The Central Role of Organisational Accountability in Data Protection

Discussion Paper 1 (of 2)

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

Centre for Information Policy Leadership

23 July 2018

Table of Contents

I. Objectives of this Paper

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

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

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

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

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

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

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

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

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

II. Background on Organisational Accountability

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

a) Implement applicable data protection requirements or goals; and

b) Be able to demonstrate such implementation.

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

the ability and the responsibility to determine appropriate, effective measures to reach those goals," complemented by the "organisation's ability to demonstrate its capacity to achieve specified privacy objectives."[6]

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

A. The Elements of Accountability

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

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

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

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

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

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

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

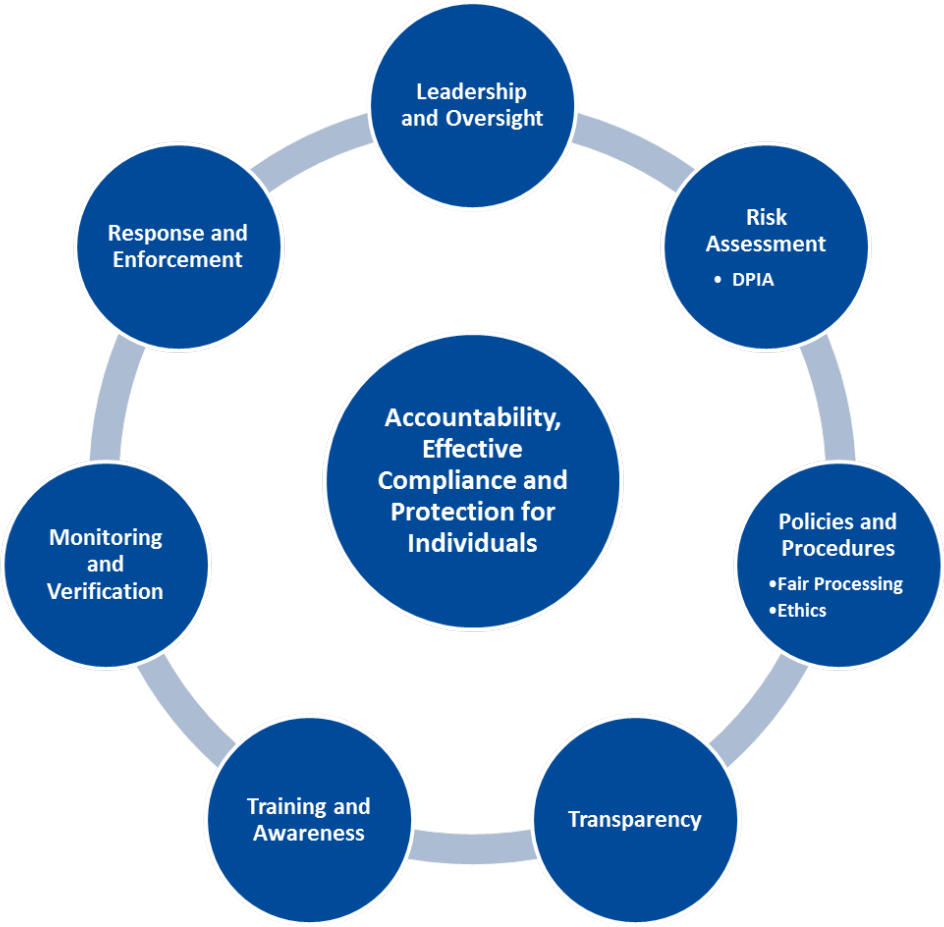

Figure 1 – CIPL "Accountability Wheel" – Universal Elements of Accountability

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

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

Table 1 – Organisational measures to implement the elements of accountability

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

B. Approaches to Implementing Accountability

Organisations can implement accountability through various means. They include:

a) Internal organisational privacy and information management programs;

b) Regulated frameworks such as EU Binding Corporate Rules (BCR)[16] and the EU-US Privacy Shield;[17]

c) Industry codes of conduct, such as the FEDMA European Code of Practice for the Use of Personal Data in Direct Marketing[18] or the CISPE Code of Conduct[19] and as envisaged in the GDPR;[20]

d) Third-party certifications and seals, such as APEC Cross-Border Privacy Rules (CBPR) and the APEC Privacy Recognition for Processors (PRP),[21] various national privacy marks, for example, Japan's JIPDEC Privacy Mark System[22] and certifications envisaged in Article 42 of the GDPR;

e) International standards, such as ISO 27018 (Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors) (hereinafter, Cloud Privacy and Security standard).[23]

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

1. Build and implement comprehensive internal data privacy and governance programs (including policies and procedures) that implement and operationalise data privacy protections that govern the organisations' use of data. These protections can be based on:

   - legal obligations in laws such as the GDPR or other data privacy laws;
   - requirements established by accountability schemes (e.g., Privacy Shield, BCR or CBPR);
   - requirements established by internal company policies, goals or internal codes of business ethics;
   - requirements of external third-party certification schemes, seals or codes of conduct; or
   - requirements of international standards, such as the ISO Cloud Privacy and Security Standard.

2. Be able to verify the implementation of such programs internally through different assessments, controls and internal audits and, in some cases externally, through external audits or certifications.

3. Be able to demonstrate the existence and effectiveness of such programs, both internally to their corporate boards, and externally to individuals, business partners, shareholders and civil society bodies representing individuals and, upon demand, to DPAs in an investigation or enforcement context, or to a third-party certifier in the context of certified accountability frameworks.

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

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

C. Accountability under the GDPR

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

1. Controllers

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

- Article 5(2): Accountability is now explicitly a data protection principle — "The controller shall be responsible for, and be able to demonstrate compliance with paragraph 1 (accountability)", i.e. the basic data protection principles contained in GDPR Article 5, such as fair processing, lawful basis for processing, purpose specification and limitation, data quality, etc.[26]

- Article 24(1): This provision concretises the concept of accountability and incorporates the risk-based approach into the GDPR.[27] Organisations must implement, review and keep up-to-date appropriate technical and organisational measures, including policies, procedures, rules and tools, to:

    a) Ensure compliance with the GDPR; and

b) Be able to demonstrate compliance.

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

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

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

2. Processors

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

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

Specific obligations on processors introduced by the GDPR include:

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

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

3. Elements of accountability in the GDPR and in general

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

Accountability Element:	Examples of controls/measures mapped to accountability elements:
Leadership and Oversight	• Executive oversight • Data privacy officer/Office of oversight and reporting • Data privacy governance • Privacy engineers
Risk Assessment	• At program level • At product or service level • In case of data breach incident • DPIA for high-risk processing • Risk to organisations • Risk to individuals

Policies and Procedures	• Internal privacy rules based on data protection principles • Information security • Legal basis and fair processing • Vendor/Processor management • Procedures for response to individual rights • Other procedures (e.g., Marketing rules, HR rules, M&A due diligence) • Data transfer mechanisms • Privacy by design • Privacy by default • Templates and tools for privacy impact assessments • Crisis management and incident response
Transparency	• Privacy policies and notices to individuals • Innovative transparency – dashboards, integrated in products/apps, articulate value exchange and benefits, part of the customer relationship • Access to information portals • Notification of data breaches
Training and Awareness	• Mandatory corporate training • Ad hoc and functional training • Awareness raising campaigns and communication strategy
Monitoring and Verification	• Internal records of processing • Documentation and evidence – consent, legitimate interest and other legal bases, notices, PIA, processing agreements, breach response • Compliance monitoring as appropriate, such as verification, self-assessments and audits • Seals and certifications
Response and Enforcement	• Individual requests and complaint-handling • Breach reporting, response and rectification procedures • Managing breach notifications to individuals and regulators • Implementing response plans to address audit reports • Internal enforcement of non-compliance subject to local laws • Engagement/Co-operation with DPAs

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

D. Implementing and Demonstrating Accountability within an Organisation

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

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

1. Comprehensive internal privacy programs

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

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

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

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

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

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

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

E. Which Organisations are Expected to be "Accountable"?

1. Controllers and processors

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

a) Their respective legal obligations under the GDPR (or other applicable law or binding instruments such as the APEC CBPR or PRP, or other certifications and codes of conduct); and

b) Contractual requirements and terms of the controller-processor agreement.

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

- The GDPR imposes increased legislative obligations on processors[34] and also provides for enhanced contractual stipulations for them.[35] It is inconceivable that processors would be able to comply with these without having a comprehensive data privacy program in place based on the elements of accountability, as discussed above.[36] It is in processors' interest to implement accountability and thus minimise any risks of regulatory or contractual non-compliance and liabilities.

- Processors will be faced with situations where they will have to demonstrate accountability to their clients (controllers), to DPAs, and even to individuals (due to joint

liability).[37] These situations will typically arise in cases of audits, investigations, breach notifications, or enforcement.

- Processors will likely want to demonstrate accountability proactively, as this will help strengthen their reputation in the information ecosystem and make them a trusted business partner. It may also provide them with a competitive edge vis-à-vis other processors. The GDPR provides that controllers must choose processors that are able to provide sufficient guarantees to protect controllers' data. The APEC CBPR require controllers to have mechanisms in place that ensure that their processors comply with the controller's data protection obligations. A processor that is able to show its commitment to data protection based on accountability will be able to drive more clients to its services.

- Processor certifications under the GDPR will be one way in which a processor may be able to gain external recognition for its accountability and data privacy program. GDPR certifications will also serve as sufficient guarantees that an organisation has implemented appropriate technical and organisational measures that meet the requirements of the GDPR. Similarly, the BCR for Processors are widely used by processors to demonstrate accountability, both to regulators and clients. The use of all these mechanisms is likely to increase even further under the GDPR and in general. In the APEC context, the APEC PRP fulfil similar functions of providing external recognition for processors of their accountability as well as providing proof of due diligence by controllers in the selection of their processors.

- Under Article 37(1) of the GDPR, processors (like controllers) have an obligation to designate a data protection officer (DPO) in specified circumstances requiring heightened internal oversight and accountability with respect to data processing activities.

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

a. The impact of accountability on contractual provisions and negotiations

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

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

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

- Processors now have their own direct obligations and accountability to individuals and regulators under the GDPR.[38] As such, processors will be concerned about managing this direct statutory liability risk to individuals and regulators in addition to any liability that the controller may try to impose contractually. It would be natural for processors to push back in contractual negotiations with controllers and say, "now that I have this direct statutory liability risk, I can no longer take on the same level of contractual risk."

- It is conceivable that a processor could end up directly liable to third parties and/or regulators for a breach that was caused (in whole or in part) by the controller. Hence, it would also be natural for the processor to require the controller to sign up to certain data protection and security obligations in the processing agreement and accept some level of liability and/or responsibility to indemnify for claims or penalties incurred by the processor to the extent they were caused by the controller. The GDPR appears to expressly contemplate that the controller's obligations would be set out in the processing agreement. GDPR Article 28(3) provides that "Processing by a processor shall be governed by a contract or other legal act [...] that sets out the subject-matter and duration of the processing, the nature and purpose of the processing, the type of personal data and categories of data subjects and the obligations and rights of the controller" (emphasis added).

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

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

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

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

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

2. Public sector organisations

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

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

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

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

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

III. The Benefits of Accountability

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

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

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

A. Accountability Benefits to Stakeholders

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

Benefits for Organisations
• Enables more effective privacy protections by requiring risk-based prioritisation of such protections.
• Assists organisations in ensuring and demonstrating legal compliance to business partners and regulators.
• Fosters a culture of internal privacy compliance and constructive engagement with DPAs.
• Fosters good data hygiene and good data management and helps to support the strategic objectives of organisations around data.
• Enables greater harmonisation of organisations' privacy policies and practices with the various requirements of the different jurisdictions in which they do business.
• Generates trust among the public and regulators that the organisation is processing personal data responsibly, potentially enhancing the reputation and goodwill of the organisation and adding value to its brand (trust advantage[42]).
• Enables organisations to engage in broader beneficial uses of personal data, including data for social good, research and responsible AI and machine learning by minimising the risks of new data uses (e.g., through incorporating privacy by design, transparency, risk assessment, etc.) and demonstrating responsible data use to regulators.
• Assists SMEs with implementing scalable privacy tools and controls within their organisations, appropriate to their size and type of operation.
• Provides legal certainty for organisations with regard to cross-border data protection compliance through participation in recognised accountability frameworks, such as BCR and CBPR.
• Enables cross-border data transfers through recognised mechanisms such as BCR and CBPR.
• Furthers the creation of interoperability between different accountability frameworks and thus global solutions to data transfers for organisations.
• Helps differentiate between organisations and provides a competitive edge to those who choose to invest in accountability relative to those who do not (accountability advantage).
• Improves overall level of privacy behaviours of organisations which in turn improves the health of the data ecosystem in general and benefits all stakeholders in the digital economy in the long run.
• Serves as a due diligence tool for controllers in identifying qualified and accountable processors.

Benefits for Individuals
• Delivers real and more effective protection of individuals and their data.
• Ensures that the protection follows personal data transferred across borders.
• Assures individuals that compliance with local legal requirements are met and increases individuals' trust in organisations' processing of their data.
• Enhances privacy protections for individuals beyond minimum requirements and empowers individuals in the management of their data (e.g., through the extension of individual rights or voluntary security breach reporting by organisations).

• Shifts the burden of protecting individuals more explicitly to organisations.
• Provides individuals with a benchmark for deciding whether to allow their data to be processed by certain organisations.
• Provides individuals' rights and interests heightened consideration and protection through required risk assessments and balancing processes.
• Permits individuals to reap the benefits of participation in the digital society.
• Enables more effective domestic and cross-border enforcement.

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

Table 3 – Benefits of Organisational Accountability to Stakeholders

B. Types and Categories of Accountability Benefits

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

Accountability as a driver towards global intra-company harmonisation

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

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

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

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

Accountability as an enabler of legal compliance

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

Accountability as a compliance tool for SMEs

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

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

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

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

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

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

Accountability as an enabler of proactive privacy protections

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

- Many accountable organisations voluntarily apply internal security breach reporting and response practices even in countries where there is no legal requirement to notify the breaches;

- Some organisations voluntarily extend the right of access to all of their customers and employees, even when there is no strict legal obligation to do so;

- Organisations that participate in voluntary data protection and privacy certifications, codes of conduct or similar accountability schemes benefit individuals and other stakeholders by going above and beyond what is required by law. Indeed, to reap the benefits of a CBPR certification, for example, some organisations might certify to the CBPR even in countries where the requirements of the CBPR exceed those found in any domestic laws; and

- Where legislative accountability requirements may not technically apply to processors, accountability schemes may nevertheless provide additional proactive data protection measures that benefit both the processors and all other stakeholders (As explained

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

Accountability as an enabler of interoperability of privacy norms

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

Accountability as an enabler of societal trust in modern data uses

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

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

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

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

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

Accountability as an enabler of constructive engagement and regulatory oversight

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

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

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

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

a backstop enforcement cooperation arrangement between international DPAs.[56] Each of these features greatly augments the oversight capacity and enforcement reach of individual DPAs.[57]

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

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

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

IV. Conclusion

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

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

References

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

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

[3] *Id*. at page 6, paragraph 15.

[4] CIPL Discussion paper on "Incentivising Accountability: How Data Protection Authorities and Law Makers Can Encourage Accountability," 23 July 2018, available at http://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_accountability_paper_2_-_incentivising_accountability_-_how_data_protection_authorities_and_law_makers_can_encourage_accountability.pdf

[5] *Supra* note 2, at page 3.

[6] The Centre for Information Policy Leadership, "Accountability: A Compendium for Stakeholders," March 2011, at page 3, available at https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/accountability-a_compendium_for_stakeholders__march_2011_.pdf.

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

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

[9] See APEC Privacy Framework, at page 28, available at https://www.apec.org/-/media/APEC/Publications/2005/12/APEC-Privacy-Framework/05_ecsg_privacyframewk.pdf.

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

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

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

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

[13]Data Protection Accountability: The Essential Elements, October 2009, available at https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/data_protection_accountability-the_essential_elements__discussion_document_october_2009_.pdf;

Demonstrating and Measuring Accountability, October 2010, available at https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/demonstrating_and_measuring_accountability_a_discussion_document__accountability_phase_ii-the_paris_project_october_2010_.pdf;

Implementing Accountability in the Marketplace, November 2011, available at https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/implementing_accountability_in_the_marketplace__accounrtability_phase_iii-the_madrid_project_november_2011_.pdf;

Accountability: A Compendium for Stakeholders, March 2011, available at https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/accountability-a_compendium_for_stakeholders__march_2011_.pdf;

Accountability: Data Governance for the Evolving Digital Marketplace, April 2011, available at https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/accountability-data_governance_for_the_evolving_digital_marketplace__april_2011_.pdf.

[14] See documents (a) and (b) in note 30.

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

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

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

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

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

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

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

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

[22] See JIPDEC PrivacyMark System at https://privacymark.org/.

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

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

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

[26] Paragraph 1 of Article 5 covers the "Principles relating to processing of personal data," Article 5(1) GDPR.

[27] For a full discussion on the risk-based approach to processing under the GDPR, see CIPL's white paper on Risk, High Risk, Risk Assessments and Data Protection Impact Assessments under the GDPR, 21 December 2016, available at https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_gdpr_project_risk_white_paper_21_december_2016.pdf.

[28] For a further discussion on risk, see CIPL papers on:

(a) A Risk-based Approach to Privacy: Improving Effectiveness in Practice, 19 June 2014, available at https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/white_paper_1-a_risk_based_approach_to_privacy_improving_effectiveness_in_practice.pdf;

(b) The Role of Risk Management in Data Protection, 23 November 2014, available at https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/white_paper_2-the_role_of_risk_management_in_data_protection-c.pdf;

(c) Protecting Privacy in a World of Big Data, The Role of Risk Management, 16 February 2016, available at https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/protecting_privacy_in_a_world_of_big_data_paper_2_the_role_of_risk_management_16_february_2016.pdf; and

(d) Comments by the Centre for Information Policy Leadership on the Article 29 Data Protection Working Party's "Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is 'likely to result in a high risk' for the purposes of Regulation 2016/679," 19 May 2017, available at https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_comments_on_the_wp29s_guidelines_on_dpias_and_likely_high_risk_19_may_2017-c.pdf.

[29] *Supra* note 2, at page 5, paragraph 12, and page 19 paragraphs 73 and 74.

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

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

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

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

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

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

[31] "Voluntary" refers to the fact that typically organisations are not required to participate in these mechanisms but may choose to do so; however, once they have opted to participate, the requirements of these mechanisms become binding and enforceable.

[32] *Supra* note 2 above, at page 6.

[33] Article 5(2) and Article 24 GDPR.

[34] See further discussion in Section II. C. 2.

[35] Article 28(3) GDPR.

[36] See further discussion in Section II.A.

[37] Article 82(4) GDPR.

[38] See, for example, Article 28 (Processor) and Article 82 GDPR (Right to compensation and liability).

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

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

[41] *Supra* note 24 at page 337.

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

[43] For example, Japan's amended privacy regime explicitly recognises APEC CBPR as a cross-border transfer mechanism. Australia's privacy law allows for "binding schemes" that ensure that the recipient of Australian personal data protects the data at the Australian level. The CBPR or PRP are such a binding scheme. Australia has stated intent to join the APEC CBPR. Guidance by the Hong Kong Privacy Commissioner on cross-border data transfers, provides for various options based on "due diligence" that could include contracts or "non-contractual oversight" means (presumably, such means include CBPR) by which an organisation can ensure that data remains protected at the Hong Kong level after transfer (See https://www.pcpd.org.hk/english/resources_centre/publications/files/GN_crossborder_e.pdf at page 7). Singapore's Personal Data Protection Regulations provide for the use of binding corporate rules for cross-border data transfers and Singapore also joined the APEC CBPR and PRP systems in March 2018. For a more detailed discussion of the benefits and potential further development of certifications, seals and marks, including BCR, under the GDPR, see CIPL's white paper on "Certifications, Seals, and Marks under the GDPR and Their Roles as Accountability Tools in Cross-Border Data Transfer Mechanisms," 12 April 2017, available at http://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_gdpr_certifications_discussion_paper_12_april_2017.pdf.

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

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

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

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

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

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

[50] Articles 28(1), (4) and (5).

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

[52] *Supra* note 24 at page 327.

[53] *Supra* note 2 at page 16, paragraph 61.

[54] CIPL's Discussion Paper "Regulating for Results – Strategies and Priorities for Leadership and Engagement," 10 October 2017, available at https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_final_draft_-_regulating_for_results_-_strategies_and_priorities_for_leadership_and_engagement__2_.pdf, (advocating a "results-based" approach to data protection oversight and enforcement that relies on constructive engagement with industry, supporting and making use of accountability frameworks, including those that employ third-party certifiers, and risk-based prioritisation of DPA tasks).

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

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

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

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

[59] *Supra* 4.