The Central Role of Organisational Accountability in Data Privacy

Report of the CIPL Accountability Mapping Project

What Good and Effective Data Privacy Accountability Looks Like: Mapping Organisations' Practices to the CIPL Accountability Framework

May 2020

Centre for Information Policy Leadership
HUNTON ANDREWS KURTH

Foreword

For so many years, accountability has been a bit of a holy grail of data privacy law, policy and corporate compliance. Everybody in the global data privacy community agreed that it was a corner stone of modern data privacy regulation—delivering effective data privacy and protections for people, driving sustainable and responsible business practices in an increasingly digital world and delivering more than just compliance with a growing body of national data privacy laws.

Accountability has been championed by visionary senior leaders and chief privacy officers in the world's leading companies. It has also been encouraged by many forward-thinking data privacy regulators and law-makers in the US, Canada, Europe, Asia-Pacific and Latin America. Yet, there has been no formal consensus, nor consistent evidence of what data privacy accountability means in practice. How do the organisations actually build and implement data privacy accountability into their business, culture and behaviours through a data privacy management programme? How are they able to operationalise legal norms into risk–based controls, policies, procedures and tools? And, finally, how do these organisations demonstrate data privacy accountability to their boards, shareholders, regulators and business partners?

That is why we at CIPL embarked on a data privacy accountability mapping project. Over six months we have been working with 17 leading organisations in different sectors to explore and assess the ways in which these organisations truly embedded data privacy accountability in their corporate DNA. Finally, we were able to put a finger on the organisational accountability pulse and get to the bottom of what best in class data privacy practices look like.

I am excited and proud to share this report with you. It is the result of years of work by CIPL on all aspects of organizational accountability. It is also the product of maturing corporate privacy management programmes and of a big shift in how enlightened organisations and their boards approach data privacy as a critical business issue and enabler of the 4th Industrial Revolution. I am extremely grateful to the chief privacy officers of the 17 organisations that took part in our project for their leadership, openness and trailblazing work.

I hope their examples and the findings of our report become the inspiration for other organisations and their senior leaders in how to build a modern data privacy management programme to address the challenges and opportunities of the digital transformation of our society and economy. I also hope that this report brings much needed consensus and sets shared expectations with data privacy regulators and policy-makers globally on what good accountability looks like.

Bojana Bellamy
President, CIPL

Table of Contents

I. About This Report – Methodology And Objectives[1]

This report (Report) is the result of the Centre for Information Policy Leadership (CIPL)[2] Accountability Mapping Project, launched in September 2019. This project consisted of interviews and document reviews of mature privacy programmes and accountability measures of 17 organisations in various industry sectors, sizes and regions—including two SMEs and a university. The main goals of the interviews and document reviews were to understand how these organisations build and implement effective data privacy practices, and how these practices map to the CIPL Accountability Framework (see Figure 1 below).

Project participants include: Accenture, The Adecco Group, BNP Paribas, Boeing, Cisco Systems, Dropbox, Doctrine, Erasmus University Rotterdam, Google, Mastercard, Novartis, Refinitiv, Symcor, Teleperformance, Twitter, Vodafone and Yoti.

This report outlines examples of how a sample of organisations of different sectors, geographies and sizes implement effective data privacy management programmes (DPMPs) that reflect the CIPL Accountability Framework. These should not be understood as:

(i) Mandatory industry standards, but rather as common or specific accountability-related activities that CIPL has observed. Except for specific and clear legal obligations, organisations have to calibrate the types, volume and granularity of their accountability activities and controls to the particularities of their industry, business model, risk profile and size.

(ii) Formal confirmation that the participating organisations meet all the standards, or that they are compliant with the applicable data privacy laws. Rather, accountability through DPMPs is likely to enable organisations to have the necessary infrastructure to be able to deliver compliance with data privacy legal and regulatory requirements.

The main objective of this Report is to promote organisational accountability in data privacy as an essential prerequisite for the 4th Industrial Revolution. In particular, it aims to:

- Promote accountability as standard market practice and a widely recognised due diligence referential in the digital world;
- Build global consensus on accountability between industry and regulators;
- Promote accountability as a country and sector agnostic framework and as a bridge between different legal regimes;
- Demonstrate that accountability is a scalable framework that works for both big and small organisations;
- Provide concrete evidence and success stories from organisations that accountability is demonstrable and enforceable; and
- Promote accountability as a board-level and a business strategy issue beyond just legal compliance.

The CIPL Accountability Framework is built on seven core elements as described in Figure 1 below. Section III of this Report outlines examples of accountability practices identified for each of these elements. Section II outlines more general findings and common trends that we have observed with all or the majority of the participating organisations.

Figure 1 – CIPL Accountability Framework – Universal Elements of Accountability

II. General Findings Applicable To All Accountable Organisations

CIPL has worked extensively on accountability (see Appendix A) and has been advocating for the uptake and implementation of accountability by organisations and regulators around the world. Through the accountability mapping exercise, we were able to test and confirm many of our prior findings, but also observe some new common trends among the accountable organisations participating in the project and test the effectiveness of our CIPL Accountability Framework (see Figure 1 above).

Accountability is globally recognised as a key building block for effective data privacy regulation and its corresponding implementation. It means that organisations:

a. Take steps such as implementing a comprehensive DPMP to translate data privacy legal requirements into risk-based, concrete, verifiable and enforceable actions and controls relating to the processing of personal data which are reviewed and adapted over time; and

b. Are able to demonstrate the existence and effectiveness of DPMPs internally (e.g. to the board and senior management) and externally (e.g. to privacy enforcement authorities, individuals, business partners and shareholders).

Our general findings and identified common trends concerning accountability are the following:

1. **All participating organisations view accountability as a journey and an internal change management process** to embed data privacy in the company's DNA that goes beyond a one-moment-in-time checkbox compliance exercise. For them, this is not a one-off project that gets delivered once and then forgotten about, but an ongoing endeavour driven by continuous risk assessments and the need for constant improvement. Implementing an accountable DPMP is an iterative and dynamic process that requires organisations to adapt constantly to internal and external factors; address regulatory, legal and technological change; and mitigate new risks. Even the most mature DPMPs have to undergo constant and ongoing adaptation and improvements.

"Mastercard's privacy journey started long ago and continues to evolve, with accountability at its core. From making GDPR and privacy by design part of our global corporate objectives, to launching our Data Responsibility Principles to guide all our data and AI practices, our approach is grounded in a commitment to innovation that places the individual at the centre of everything we do".
– Caroline Louveaux, Chief Privacy Officer, Mastercard

2. **Project participants consider the CIPL Accountability Framework as an ideal and well-established architecture to build and organise an effective DPMP**, that translates legal requirements into actionable controls. They also find it to be a useful framework to report and communicate consistently on their DPMP and efforts, both internally to senior leaders and boards and externally to regulators and investors. Finally, the CIPL Accountability Framework enables them to be systematic and measure their DPMP and accountability journey over time.

3. **All the participating organisations and their privacy officers[3] recognise accountability as a business topic and driver, enabling responsible innovation and business sustainability**. Accountability helps organisations anticipate and adapt to new business models, digitalisation and globalisation. It is very much linked to organisations' business, digital and data strategies and data-driven innovation. Accountable organisations are more agile. They can better anticipate and react to different business and regulatory changes, as well as to crisis situations. They already have established policies, procedures, governance and tools that enable them to take proactive steps as well as directions from top management that drive smooth implementation of such steps. As one of the chief privacy officers (CPOs) said: "Accountability is a glue that binds everything together in an organisation, and avoids any contradictions".

4. **Organisations report that accountability results in business benefits and efficiencies** by reducing delays in sales, reducing the number and cost of data breaches, scaling compliance activities and improving overall operational efficiencies. A recent report by Cisco confirmed that accountable organisations see higher returns of investment on data privacy.[4] This chimes well with organisations' senior leaders and boards. They increasingly recognise the business value of data privacy accountability and position data privacy as part of a larger data strategy, digital responsibility and trust. Some even link accountability to corporate social responsibility.

"Companies with higher accountability scores (as assessed using the Accountability Wheel5 of the Centre for Information Policy Leadership) experience lower breach costs, shorter sales delays, and higher financial returns".
– Cisco 2020 Privacy Benchmarking Stud

5. **Processors are also strongly embracing accountability**. It enables them to differentiate in the marketplace and build trust in the digital supply chain with clients who are looking for accountable business partners to fulfil their own obligations. Processors take steps to be accountable even when they may not be legally or contractually required to do so. Many see the value of external certifications to demonstrate data privacy accountability to their clients and business partners.

6. **In all the participating organisations, senior leaders recognise the importance of "tone from the top" and leading by example**. They articulate clearly the importance of data privacy and tie it to the strategic business objectives and corporate values. As a consequence, employees understand that protecting personal data and practicing responsible data use are a collective effort and everyone's responsibility (and not only the responsibility of privacy officers and legal teams). In turn, this cascading downwards of accountability goals and behaviours brings about a real change of culture in the organisation and increases trustworthiness with customers, clients and business partners.

> *"If you're doing privacy just for compliance, you've already failed. Privacy is an ethical responsibility and business imperative".*
> *– Harvey Jang, Vice President & Chief Privacy Officer, Cisco*

7. **Accountability is sector agnostic and scalable**. Our mapping exercise revealed that organisations of all types, sizes, sectors (including the public sector), geographical footprints and varying corporate cultures can develop and implement an accountable DPMP. The programme, the specific activities (policies, procedures, controls and tools) and the human and financial resources will be different, appropriate to the specific context, risks, goals and size of each organisation. In particular, while smaller organisations can and do take steps to be accountable, they calibrate measures differently than larger, multinational organisations, sometimes with more agility. But the overall accountability architecture, as suggested by the CIPL Accountability Framework, can be the same, irrespective of their industry sector and size.

8. **All the participating organisations proactively manage privacy risks and adopt a risk-based approach to their DPMP**. They build and implement their DPMP and activities taking into account the level of risk of their processing operations to individuals, as well as the risks to their organisations. Risk management enables them to prioritise their accountability measures and make their programme more effective in practice.

9. **Accountability frameworks, such as the CIPL Accountability Framework, are law-agnostic**. Organisations report that they use internally similar accountability frameworks in other areas of corporate compliance, such as anticorruption, anti-money laundering, competition law, export controls and information security. This makes it more familiar for senior management and boards, and enables consistent reporting on, and communication concerning, all the corporate risks and focus areas.

10. **Accountable organisations are driving global convergence in data privacy laws and best practices**. Accountable organisations build and implement a single global DPMP with a common set of controls, procedures and tools, often based on converging norms, to address legal requirements in all countries where they operate as consistently as possible. This makes it easier to promote, communicate and monitor a single set of best practices. This is also helpful for national regulators around the globe, as they are able to align their views and expectations of data privacy compliance activities as they witness and work with consistent and global accountability frameworks.

"Data protection and privacy are core to our business as a professional services company. Building our data privacy program around company values, our ethics code and accountability globally, helps us apply the same high standards everywhere—no matter how developed the law in a country might be".
– Florian Thoma, Senior Director - Global Data Privacy, Accenture

III. Specific Findings And Examples Of Effective Accountability

Case Study 1. Data Privacy made No.1 corporate priority

The CEO of an organisation added data privacy as the No.1 priority for all its employees in 2020, measured by specific KPIs. Some teams have been directed to spend a minimum of 30% of their annual resources on data privacy. In the previous year, 2019, data privacy was made a priority for all engineering teams.

Case Study 2. "What is privacy for you?" – Short videos with executives

An organisation recorded a non-rehearsed, spontaneous short video with the CFO and other senior executives. They were asked questions such as "What is privacy for you?", "How has privacy changed your job?", "Why do you care about privacy?" It has been the most-seen video campaign in the history of the organisation.

Case Study 3. Code of Conduct for AI and big data with appropriate oversight

An organisation is drafting an internal code of conduct for research based on big data and Artificial Intelligence. It has appointed a privacy and ethics board, with an efficient and transparent procedure for approval of projects

1. Leadership & Oversight

Leadership and oversight are the anchor of organisational accountability. They define the organisation's ambition, commitment and governance, so that the DPMP and data privacy procedures and controls are effective and embedded within its culture.

Through the accountability mapping exercise, CIPL has found certain common features of leadership and oversight in all the participating organisations. These include organisation leaders making a clear and formalised commitment to data privacy protection; establishing an internal data privacy network that includes individuals whose primary responsibility is data privacy; putting in place comprehensive and effective DPMPs; and ensuring that there is executive-level oversight of data privacy activities.

1.1 Committing from the top ("Tone from the Top")

We have observed that organisations' boards and senior leaders specifically commit to data privacy in many different ways, which results in data privacy becoming a mandate for the entire organisation. Commonly and traditionally, boards and senior executives address data privacy as risk and compliance topics. However, increasingly, they also address it as part of a broader business and data strategy imperative, as well as part of the organisation's digital trust agenda. In many cases, senior leaders link data privacy to the organisation's code of business practices and corporate values, which must be followed by all employees in their daily activities.

Often, senior leaders require that data privacy be included in the top priorities and performance goals of all senior executives, which they then cascade to their teams and other employees. In some organisations, senior executives are required to complete an annual personal certification that they comply with data privacy policy and programme requirements (among some other key corporate focus and compliance areas).

Our mapping exercise revealed that in all participating organisations, CEOs and senior leadership communicate regularly on the importance of data privacy to the entire organisation through the intranet, blog posts, videos and emails. In particular,

Case Study 4. CEO ensures data privacy is a priority for executives

The CEO of a business-to-business organisation sees accountability and data privacy as a personal responsibility as well as a strategic imperative. She takes efforts to cascade this priority down to executives by addressing these topics in senior leadership meetings, giving formal statements at the occasion of the Privacy Day in January, etc. In addition, the budget allocated to the CPO comes directly from the CEO.

Case Study 5. Real decision-making power of the CPO

A CPO is the "decider" with 51% of the vote for decisions concerning data privacy matters.

Case Study 6. The CPO has thought leadership in the mandate

The CPO of a multinational business-to-business organisation has 25% of her mandate assigned to thought leadership and regulatory engagement, with a special budget. The CPO sets the priorities for external engagements based on market knowledge, peer and competitor activities and regulatory and legal developments.

Case Study 7. The global DPO ultimately reports to the CEO

In an organisation, data privacy is the only area of law that is handled by a global function, led by the global statutory DPO with all local privacy leads reporting directly to her. She reports to the general counsel, who reports to the CEO.

CEOs in these organisations lead by example and are vocal about the importance of data privacy, both internally and externally and often on a personal level. They also get personally involved in data privacy activities, such as by attending oversight committee meetings, reviewing responses to regulatory filings and requesting special briefings and reports on privacy.

1.2 Individuals responsible for data privacy—privacy officers

Privacy officers are the individuals most frequently responsible for data privacy within organisations. They are senior leaders responsible for setting data privacy strategy, and for building, implementing and overseeing DPMPs. They often sit within existing corporate functions (e.g. legal, compliance, risk, products, operations) or, in rarer cases, are a stand-alone function. Privacy officers may also have responsibilities for external engagement and representation, including regulatory engagement with data protection authorities (DPAs), policymakers and standards bodies.

Privacy officers are positioned in the organisation in a manner that allows them to exercise their role effectively and to have authority and impact. They generally escalate risks and issues to senior management and in some cases to the board and may even have authority to say no.

With data privacy-related matters arising across the entire organisation, privacy officers often have to work in a cross-functional manner and engage regularly with other business and functional leaders. Depending on the organisational structure, they leverage existing internal steering or oversight committees, or set up specific ones, to review issues related to data privacy and ethics.

"Privacy officers should aim to build sustainable privacy governance frameworks or programmes that embed data privacy compliance and make it business as usual".[6]
– Emma Butler, Data Protection Officer, Yoti

Just like with the "tone from the top", many organisations insist on the importance of "tone from the middle" and privacy officers are a key component of this. This helps to make privacy accountability everybody's responsibility and results in a more effective DPMP.

Reporting lines of privacy officers and reporting tools

Organisations set up different internal reporting lines for privacy officers that are adapted to their business, corporate structure and culture and risk profile. Privacy officers regularly report into legal, compliance, general secretariat, cyber, IT or risk. In all cases, they are positioned between just one to three levels down from the top management/CEO.

Case Study 8. Encouraging employees to pursue a data privacy career

An organisation has developed a programme to encourage employees to follow a data privacy career. Interested employees who sign up to the programme receive privacy training and are given opportunities to get certified in privacy. They also commit to raising awareness of privacy to the business. The organisation is further considering sending top employees to secondments with the UK Information Commissioners' Office.

Case Study 9. CPO reporting to the board

A CPO provides the board a regular reporting on the risks to individuals and the organisation linked to the personal data processing operations. Risks are classified and measured quantitatively. The risk is given a rating from 1 to 5 for both likelihood and consequence. A "5" in consequence could mean that significant regulatory fines are possible, but also that there is a possibility of expensive litigation or significant negative impacts on stock price or company brand. A "5" in likelihood would mean that a serious incident is highly probable or near certain and a "1" would mean that current controls would prevent most serious incidents.

In some organisations, privacy officers report on their work directly to the CEO or to oversight boards to provide status updates on the DPMP or escalate strategic decisions. Some organisations also mandate regular reporting at local and regional management levels (e.g. to local boards, local managing directors, business or product managers).

Organisations have adopted and/or developed specific tools to support oversight and reporting. These include visual dashboards, key performance indicators (KPIs), controls, third-party support (such as auditors' and consultants' reports). Some metrics used in these tools include:

- Percentage of progress on risk assessments;
- Privacy-related risks and issues identified;
- Number of data breaches;
- Number and results of Privacy Impact Assessments (PIAs) or Data Protection Impact Assessments (DPIAs);
- Number and types of privacy complaints and enquiries received;
- Number of individuals exercising their rights (access, correction, deletion, objection);
- Numbers and type of regulatory interaction and investigations; and
- Percentage of completion of mandatory training.

Support to privacy officers at local and business level

Due to the number of tasks required of privacy officers, organisations often provide extra support to them at the local/geographical and business levels. This also benefits the organisation's accountability in general, as it cascades the responsibilities and embeds a culture of data privacy more deeply within the organisation.

Individuals who support privacy officers locally or at the business level can have:

- Different titles, such as privacy lead or privacy ambassador;
- Different levels of seniority;
- Privacy responsibilities on either full-time or part-time basis; and
- Different backgrounds (e.g. engineers, lawyers, business, etc.).

Their responsibilities include:

- Acting as the privacy voice to front-line functions and day-to-day operations;
- Addressing privacy questions;
- Identifying and resolving privacy issues at a local level; and
- Escalating privacy risks to privacy officers.

Case Study 10. Privacy training and certifications provided to all employees

An organisation requires all members of its extended privacy team (including lawyers and engineers) to complete internal basic training, obtain IAPP CIPP certifications and participate in a half-day privacy engineering workshop/training. This training is also made available and optional for all other interested employees. The organisation has sponsored more than 200 certifications.

Case Study 11. A DPMP helped an organisation obtain a privacy certification

A business-to-business organisation has recently obtained a privacy certification for all its activities globally that required it to maintain a global DPMP. The organisation, however, already had a mature accountability-based DPMP in place. It was able to leverage it and speed up the certification approval.

Case Study 12. A look at an internal ethics and trust committee

An organisation has set up an internal ethics and trust committee. The organisation seeks representation from across the business as well as diversity when designating members to this committee, which includes the CEO, the DPO and senior managers across the business. One of the responsibilities of the committee is to develop an ethics framework.

Investing in data privacy talent

In order to drive accountability deeper into the organisation, organisations make efforts to build and strengthen their internal privacy talent and networks. This includes making data privacy-related positions attractive to employees as part of talent management and presenting them as a career opportunity. They also provide training and certification opportunities to employees and enable them to attend privacy conferences and events and engage with the wider privacy community.

"Privacy officers meet regularly to discuss privacy risks, and are better recognised and acknowledged by other employees in the organisation. Bringing them together in a team gives them a feeling of belonging and keeps them motivated that their work is having a positive impact".
– Marlon Domingus, Data Protection Officer, Erasmus University Rotterdam

Privacy officers regularly organise internal meetings with their teammates responsible for data privacy (e.g. privacy forums, privacy off-sites, privacy fairs, DPO days or annual meetings). During these meetings, they share best practices, define their annual strategy, assess the state of the DPMP, define common best practices and standards, issue concrete deliverables applicable throughout the organisation and build solutions together to improve it. These can be online or face-to-face, regional or global gatherings. Some organisations also invite external experts and regulators to deliver presentations on hot topics.

1.3 Establishing effective Data Privacy Management Programmes (DPMPs) and governance

Effective accountability requires the implementation of DPMPs, which can include the designation of oversight committees as well as the establishment of appropriate privacy governance.

Implementing DPMPs

All organisations that took part in the CIPL accountability mapping project have put in place comprehensive DPMPs. These DPMPs vary per organisation, but all cover in their own ways all elements of the CIPL Accountability Framework (See Figure 1 above). When setting up DPMPs, organisations take into account their existing corporate governance structure, their culture, geography, size and business, as well as their functions as controller and/or processor.

Certain organisations rely on existing accountability frameworks as model architectures for their DPMPs rather than create a new one from scratch. Some organisations have chosen to rely on the CIPL Accountability Framework, while others also rely on frameworks provided by certification schemes (see Section 6.3).

Case Study 13. A look at an external oversight committee

An organisation has appointed an external oversight committee. It is independent and transparent, and its members have a broad range of backgrounds and experience. The committee members' salary is equivalent to the salary of members of boards of the public sector. Their mandate is to advise on uses of data from a non-commercial perspective. The organisation publishes the committee's composition, terms of reference and minutes of meetings on its website.

Case Study 14. A top-down approach to privacy governance

An organisation has established a team of regional privacy lawyers and privacy officers who report to the CPO. They identify legal and regulatory requirements applicable to the countries in the region. These recommendations are reviewed against their global privacy programme, policies and requirements to determine whether and what local variations should apply to businesses across the globe, thereby leveraging global controls as much as possible.

The contents of DPMPs vary by organisation. Some organisations strictly abide by legal requirements to which they are subject, while others apply a consistent global data privacy standard across the entire organisation. Examples of the latter approach include applying globally the principles of the General Data Protection Regulation (GDPR) or BCR, such as enabling all individuals, including non-EU individuals, to exercise GDPR rights. Regulated industries, such as healthcare or banking, may also have to apply specific or additional governance models and controls in their DPMP, as required by their sectoral regulator.

Designating additional boards and oversight committees

Organisations often need to make decisions that are technical, strategic and specific to certain data processing activities—such as concerning the development of Artificial Intelligence technology, or data ethics. This leads them to increasingly designate cross-functional boards and committees, which provide additional oversight and advice on data privacy activities.

Some organisations also appoint external advisory committees when they seek further expertise and independence in respect of key data privacy-related decisions.

Both internal and external committees are usually composed of experienced and recognised experts in the relevant fields. External committees may also include representatives from academia and civil society. External committee members may work on a voluntary or paid basis.

Privacy governance

Organisations often define privacy governance models. These provide a structure for privacy officers and individuals responsible for privacy to work together, for privacy-related decision making and for oversight of privacy risks.

Organisations often replicate existing governance structures used in other areas of compliance in their privacy governance, such as the "three lines of defence" model. Privacy governance also varies from a top-down approach (actions mandated and driven by the top level) to a bottom-up approach (principles at the top level and flexibility for implementation by businesses, with accountability and ownership at the business level).

We have also observed that some organisations created a specific and stand-alone corporate function dedicated to data privacy—similar to HR, finance, marketing or communications.

Case Study 15. Data privacy integrated into the Enterprise Risk Management (ERM) through reporting lines

The person responsible for data privacy risk management of a large organisation reports both to the Group DPO and to the Group ERM head. This demonstrates that privacy is integrated into and given the same weight and importance as other risks registered in the overall ERM framework of the organisation.

Case Study 16. Managing risks related to the DPMP

Business lines are responsible for implementing an organisation's DPMP. They work closely with members of the privacy team. Activities related to the programme are captured in an operational privacy risk register, and the organisation subsequently drafts and approves related risk statements. Responsibilities for these risks are assigned to senior people within the business, who report back regularly on 25 KPIs. The reports feed the annual privacy plan of the organisation.

Case Study 17. Reassessing high-risk products—a refresh cycle

An organisation incorporated a "Sustain Phase" in its product and services assessment process. This phase consists of an annual review of all products that were initially classified as high risk from a data privacy perspective. The privacy office works with audit and with those who make use of privacy management tools to support this review.

2. RISK ASSESSMENT

Assessing and mitigating the risks that data processing projects, products or services may create for individuals and subsequently for organisations are also essential elements of accountability. Risk assessments also include calibrating and conducting periodic reviews of the organisation's overall DPMP and data uses in light of changes in business models, law, technology and other factors and adapting the programme to changing factors and levels of risk.

We observed that accountable organisations implement many different ways to identify, assess and manage privacy risks. These include integrating privacy risks within their existing risk management framework; managing privacy risks at both the DPMP and product/service level; and assessing privacy risks that relate specifically to the use of vendors and third parties.

2.1 Integrating privacy within risk management

Many organisations integrate data privacy into their enterprise-wide risk management framework (ERM) and include privacy as part of their top three to five risks. Organisations stress the importance of having a holistic and aligned approach on how they manage and report on privacy risks. This enables organisations to define how much risk the organisations are willing to take and ensures visibility of privacy matters internally, which then drives funding, prioritisation and strategy. One organisation even translated its ERM into a more specific privacy risk framework, with the goal of enabling the business to understand what privacy risks actually are.

"Privacy and accountability are central to our data- driven innovation and to how we balance rewards and risks. Incorporating a privacy risk framework into our product development process helps raise privacy awareness across the organisation, reinforces the business-critical nature of privacy, and ultimately protects our brand".
– Caroline Louveaux, Chief Privacy Officer, Mastercard

As part of the ERM, organisations maintain risk registers that also include data privacy risks. These registers are reviewed and updated on a regular basis. They are also updated following the tracking and assessment of risks at the programme and product/service levels. Risks have to be signed off on by senior executives and/or business leads.

In addition, many organisations assign responsibilities for managing privacy risks to specific individuals within the business, or sometimes directly to privacy officers. This ensures that risks are appropriately managed and followed up on. Some organisations even appoint specific teams dedicated to managing privacy risks.

Risks registered as part of the ERM may also lead to internal and external audits, and may be identified as a result of audits (see Section 6.1).

Case Study 18. Taxonomy used to classify privacy risks

An organisation has developed a group risk taxonomy that reflects the requirements of the GDPR. The Group DPO led this work, which included going through the GDPR article by article and identifying possible data protection risks. This taxonomy enabled the organisation to implement a risk-based approach and use it for the DPIA methodology when assessing risks to individuals.

Case Study 19. Awareness has driven volume increase of PIAs and DPIAs

In 2019, a multinational organisation saw a 40% increase on PIAs and DPIAs completed. The organisation undertook over 4,000 assessments. The organisation acknowledged that this was due to the increased privacy awareness within the organisation post-GDPR. Privacy officers were required to prioritise their activities on a daily basis in order to manage the increased workload.

Case Study 20. A different approach—undertaking "reverse DPIAs"

Due to the high number of projects in an organisation, its DPO developed an approach to cluster projects and increase the efficiency in undertaking DPIAs. The DPO identified eight common categories from assessing 3,000 projects. Project leads are required to categorise new projects in one of the eight categories, and embed in the project design predefined mitigation actions for risks that are common to that particular category. DPIAs go through a peer-review by project managers for quality assurance.

2.2 Managing data privacy risks at the level of the DPMP

All organisations put in place some kind of mechanism to track the development of their DPMPs and assess programme-related risks such as delay in workstreams and actions, or any unintended negative impact on the organisation. These mechanisms include regular reporting, self-assessment, automated tools, etc.

There are internal and external elements that may impact an organisation's DPMPs, including changes in the regulatory and technological landscape; incident trends; due care standards and safeguards; and changes in technology, people, business processes, risks and priorities. These force organisations to constantly reassess their DPMPs to make sure they evolve based on new factors and risks and to prioritise workstreams and actions accordingly.

In addition to internal reviews, some organisations hire external third parties (e.g. consultants or law firms) to review, benchmark and assure that their DPMPs are "fit for the purpose". They update the DPMPs following these reviews. These reviews may happen at regular intervals (every 1, 2 or 3 years) or on an ad hoc basis.

2.3 Assessing data privacy risks at the project, product or service level

Scope of the assessments

Organisations track and assess privacy risks at the project, product and service levels. These assessments can:

- Be specific to data privacy (e.g. PIAs and DPIAs—see below), and
- Have a wider scope than data privacy but still capture data privacy risks, including:
  - Assessments of processors/vendors;
  - Product or service reviews;
  - M&A due diligence;
  - Compliance approvals;
  - AI impact assessments;
  - Audits (see Section 6.1);
  - Information security assessments; and
  - Approval of new IT systems and databases, etc.

The teams responsible for these assessments work alone or with the support of other teams, such as risk and compliance or product design and engineers.

Organisations often use outsourced automated risk and compliance tools to manage data privacy risks. This includes aggregating all controls, compliance results, executing assurance activities, tracking KPIs and extracting reports.

Case Study 21. Sharing risks between processors and their clients

A processor organisation adds to the contracts with major clients a requirement to perform security risk assessments on an annual basis. During the assessment, the organisation reviews how the client's systems and employees interact with the tools, programmes, processes, data and software provided. This assessment is performed at no costs to the client, and results in a report with recommendations for the client and the organisation to mitigate the identified risks. The client has an opportunity to disagree with any points raised in the report, after which the client and the organisation discuss in good faith how to resolve these points. Handling and mitigating these risks will require that the organisation and its clients maintain trusted relationships. From a processor's perspective, pushing to get clear instructions and highlighting weaknesses in instructions that do not protect personal data create trust and enhance the relationship while increasing data protection.

Case Study 22. Data privacy is a deal breaker

As a result of due diligence, an organisation often decides not to engage with vendors that represent a high risk from an information security and data privacy perspective. Examples of such decisions include when a tech vendor did not give the requested representations and when a small vendor did not have safeguards for international data transfers in place.

Large organisations also develop data privacy-specific self-assessment processes and tools. These enable the business to assess privacy risks on their own, therefore unburdening privacy officers who might not have enough resources to manage risks at the local level. Instead, privacy officers might monitor local assessments such as by undertaking periodic reviews.

If the product or service relates to the use of Artificial Intelligence or another innovative technology, organisations may include ethics elements in the risk assessment.

Organisations mitigate identified risks by making changes to their products and services (e.g. by implementing data privacy by design and by default). They often incorporate a review cycle in the product/service development process in order to reassess relevant risks.

Undertaking PIAs and DPIAs

As mentioned above, organisations undertake data privacy-specific assessment of their products and services, mainly using PIAs and DPIAs. Through these assessments, they are able to specifically identify whether data processing activities may result in a risk to individuals. This leads to recommended mitigation activities which may include changes in the product or service.

Organisations develop specific processes to undertake PIAs and DPIAs. They also embed triggers for these in their business processes, including risk assessment and review processes, product and service development, maintenance of records, etc. Some organisations have also embedded questionnaires in their data inventory/ records of processing tools that can generate flags and trigger PIAs and DPIAs.

Privacy officers of large organisations often develop templates, questionnaires, toolkits, guidance and FAQs to enable businesses to undertake PIAs and DPIAs themselves. They also develop processes for the business to escalate the PIA and DPIA to the privacy experts and team when appropriate. This aims at reducing the burden on privacy officers, who may not have the necessary resources to undertake all necessary PIAs and DPIAs themselves, and at establishing ownership of and accountability for controlling data privacy risks with the business.

"One key element of our program has been the focus on integrating data privacy related risk assessments and controls directly into the relevant business processes. With this approach we further embedded responsible data use in our business activities and we enabled the business to take on accountability".
– Knut Mager, Global Head Data Privacy, Novartis

Privacy officers also often provide support to the business on PIAs and DPIAs by answering questions, helping complete questionnaires, organising DPIA clinics, doing on-site visits and meeting in person with the relevant teams. They also review escalated PIAs and DPIAs completed by the business, in particular when they flag a high risk.

Some organisations use automated tools for undertaking and managing PIAs and DPIAs more efficiently. These tools also support organisations keeping evidence of risk assessments in a systematic and centralised manner.

In addition, a processor organisation has reported that it shares its DPIA templates with clients. This is to achieve consistency in the process, definitions and understanding of how a particular technology works, which results in enhanced trust between the organisation and their clients. Similarly, another organisation reported that it shares their DPIA template with regulators for external assurance.

2.4 Assessing data privacy risks relating to business partners

Assessing data privacy-related risks of business partners is also important. These include contractors, vendors, clients or any other partners with whom the organisation may share personal data for business purposes.

Commonly, privacy officers work with procurement to include privacy questions in the existing due diligence questionnaires. These questions help privacy officers identify whether the third party provides the appropriate level of protection according to the identified risk and to the standards of protection of the organisation that is sharing the personal data.

Risk is often measured by triaging third parties into different high-medium-low risk categories depending on circumstances such as whether they process large volumes of personal data, the types of data processed, the technical and organisational measures they have in place, whether they have had a recent data breach, etc. More detailed assessments, including on-site visits and infrastructure reviews, may be undertaken if the third party is classified as medium or high risk. Security, information management and privacy and security certifications are also important positive factors in the risk assessment.

Organisations increasingly undertake these assessments in the context of mergers and acquisitions. This enables them to verify the maturity of the third party's DPMP and assess the risk of the merger or the acquisition to individuals and to the organisation.

The third party may be classified as high risk following this assessment but may not have the appropriate and expected mitigation measures in place. When this is the case, organisations may require that the third party puts in place the expected protective measures or alternatively may decide not to work with the third party.

Organisations embed in the third-party assessment process a review cycle that enables them to re-assess third parties over a certain period of time, in particular those third parties that were classified as high risk. They also request updates on any certifications that may have been taken into account during the assessment. Organisations may decide to end the business and contractual relationship if they find that the third party no longer provides the appropriate protective measures.

Case Study 23. Governance on policies and processes

An organisation has implemented robust governance around its data privacy policies and procedures. Its global privacy policy was developed taking into account the existing BCR. As a result, if businesses comply with the policy, they are also complying with the BCR. The organisation also leverages existing business processes and embeds data privacy protection directly in the business processes for efficiency purposes.

Case Study 24. A look into privacy by design process

The privacy office of an organisation provides privacy by design guidelines to the product development and innovation teams. The guidelines require these teams, during the product design stage, to document any actions taken and apply the principles of transparency, lawfulness, data minimisation, accuracy and storage limitation. They also require them to review vendors, seek approval for data sharing outside of the organisation and design the product in a way that allows individuals to exercise their rights. The product development and innovation teams are required to consult the guidelines before initiating changes to existing or new products, applications, processes, systems and infrastructure. They are also required to attach the guidelines to the respective project plans and are later asked to confirm that they have complied with their requirements. This information is passed on to the privacy office, which assesses whether additional requirements apply to the new product or service.

3. POLICIES AND PROCEDURES

Organisations establish internal written policies and procedures to operationalise legal requirements, data privacy principles and industry standards, as well as their own internal rules, values and goals. Through policies and procedures, organisations create concrete processes, actions and controls, and designate roles and responsibilities to management and all employees.

Our mapping exercise revealed that all organisations have put in place an overarching privacy policy that establishes principles to be followed by all employees when handling personal data. Most organisations have also put in place more specific policies and procedures relating to data privacy by design and by default, vendor management (see Section 2.4) and data breaches. All organisations also adopt measures to enable lawful international data transfers.

3.1 Establishing internal privacy policies and procedures based on data privacy principles

All organisations have adopted specific data privacy policies (Privacy Policies). In some cases, these have global scope. These policies set out principles and requirements that employees should follow when engaging in data processing activities.

Organisations, particularly larger ones, also adopt additional Privacy Policies that are specific to regions, countries, types of business, products and services or support functions. These narrower Privacy Policies often refer to, and derive from, the global Privacy Policy.

Organisations update other existing internal policies to align with the global privacy policy (e.g. information security, HR, marketing, business ethics line reporting, etc.).

Privacy policies are often aligned with external standards such as the ones set out by the OECD or APEC, or the GDPR, or any other national law. External standards such as BCR, CBPR, ISO standards and Privacy Shield are also reflected and further operationalised in organisations' privacy policies.

Policies and procedures are reviewed and updated on an ongoing basis to take into account business, legal and regulatory changes. For instance, the coming into effect of the EU GDPR, the California Consumer Privacy Act (CCPA) and the new Brazil data protection law prompted major reviews of organisations' global policies and procedures, as well as of their DPMPs.

In addition, organisations adopt processes, technical requirements, controls and specific guidance to support the operationalisation of data privacy requirements. These provide more detailed and practical guidance to the business concerning how they should handle data processing activities.

Case Study 25. Kit for Brexit Policies and Processes

A DPO developed a kit with guidance and templates for the organisation to adapt its policies and processes after Brexit. The DPO considers it important for the organisation to anticipate changes to the regulatory landscape.

Case Study 26. Data privacy and protections flow through the ecosystem

A business-to-consumer organisation believes that protecting individual's data privacy cannot be done in a silo. This is part of a large ecosystem that also includes vendors, partners and third parties who process personal data. If these third parties do not implement appropriate measures, ultimately the organisations' customers will not be protected regardless of the organisation's own efforts. Therefore, the organisation ensures that its vendors, partners and third parties are also held accountable, such as through contractual requirements, monitoring of their performance and ultimately terminating relationships.

Organisations' approach to adopting policies and procedures varies depending on their type, size, corporate structure and other factors. For instance, we have observed that smaller organisations tend to favour a more centralised approach in order to operate in a more agile manner. In turn, larger organisations may choose either a centralised or decentralised approach depending on how privacy officers choose to manage privacy risks, or depending on whether the privacy team/compliance is global or local.

3.2 Implementing specific policies and procedures

Data privacy by design and by default

Privacy officers increasingly work with product, engineering and design/User Experience (UX) teams to ensure that they understand and implement privacy by design and by default. They are often involved in the entire product development life cycle—from planning to developing, testing and launching.

Privacy officers and relevant teams develop guidelines and FAQs specific to privacy by design. Design and product teams consult this guidance at the start of every new project to configure and develop products accordingly. They also use the guidance provided to undertake PIAs and DPIAs (see Section 2.3).

Some organisations have policies that allow design teams to launch new products and services only after they submit a preliminary privacy assessment to privacy officers. They also develop a baseline architecture that incorporates privacy and security requirements by design, and mandate that any new product be developed from this baseline.

In addition, processors often implement privacy by design processes even though they are not always legally required to do so. This enables them to anticipate due diligence reviews from controllers or other partners and enhance their trusted relationship with clients.

"A big part of our product philosophy is to make things that are genuinely helpful and demonstrate our responsibility. For my team(s), that means offering privacy tools that are easy to use; surfacing those tools in more places; and making the services themselves more private".
– William Malcolm, Legal Director - Privacy, Google

Third-party management

Organisations implement policies and procedures to manage relationships with third parties and to ensure that individuals' data privacy is protected across the entire ecosystem. This includes identifying appropriate third parties, assessing their risks (see Section 2.4), negotiating contracts, managing different contracts, managing the services provided, responding to queries, conducting ongoing reassessment of the third party and terminating the relationship.

Case Study 27. A look into table-top exercises

Many organisations organise table-top exercises as a preventive measure to prepare employees to act appropriately in real-life scenarios. This involves employees across the organisation, including senior management, as well as board members. Employees are not always aware that a table-top will happen. For instance, they can receive an email or a call in the middle of the night or during the day saying that there will be a meeting at 11pm that same day. Also, the email or call might simulate an actual breach without informing them that it is a table-top exercise, so they may enter the breach management process thinking it is an actual breach. Even though these exercises occur during a limited time (1 or 2 days), organisations take months preparing them and often hire external consultants and law firms to support them. This is followed by a post-mortem exercise to identify learnings and enhance the data breach response process going forward.

Case Study 28. Plans for managing data breaches using machine learning

An organisation is using big data and machine learning to better understand and manage data breaches. It is developing a prototype to identify patterns arising from historical data relating to data breaches, which should give them insights on whether certain types of breaches are more likely to occur in certain groups and periods of time (for instance, more laptops being lost or stolen during holiday seasons). It also has longer-term plans to use machine learning to identify and assess risks automatically and present them in the privacy dashboard.

Legal (which may or may not include the privacy team), procurement and sometimes information security are often the functions responsible for managing contractual relationships with third parties.

Large organisations typically engage with a high number of third parties, with multiple different contracts in place for each of them. In some cases, they develop or outsource automated systems to store contracts, data processing agreements, addenda, due diligence checklists and audit reports.

In their contracts with third parties, organisations often impose compliance with or to the same level as the organisations' internal policies. When organisations find that the third party is non-compliant (e.g. outdated system, repeated breaches), they take measures from notifying them and recommending mitigation actions, to terminating the contract.

"The definition of accountability is critical for me—an obligation or willingness to accept responsibility and to account for one's actions. All forward-thinking executives need to take this to heart: being accountable for their company's actions to its key stakeholders—shareholders, clients, customers, regulators and employees. And with honest and transparent accountability comes TRUST. In today's world, there will not be a successful enterprise without trust".
– Alan Winters, Group Chief Administrative and People Officer, Deputy Global Compliance Officer, Group Chief Privacy and Data Protection Officer, Teleperformance

Information security and data breaches

Organisations put in place robust information security policies, procedures and controls (e.g. acceptable use policy of IT resources, data access, resilience, crisis management, data breach prevention, business continuity plan, etc.). These help organisations manage their security and data privacy risks. Privacy officers often work closely with information security to manage these risks.

In addition, organisations put in place specific policies and procedures for handling security incidents, which may include personal data breaches. These processes also include steps and guidance on when and how to notify data breaches to individuals and DPAs where appropriate (see Section 7.3).

Organisations assign roles and responsibilities for handling data breaches that often include designating a specific cross-functional response team to handle security incidents. This team is often required to work on a 24/7 basis. All employees responsible for handling data breaches are provided special training.

Several teams are commonly involved in the breach management process, including external advisors. They include: the privacy officer and privacy teams, information security, risk and compliance, legal, government relations, external law firms, forensic organisations, communications and public relations (e.g. if a breach needs to be notified to individuals, regulators or to deal with any media enquiries). Executives and senior leaders are also involved depending on the seriousness of the incident.

Organisations conduct regular table-top exercises on data breaches with response teams, employees and even for the executive committee and the board. These exercises test their incident detection and response policies and procedures and prepare these teams for the possible occurrence of real data breaches.

> *"Reducing the number of reported incidents isn't our goal. A decrease in reporting may just mean people haven't recognized that there was a problem. Instead, we want to encourage reporting so we can determine root causes and make improvements to controls, which will then reduce the number of systemic or serious problems".*
> *– Marie Olson, Deputy Chief Privacy Officer, Boeing*

Organisations make available to employees a variety of tools to report security incidents, including:

- Intranet-based online forms that lead to ticketing tools;
- Help desks;
- Dedicated 24/7 telephone hot lines available in the local languages;
- Dedicated email addresses; and
- "Ask security" buttons.

All employees are informed about these tools and trained to use them where relevant. Organisations also commonly ask employees to contact their line manager in case of any questions, and managers are trained to address these enquiries appropriately.

In addition, organisations apply mechanisms to monitor security incidents, including: designating a specific team of engineers within information security to monitor threat actors, undertaking regular testing across countries, developing automated tools to monitor information that is sent outside of the organisation, implementing security operating centres (SOCs) or data loss prevention tools, performing regular penetration tests, developing security-related Artificial Intelligence and machine-learning solutions, etc.

Some organisations are developing or outsourcing tools to automatically evaluate the level of risk of security incidents, and to manage them. Some organisations also identify third parties who may be engaged to support managing a data breach, such as forensic experts, communications consultants, public relations consultants, law firms, call centres and credit monitoring services.

Following the identification of a data breach, organisations take a variety of mitigation measures including:

- Operational, process, product and system changes;
- Additional controls;
- Improvement of employee training;
- Termination of contracts with vendors and employees in severe cases; etc.

Organisations also take measures to prevent future breaches, including:

- Discussing lessons learned with local managers in order to support improving local processes;
- Monitoring and using metrics to report breaches to the executive level; and
- Presenting case studies to the board of directors in order to explain the impact in the organisation and proposing prevention solutions, etc.

3.3 Enabling international data transfers

Organisations put in place policies and legal mechanisms to ensure that international data flows (whether intra-group or external) comply with applicable laws. These include entering into specific contractual clauses, standard contractual clauses or intragroup agreements; applying for BCR or certifications (such as CBPR); or self-certifying to the Privacy Shield.

Some of these frameworks, such as BCR and CBPR, enable larger efficiencies for global organisations to manage compliance in respect of multiple data flows and in multiple countries. They also enable the organisation to raise the level of compliance for all entities to a common standard, and often serve as the backbone of the organisation's DPMP (see Section 1.2).

Case Study 29. Centralising multiple privacy statements

An organisation used to have multiple privacy statements across various websites, which required any updates to be made multiple times. It decided to move to a common standard privacy statement, which is monitored and controlled centrally by the privacy office. It leveraged technology to link all the websites' privacy statement references to one location and drafted the central privacy statement so that it covers all data processing activities from across the different business lines. In this way, the central privacy statement is consistently reflected across the various organisation's websites.

Case Study 30. User testing helps enhance transparency

An organisation applies user testing to all of their products and certain aspects of their products. This includes application screens with information provided on data privacy, security and biometrics, which link to the privacy notice. This allows them to obtain useful feedback from users on product design and enhance the transparency towards their users.

4. TRANSPARENCY

Transparency is a key element of trust. Project participants all see transparency as a way to achieve credibility externally, to increase and maintain their reputation, but also, importantly, to help drive accountability internally. Transparency compels everybody from senior leaders to engineers to consider accountability and how to live up to the promises made externally. Accountable organisations are transparent towards a wide variety of stakeholders internally and externally about their DPMP, data processing and uses, benefits and/or potential risks of data processing, and other elements of data privacy. Stakeholders include individuals, business partners, investors, clients and regulators.

We have observed that organisations take a wide variety of measures to be transparent towards these stakeholders, as outlined below. Some of these measures derive from legal requirements (e.g. to provide formal privacy notices). Other measures follow industry common practice or are led by user-centric design considerations. Accountable organisations also often develop innovative ways to communicate with, and be transparent to, their stakeholders.

4.1 Transparency to individuals

Organisations provide privacy notices[7] to individuals informing them about the processing activities and their data privacy rights. These can be general with a global scope (i.e. address data processing activities of the entire organisation in multiple countries) or be specific to regions/countries, products, services, systems or target audiences (e.g. children, employees, students, applicants, etc.). Most organisations apply a layered approach to their privacy notices.

Organisations provide privacy notices through a wide variety of channels (e.g. mobile applications, webpages, phone lines, voice assistants, Internet of Things, etc.). Organisations are constantly developing more creative ways to provide such notices clearly and most effectively, anticipating possible questions individuals may have. Consumer-facing organisations, especially, often provide innovative, user-centric transparency, taking into account the user experience when developing privacy notices. Privacy officers regularly work with other teams, such as UX, design, legal and engineering.

Organisations have developed processes to ensure that privacy notices are kept up to date with business and processing changes. This includes directories listing all privacy notices available, specific folders, systems, etc. They identify the need to update privacy notices through monitoring activities (see Section 6), and they keep version control of privacy notices provided to individuals.

Organisations also use resources other than formal privacy notices to relay key messages to individuals. These include privacy portals, dashboards, videos, FAQs, animations, icons, dedicated privacy centres updated on an ongoing basis, etc. They also link privacy notices to other relevant documents and webpages providing further information (e.g. outline of legal bases relied upon, online forms for exercising data privacy rights, privacy and security portals).

Case Study 31. Various sources of information beyond the privacy notice

Some organisations adopt a layered approach to transparency and link online privacy notices to separate domains with additional information about data processing and privacy controls (such as managing ad preferences). They include the notices in privacy hubs/centres where individuals can also find other relevant information, such as about security, data of deceased individuals, false information, election integrity, data breaches, how the organisation is complying with data privacy laws, etc.

Case Study 32. Making it simple and efficient for clients to understand data flows

An organisation requires product PIAs to go through a three-step review. Firstly, engineers do the first draft (with the support of Product Counsel) to provide the raw data and facts about the personal data being processed by the activity, initiative or product. It is then reviewed by the privacy team for risk assessment, consultation, calibration and consistency. Finally, the data flows processing information is published in a plain-language, privacy data sheet with an infographic to enable customers and users to understand what data is collected and how it is processed in the context of their use of the product.

4.2 Transparency to third parties

Organisations take measures to be transparent about their DPMP and data processing to third parties, including business partners, clients, shareholders, investors, vendors and the general public.

We have observed that processors and business-to-business organisations find it particularly important to be transparent towards business partners and clients. This reinforces trust in their contractual and business relationship. It may often represent a key buying factor for clients and a competitive differentiator.

Similarly, investors are increasingly interested in understanding how the organisation satisfactorily manages privacy risks. They proactively request information to the organisation about their DPMPs, for instance.

Examples of transparency measures towards third parties include:

- Publishing transparency reports on government access to data;
- Outlining privacy risks in quarterly risk reports;
- Enabling clients to access the results of PIAs and DPIAs;
- Meeting with business partners to discuss privacy topics and advancements on the organisation's DPMP;
- In some instances, allowing clients to access the product source code to assess the privacy controls;
- Developing visual tools to help external stakeholders better understand the organisation's data processing activities;
- Taking public stances and positions concerning data security and privacy; and
- Engaging proactively with the media where appropriate to discuss privacy topics such as data breaches and new product developments.

4.3 Transparency to regulators

Organisations take steps to maintain a transparent and trustworthy relationship with the key national DPAs, including also the lead DPA under the GPDR. They may also engage with other regulators on data privacy issues, such as competition, telecom, finance, health/medicine and consumer authorities.

Organisations regularly report back internally to senior leadership and relevant teams, such as legal, engineering, product development, sales, compliance and others, on the feedback obtained from regulators during such engagements. These teams often make product/service/process changes following this feedback. It is important for the privacy officer and regulatory engagement teams to demonstrate to regulators that their views are being taken into account and acted upon by the organisation.

Case Study 33. Product reviews by clients

A business-to-business organisation allows top-tier customers to review and evaluate the products, even at the source code level, to validate the technical security posture. This allows customers to "trust, but verify" and helps to build and maintain trust in the relationship.

Case Study 34. Transparency towards clients enabled through visual tools

An organisation is investing in Artificial Intelligence technology to prevent and manage potential fraud activities in the context of its business-to-business operations. In order to support its clients and enable them to better understand the privacy protections implemented in its new AI product, the organisation has developed a visual tool to illustrate the personal data processing.

Examples of transparency activities towards regulators include:

- Regularly meeting with DPAs to discuss initiatives and developments in the DPMP;
- Responding to public consultations and attending events organised by regulators in the context of these consultations;
- Informing regulators upfront of upcoming product and service changes that impact data processing and seeking their feedback;
- Setting up dedicated channels for DPAs to communicate with the relevant teams within the organisation, such as an email address that directs every email of the DPA to the DPO team;
- Taking part in innovative regulatory oversight, such as regulatory sandboxes (e.g. the sandboxes led by the UK Information Commissioner's Office[8] and the Singapore PDPC);
- Participating in multistakeholder roundtables and workshops organised by think tanks, global or local industry organisations, and NGOs; and
- Engaging and showcasing their privacy capabilities and product development during key industry and regulatory conferences and events.

Case Study 35. Turning training into "martial arts"

An organisation used a "martial arts format" to privacy and information security training, calling it a "ninja training". Employees advance to different "belts" as they complete training modules and gain experience. The organisation used this strategy to make training fun and motivate, reward and encourage employees to take the more detailed training modules, even if they were not mandatory for their role.

Case Study 36. The 10 privacy commandments

An organisation created the "10 commandments" for privacy. These are visually represented in an infographic, which provides a simplified message to employees on how to comply with key privacy requirements. The organisation distributed the infographic during the DPMP building phase, but employees continue to follow it beyond the DPMP. During September and October, when this organisation runs a series of data privacy awareness activities, the 10 commandments are reinforced throughout the organisation.

5. TRAINING AND AWARENESS

Training and awareness are key elements of embedding data privacy and accountability in the culture of the organisation. They ensure that all employees and other staff understand their shared responsibilities in delivering an effective DPMP. Organisations provide training and awareness that is linked to the DPMP, its objectives and requirements, as well as targeted and role-specific activities (e.g. reminders to report any security incidents and data breaches). Commonly, organisations raise awareness of the importance of data privacy in general and, more specifically, how data privacy requirements translate into employees' roles and responsibilities.

We have observed that certain training and awareness activities are common to all organisations, such as mandatory corporate global annual e-learning modules. Nevertheless, it is in training and awareness that organisations find creative ways to communicate with their employees and innovate on how they build a privacy culture and change behaviours on the ground.

5.1 Providing privacy training

Organisations provide mandatory corporate privacy training to all staff globally, often on an annual or multiyear-cycle basis. This includes full-time staff, part-time staff, contractors, interns and secondees. They receive training both at the time of joining the organisation and then at regular intervals. This often requires employees to formally acknowledge that they have received training, understand the policies and commit to respect them—for instance by signing such policies.

Organisations also provide specialised, more in-depth privacy training to business functions and/or employees whose roles involve more data processing activities. These include legal, engineering, product development, data analysts, human resources, marketing, information security, incident management teams. Organisations also provide one-off training to senior leadership and board members.

Training may be privacy-specific or may be included in a wider context such as a module within information security, ethics and compliance training. Organisations often use e-learning platforms, videos and other interactive and innovative elements, sometimes with quizzes and gamification elements. Depending on the size and structure of the organisation and the relative seniority and importance of the employee's role in processing personal data, training is also provided face-to-face.

Organisations monitor and track employees' completion of training modules and keep a record of their results. Training KPIs are often used by privacy officers to report on the effectiveness of the DPMP (see Section 1.1). Management is often responsible for following up with employees who have not completed their training in due time or have achieved undesirable results.

Privacy officers develop and make available to employees additional practical resources to complement the privacy training, such as guidelines, playbooks, case studies, FAQs, templates (such as DPIA, or data processing agreement templates), links to key resources developed by DPAs (e.g. breach examples provided by the Information Commissioner's Office or the CNIL PIA tool), etc.

Case Study 37. "An image speaks louder than a thousand words"—using a mascot to symbolise the DPMP

An organisation rolled out an internal privacy competition to create a mascot to represent its DPMP. The privacy team uses the mascot and its name in creative and engaging ways, and it is now fully recognisable and critical to driving the organisation's data privacy communications and awareness programme. For example, the team created a "dating profile" for the mascot, where it mentions that it initially did not fit in but now with people's acceptance of privacy this is no longer the case. The mascot is regularly featured in internal communications and is referred to by senior leaders.

Privacy officers often store all privacy training modules and additional resources in dedicated privacy hubs on the organisation's intranet or SharePoint, which are available to all employees.

5.2 Raising awareness of data privacy through communication campaigns and strategies

All organisations build and implement a more strategic, comprehensive and company-wide data privacy communication and awareness plan. They formally plan, budget and set up campaigns and communication strategies that are tailored to their business and culture. These can be global, local or both. Depending on the organisation, some find that local initiatives may be more effective than general initiatives that come from the organisation's headquarters.

Examples of awareness-raising activities include:

- CEO and senior leaders address privacy topics at company-wide meetings such as town halls and all-hands meetings;
- CEO's, senior leaders' and local managers' videos, talking about the importance of privacy;
- Dedicating special days, weeks or a month to discussing privacy topics and developing privacy solutions, which can also involve team meetings or on-site or off-site events;
- Leveraging special dates, such as the data privacy day on 28 January or GDPR anniversaries to issue special communications, providing extra training modules to employees, and organising dedicated privacy events;
- Regular, concise, visual and practical communications and reminders to all employees to address specific topics such as privacy "do's and don'ts", FAQs, privacy by design, DPIAs and escalating data breaches, etc.;
- Dedicated data privacy community of practice or distribution lists to which employees can sign up if they wish, addressing privacy topics in more detail;
- Specific brand for the DPMP and adding branding elements to related communications such as catchy names, icons, colour schemes, mascots, dolls, etc.;
- Eye-catching infographics which are shared with employees online and offline, as well as other collaterals, such as posters, stickers and tip sheets, distributed in key office and communal areas;
- Tapping into internal communication and marketing teams to develop catchphrases in internal communication campaigns, such as "Privacy is the new normal"; and
- Launching privacy quizzes and competitions, such as a prize for the "best video on what privacy means to you and the company".

"Privacy is more than a legal topic. It is a business and personal topic that concerns us all. Thus, the way we communicate about privacy must be uncomplicated, user friendly, and personalised".
– Anny Pinto, Chief Privacy Officer & Legal Head Group IT, The Adecco Group

Case Study 38. A look into a monitoring life cycle

An organisation has implemented an annual cycle of privacy monitoring based on risk statements and control requirements. The organisation has implemented tools for testing such controls. Employees are not expected to deliver 100% compliance on them, but rather a percentage in order to achieve a substantive level of compliance. The privacy team reviews the assessments and the results are included in executive risk reports that are escalated to local management and also to the CEO. The organisation believes that DPMPs should enable calibration—different business units will always be in different stages of compliance—but all will be required to comply with the baseline requirements.

Case Study 39. Insights gathered through review resulting from records of processing activities

An organisation leveraged and customised an existing application to implement records of processing activities, required by the GDPR. It observed that it was difficult to review and use data within this application, and that the solution required users to also leverage a separate manual process to perform the privacy impact assessment (PIA). Therefore, it migrated to a dedicated software solution that can be more readily updated, centralises all relevant processes and can also produce management information. In parallel, it reviewed, validated and consolidated the information that went into this new solution. As a result, the organisation obtained greater insight into the personal data processed by the business, as it has improved visibility of data across circa 1500 applications and 300 products.

6. MONITORING AND VERIFICATION

Monitoring and verifying the implementation, internal compliance and effectiveness of the DPMP ensure that the accountability loop is closed. Accountable organisations make use of internal and external audits, as well as other monitoring mechanisms to test compliance with their DPMP, policies, procedures and controls. They also make use of certification schemes to review and assure their data privacy compliance activities. They take steps to act upon audit and monitoring findings, including reviewing and updating their DPMPs, policies and procedures, products, services and systems.

6.1 Conducting internal and external audits and reviews

Internal audit

Large organisations use their internal independent control and audit functions to verify compliance with the DPMP, privacy policies and data privacy-related legal requirements. The audits can be as broad as assessing the overall compliance with the DPMP or more targeted to key policies, key business areas and the riskiest privacy areas. Organisations use audits to measure the effectiveness of specific data privacy controls or accountability elements, or the overall DPMP.

Privacy officers often work closely with internal audit to embed privacy elements in existing audit programmes. In some cases, they choose to create privacy-specific audit programmes. They also provide specialist data privacy training to internal audit teams to build the capabilities and enable these teams to carry out specific data privacy-related audits.

The frequency and scope of internal audits vary across organisations from one to every three years. Some organisations carry out several separate data protection audits per year.

Organisations act upon audit findings and put in place remedial action plans (see Section 7.1).

External audits and reviews

Organisations also hire certified external auditors, as well as consultants and law firms to undertake additional privacy-related audits and reviews. Some organisations even allow third parties, such as clients, to perform certain audits of the organisations' DPMP, data privacy activities, products and services. Some organisations also engage in peer-to-peer reviews, which allow them to benchmark their DPMPs against peers' programmes.

Organisations that participate in various data privacy frameworks and certifications, such as BCR, Privacy Shield, CBPR and ISO, also have to go through periodic external audits and reviews as required by these schemes (see Section 6.3).

Case Study 40. Peer review of the DPMP

Every two years, an organisation invites select clients and partners to a privacy audit day to enable a peer review, benchmark and assessment of its DPMP. In return, clients and partners share their own experiences and compliance efforts with the organisation. This enables these organisations to benchmark their programme against one another and to learn from other organisations' best practices they can replicate into their own programme.

Case Study 41. Privacy team monitoring through KPIs

The privacy team of an organisation monitors compliance with privacy controls on a quarterly basis, through reports by local DPOs that include KPIs. Obtaining these reports and the KPIs is vital for the privacy team to monitor the ongoing maintenance of privacy standards internally. All teams involved work intensively to have these ready every quarter. They also get buy-in and understanding from all stakeholders of the importance of this activity, and that this is everyone's responsibility. They believe that programmes are designed to be cyclical and that organisations know that they will be effective by keeping this cycle alive and moving it forward.

6.2 Monitoring and testing the effectiveness of privacy compliance activities

Organisations continually test the effectiveness of their DPMPs, as well as of risk assessments, in order to ensure that they provide the expected results and their programmes are still "fit for purpose". These are performed centrally by the privacy office team, and also in a decentralised way, by business, functional or geography/ regional teams. Methods used include:

- Periodic programme reviews;
- Self-assessment tools;
- KPIs (see Section 1.1);
- Risk assessments undertaken in the context of the ERM (see Section 2.1);
- PIAs and DPIAs (see Section 2.3); and
- On-site visits by privacy officers to monitor local compliance and compliance of specific products and services after launch.

Some organisations monitor internal data flows using technologies and tools, such as privacy scanning and automated fileshare scanning. This allows them to identify for instance whether data is being shared inappropriately within and outside of the organisation, and whether access restriction controls are effective. It also allows them to delete records identified as no longer needed.

An organisation also has technical teams responsible for monitoring the data life cycle and the architecture behind systems and security controls. Their activities feed data maps and records of processing activities. Results are reported to engineers and privacy officers if changes are needed in systems and processes.

Some organisations monitor third parties' use of personal data through Application Programme Interfaces (APIs) in cases when the third party is a data partner and receives personal data that the organisation collects. The partnership can be terminated if the organisation finds that the data partner is not following the rules of their agreement.

6.3 Obtaining corporate data privacy certifications

Organisations increasingly participate in data privacy-related certification schemes. Some even obtain multiple certifications. Examples of commonly used schemes include:

- Certifications provided by the International Organization for Standardization (ISO);
- Certifications provided by the National Institute of Standards and Technology (NIST);
- APEC Cross-Border Privacy Rules (CBPR) System;
- APEC Privacy Recognition for Processors (PRP);
- EU-US Privacy Shield; and
- Binding Corporate Rules (BCR).

The motives for obtaining these certifications vary between the organisations. In general, they all seek to realise concrete values from achieving an external certification of their data privacy activities and their DPMP. Some are driven by the need to demonstrate compliance to regulators, and some to third parties (clients and business partners). Some indicate that these certifications are increasingly seen as a condition of "doing business" and are often required in procurement processes. Some organisations also want an independent validation of internal efforts to be able to showcase their success and the return on data privacy investment to their boards and executive committees. Finally, certifications enable organisations to be more agile and efficient and respond quicker to external stakeholders (from clients and business partners to regulators).

All these certifications require that organisations go through extensive and periodic third-party external reviews and audits to verify their continued compliance with the framework and standards, or to renew their certification scheme.

Case Study 42. Self-help tools for individuals' requests concerning their data privacy rights

An organisation receives globally 1500 individual data privacy requests per month, which are handled by the DPO team. It has created a specific self-help automated tool, which allows individuals to download a machine-readable archive of information associated with their accounts. 2.2 million individuals used this tool in the months following the entry into force of the GDPR. In addition, the organisation developed online forms available in multiple languages to enable individuals to request further information. This organisation also takes part in a project with other peer organisations to create an open-source, service-to-service data portability platform.

Case Study 43. Data access requests process tested by client doing "mystery shopping"

A client decided to test an organisation's process to handle data access requests. The client did a "mystery shopping" — they made an access request without mentioning that they were a client. They were surprised with how promptly and proactively the organisation responded to the request. This led to increased sales with this same client, and therefore generated additional revenues to the organisation.

7. RESPONSE AND ENFORCEMENT

The last accountability element, response and enforcement, requires organisations to have in place procedures and controls to act upon findings of audits and reviews, address enquiries from regulators and requests and complaints from individuals, notify data breaches and take enforcement actions against internal non-compliance. More broadly, this is about setting up a response plan and taking action when elements of a DPMP do not work quite the way they are intended to work.

7.1 Acting upon findings of audits and reviews

Organisations act upon the findings of internal and external audits and reviews (see Section 6.1). This includes following up on the necessary corrective actions, reviewing and putting in place new privacy controls, assigning actions to business owners, reviewing the elements of DPMP, providing feedback and recommendations to internal teams, reporting to senior management and boards on the completed actions, etc.

7.2 Managing individual rights requests, queries and complaints

Organisations put in place policies, procedures and tools to manage requests from individuals. These requests relate to the exercise of data privacy rights (such as access, correction, objection, deletion), as well as to data privacy queries or complaints.

Several functions and stakeholders within the organisations are involved in these processes, including privacy officers, legal, human resources, information technology, information security, data managers and business lines. In some cases, organisations appoint specific teams dedicated to handling individuals' requests.

Depending on the size of the organisation and the nature of the business, privacy officers develop standard template responses for business lines to use when receiving enquiries and complaints. They also develop guidance and training to support these teams, to identify privacy-related enquiries and complaints and to escalate where necessary.

Organisations build and implement specific channels and tools for individuals to make requests and complaints (e.g. web forms, DPO lines, portals, self-help tools such as Download Your Data/Information, etc.). However, individuals also make requests using unexpected channels (e.g. customer service, call centres or even addressing the specific organisation entity or branches). Organisations work to predict these cases and update internal processes accordingly, so that requests are directed internally through the appropriate channels.

Organisations have been increasingly developing or outsourcing manual and automatic processes and tools to handle individuals' requests (e.g. ticketing tools and systems). These tools are particularly helpful for organisations that have observed a surge in requests (some of which originated from class actions or activists' encouragement) after the entry into force of new laws such as the GDPR or CCPA, or after the organisation has defined new/global procedures to handle these requests.

Case Study 44. A teachable moment

An organisation distributes from time to time electronic postcards to all employees illustrating an anonymised real example of non-compliance with data privacy policy and controls that resulted in disciplinary measures. The organisation believes that real examples are a perfect opportunity to deliver a teachable moment and to continuously raise awareness about required and desired behaviours.

Case Study 45. Ongoing collaboration with regulators

Following a regulatory investigation, an organisation made a commitment to meet with the regulator at least every six months to present the progress made on its DPMP.

Case Study 46. Process changes after feedback from regulators

A DPA contacted an organisation after receiving data subject complaints about how the organisation handled individual requests concerning the exercise of data protection rights. Both the DPA and the organisation acted in a collaborative and engaged manner. The DPO of this organisation promptly presented all information requested by the DPA, including all of its template responses to individual requests. In turn, the DPA provided a series of feedback and recommendations. The organisation updated the Privacy Centre page on its website accordingly. This strengthened their relationship with the DPA, enabling the complaints cases to be quickly closed. It also improved the internal process for exercise of individuals' rights, ultimately resulting in fewer complaints ending up with the DPA.

7.3 Notifying individuals and regulators in cases of breaches of personal data

Organisations notify breaches of personal data to regulators and individuals when necessary, relevant and required by law.

In order to avoid unnecessary notification, privacy teams develop breach management and notification processes (see Section 3.2) and guidelines to help the relevant teams identify when the data breach meets a determined set of criteria that makes it a reportable breach. Organisations may also choose to voluntarily notify breaches to individuals and/or regulators, even when not clearly required by law, in order to safeguard their trusted relationships with regulators.

7.4 Enforcing internal non-compliance with privacy rules

Organisations take performance and disciplinary actions against staff to enforce their DPMP, privacy policies and procedures.

Enforcement measures vary depending on the seriousness and repetitiveness of the infringement or a non-compliance, and often depend on the local employment laws. Disciplinary actions span from written warnings to termination of employment. They also include further training and awareness-raising when non-compliance is unintentional and the employees can learn from their own mistakes.

An influencing factor in decisions concerning the enforcement action to be taken includes whether employees take responsibility for their actions and demonstrate a willingness to change and support mitigating possible harms.

Some organisations have a zero-tolerance policy with certain issues such as negligent data breaches. As a result, contracts may be terminated if employees are found actively and negligently responsible for a serious data breach.

Organisations implement additional training and awareness-raising activities to staff following a serious infringement of privacy rules, or after noticing that certain infringements have a particular repetitive nature.

7.5 Collaborating with regulatory requests and investigations

Organisations mobilise resources and collaborate with DPAs during enquiries and investigations, to continue to demonstrate their accountability to the regulators. Regulators may investigate organisations following a privacy complaint, in the context of a reported data breach, in the context of a new product/service launch, following media reports or as a part of the regulator's "horizon scanning" or information-gathering activities.

"We have heard from regulators that we are approachable and not secretive. We believe that this is because accountability has enabled us to be ready to engage".
– Della Shea, Vice President, Data Governance & Chief Privacy Officer, Symcor

Depending on the scope of the regulatory request or investigation, organisations dedicate a substantial amount of resources to locating and making available any information requested, drafting responses, engaging with the DPA, hosting them in case of on-site visits and investigations, etc.

Organisations sometimes choose to dedicate employees to managing the response to regulators, and/or hire consultants and specialised law firms to support them. In all organisations, privacy officers are often involved in regulatory engagement, enquiries or investigations. In many cases, they are responsible for leading such engagement, with the support and participation of other teams in legal, product engineers, data scientists, government relations, or a concerned business or support function.

For more efficient collaboration and communication with DPAs, some organisations also put in place dedicated DPA channels, such as email addresses that direct DPAs to the mailboxes of privacy officers.

IV. Appendix A. CIPL's Work On Accountability

For more than a decade, the Centre for Information Policy Leadership (CIPL) has pioneered organisational accountability as a key building block of effective data privacy regulation and its corresponding implementation.

In addition to organising numerous events on the topic of accountability around the globe with industry and regulators, CIPL has published a number of papers in addition to this one (available on https://www.informationpolicycentre.com/cipl-white-papers.html).

- General accountability papers:
  - CIPL White Paper - Organisational Accountability - Past, Present and Future (30 October 2019)
  - CIPL Accountability Paper - Q&A on Organisational Accountability in Data Protection (03 July 2019)
  - CIPL Accountability Discussion Paper Intro - Introducing Two New CIPL Papers on The Central Role of Organisational Accountability in Data Protection (23 July 2018)
  - CIPL Accountability Discussion Paper 1 - The Case for Accountability: How it Enables Effective Data Protection and Trust in the Digital Society (23 July 2018)
  - CIPL Accountability Discussion Paper 2 - Incentivising Accountability: How Data Protection Authorities and Law Makers Can Encourage Accountability (23 July 2018)
  - Data Protection Accountability: The Essential Elements A Document for Discussion (October 2009)
- Accountability in context:
  - CIPL White Paper - What Does the USMCA Mean for a US Federal Privacy Law? (17 January 2020)
  - CIPL White Paper - Organisational Accountability in Light of FTC Consent Orders (13 November 2019)

- CIPL White Paper - Organisational Accountability - Existence in US Regulatory Compliance and its Relevance for a US Federal Privacy Law (03 July 2019)
- Certifications Paper - Certifications, Seals and Marks under the GDPR and Their Roles as Accountability Tools and Cross-Border Data Transfer Mechanisms (12 April 2017)
- The Role of Enhanced Accountability in Creating a Sustainable Data-Driven Economy and Information Society (21 October 2015)
- Implementing Accountability in the Marketplace - A Discussion Document (November 2011)
- Demonstrating and Measuring Accountability - A Discussion Document (October 2010)
- Trusted Information Management: Data Privacy & Security Accountability in Outsourcing (September 2007)
- Outsourcing in India: Designing A Privacy Accountability Self-Regulatory Organization (June 2007)

V. Appendix B. Illustrating Accountability

Examples of accountability practices and content of Data Privacy Management Programmes (DPMPs)

Leadership and Oversight

- Tone from the top and leading by example
- Tone from the middle – management and local level
- Privacy officers, team and local support
- Investing in data privacy talent
- Reporting lines and tools
- Establishing DPMPs and governance
- Internal/External Oversight Boards and Committees

Risk Assessment

- Defining and registering data privacy risks
- Understanding risks to individuals
- Integrating data privacy within risk management
- Managing data privacy risks:
  - at DPMP level
  - at product, service and project levels
  - of business partners and third parties
- Undertaking PIAs and DPIAs

Policies and Procedures

- Internal rules operationalising data privacy requirements
- Legal basis and fair processing
- Data privacy by design
- Information security and data breaches
- Third party management
- Data transfers mechanisms
- Data maps and records of processing activities
- Other rules (e.g. marketing, HR, M&A)

Transparency

- Transparency to individuals – privacy notices and innovative channels and tools (e.g. privacy portals, user experience and user-centric design, customer journey, dashboards, videos, icons, illustrations, animations)
- Transparency to third parties
- Transparency to regulators

Training and Awareness

- Mandatory corporate training
- Ad hoc and functional training
- Awareness-raising campaigns and communication strategies (e.g. senior leadership videos, data privacy-dedicated dates and events, regular communications, data privacy distributions lists, DPMP branding, quizzes and competitions)

Monitoring and Verification

- Internal and external audits and reviews
- Monitoring, testing, measuring and reporting on effectiveness of the DPMP and on data privacy compliance activities
- Corporate data privacy certificationsDocumentation and evidence (consent, legal bases, privacy notices, PIAs and DPIAs, processing agreements, breach response)

Response and Enforcement

- Acting upon findings of audits and reviews
- Managing individual rights requests and complaints-handling
- Data breach internal reporting and external notification
- Internal enforcement of non-compliance subject to local laws
- Engagement and cooperation with DPAs and other regulators

[1] The findings of this report are also not to be construed as legal advice or as representing the views of any individual CIPL member company or the law firm of Hunton Andrews Kurth LLP.

[2] CIPL is a global data privacy and cybersecurity think tank in the law firm of Hunton Andrews Kurth LLP and is financially supported by the law firm and 90+ 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 submission should be construed as representing the views of any individual CIPL member company or of the law firm of Hunton Andrews Kurth.

[3] CIPL is broadly using "privacy officers" to describe individuals who are responsible for data privacy in the organisation. This can include: CPO, DPO, DPO staff, privacy lawyers, privacy managers, members of the privacy team, etc.

[4] CISCO 2020 Data Privacy Benchmark Study entitled "From Privacy to Profit: Achieving Positive Returns on Privacy Investments", available at <https://www.huntonprivacyblog.com/wp-content/uploads/sites/28/2020/02/2020-data-privacy-cybersecurity-series-jan-20201.pdf>.

[5] Referred to in this report as the "CIPL Accountability Framework".

[6] In the context of the requirement to appoint data protection officers as per Articles 37-39 of the General Data Protection Regulation.

[7] Some organisations, in particular US organisations, use the term "privacy policy" to refer to "privacy notice", which is a term mostly used in the EU. Any reference to "privacy notice" in this report should be understood also as "privacy policy".

[8] See The Guide to the Sandbox (beta phase) at the UK ICO's website <https://ico.org.uk/for-organisations/the-guide-to-the-sandbox-beta-phase/>.

About the Centre for Information Policy Leadership

CIPL is a global data privacy and cybersecurity think tank in the law firm of Hunton Andrews Kurth LLP and is financially supported by the law firm and 90 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/.**

If you would like to discuss this paper, learn more about CIPL membership or find out how CIPL can help you build or implement a comprehensive Data Privacy Management Programme, please contact Bojana Bellamy bbellamy@HuntonAK.com and Michelle Marcoot mmarcoot@HuntonAK.com

Centre for Information Policy Leadership
HUNTON ANDREWS KURTH

DC
2200 Pennsylvania Avenue
Washington, DC 20037
+1 202 955 1563

London
30 St Mary Axe
London EC3A 8EP
+44 20 7220 5700

Brussels
Park Atrium
Rue des Colonies 11
1000 Brussels
+32 2 643 58 00