Centre for Information Policy Leadership
Hunton Andrews Kurth

3 July 2019

CIPL Accountability Q&A

This document addresses some commonly asked questions about the concept of organizational accountability in data protection.

1. What is "accountability"?
2. What is "accountability" not?
3. What must organizations do to be "accountable"?
4. What are the core elements of accountability?
5. What specifically do the core elements of accountability require of companies?
6. How does the risk-based approach to privacy relate to accountability?
7. Is accountability enforceable?
8. Accountability is in the GDPR – is it a foreign concept to US law?
9. Is accountability just another way of saying "comply with the law"?
10. How can organizations implement and demonstrate accountability?
11. Is accountability only feasible for large organizations with lots of resources?
12. What formal accountability schemes are available to help companies be accountable?
13. How does accountability benefit companies?
14. How does accountability benefit individuals?
15. How does accountability help privacy enforcement authorities?
16. What benefits do formal accountability schemes, such as CBPRs, offer?
17. Why should lawmakers and regulators provide companies with incentives to be accountable?

1. What is "accountability"?

- **Accountability is globally recognized as a key building block for effective privacy and data protection regulation**. It requires organizations to implement a comprehensive privacy program governing all aspects of collecting and using personal information and to be able to verify and demonstrate the existence and effectiveness of such programs internally (to Board and senior level management) and externally on request (to privacy enforcement authorities, individuals and business partners).

- **Accountability gives effect to legal requirements and data privacy laws**. Having a comprehensive privacy program in place is the foundation for compliance with all applicable privacy obligations established by law, regulation or other standard. The specific core elements of accountability-based privacy programs, such as risk assessment, ensure ongoing privacy compliance and that the program remains current when technologies and business practices change over time.

- **Accountability delivers "corporate digital responsibility" fit for the 21st century and modern data driven economies**. It ensures effective protection for individuals and their data and enables digital trust and responsible use, sharing and flows of data. Moreover, accountability provides the tools for protecting personal information and places the responsibility of doing so on organizations that use such information, while also facilitating appropriate individual choice and control over such information.

2. What is "accountability" <u>not</u>?

- **<u>Accountability is not self-regulation</u>**. Rather, it operationalizes and translates principles-based legal rules into concrete policies, procedures, controls and governance to deliver compliance. It sits on top of and is in addition to other legal requirements – it does not replace them. Because laws that include accountability may be principles-based (rather than being overly detailed), they enable the adaptation of such principles to specific industry sectors and differing levels of risk, either through additional guidance by a regulator or by companies themselves through risk assessments and other accountability tools, as appropriate.

- **<u>Accountability is also not a "carte blanche" or free pass to use data in any way an organization wants</u>**. It requires organizations to be thoughtful about uses of data, to implement all applicable data protection requirements (including risk assessments and appropriate mitigations) and to be able to demonstrate that implementation. Accountability demands that organizations commit to acting responsibly in respect of both the use and protection of data.

- **<u>Accountability is not a self-serving concept pushed by industry</u>**. Accountability provides significant benefits for privacy enforcement authorities, individuals and society.

- **<u>Accountability is not an excuse for when things go wrong</u>**. It minimizes the risk of non-compliance and prepares organizations to be responsive and responsible when data incidents do occur. Demonstrated accountability can serve as a mitigating factor in enforcement but it does not give organizations a get out of jail free card and is fully enforceable.

3. What must organizations do to be "accountable"?

Accountability requires organizations to:

- Implement within the company a comprehensive privacy program covering all core elements of accountability that enables compliance with applicable laws, regulations or industry standards;

- Verify the effectiveness and delivery of such a privacy program and ensure continuous improvement; and

- Be able to demonstrate the existence and effectiveness of such a program internally (to Board and senior level management) and externally on request (to regulators, business partners and individuals).

4. What are the core elements of accountability?

- The core elements of accountability are: leadership and oversight; risk assessment; policies and procedures; transparency; training and awareness; monitoring and verification; and response and enforcement.

- A privacy law typically addresses each of these elements in some fashion. Ideally, the law will provide enough flexibility for a company to tailor each of these elements to their specific risks

and requirements through their own risk assessment processes that are part of their accountability-based privacy programs.

- Even in the absence of a law, organizations can create privacy programs that incorporate and address each of the core elements of accountability and implement such programs as a matter of corporate policy and practice.

5. What specifically do the core elements of accountability require of companies?

Companies must take concrete steps to establish policies, procedures and controls that apply the above core elements of accountability to the collection, use, sharing and any other processing and protection of personal information. These include:

- **Establishing leadership and oversight for data protection and the responsible use of data**, including governance, reporting, buy-in from all levels of management and appointing appropriate personnel to oversee the organization's accountability program and report to management and the board.

- **Assessing and mitigating the risks** that data collection and processing may raise to individuals, including weighing the risk of the information use against its benefits. Risk assessment also means conducting periodic reviews of the organization's overall privacy program and information uses in light of changes in business models, law, technology and other factors and adapting the program to changing levels of risk.

- **Establishing internal written policies and procedures** that operationalize legal requirements, create concrete processes and controls to be followed by the organization, and reflect applicable law, regulations, industry standards as well as the organization's values and goals.

- **Providing transparency to all stakeholders internally and externally** about the organization's data privacy program, procedures and protections, the rights of individuals in relation to their data and the benefits and/or potential risks of data processing. This may also include communicating with relevant data privacy authorities, business partners and third parties about the organization's privacy program.

- **Providing training for employees** to ensure awareness of the internal privacy program, its objectives and requirements, and implementation of its requirements in line with the employees' roles and job responsibilities. This ensures that data privacy is embedded in the culture of the organization so that it becomes a shared responsibility.

- **Monitoring and verifying the implementation and effectiveness of the program and internal compliance** with the overall privacy program, policies, procedures and controls through regular internal or external audits and redress plans**.**

- **Implementing response and enforcement procedures** to address inquiries, complaints, data protection breaches and internal non-compliance, and to enforce against acts of non-compliance.

6. How does the risk-based approach to privacy relate to accountability?

- An effective privacy law must be risk based. That means that companies must be required to assess the risks of harm to individuals associated with their proposed information uses, weigh them against the desired benefits of the uses and devise appropriate measures to reduce or eliminate such risks as much as possible. Understanding the risks of their specific information uses allows companies to create more effective protections against the actual risks at hand.

- The risk-based approach also enables companies to prioritize and calibrate their compliance and accountability measures specifically to their context as opposed to engaging in one-size-fits-all and potentially wasteful and unnecessary compliance activities. This approach increases privacy protections for individuals and maximizes the productivity of available compliance dollars in companies in areas where the risk is higher.

- Risk assessment and the risk-based approach to privacy compliance is a core element of accountability. Organizations must build, implement and calibrate their privacy program based on risk to individuals, as well as the risk to organizations from non-compliance. As such, accountability and the risk-based approach to privacy go hand in hand.

7. Is accountability enforceable?

- Yes. Accountability is enforceable. Where a law requires accountability, the absence of a verifiable and demonstrated privacy program or any demonstrable policies and procedures for complying with the legal requirements in that law would be an enforceable violation in and of itself, even if no other violation occurred. Thus, accountability requires that organizations have a comprehensive internal compliance program that they can demonstrate on request.

- Even in the absence of formal requirements to have privacy programs, most privacy enforcement authorities now expect responsible companies that handle personal data to have comprehensive internal programs governing their information uses in place. In an investigation or enforcement context, such authorities will look to whether the company has implemented such a program.

- Many privacy frameworks and data protection laws have incorporated accountability as a matter of basic obligation or best practice and provide the means to enforce the requirement. Further, the U.S. Federal Trade Commission in its enforceable consent decrees requires, when relevant, that companies implement the full range of accountability measures through privacy programs and mandated periodic audits to verify compliance.

8. Accountability is in the GDPR – is it a foreign concept to US law?

- No. Accountability is one of the "Fair Information Practices Principles", which is guidance for data governance developed in the United States in the 1970s that has formed the basis for law, regulation and international agreements governing privacy, data protection and data flows, including the OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data and the APEC Privacy Framework. Since the early 2000's policymakers, data privacy enforcement authorities, experts, companies and advocates have engaged in an effort – led by

policymakers and experts in the United States – to further define and describe how accountability can be relied on to protect data in a way that takes into account the realities of 21st century data technologies, business models, collection and use.

- Moreover, the elements of accountability have been relied on in other areas of U.S. corporate law and compliance, including anti-corruption, white-collar crime and corporate fraud, anti-money laundering, healthcare, export control and competition law. U.S. organizations, regulators and courts have used these elements to determine whether an organization has maintained an effective and comprehensive compliance program in any given regulatory area.

- Finally, accountability is also a core component of the APEC Cross-border Privacy Rules (CBPR) system, which was developed through an international process in which the United States was a key player.

9. Is accountability just another way of saying "comply with the law"?

No. Accountability is a framework that enables organizations to implement governance, policies, procedures and controls that enable legal compliance, give effect to high-level legal principles and requirements and protect data and individuals. In addition, while accountability's first goal is to deliver compliance, it also drives privacy practices beyond legal compliance to incorporate additional protections that are based on a company's additional policies and ethical considerations. Thus, it accomplishes two principal objectives:

- It requires companies to implement a comprehensive and demonstrable program that enables them to comply with the full range of applicable privacy requirements, consistent with the size of their business and nature of information uses.

- It promotes a general culture of privacy that may go above and beyond what is required by law and incorporate additional considerations of best practice, consumer interest, fairness and business ethics where appropriate.

10. How can organizations implement and demonstrate accountability?

- Accountability can be implemented within organizations through a variety of mechanisms. Organizations can implement their own custom-made internal policies and programs tailored to their company's size, structure and data processing activities. In addition, organizations may also participate in formal accountability schemes involving some form of third party review and approval, which help to demonstrate accountability, such as Binding Corporate Rules (BCRs), APEC Cross-border Privacy Rules (CBPRs), APEC Privacy Recognition for Processors (PRPs), ISO standards or other privacy certifications that set forth specific requirements.

- Such formal accountability schemes can help companies of all sizes (including micro-enterprises and SMEs) meet relevant legal and accountability requirements without developing their own custom-made program. They also enable organizations to readily demonstrate accountability and their program to regulators, business partners, clients and individuals.

- Organizations can also take advantage of officially recognized enforceable codes of conduct that may be developed by trade associations or professional organizations in the future.

11. Is accountability only feasible for large organizations with lots of resources?

- No. Accountability is a scalable concept that can be implemented by organizations of all sizes. The risk-based approach, which is a key component of accountability, means that organizations must build their program to address the relevant risks they face. Smaller companies handling smaller amounts of personal data will not need to build a program to the degree that a large multinational company would.

12. What formal accountability schemes are available to help companies be accountable?

Companies seeking a formal accountability scheme instead of, or in addition to, a custom-made internal program have a range of options. These include:

- Binding Corporate Rules (BCRs)
- APEC Cross-border Privacy Rules (CBPRs)
- APEC Privacy Recognition for Processors (PRPs)
- The U.S. Privacy Shield
- ISO Standards
- Third party certification programs
- Recognized codes of conduct

13. How does accountability benefit companies?

Accountability benefits companies by:

- Requiring them to establish comprehensive internal privacy programs designed to achieve compliance with all relevant legal requirements, other external standards and/or company-specific privacy goals;

- Helping them to demonstrate legal compliance to privacy enforcement authorities and business partners;

- Acting as a mitigating factor in enforcement actions or in the setting of fines by demonstrating good faith efforts to comply with the law and to deal with data responsibly;

- Promoting more effective privacy protections by requiring organizations to set program priorities based on risk and to define and implement mitigation measures based on risk;

- Fostering a culture of internal privacy compliance within the company and constructive engagement with privacy enforcement authorities;

- Generating trust with the public and with privacy enforcement authorities that the organization is

processing personal data responsibly, thereby enhancing brand and reputation;

- Enabling organizations to better harmonize their privacy policies and practices with the requirements of the various jurisdictions in which they do business;
- Enabling organizations to engage in broader beneficial uses of personal data, including research for the public social good and AI and machine learning, by minimizing the risks of new data uses and requiring companies to demonstrate responsible data use to data privacy enforcement authorities;
- Providing legal certainty with regard to cross-border data protection when implemented through recognized accountability frameworks, such as the CBPR;
- Serving as a due diligence tool for data controllers (companies that control the collection and use of personal information) by identifying qualified and accountable data processors, service providers or vendors that are certified under formal accountability schemes, such as the CBPR and PRP; and
- Improving the overall level of privacy behaviors of organizations which creates a network of companies with mature and responsible privacy practices across the data marketplace and ecosystem.

14. How does accountability benefit individuals?

Accountability delivers real and effective protections for individuals and their data. Specifically, accountability:

- Assures individuals that companies are complying with the law and enhances their trust in organizations' use of their data;
- Shifts the burden of protecting individuals more explicitly to organizations and away from individuals;
- Addresses "consent fatigue" caused by excessive reliance on "individual control" and "consent" requests by providing for alternative mechanisms (e.g. risk assessments; transparency; redress) that more effectively protect individuals in many contexts.
- Ensures that individuals' data is protected even when it is transferred across borders;
- Helps individuals decide whether to give their personal information to organizations by making accountability a benchmark for that decision; and
- Makes enforcement of privacy laws more effective both within the U.S. and across borders.

15. How does accountability help privacy enforcement authorities?

Accountability provides benefits to privacy enforcement authorities by:

- Reducing the oversight, complaint-handling and enforcement burdens of privacy enforcement authorities through the overall enhanced privacy practices of companies and by involving approved third parties to carry out some of the oversight and complaint-handling tasks in the context of formal accountability schemes, such as the CBPR or other privacy certifications or codes of conduct;
- Allowing privacy enforcement authorities to be selective and strategic in their enforcement decisions in light of their limited resources;
- Enabling them to engage in a positive and constructive way with accountable companies;
- Streamlining investigations and enforcement by requiring companies to document their internal privacy programs and decision-making and to be able to demonstrate these to privacy enforcement authorities on request;
- Creating a more uniform data protection environment that streamlines investigations and enforcement actions, including across borders; and
- Encouraging a data protection race to the top rather than to the bottom.

16. What benefits do formal accountability schemes, such as CBPRs, offer?

- Independent from the benefit they may have as cross-border transfer mechanisms in some jurisdictions, formal accountability schemes, such as Binding Corporate Rules (BCRs), APEC CBPRs, APEC PRPs, codes of conduct or certifications and ISO standards can benefit companies that may not have the resources or expertise to independently devise fully-fledged internal privacy programs without the assistance of a third party. By meeting the requirements of these mechanisms, companies establish within their organizations the conditions necessary to be accountable and set themselves up to successfully comply with applicable privacy laws or standards.
- As these schemes are formally recognized by data privacy enforcement authorities or laws, these mechanisms offer companies the legal certainty necessary to process personal information lawfully and with confidence.
- In addition, these formal accountability mechanisms foster trust with data privacy enforcement authorities and individuals.

17. Why should lawmakers and regulators provide companies with incentives to be accountable?

- Accountability provides many concrete benefits to all stakeholders – companies, privacy enforcement authorities and individuals. Many of the benefits to companies (e.g. enabling data driven innovation, providing a reputational advantage and generating trust), as well as the risk of enforcement, will motivate companies to properly implement accountability throughout their organization. However, given its critical importance to the digital economy, lawmakers and privacy enforcement authorities should provide specific additional incentives that encourage companies to adopt accountability measures and reward those that invest in privacy and accountability.

- Such incentives could include recognizing demonstrated accountability or participation in formal accountability schemes (e.g. CBPR and other privacy certifications) as mitigating factors in enforcement contexts or in the setting of fines, or recognizing participation in such accountability schemes as evidence of due diligence when selecting third party processors or vendors to whom it is safe to transfer personal information.

- Providing incentives for companies to be accountable will speed its adoption and promote the benefits of accountability that accrue to companies, individuals and data privacy enforcement authorities as well as generally raise the level of compliance and accountability across the digital economy.

If you would like to discuss this Q&A in more detail or require additional information, please contact Bojana Bellamy, bbellamy@huntonAK.com, Markus Heyder, mheyder@huntonAK.com, Nathalie Laneret, nlaneret@huntonAK.com or Sam Grogan, sgrogan@huntonAK.com.

Additionally, for more detailed information on accountability, please see CIPL's white papers on "The Case for Accountability: How it Enables Effective Data Protection and Trust in the Digital Society"[1] and "Incentivising Accountability: How Data Protection Authorities and Law Makers Can Encourage Accountability".[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 77 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/.

References

[1] The Case for Accountability: How it Enables Effective Data Protection and Trust in the Digital Society, 23 July 2018, available at https://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.

[2] Incentivising Accountability: How Data Protection Authorities and Law Makers Can Encourage Accountability, 23 July 2018, available at https://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.