-a_compendium_for_stakeholders_march_2011_.pdf).

<sup>7</sup> The GDPR formally incorporates accountability as a requirement for data controllers (Article 5(2) GDPR). See further discussion in Section II. C. 1. of this document.

<sup>8</sup> See OECD Revised Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, 2013, at page 15, available at [http://oecd.org/sti/ieconomy/oecd\\_privacy\\_framework.pdf](http://oecd.org/sti/ieconomy/oecd_privacy_framework.pdf).

<sup>9</sup> See APEC Privacy Framework, at page 28, available at [https://www.apec.org/-/media/APEC/Publications/2005/12/APEC-Privacy-Framework/05\\_ecsg\\_privacyframewk.pdf](https://www.apec.org/-/media/APEC/Publications/2005/12/APEC-Privacy-Framework/05_ecsg_privacyframewk.pdf).

<sup>10</sup> The Privacy Commissioners of Canada, Hong Kong, Singapore and Australia have issued regulatory guidance on privacy programs and their requirements (See documents (a) – (d) in note 30 below). The Mexican Data Protection Commission has released guidance on the principles of data protection, including accountability (See document (e) in note 30 below) and the Mexican Federal Law on Protection of Personal Data Held by Individuals specifically includes accountability as one of the key data protection principles (See [www.diputados.gob.mx/LeyesBiblio/pdf/LFPDPPP.pdf](http://www.diputados.gob.mx/LeyesBiblio/pdf/LFPDPPP.pdf)). Similarly, the Colombian Data Protection Commission has released guidelines on the development of accountability in Colombian data protection law (See document (f) in note 30 below). The New Zealand Privacy Commissioner also issued a Credit Reporting Privacy Code embedding an accountability approach within credit reporting (See <https://privacy.org.nz/the-privacy-act-and-codes/codes-of-practice/credit-reporting-privacy-code/>). In the U.S., the Federal Trade Commission's consent decrees spell out the requirements of accountable corporate privacy programs, signaling to organisations what it expects of them. Other regulators, such as the UK ICO, have for some time

required organisations to implement various elements of accountability in some enforcement actions, including the recent action against Royal Free London NHS Foundation Trust (See <https://ico.org.uk/media/action-weve-taken/undertakings/2014352/royal-free-undertaking-03072017.pdf>).

<sup>11</sup> See Modernised Convention for the Protection of Individuals with Regard to the Processing of Personal Data, available at [https://search.coe.int/cm/Pages/result\\_details.aspx?ObjectId=09000016807c65bf](https://search.coe.int/cm/Pages/result_details.aspx?ObjectId=09000016807c65bf).

<sup>12</sup> See notes 8 and 9 above, generally. In addition, see “Bridge 8: Accountability” in the report “Privacy Bridges: EU and US Privacy Experts in Search of Transatlantic Privacy Solutions,” 37<sup>th</sup> International Privacy Conference, Amsterdam, 2015, at page 37, available at <https://privacybridges.mit.edu/sites/default/files/documents/PrivacyBridges-FINAL.pdf> which identifies the common elements of enforceable corporate accountability programs.

<sup>13</sup> Data Protection Accountability: The Essential Elements, October 2009, available at [https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/data\\_protection\\_accountability-the\\_essential\\_elements\\_discussion\\_document\\_october\\_2009.pdf](https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/data_protection_accountability-the_essential_elements_discussion_document_october_2009.pdf);

Demonstrating and Measuring Accountability, October 2010, available at [https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/demonstrating\\_and\\_measuring\\_accountability\\_a\\_discussion\\_document\\_accountability\\_phase\\_ii-the\\_paris\\_project\\_october\\_2010.pdf](https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/demonstrating_and_measuring_accountability_a_discussion_document_accountability_phase_ii-the_paris_project_october_2010.pdf);

Implementing Accountability in the Marketplace, November 2011, available at [https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/implementing\\_accountability\\_in\\_the\\_marketplace\\_accountability\\_phase\\_iii-the\\_madrid\\_project\\_november\\_2011.pdf](https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/implementing_accountability_in_the_marketplace_accountability_phase_iii-the_madrid_project_november_2011.pdf);

Accountability: A Compendium for Stakeholders, March 2011, available at [https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/accountability-a\\_compendium\\_for\\_stakeholders\\_march\\_2011.pdf](https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/accountability-a_compendium_for_stakeholders_march_2011.pdf);

Accountability: Data Governance for the Evolving Digital Marketplace, April 2011, available at [https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/accountability-data\\_governance\\_for\\_the\\_evolving\\_digital\\_marketplace\\_april\\_2011.pdf](https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/accountability-data_governance_for_the_evolving_digital_marketplace_april_2011.pdf).

<sup>14</sup> See documents (a) and (b) in note 30.

<sup>15</sup> See, for example, United States Sentencing Commission, 2016 Guidelines Manual, Chapter 8, S.8B2.1. Effective Compliance and Ethics Programs, available at <https://www.ussc.gov/sites/default/files/pdf/guidelines-manual/2016/GLMFull.pdf>; Criminal Division of the United States Department of Justice and the Enforcement Division of the United States Securities and Exchange Commission, A Resource Guide to the U.S. Foreign Corrupt Practices Act, Hallmarks of Effective Compliance Programs in Chapter 5 on Guiding Principles of Enforcement at page 57-62, November 2012, available at <https://www.justice.gov/criminal/fraud/fcpa/guidance/guide.pdf>; IDW PS 980, Institute of German Auditors, German Standard for Auditing Compliance Management Systems, available at <https://www.idw.de/idw/verlautbarungen/idw-ps-980/43124>. See also Hodges C., Ethical Business Practice and Regulation (Hart Publishing 2017), at page 171 discussing Bribery as a developing example of ethical regulation. The UK Bribery Act 2010 established a new strict liability corporate offence of failure to prevent bribery by associated persons – if however, an organisation can prove it had adequate procedures for preventing bribery by associated persons in place, it may escape liability. There is no definition of “adequate procedures” but the UK Ministry of Justice published guidance on the Act and articulated six principles to inform procedures organisations can put in place to prevent bribery (See The Bribery Act 2010: Guidance

---

about procedures which relevant commercial organisations can put into place to prevent persons associated with them from bribing, available at <https://www.justice.gov.uk/downloads/legislation/bribery-act-2010-guidance.pdf>). The guidance applies many of the same accountable elements of data privacy programs within the domain of anti-bribery legislation. These include a top-level commitment to preventing bribery (i.e. leadership and oversight); risk assessments of internal and external risks of bribery and due diligence procedures (i.e. risk assessments); policies and procedures proportionate to the bribery risks faced by the organisation (i.e. policies and procedures); communication, including training of bribery prevention policies and procedures throughout the organisation (i.e. training and awareness); and monitoring and reviewing procedures designed to prevent bribery by persons associated with it and making improvements where necessary (i.e. monitoring and verification).

<sup>16</sup> See WP29's WP256 Working Document setting up a table with the elements and principles to be found in Binding Corporate Rules, available at [https://ec.europa.eu/newsroom/just/document.cfm?doc\\_id=48798](https://ec.europa.eu/newsroom/just/document.cfm?doc_id=48798) and WP257 Working Document setting up a table with the elements and principles to be found in Processor Binding Corporate Rules, available at [https://ec.europa.eu/newsroom/just/document.cfm?doc\\_id=48799](https://ec.europa.eu/newsroom/just/document.cfm?doc_id=48799). BCR are not only a mechanism for legitimising cross-border data transfers of data, but also a full-blown accountability framework.

<sup>17</sup> See EU-US Privacy Shield Framework, available at <https://www.privacyshield.gov/Privacy-Shield-Principles-Full-Text>. Similarly, the EU-US Privacy Shield is also based on accountability and requires organisations to implement a comprehensive set of policies, procedures and tools.

<sup>18</sup> Federation of European Direct Marketing, European Code of Practice for the Use of Personal Data in Direct Marketing, available at <https://www.fedma.org/wp-content/uploads/2017/06/FEDMACodeEN.pdf>.

<sup>19</sup> Cloud Infrastructure Service Providers in Europe, Code of Conduct available at <https://cispe.cloud/code-of-conduct/>; see letter to WP29 on the draft Code [http://ec.europa.eu/newsroom/article29/item-detail.cfm?item\\_id=615033](http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=615033).

<sup>20</sup> Article 24(3) GDPR recognises the importance of approved codes of conduct and certification mechanisms under Articles 40 and 42 GDPR for the purpose of demonstrating accountability. Article 28(5) of the GDPR recognises their use as due diligence tools to establish "sufficient guarantees" of compliance of processors.

<sup>21</sup> See APEC CBPR and PRP system documents, available at <http://www.cbprs.org/GeneralPages/APECCBPRSystemDocuments.aspx>. The APEC CBPR and PRP have emerged as a significant accountability and cross-border transfer frameworks in the Asia-Pacific region (See [www.cbprs.org](http://www.cbprs.org)).

<sup>22</sup> See JIPDEC PrivacyMark System at <https://privacymark.org/>.

<sup>23</sup> See ISO/IEC 27018:2014 Information technology - Security techniques - Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors, available at <https://www.iso.org/standard/61498.html>.

<sup>24</sup> Yeong Zee Kin, "From Compliance to Accountability" in *Data Protection Law in Singapore – Privacy and Sovereignty in an Interconnected World* (Simon Chesterman ed) (Academy Publishing, 2nd Ed, 2018) Ch 11. at page 325.

<sup>25</sup> See ISO/IEC 27000 family - Information security management systems, available at <https://www.iso.org/isoiec-27001-information-security.html>.

<sup>26</sup> Paragraph 1 of Article 5 covers the “Principles relating to processing of personal data,” Article 5(1) GDPR.

<sup>27</sup> For a full discussion on the risk-based approach to processing under the GDPR, see CIPL’s white paper on Risk, High Risk, Risk Assessments and Data Protection Impact Assessments under the GDPR, 21 December 2016, available at [https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl\\_gdpr\\_project\\_risk\\_white\\_paper\\_21\\_december\\_2016.pdf](https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_gdpr_project_risk_white_paper_21_december_2016.pdf).

<sup>28</sup> For a further discussion on risk, see CIPL papers on:

(a) A Risk-based Approach to Privacy: Improving Effectiveness in Practice, 19 June 2014, available at [https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/white\\_paper\\_1-a\\_risk\\_based\\_approach\\_to\\_privacy\\_improving\\_effectiveness\\_in\\_practice.pdf](https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/white_paper_1-a_risk_based_approach_to_privacy_improving_effectiveness_in_practice.pdf);

(b) The Role of Risk Management in Data Protection, 23 November 2014, available at [https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/white\\_paper\\_2-the\\_role\\_of\\_risk\\_management\\_in\\_data\\_protection-c.pdf](https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/white_paper_2-the_role_of_risk_management_in_data_protection-c.pdf);

(c) Protecting Privacy in a World of Big Data, The Role of Risk Management, 16 February 2016, available at [https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/protecting\\_privacy\\_in\\_a\\_world\\_of\\_big\\_data\\_paper\\_2\\_the\\_role\\_of\\_risk\\_management\\_16\\_february\\_2016.pdf](https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/protecting_privacy_in_a_world_of_big_data_paper_2_the_role_of_risk_management_16_february_2016.pdf); and

(d) Comments by the Centre for Information Policy Leadership on the Article 29 Data Protection Working Party’s “Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is ‘likely to result in a high risk’ for the purposes of Regulation 2016/679,” 19 May 2017, available at [https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl\\_comments\\_on\\_the\\_wp29s\\_guidelines\\_on\\_dpias\\_and\\_likely\\_high\\_risk\\_19\\_may\\_2017-c.pdf](https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_comments_on_the_wp29s_guidelines_on_dpias_and_likely_high_risk_19_may_2017-c.pdf).

<sup>29</sup> *Supra* note 2, at page 5, paragraph 12, and page 19 paragraphs 73 and 74.

<sup>30</sup> See (a) Office of the Privacy Commissioner for Personal Data, Hong Kong, Privacy Management Programme: A Best Practice Guide, 2014, available at [https://www.pcpd.org.hk/pmp/files/PMP\\_guide\\_e.pdf](https://www.pcpd.org.hk/pmp/files/PMP_guide_e.pdf);

(b) the Office of the Privacy Commissioner of Canada (OPC), and the Offices of the Information and Privacy Commissioners (OIPCs) of Alberta and British Columbia, Getting Accountability Right with a Privacy Management Program, 2012, available at [https://www.priv.gc.ca/media/2102/gl\\_acc\\_201204\\_e.pdf](https://www.priv.gc.ca/media/2102/gl_acc_201204_e.pdf);

(c) Personal Data Protection Commission of Singapore, Guide to developing a data protection management programme, 2017, available at <https://www.pdpc.gov.sg/-/media/Files/PDPC/PDF-Files/Other-Guides/guide-to-developing-a-dpmp---011117.pdf>;

(d) Office of the Australian Information Commissioner, Privacy management framework: enabling compliance and encouraging good practice, available at <https://www.oaic.gov.au/agencies-and-organisations/guides/privacy-management-framework>;

(e) National Institute for Transparency, Access to Information and Personal Data Protection, Principios rectores de la Protección de Datos Personales, available at [https://inicio.inai.org.mx/GuiasTitulares/Guia%20Titulares-02\\_PDF.pdf](https://inicio.inai.org.mx/GuiasTitulares/Guia%20Titulares-02_PDF.pdf); and

---

(f) Superintendente Delegado para la Protección de Datos Personales, Guía para la implementación del Principio de Responsabilidad Demostrada (Accountability), available at <http://www.sic.gov.co/noticias/guia-para-la-implementacion-del-principio-de-responsabilidad-demostrada>.

<sup>31</sup> “Voluntary” refers to the fact that typically organisations are not required to participate in these mechanisms but may choose to do so; however, once they have opted to participate, the requirements of these mechanisms become binding and enforceable.

<sup>32</sup> *Supra* note 2 above, at page 6.

<sup>33</sup> Article 5(2) and Article 24 GDPR.

<sup>34</sup> See further discussion in Section II. C. 2.

<sup>35</sup> Article 28(3) GDPR.

<sup>36</sup> See further discussion in Section II.A.

<sup>37</sup> Article 82(4) GDPR.

<sup>38</sup> See, for example, Article 28 (Processor) and Article 82 GDPR (Right to compensation and liability).

<sup>39</sup> HMG Security Policy Framework, May 2018, available at <https://www.gov.uk/government/publications/security-policy-framework/hmg-security-policy-framework>.

<sup>40</sup> HMG Data Ethics Framework, June 2018, available at <https://www.gov.uk/government/publications/data-ethics-framework/data-ethics-framework>. The Data Ethics Framework guides the design of appropriate data use in government and the wider public sector.

<sup>41</sup> *Supra* note 24 at page 337.

<sup>42</sup> See *The Trust Advantage: How to Win with Big Data*, Boston Consulting Group, November 2013, available at <https://www.bcg.com/publications/2013/marketing-sales-trust-advantage-win-with-big-data.aspx>.

<sup>43</sup> For example, Japan’s amended privacy regime explicitly recognises APEC CBPR as a cross-border transfer mechanism. Australia’s privacy law allows for “binding schemes” that ensure that the recipient of Australian personal data protects the data at the Australian level. The CBPR or PRP are such a binding scheme. Australia has stated intent to join the APEC CBPR. Guidance by the Hong Kong Privacy Commissioner on cross-border data transfers, provides for various options based on “due diligence” that could include contracts or “non-contractual oversight” means (presumably, such means include CBPR) by which an organisation can ensure that data remains protected at the Hong Kong level after transfer (See [https://www.pcpd.org.hk/english/resources\\_centre/publications/files/GN\\_crossborder\\_e.pdf](https://www.pcpd.org.hk/english/resources_centre/publications/files/GN_crossborder_e.pdf) at page 7). Singapore’s Personal Data Protection Regulations provide for the use of binding corporate rules for cross-border data transfers and Singapore also joined the APEC CBPR and PRP systems in March 2018. For a more detailed discussion of the benefits and potential further development of certifications, seals and marks, including BCR, under the GDPR, see CIPL’s white paper on “Certifications, Seals, and Marks under the GDPR and Their Roles as Accountability Tools in Cross-Border Data Transfer Mechanisms,” 12 April 2017, available at [http://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl\\_gdpr\\_certifications\\_discussion\\_aper\\_12\\_april\\_2017.pdf](http://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_gdpr_certifications_discussion_aper_12_april_2017.pdf).

---

<sup>44</sup> In fact, there is an ongoing effort between the European Commission, the EDPB and the APEC Data Privacy Subgroup to develop tools to make it easier for companies that seek approval under both the CBPR and GDPR-based transfer mechanisms, such as certifications and BCR.

<sup>45</sup> Of course, it may be the case that certain local requirements are not covered by a formal, multilateral accountability scheme and, therefore, must be addressed by an organisation outside of the scheme. Indeed, the CBPR specifically allow for such add-on obligations based on local variation. But this does not substantially diminish the fact that accountability schemes simplify and streamline compliance management and, therefore, enhance the likelihood of local compliance.

<sup>46</sup> See CNIL SME Toolkit, available at <https://www.cnil.fr/fr/la-cnil-et-bpifrance-sassocient-pour-accompagner-les-tpe-et-pme-dans-leur-appropriation-du-reglement>.

<sup>47</sup> See UK ICO Data Protection Self-Assessment Toolkit, available at <https://ico.org.uk/for-organisations/resources-and-support/data-protection-self-assessment/>.

<sup>48</sup> See Spanish AEPD tool for SMEs to help facilitate compliance with the GDPR, available at, <https://www.aepd.es/reglamento/cumplimiento/cumplimiento-pymes.html>.

<sup>49</sup> In a March 2018 presentation on data privacy updates for SMEs, the PCPD listed publishing a privacy toolkit for SMEs on compliance with the Personal Data (Privacy) Ordinance as one of the PCPD's initiatives to support SMEs. Presentation available at [https://www.pcpd.org.hk/english/news\\_events/speech/files/Data\\_Privacy\\_Updates\\_for\\_SME\\_14Mar.pdf](https://www.pcpd.org.hk/english/news_events/speech/files/Data_Privacy_Updates_for_SME_14Mar.pdf).

<sup>50</sup> Articles 28(1), (4) and (5).

<sup>51</sup> The WP29 specifically emphasised how accountability can be used to proactively take and demonstrate data protection measures that go beyond what is required by the applicable law. *Supra* note 2 at page 6, paragraph 14.

<sup>52</sup> *Supra* note 24 at page 327.

<sup>53</sup> *Supra* note 2 at page 16, paragraph 61.

<sup>54</sup> CIPL's Discussion Paper "Regulating for Results – Strategies and Priorities for Leadership and Engagement," 10 October 2017, available at [https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl\\_final\\_draft\\_-\\_regulating\\_for\\_results\\_-\\_strategies\\_and\\_priorities\\_for\\_leadership\\_and\\_engagement\\_2\\_.pdf](https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_final_draft_-_regulating_for_results_-_strategies_and_priorities_for_leadership_and_engagement_2_.pdf), (advocating a "results-based" approach to data protection oversight and enforcement that relies on constructive engagement with industry, supporting and making use of accountability frameworks, including those that employ third-party certifiers, and risk-based prioritisation of DPA tasks).

<sup>55</sup> *Supra* note 2, at page 16, paragraph 60, highlighting that under accountability organisations will have to be able to demonstrate their implementation measures on demand.

<sup>56</sup> An example is the APEC Cross-border Privacy Enforcement Arrangement (CPEA) designed to provide for enforcement cooperation on matters involving violations of the APEC CBPR or other privacy matters. The CPEA is available at <http://www.apec.org/~media/Files/Groups/ECSG/CBPR/CBPR-CrossBorderPrivacyEnforcement.pdf>.

---

<sup>57</sup> For example, much of everyday complaint-handling, small-scale consumer disputes and failures to comply with applicable requirements might never get resolved or rise to the attention of an enforcement authority, but will get resolved within the context of an accountability scheme that provides for complaint-handling and dispute resolution. This is also one of the key themes of CIPL's Regulating for Results discussion paper (See note 54 above).

<sup>58</sup> *Supra* note 2 at page 18, paragraph 68, and *supra* note 43, CIPL white paper on Certifications, Seals, and Marks under the GDPR and Their Roles as Accountability Tools in Cross-Border Data Transfer Mechanisms at page 12.

<sup>59</sup> *Supra* 4.



## **The Central Role of Organisational Accountability in Data Protection**

**Discussion Paper 2 (of 2)**

# **Incentivising Accountability: How Data Protection Authorities and Law Makers Can Encourage Accountability**

Centre for Information Policy Leadership

**23 July 2018**

**Table of Contents**

**I. Objectives of this Paper** ..... 3

**II. Why Accountability Should be Incentivised** ..... 3

    A. Accountability Beyond Purely Legal Compliance..... 3

    B. The Benefits of Accountability ..... 4

        1. Benefits to Organisations Serving as “Internal Incentives” for Accountability ..... 6

        2. Benefits to Individuals and DPAs that Warrant External Incentives ..... 6

**III. Who Should Incentivise Accountability** ..... 7

    A. DPAs ..... 7

    B. Law and Policy Makers ..... 7

**IV. How Accountability Should be Incentivised** ..... 8

    A. Incentives for Implementing Accountability..... 10

    B. Balancing Incentives with Enforcement Powers..... 12

**V. Conclusion** ..... 12

## I. Objectives of this Paper

In the first paper in this series — “The Case for Accountability: How it Enables Effective Data Protection and Trust in the Digital Society” (first CIPL paper) — CIPL<sup>1</sup> explained the general consensus on the meaning of accountability; accountability’s central importance to data protection, corporate digital responsibility and the digital economy; and the benefits it conveys to all stakeholders. The objectives of this second paper are, first, to make the case for specifically incentivising organisational accountability and, second, to provide specific suggestions for what such incentives might be. Importantly, the objective in promoting an approach of incentivising accountability is not to weaken or hinder the powers of data protection authorities (DPAs) and, consistent with CIPL’s 2017 discussion paper “Regulating for Results – Strategies and Priorities for Leadership and Engagement”<sup>2</sup> (Regulating for Results), it enables DPAs to use other tools in their regulatory toolbox to enable good data practices and compliance.

Furthermore, this discussion paper is intended to promote further thinking to define such incentives. CIPL looks forward to conducting further work in the future on this essential aspect of accountability and to further engaging on this topic with all stakeholders in the digital ecosystem.

## II. Why Accountability Should be Incentivised

### A. Accountability Beyond Purely Legal Compliance

As demonstrated in the first CIPL paper, accountability may go beyond pure legal compliance. Law and regulation now increasingly require basic accountability (e.g., in the GDPR) and, as such, help ensure compliance with applicable legal requirements. But accountability manifests along a continuum. An organisation’s implementation of measures and controls may go above and beyond what the law requires. This might be referred to as “heightened accountability.”

As discussed in detail in the first CIPL paper, such heightened accountability provides numerous significant benefits to all stakeholders, including organisations, individuals and DPAs. In this paper, we demonstrate how these benefits, particularly those to individuals and DPAs, warrant significant support from DPAs through encouragement and specific incentives for implementing such heightened accountability. The paper also makes the case that policy and law makers should include effective incentives for accountability in any new or revised data protection regimes.

Examples of heightened accountability that exceed the basic legal requirements include:

- Implementing risk mitigations and controls or undertaking other protective measures that are not specifically required by law;

- Linking privacy management programs to values in the organisation’s code of business ethics and reflecting ethical decision-making in the organisation’s privacy policies and procedures;
- Participating in non-mandatory privacy certifications and codes of conduct or similar formal privacy accountability schemes, such as Binding Corporate Rules (BCR)<sup>3</sup>, APEC Cross-Border Privacy Rules (CBPR)<sup>4</sup>, APEC Privacy Recognition for Processors (PRP)<sup>5</sup>, Privacy Shield<sup>6</sup> and future GDPR certifications and codes;
- Applying certain controls and requirements of privacy management programs to an organisation’s operations in countries without data privacy laws; and
- Requiring heightened accountability of business partners in the ecosystem.

The table below sets forth the reasons why law makers and DPAs should incentivise accountability. However, accountability should be particularly encouraged, incentivised and rewarded where it goes above what is minimally required by law, as such heightened accountability provides substantial additional benefit to individuals, society and DPAs. This approach is consistent with many other areas of law and compliance where legislators and regulators specifically offer incentives for good corporate behaviour and comprehensive compliance programs.<sup>7</sup>

## **B. The Benefits of Accountability**

CIPL outlined in detail the benefits of accountability in the first paper in this series. While this paper does not repeat that discussion, the benefits are summarised in the following table:

<b>Benefits for Regulators</b>
• Provides assurance to DPAs that organisations are identifying and prioritising high-risk data processing.
• Reduces the oversight, complaint-handling and enforcement burdens of DPAs through the involvement of third-party certifiers, Accountability Agents and third-party dispute resolution bodies.
• Allows DPAs to be more selective and strategic with their often limited resources in pursuing their overall mission.
• Promotes constructive engagement with accountable organisations.
• Improves cross-border privacy enforcement cooperation through the creation of mutually recognised requirements and processes, such as in BCR and CBPR.
• Assists DPAs in carrying out investigations and enforcement actions by bridging together different legal regimes and providing a more uniform data protection environment.
• Simplifies investigations and enforcement actions and enables companies to demonstrate compliance to DPAs by requiring organisations to maintain records of processing.
• Keeps organisations honest in terms of claims made to the public by facilitating exposure of false claims.

<b>Benefits for Individuals</b>
• Delivers real and more effective protection of individuals and their data.
• Ensures that the protection follows personal data transferred across borders.
• Assures individuals that compliance with local legal requirements are met and increases individuals' trust in organisations' processing of their data.
• Enhances privacy protections for individuals beyond minimum requirements and empowers individuals in the management of their data (e.g., through the extension of individual rights or voluntary security breach reporting by organisations).
• Shifts the burden of protecting individuals more explicitly to organisations.
• Provides individuals with a benchmark for deciding whether to allow their data to be processed by certain organisations.
• Provides individuals' rights and interests heightened consideration and protection through required risk assessments and balancing processes.
• Permits individuals to reap the benefits of participation in the digital society.
• Enables more effective domestic and cross-border enforcement.
<b>Benefits for Organisations</b>
• Enables more effective privacy protections by requiring risk-based prioritisation of such protections.
• Assists organisations in ensuring and demonstrating legal compliance to business partners and regulators.
• Fosters a culture of internal privacy compliance and constructive engagement with DPAs.
• Fosters good data hygiene and good data management and helps to support the strategic objectives of organisations around data.
• Enables greater harmonisation of organisations' privacy policies and practices with the various requirements of the different jurisdictions in which they do business.
• Generates trust among the public and regulators that the organisation is processing personal data responsibly, potentially enhancing the reputation and goodwill of the organisation and adding value to its brand (trust advantage <sup>8</sup> ).
• Enables organisations to engage in broader beneficial uses of personal data, including data for social good, research and responsible AI and machine learning by minimising the risks of new data uses (e.g., through incorporating privacy by design, transparency, risk assessment, etc.) and demonstrating responsible data use to regulators.
• Assists SMEs with implementing scalable privacy tools and controls within their organisations, appropriate to their size and type of operation.
• Provides legal certainty for organisations with regard to cross-border data protection compliance through participation in recognised accountability frameworks, such as BCR and CBPR.
• Enables cross-border data transfers through recognised mechanisms such as BCR and CBPR.
• Furthers the creation of interoperability between different accountability frameworks and thus global solutions to data transfers for organisations.
• Helps differentiate between organisations and provides a competitive edge to those who choose to invest in accountability relative to those who do not (accountability advantage).
• Improves overall level of privacy behaviours of organisations which in turn improves the health of the data ecosystem in general and benefits all stakeholders in the digital economy in the long run.
• Serves as a due diligence tool for controllers in identifying qualified and accountable processors.

*Table 1 – Benefits of Organisational Accountability to Stakeholders*

## 1. Benefits to organisations serving as “internal incentives” for accountability

As demonstrated by *Table 1*, accountability provides specific and direct benefits to organisations. Such benefits could be seen as “internal incentives” for organisations, in that no further encouragement should be necessary from DPAs or law and policy makers for organisations to implement accountability. This is particularly true with respect to the benefit of ensuring and demonstrating legal compliance, thereby reducing the threat and consequences of legal enforcement. Clearly, laws requiring accountability also provide a concomitant incentive to implement it at least to the level required by law.

There are also other “internal incentives” beyond the threat of enforcement. These apply regardless of whether the accountability is of the required or of the non-mandatory “heightened accountability” kind, and these internal incentives increase as the accountability moves up on the accountability spectrum. They include:

- a) Using formal accountability mechanisms like certifications or BCR to enable efficiencies and drive the benefits of being able to share personal data across borders within the organisation and its business partners;
- b) Providing assurances in a due diligence process, such as in vendor selection or M&A;
- c) Increasing trust and confidence among an organisation’s customers or DPAs;
- d) Improving the organisation’s reputation among business partners and/or the public; and
- e) SMEs (that may have limited data protection expertise or staff) receiving assistance from third-party certifiers in developing their internal privacy programs.

Thus, organisations have a range of internal incentives to implement accountability of any degree along the spectrum. In many cases “enlightened self-interest” can provide the necessary motivation for organisations to place at the high end of the accountability spectrum. Some of these incentives are increasingly recognised and also formally incentivised by law makers, including in the GDPR. Nevertheless, the more accountability aims beyond what is required, the more it would be helpful to support it through additional “external incentives.” As organisations increasingly face competing (and sometimes conflicting) regulatory priorities coupled with market pressures to drive value for shareholders, providing organisations a figurative “return on investment” on data privacy compliance and accountability would be advantageous for any DPA and law and policy maker.

## 2. Benefits to individuals and DPAs that warrant external incentives

*Table 1* above sets forth significant benefits of accountability to individuals and DPAs. Benefits to individuals centre on improved privacy protections, increased individual empowerment, heightened trust in the digital economy and more effective redress. The benefits to the DPAs boil down to a significant augmentation of their limited enforcement and oversight resources

through better actual compliance by organisations and better ability to demonstrate such compliance, which streamlines investigations and enforcement; assurance that organisations are engaged in a risk-based approach to data protection; involvement of third-party certification bodies that provide front-line oversight, “enforcement” and complaint-handling in the context of formal accountability schemes such as privacy certifications and codes of conduct; and improved cross-border enforcement in the context of such accountability schemes.

Given these wide-ranging benefits to individuals (whose collective interests DPAs represent) and to the DPAs themselves, accountability should not be left solely to the threat of sanctions under the applicable law or to the enlightened self-interest of the organisation. It should also be actively promoted through “external incentives.” This is particularly important in connection with non-mandatory heightened accountability. From an organisation’s perspective, particularly at the highest level of management, investing in levels of accountability that exceed what is required begs the question of justification, especially where the internal incentives are perceived as sufficiently realised. This is where external incentives have a crucial role to play. Such incentives will, in effect, function as an additional “return on investment” on any heightened accountability the organisation implements and thus will help drive corporate best practices in responsible data use and management.

### **III. Who Should Incentivise Accountability**

External incentives for accountability should come primarily from DPAs and law makers.

#### **A. DPAs**

As noted in CIPL’s Regulating for Results discussion paper,<sup>9</sup> the DPAs’ leadership role should include encouraging and incentivising organisations to adopt accountability frameworks, particularly the kinds that go above and beyond what is minimally required.<sup>10</sup> Indeed, DPAs have become de facto data regulators and society’s arbiters of responsible use of personal data in the modern information age. As such, they have a particular responsibility to find ways to incentivise the broad-scale implementation of accountability.

#### **B. Law and Policy Makers**

Law and policy makers too must be concerned about accountability and individuals’ trust in the digital society as this is crucial for reaping the benefits of the fourth industrial revolution. Only accountability can deliver that, coupled with sensible regulation. Accordingly, law and policy makers in jurisdictions that have not yet done so should specifically incentivise accountability through any new or updated data protection laws and regulations to enable the trusted information age.

#### IV. How Accountability Should be Incentivised

Incentivising accountability could be viewed as a core component of a results-based approach by DPAs to data protection oversight and enforcement. As CIPL has advocated over the past year and as further described in CIPL's Regulating for Results discussion paper,<sup>11</sup> the results-based approach relies to a significant extent on constructive engagement between DPAs and accountable organisations. Prioritising the encouragement and incentivising of desired conduct over penalising undesirable conduct is a core principle of constructive engagement.

There is a broad range of incentives that could be deployed to encourage broader implementation of accountability. As further discussed below, some laws already include, and some DPAs already pursue policies that provide, relevant incentives in this context. Some potential incentives have never been tried in the data protection context, as far as we know.

For example, perhaps the most impactful incentive would be to allow controllers that can effectively demonstrate accountability beyond pure legal compliance to pursue a broader range of reasonable and beneficial uses of personal data. Such broader range of uses could occur in the context of participation in "regulatory sandboxes" specially designed for this purpose.<sup>12</sup> A regulatory sandbox allows qualifying (here accountable) businesses to test innovative products, services, business models and delivery mechanisms in the real market, with real consumers. In the data protection context, this could include testing new data processing activities, data collection methods, or the offering of new information services with appropriate regulatory safeguards and oversight. Of course, given that they permit the processing of real consumers' data and that statutory data protection requirements will still apply to such data processing, further thinking on how such sandboxes would work will be required.

Another impactful incentive could be interpreting data protection principles and requirements (e.g., compatible purposes and fair processing) through the lens of risk and more flexibly for organisations that demonstrate heightened accountability. This would be consistent with the GDPR, which allows for the risk-based calibration of organisations' compliance measures and mitigations. It would be useful to conduct further work on such risk-based and flexible interpretation of data protection principles in the future.

Other incentives include formally recognising demonstrated or certified accountability (e.g., codes and certifications) as:

- 1) a mitigating factor in enforcement actions and in assessing sanctions and/or levels of fines;
- 2) evidence of due diligence when selecting data processors or service providers; and
- 3) a formal cross-border data transfer mechanism.

Again, some legislators have already taken some steps to provide these incentives, such as in the GDPR and several other national data protection laws.

An important initial step on the issue of incentives generally would be for DPAs to formally express their support for verified or certified accountability schemes, such as future GDPR codes of conduct and certifications, BCR, APEC CBPR and PRP, the Privacy Shield or similar mechanisms. It has been the practice of some DPAs to state informally that they take participation in accountability mechanisms such as CBPR or BCR and other certifications into account when making enforcement-related decisions and that they can be used as evidence of reasonable and good-faith efforts to comply with relevant requirements. However, informal statements to that effect do not provide sufficient assurances to organisations and their Boards that the advantages of doing more than necessary are sufficiently predictable and tangible. Thus, any support for accountability and any articulation of specific incentives should as much as possible be codified by law (as has been done in the GDPR to some extent; see below). If that is not possible, or as an interim measure, such articulation of incentives should take the shape of official policy positions by DPAs in jurisdictions where the law is silent on this issue but the DPAs may, in their discretion, consider participation in formal accountability schemes as mitigating factors in their enforcement decisions.

As stated, the GDPR has started to codify possible incentives to participate in such accountability schemes. For example, Article 83(2)(j) provides that “in deciding whether to impose an administrative fine and deciding on the amount [...] due regard shall be given to [...] adherence to approved codes of conduct [...] or approved certification mechanisms [...].” Discussing that provision, the WP29 guidelines on administrative fines<sup>13</sup> note that “[i]n case of a breach of one of the provisions of the Regulation, adherence to an approved code of conduct might be indicative of how comprehensive the need is to intervene with an effective, proportionate, dissuasive administrative fine or other corrective measure from the supervisory authority.”<sup>14</sup>

Further, the WP29 guidelines on administrative fines also state that

[w]here the controller or processor has adhered to an approved code of conduct, the supervisory authority may be satisfied that the code community in charge of administering the code takes the appropriate action themselves against their member, for example through the monitoring and enforcement schemes of the code of conduct itself. Therefore, the supervisory authority might consider that such measures are effective, proportionate or dissuasive enough in that particular case without the need for imposing additional measures from the supervisory authority itself. Certain forms of sanctioning non-compliant behaviour may be made through the monitoring scheme, according to article 41 (2) c and 42 (4), including suspension or exclusion of the controller or processor concerned from the code community. Nevertheless, the powers of the monitoring body are “without prejudice to the tasks and powers of the

competent supervisory authority”, which means that the supervisory authority is not under an obligation to take into account previously imposed sanctions pertaining to the self-regulatory scheme.<sup>15</sup>

Statements such as this are helpful in encouraging and incentivising participation in accountability schemes, particularly where they are reiterated with regard to specific codes and certifications as they become available.

In addition, the GDPR also provides in Article 28(5) that “adherence of a processor to an approved code of conduct as referred to in Article 40 or an approved certification mechanism as referred to in Article 43 may be used as an element by which to demonstrate sufficient guarantees as referred to in [Article 28(1) and (4)].” In jurisdictions where such use of verified or certified accountability as evidence of due diligence and compliance is not yet formally recognised by law (as it is under the GDPR), DPAs could nevertheless formally endorse such use in connection with their ability to make discretionary enforcement decisions.

#### **A. Incentives for Implementing Accountability**

As discussed in the first paper in this series and in the section on benefits of accountability, organisations have some internal incentive to deliver accountability and implement comprehensive privacy management programs (See discussion in Section II. B. 1. above). This section discusses how DPAs, law makers and policy makers can additionally encourage and incentivise companies to implement accountability beyond their own internal incentives to encourage more wide-spread adoption of accountability by organisations of all types, sizes and structures.

The following table sets forth some of the specific incentives DPAs and/or law and policy makers could provide to organisations<sup>16</sup> to encourage active implementation of accountability:

Using demonstrated accountability<sup>17</sup> as a differentiating or mitigating factor in investigation or enforcement contexts

For example:

- As one of the discretionary factors in considering whether to initiate an investigation or enforcement action.
- As a mitigating factor in assessing the type of penalties and levels of fines.
- As a mitigating factor in case of an individual failure/human error, where the organisation is able to demonstrate that it took the reasonable precautions to prevent the failure or error.

DPAs should communicate this policy regularly and refer to it in specific enforcement cases.

Using demonstrated accountability as a “licence to operate” and use data responsibly, based on organisations’ evidenced commitment to data protection

As one of the bases for:

- Facilitating responsible AI, machine learning, automated decision-making and other big data applications because of the risk assessment, mitigations and other controls in the accountability program.
- Allowing broader use of data for social good and research.
- Participation in relevant “regulatory sandbox” initiatives.

Publicly recognising best in class organisations and showcasing accountable “best practices” (including those that may be an aggregation of such best practices compiled and generalised by regulators)
<ul style="list-style-type: none"> <li>• To promote reputation and trust of accountable organisations.</li> <li>• To promote healthy peer pressure and competition in the marketplace.</li> </ul>
Supporting and guiding organisations (particularly small and emerging companies) on a path towards accountability, either individually or through association bodies
For example: <ul style="list-style-type: none"> <li>• Compliance Agreements used by the Canadian Office of the Privacy Commissioner.</li> </ul>
Co-funding between DPAs and industry for research into novel accountability tools
<ul style="list-style-type: none"> <li>• Similar to proposals contained in the Privacy Bridges Report of 37<sup>th</sup> International Privacy Conference, Amsterdam 2015<sup>18</sup> (See Bridge 10 on Collaborating on and Funding for Privacy Research Programs).</li> <li>• Specific grants by regulators such as the UK ICO and Canadian Federal and Provincial regulators to fund research projects in accountability.</li> </ul>
Offer to play proactive advisory role to organisations seeking to implement accountability
<ul style="list-style-type: none"> <li>• In context of novel technology or business models.</li> <li>• Offer specific resources, including documentation and dedicated contact persons, to support the implementation of heightened accountability.</li> </ul>
Using accountability as evidence of due diligence
For example: <ul style="list-style-type: none"> <li>• In a selection process of processors and other vendors.</li> <li>• In M&amp;A transactions.</li> </ul>
Using formal accountability schemes as evidence of uniform and high level privacy protection to enable cross-border data transfers within the company group and to third parties
<ul style="list-style-type: none"> <li>• APEC CBPR and PRP; EU BCR; GDPR certifications.</li> </ul>
Articulate proactively the elements and levels of accountability to be expected
<ul style="list-style-type: none"> <li>• For instance, at what point would expecting accountability measures constitute undue hardship to organisations?<sup>19</sup></li> <li>• Based on the concept of proportionality and a risk-based approach to accountability measures.</li> </ul>

*Table 2 – Incentives for Implementing Accountability*

Indeed, providing incentives along the lines of the above for the implementation of accountability is consistent with, and follows from, the explicit recognition by the WP29 and many other DPAs of the numerous benefits of accountability. As stated, organisations have choices for achieving compliance and implementing accountability. They range from bare bones compliance to gold plate corporate digital responsibility. The higher the aim, the stronger the need to justify the organisational resources required for the desired level of accountability. Clear and affirmative pronouncements by DPAs about the specific advantages of aiming high would go a long way to helping data protection officers and other relevant staff obtain the necessary buy-in and resources from their corporate leadership, particularly where the accountability measures exceed the legal requirements. Embedding such incentives in the law would help both DPAs and organisations.

## **B. Balancing Incentives with Enforcement Powers**

When providing such incentives, DPAs must safeguard against any weakening of their legitimate data protection enforcement obligations or the appearance of such weakening. DPAs are functionally independent bodies and while they have an important role to play in supporting companies on the road towards implementing accountability, there is a fine line to draw between assistance and leniency. The incentives are intended to encourage the uptake of accountability rather than to downplay a DPA's prerogative to take appropriate action where necessary. Thus, for example, using demonstrated accountability as a mitigating factor in an enforcement context or as evidence of due diligence in a contracting context should occur within clearly articulated guidelines. Using demonstrated accountability as a basis for facilitating broader uses of data, such as in a regulatory sandbox setting, should be clearly defined and subject to appropriate oversight. And, when DPAs showcase accountability "best practices" as an incentive for more organisations to implement such practices, they must do so in a way that does not compromise the DPA's subsequent ability to enforce against organisations that purport to adhere to such best practices but failed to do so in practice. In short, any proactive incentivising of accountability, through whatever mechanism, must keep in mind one of the ultimate goals of accountability — enabling trust in the digital economy and society.

## **V. Conclusion**

DPAs have been on the forefront of promoting accountability's broad global acceptance as a comprehensive and coherent framework for the responsible and beneficial use of data, including by advocating for its inclusion in data protection law. In so doing, they have helped to cement accountability's status as the cornerstone of modern data protection. The next chapter in the story of accountability is ensuring its broad-scale adoption and actual implementation across all industries, types and sizes of organisations and regions beyond what is merely required by law. Thus, the next frontier for accountability is for DPAs and law and policy makers to define clear incentives for implementing it. Such incentives will help organisations justify the resources and efforts necessary to maximise their accountability measures where they go beyond the requirements of the law. Taking accountability seriously and proactively incentivising it is essential to creating trust in the digital economy and society and, in fact, will be game-changing in that respect.

If you would like to discuss this paper further or require additional information, please contact Bojana Bellamy, [bbellamy@HuntonAK.com](mailto:bbellamy@HuntonAK.com), Markus Heyder, [mheyder@HuntonAK.com](mailto:mheyder@HuntonAK.com), Nathalie Laneret, [nlaneret@HuntonAK.com](mailto:nlaneret@HuntonAK.com) or Sam Grogan, [sgrogan@HuntonAK.com](mailto:sgrogan@HuntonAK.com).

## References

---

<sup>1</sup> CIPL is a global data privacy and cybersecurity think tank in the law firm of Hunton Andrews Kurth and is financially supported by the law firm and 63 member companies that are leaders in key sectors of the global economy. CIPL's mission is to engage in thought leadership and develop best practices that ensure both effective privacy protections and the responsible use of personal information in the modern information age. CIPL's work facilitates constructive engagement between business leaders, privacy and security professionals, regulators and policymakers around the world. For more information, please see CIPL's website at <http://www.informationpolicycentre.com/>. Nothing in this paper should be construed as representing the views of any individual CIPL member company or of the law firm of Hunton Andrews Kurth.

<sup>2</sup> CIPL's Discussion Paper "Regulating for Results – Strategies and Priorities for Leadership and Engagement", 10 October 2017, available at [https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl\\_final\\_draft\\_-\\_regulating\\_for\\_results\\_-\\_strategies\\_and\\_priorities\\_for\\_leadership\\_and\\_engagement\\_2.pdf](https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_final_draft_-_regulating_for_results_-_strategies_and_priorities_for_leadership_and_engagement_2.pdf).

<sup>3</sup> See WP29's WP256 Working Document setting up a table with the elements and principles to be found in Binding Corporate Rules, available at [https://ec.europa.eu/newsroom/just/document.cfm?doc\\_id=48798](https://ec.europa.eu/newsroom/just/document.cfm?doc_id=48798) and WP257 Working Document setting up a table with the elements and principles to be found in Processor Binding Corporate Rules, available at [https://ec.europa.eu/newsroom/just/document.cfm?doc\\_id=48799](https://ec.europa.eu/newsroom/just/document.cfm?doc_id=48799).

<sup>4</sup> See APEC CBPR and PRP system documents, available at <http://www.cbprs.org/GeneralPages/APECCBPRSystemDocuments.aspx>.

<sup>5</sup> *Id.*

<sup>6</sup> See EU-US Privacy Shield Framework, available at <https://www.privacyshield.gov/Privacy-Shield-Principles-Full-Text>.

<sup>7</sup> For example, in the context of Anti-Bribery Legislation, Section 7 of the UK Bribery Act 2010 provides that a relevant commercial organisation is guilty of an offence if a person associated with it bribes another person intending to obtain or retain business or a business advantage. However, it is a defence for the organisation to prove it had "adequate procedures" in place to prevent those associated with it from undertaking such conduct. The UK Ministry of Justice provided guidance on what adequate procedures entail (see The Bribery Act 2010: Guidance about procedures which relevant commercial organisations can put into place to prevent persons associated with them from bribing, available at [https://www.gov.uk/government/uploads/system/uploads/attachment\\_data/file/181762/bribery-act-2010-guidance.pdf](https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/181762/bribery-act-2010-guidance.pdf)). Adequate procedures include a top-level commitment to preventing bribery; risk assessments of internal and external risks of bribery and due diligence procedures; policies and procedures proportionate to the bribery risks faced by the organisation; communication, including training of bribery prevention policies and procedures throughout the organisation; and monitoring and reviewing procedures designed to prevent bribery by persons associated with it and making improvements where necessary. Concurrently, the Director of Public Prosecutions and the Director of the Serious Fraud Office issued joint guidance for prosecutors setting out the Directors' approach to deciding whether to bring a prosecution under the Bribery Act 2010 (See Bribery Act 2010: Joint Prosecution Guidance of The Director of the Serious Fraud Office and The Director of Public Prosecutions, available at <https://www.sfo.gov.uk/?wpdmdl=1456>). The guidance notes that "Prosecutors must look carefully at all the circumstances in which the alleged bribe occurred including the adequacy of any anti-bribery procedures. A single instance of bribery does not necessarily mean that an organisation's procedures are inadequate. For example, the actions of an agent or an employee may be wilfully contrary to very robust corporate contractual requirements, instructions or guidance."

---

Implementing accountable anti-bribery procedures clearly acts as an incentive for organisations not only to achieve compliance with the law or providing a defence in a prosecution proceeding, but to avoid a prosecution altogether when an instance of bribery does occur by a person associated with the organisation. Similarly, in the U.S., the Criminal Division of the United States Department of Justice and the Enforcement Division of the United States Securities and Exchange Commission in their guidance on the U.S. Foreign Corrupt Practices Act, note that “[i]n appropriate circumstances, DOJ and SEC may decline to pursue charges against a company based on the company’s effective compliance program, or may otherwise seek to reward a company for its program, even when that program did not prevent the particular underlying FCPA violation that gave rise to the violation.” Additionally, the guidance notes that the “DOJ and SEC recognize that positive incentives can also drive compliant behavior. These incentives can take many forms such as personnel evaluations and promotions, rewards for improving and developing a company’s compliance program, and rewards for ethics and compliance leadership.” See A Resource Guide to the U.S. Foreign Corrupt Practices Act, November 2012, available at <https://www.justice.gov/criminal/fraud/fcpa/guidance/guide.pdf> at pages 56, 59 and 60.

<sup>8</sup> See The Trust Advantage: How to Win with Big Data, Boston Consulting Group, November 2013, available at <https://www.bcg.com/publications/2013/marketing-sales-trust-advantage-win-with-big-data.aspx>.

<sup>9</sup> *Supra* note 2.

<sup>10</sup> *Id.* at pages 6, 31, 35 and 38.

<sup>11</sup> *Supra* note 2.

<sup>12</sup> For example, the UK Financial Conduct Authority’s regulatory sandbox model has supported 60 firms to test their innovations in financial services with real customers in the live market under controlled conditions. See <https://www.fca.org.uk/firms/regulatory-sandbox/global-sandbox>.

<sup>13</sup> See WP29’s WP253 Guidelines on the application and setting of administrative fines for the purposes of the Regulation 2016/679, available at [http://ec.europa.eu/newsroom/just/document.cfm?doc\\_id=47889](http://ec.europa.eu/newsroom/just/document.cfm?doc_id=47889) at page 15.

<sup>14</sup> *Id.*

<sup>15</sup> *Id.*

<sup>16</sup> In addition to providing specific incentives to organisations, DPAs and law and policy makers should also consider how to incentivise and encourage third-party certification bodies and “Accountability Agents” to become involved in delivering organisational accountability through formal accountability schemes such as certifications. The success of “heightened accountability” through formal accountability schemes such as certifications depends in no small part on the willingness of competent certification bodies and Accountability Agents of all sizes to enter the market.

<sup>17</sup> “Demonstrated accountability” includes all the essential elements of accountability (i.e., leadership and oversight, risk assessment, policies and procedures, transparency, training and awareness, monitoring and verification, and response and enforcement). Thus, the degree to which each of the accountability elements are demonstrably implemented within an organisation will impact the degree to which such implementation can serve as a mitigating factor.

---

<sup>18</sup> Privacy Bridges: EU and US Privacy Experts in Search of Transatlantic Privacy Solutions, 37<sup>th</sup> International Privacy Conference, Amsterdam, 2015, at page 40, available at <https://privacybridges.mit.edu/sites/default/files/documents/PrivacyBridges-FINAL.pdf>.

<sup>19</sup> Some regulators, as a matter of their statutory duty, already consider the impact on organisations of adopting regulator recommendations as to best practices. Making these determinations for more of their recommendations and suggested best practices will include conducting more detailed impact assessments to measure the costs and benefits to organisations of adopting such practices.