Centre for Information Policy Leadership
Hunton Andrews Kurth LLP

30 October 2019

Organisational Accountability – Past, Present and Future

For more than a decade, the Centre for Information Policy Leadership (CIPL) has pioneered organisational accountability as a key building block of effective data protection and privacy regulation. With origins in late 1970s corporate governance rules and now an important part of European data protection law, organisational accountability is a vital tool with which policymakers can shape the future and deliver a Europe fit for the Digital Age.

1. INTRODUCTION

Since 2001, the Centre for Information Policy Leadership (CIPL) has cultivated a trusted and neutral dialogue between regulators and business across the world, in support of data innovation and effective privacy regulation. In 2009 it initiated an Accountability Project[1] to shape an approach to data protection and privacy that would support the information economy by taking account of rapid technological development, ubiquitous data collection, powerful analytics, and global information flows.

By 2016 the principle of accountability was reflected in Europe's General Data Protection Regulation, requiring data controllers to implement appropriate technical and organisational measures. Speaking in Berlin in May that year, the former European Data Protection Supervisor Giovanni Buttarelli explained that he had met with companies that were dealing with accountability in a modern way, by embedding ethics within the design of digital applications right from the start. In many ways, he said, "Ethics is the new accountability".[2]

Incoming European Commission president Ursula von der Leyen's attention to ethics in Artificial Intelligence (AI) is set in the context of growing understanding of the importance of ethical business practice[3]. This is closely connected with the development and implementation of organisational accountability, which has been effective in wide-ranging contexts. CIPL has championed the concept of organisational accountability for many years. This paper highlights the past, present and future applications of accountability in the context of the European digital policy agenda.

[1] Data Protection Accountability: The Essential Elements. CIPL, 2009: http://bit.ly/2lubOPC

[2] Keynote speech at EDPD Conference 2017: http://bit.ly/2jXFYKy

[3] C Hodges and R Steinholtz, Ethical Business Practice and Regulation: A Behavioural and Values-Based Approach to Compliance and Enforcement (Hart, 2017); C Mayer, Prosperity (Oxford University Press, 2018).

2. THE CONCEPT OF ORGANISATIONAL ACCOUNTABILITY

Accountability is a mainstay of privacy and data protection regulation globally. In the United States, the concept can be traced back to the 1977 Foreign Corrupt Practices Act (FCPA)[4] and the 2002 Sarbanes-Oxley Act (SOX Act)[5]. From 1987 it appeared in the United States' US Sentencing Commission Federal Sentencing Guidelines, and from 2019 it was adopted as part of the Department of Justice guidance for white-collar prosecutors[6]. Key elements of accountability are well established in Anti-Money Laundering regulations[7] and in regulatory guidance for various segments of the US healthcare industry including hospitals, nursing homes, third party billing services and medical equipment suppliers[8]. The French Law on the Corporate Duty of Vigilance embeds human rights in national law, with a focus on corporate reporting about how human rights are respected in their business activities.

In the context of the 2010 UK Bribery Act, UK Ministry of Justice guidance for companies includes six principles, aligned with those of organisational accountability: proportionate procedures, top-level commitment, risk assessment, due diligence, communication and training, monitoring and review[9]. The French anti-corruption agency promotes good practices that may be taken into account in case of infringement. They include: senior management commitment to implementing a culture of integrity, transparency and compliance; the adoption of internal codes of conduct; implementation of whistle-blowing systems; mapping risks and implementing internal controls and audits; and the training of staff on corruption risks[10]. These are all core elements of organisational accountability.

Accountability is also referred to as corporate responsibility, governance, stewardship or duty. The business function responsible is sometimes called "sustainability", and accountability is associated with co-regulation and voluntary codes of practice. But regardless of these associations or the specific contexts in which it is implemented, an accountable organisation is one that can demonstrate that it has effective internal processes in place to comply with its legal and regulatory obligations. Thus, accountability can be described as a framework that operationalizes and translates principles-based laws into effective internal policies, procedures, controls and governance programs, with external guidance from regulators and advisers. This requires organisations to be thoughtful about risks to its business and the individuals it affects, to establish controls and incentives that drive responsible and ethical behaviour, and to demonstrate that this is the case. It requires organisations to show that they are fully cognisant and in control of their impact on people and the environments in which they operate.

---

[4] Public Law 95-213: Foreign Corrupt Practices Act of 1977. (91 Stat. 1494; 1977): http://bit.ly/2m1eHYg

[5] Public Law 107-204: Sarbanes-Oxley Act of 2002. (116 Stat. 745; 30 July 2002): http://bit.ly/2kyK3oQ

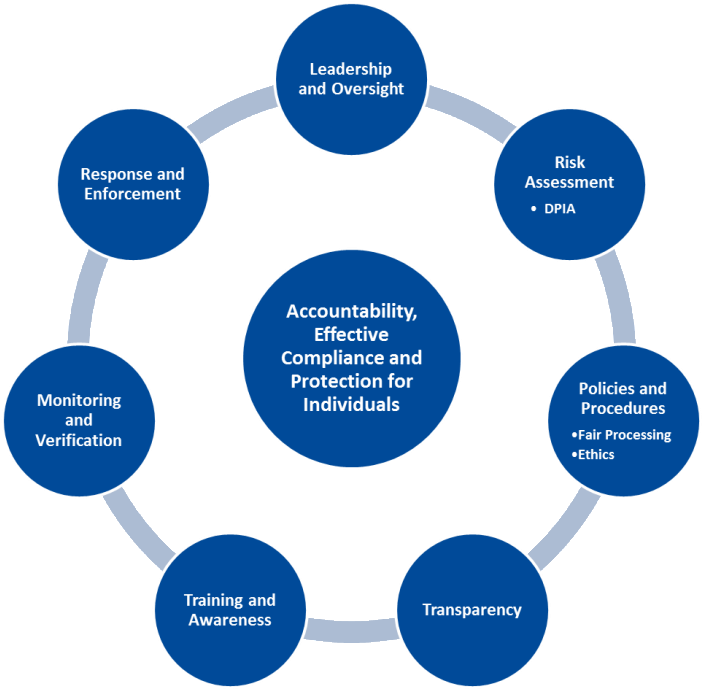
[6] United States Sentencing Commission Federal Sentencing Guidelines Manual 2018, Chapter Eight: Sentencing of Organizations, 2018: http://bit.ly/2m3bo2N

[7] Federal Financial Institutions Examination Council (FFIEC) Bank Secrecy Act/Anti-Money Laundering Examination Manual: https://bsaaml.ffiec.gov/manual

[8] For example, Department of Health and Human Services' 2005 Compliance Program Guidance for Hospitals: http://bit.ly/2kadayG

[9] https://www.justice.gov.uk/downloads/legislation/bribery-act-2010-guidance.pdf

[10] https://www.vie-publique.fr/en-bref/19802-lutte-anticorruption-publication-du-referentiel-francais



CIPL "Accountability Wheel" – Universal Elements of Accountability

CIPL has pioneered the development of accountability as an effective regulatory approach in the context of privacy and data protection. The CIPL "Accountability Wheel" identifies the seven universal elements of accountability, each of which are encompassed and addressed by accountability-based data privacy and governance programs.

Accountable organisations can demonstrate the effectiveness of their internal controls both internally, to senior management, and externally to regulators, individuals and business partners. In the context of significant organisational and technological complexity, this is a vital way in which risks and issues can be identified and corrected.

It is important for regulators to realise that when organisations are able to identify gaps and areas for improvement and take action to correct them, it is to be seen as a positive sign of an organisation's capacity to auto-control itself and to catalyse a virtuous circle of continuous improvement. It is through such positive cycles of improvement that organisational accountability can deliver positive change for both individual organisations and wider society.

3. PRIVACY AND DATA PROTECTION

Europe's General Data Protection Regulation (GDPR) requires organisations to implement appropriate technical and organisational measures to ensure and demonstrate compliance. CIPL's extensive engagement with regulators and business has established a mature model of organisational accountability based on seven essential elements[11]:

1. **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;

2. **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;

3. **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;

4. **Providing transparency to all stakeholders internally and externally** about the organization's data privacy program, procedures and protections, data uses, 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;

5. **Providing training for employees and raising awareness** of the internal privacy program, its objectives and requirements, and implementation of its requirements in line with the employees' roles and job responsibilities, as well as of the importance of privacy and data protection in general. This ensures that data privacy is embedded in the culture of the organization so that it becomes a shared responsibility;

6. **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, other monitoring mechanisms and redress plans;

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

These essential elements of accountability improve the protection of individuals and their data, even as it is processed in complex ways and transferred across international borders. This is helping to build trust in digital services, by placing the burden of protecting individuals more explicitly on to the organisations involved. This increases individual engagement and empowerment and ensures more effective redress. Finally, it helps regulators to focus their enforcement and oversight resources in the

[11] Discussed in detail in CIPL's July 2018 paper, "The Case for Accountability: How it Enables Effective Data Protection and Trust in the Digital Society": http://bit.ly/2koS7IT

areas of greatest impact, with opportunities for third-party providers of oversight and certification to add capacity and specialist expertise.

According to Cisco's 2019 Data Privacy Benchmark Study, companies that have implemented the GDPR and organisational accountability are much less likely to experience a data breach, and when a breach occurs, fewer data records are impacted and system downtime is shorter. This better protects the data of individuals, in addition to reducing the overall financial loss from a data breach on organisations. [12]

In relation to privacy and data protection, organisational accountability is a model endorsed by policymakers around the world. CIPL has championed and developed the concept and has been fortunate to be closely involved in its implementation across a variety of contexts. Based on this wide-ranging experience of regulatory contexts, CIPL believes that here in Europe there is unrealised potential for certifications and codes of conduct to help organisations with achieving and demonstrating accountability.

As policymakers evaluate the GDPR, they should therefore consider that certifications do not yet cover the full scope of accountability-based data privacy and governance programs. Beyond this, the development of evaluation frameworks, certifications and codes of conduct is one way to consolidate and grow the promise of organisational accountability beyond the scope of privacy and data protection to support delivery of a Europe fit for the Digital Age.

4. ACCOUNTABILITY IN AI AND DIGITAL SERVICES

The German Chancellor Angela Merkel said that it will be the job of the next Commission to deliver something similar to GDPR that "makes it clear that artificial intelligence serves humanity."[13] Margrethe Vestager, Executive Vice-President-designate for a Europe fit for the Digital Age, will be tasked work quickly to coordinate "a European approach on artificial intelligence, including its human and ethical implications"[14]. This includes the use and sharing data to develop new technologies and business models that create wealth for business and society. It is important that this work does not duplicate or overlap with the GDPR, but that it learns and builds out from successful implementations of organisational accountability in the context of the GDPR.

The European Commission's High-Level Expert Group on Artificial Intelligence advocates a risk-based approach, which is consistent with the extension of accountability principles, to ensure that AI and other digital services are ethical and aligned with fundamental rights. It recently published its Ethics Guidelines for Trustworthy Artificial Intelligence [15] and called for feedback from organisations through a piloting survey. As CIPL has previously highlighted, understanding and resolving the scope of data protection law and principles in the rapidly changing context of AI is not an easy task, but it is essential to avoid burdening AI with unnecessary regulatory requirements or with uncertainty about whether or not regulatory requirements apply [16].

[12] "Cisco 2019 Data Privacy Benchmark Study Shows Organizations Gaining Business Benefits from Data Privacy Investments", January 24th 2019: http://bit.ly/32UYRPx
[13] Next European Commission takes aim at AI, Politico: https://politi.co/2kybuz5
[14] See President-elect von der Leyen's Mission Letter to Margrethe Vestager: http://bit.ly/31uQrgp
[15] AI HLEG Ethics Guidelines for Trustworthy Artificial Intelligence: http://bit.ly/2psXZ62
[16] Artificial Intelligence and Data Protection in Tension, CIPL 2018: http://bit.ly/33M3taK

5. CONCLUSION

Organisational accountability is a powerful tool in the hands of the political and business leaders that are shaping 21st century Europe. It places the responsibility for ethical behaviour and the protection of individuals on the organisations that are best placed to achieve it.

The GDPR is an example of how accountability can be required by law: the presence of a verifiable and demonstrated privacy program is an element that will be taken into account in enforcement cases, and can serve as a mitigation in the event of a problem. The accountability concept has a long history in US law and is incorporated into international agreements governing privacy, data protection and data flows, such as the OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data and the APEC Privacy Framework. Even in the absence of any formal requirement, privacy enforcement authorities will normally examine a company's internal controls and privacy program as part of any investigation.

Accountability is a scalable and transferrable concept that is implemented by organizations of all types and sizes. The risk-based approach is an essential element of the approach: it leads organisations to address the relevant risks, faced by both the individuals involved and the organisation itself, in proportion to the scale and extent of their operations. Organisational accountability is therefore an attractive and effective tool with which to tackle the complex challenge of building trust and confidence in business for Europe's digital age.

NEXT STEPS

This paper is part of CIPL's initiative to actively share its experience of organisational accountability in adjacent policy areas in support of the effective regulation of digital markets and the development of a Europe fit for the digital age. If you would like more information please see CIPL's website at www.informationpolicycentre.com, or to discuss our work in more detail please contact Nathalie Laneret at nlaneret@huntonAK.com.

CIPL is a global data privacy and cybersecurity think tank based in Brussels, Washington, DC and London. It has 77 member companies that are leaders in key sectors of the global economy. Founded in 2001 by Hunton Andrews Kurth LLP (formerly Hunton & Williams), it cultivates trusted and neutral dialogue between regulators and business across the world, to enable innovation in privacy and data security policy.