23 JULY 2018

Centre for Information Policy Leadership
Hunton Andrews Kurth

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.[1] 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[2] (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).[3]

- 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

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

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

Benefits for Organisations
• 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[4]).
• 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.

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[5]:

Incentives for Implementing Accountability

Using demonstrated accountability[6] 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 37th International Privacy Conference, Amsterdam 2015[7] (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?[8] • 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."[9]

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

[1] 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).

[2] 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.

[3] The European Data Protection Board (EDPB) might consider re-issuing the WP29 Opinion on accountability.

[4] 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.

[5] 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.

[6] "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.

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

[8] 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.

[9] "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.