The Central Role of Organisational Accountability in Data Protection

Discussion Paper 2 (of 2)

Incentivising Accountability: How Data Protection Authorities and Law Makers Can Encourage Accountability

Centre for Information Policy Leadership

23 July 2018

Table of Contents

I. Objectives of this Paper

In the first paper in this series — "The Case for Accountability: How it Enables Effective Data Protection and Trust in the Digital Society" (first CIPL paper) — CIPL[1] explained the general consensus on the meaning of accountability; accountability's central importance to data protection, corporate digital responsibility and the digital economy; and the benefits it conveys to all stakeholders. The objectives of this second paper are, first, to make the case for specifically incentivising organisational accountability and, second, to provide specific suggestions for what such incentives might be. Importantly, the objective in promoting an approach of incentivising accountability is not to weaken or hinder the powers of data protection authorities (DPAs) and, consistent with CIPL's 2017 discussion paper "Regulating for Results – Strategies and Priorities for Leadership and Engagement"[2] (Regulating for Results), it enables DPAs to use other tools in their regulatory toolbox to enable good data practices and compliance.

Furthermore, this discussion paper is intended to promote further thinking to define such incentives. CIPL looks forward to conducting further work in the future on this essential aspect of accountability and to further engaging on this topic with all stakeholders in the digital ecosystem.

II. Why Accountability Should be Incentivised

A. Accountability Beyond Purely Legal Compliance

As demonstrated in the first CIPL paper, accountability may go beyond pure legal compliance. Law and regulation now increasingly require basic accountability (e.g., in the GDPR) and, as such, help ensure compliance with applicable legal requirements. But accountability manifests along a continuum. An organisation's implementation of measures and controls may go above and beyond what the law requires. This might be referred to as "heightened accountability."

As discussed in detail in the first CIPL paper, such heightened accountability provides numerous significant benefits to all stakeholders, including organisations, individuals and DPAs. In this paper, we demonstrate how these benefits, particularly those to individuals and DPAs, warrant significant support from DPAs through encouragement and specific incentives for implementing such heightened accountability. The paper also makes the case that policy and law makers should include effective incentives for accountability in any new or revised data protection regimes.

Examples of heightened accountability that exceed the basic legal requirements include:

- Implementing risk mitigations and controls or undertaking other protective measures that are not specifically required by law;

- Linking privacy management programs to values in the organisation's code of business ethics and reflecting ethical decision-making in the organisation's privacy policies and procedures;

- Participating in non-mandatory privacy certifications and codes of conduct or similar formal privacy accountability schemes, such as Binding Corporate Rules (BCR)[3], APEC Cross-Border Privacy Rules (CBPR)[4], APEC Privacy Recognition for Processors (PRP)[5], Privacy Shield[6] and future GDPR certifications and codes;

- Applying certain controls and requirements of privacy management programs to an organisation's operations in countries without data privacy laws; and

- Requiring heightened accountability of business partners in the ecosystem.

The table below sets forth the reasons why law makers and DPAs should incentivise accountability. However, accountability should be particularly encouraged, incentivised and rewarded where it goes above what is minimally required by law, as such heightened accountability provides substantial additional benefit to individuals, society and DPAs. This approach is consistent with many other areas of law and compliance where legislators and regulators specifically offer incentives for good corporate behaviour and comprehensive compliance programs.[7]

B. The Benefits of Accountability

CIPL outlined in detail the benefits of accountability in the first paper in this series. While this paper does not repeat that discussion, the benefits are summarised in the following table:

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.

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 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[8]).
• 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.

Table 1 – Benefits of Organisational Accountability to Stakeholders

1. Benefits to organisations serving as "internal incentives" for accountability

As demonstrated by *Table 1*, accountability provides specific and direct benefits to organisations. Such benefits could be seen as "internal incentives" for organisations, in that no further encouragement should be necessary from DPAs or law and policy makers for organisations to implement accountability. This is particularly true with respect to the benefit of ensuring and demonstrating legal compliance, thereby reducing the threat and consequences of legal enforcement. Clearly, laws requiring accountability also provide a concomitant incentive to implement it at least to the level required by law.

There are also other "internal incentives" beyond the threat of enforcement. These apply regardless of whether the accountability is of the required or of the non-mandatory "heightened accountability" kind, and these internal incentives increase as the accountability moves up on the accountability spectrum. They include:

a) Using formal accountability mechanisms like certifications or BCR to enable efficiencies and drive the benefits of being able to share personal data across borders within the organisation and its business partners;

b) Providing assurances in a due diligence process, such as in vendor selection or M&A;

c) Increasing trust and confidence among an organisation's customers or DPAs;

d) Improving the organisation's reputation among business partners and/or the public; and

e) SMEs (that may have limited data protection expertise or staff) receiving assistance from third-party certifiers in developing their internal privacy programs.

Thus, organisations have a range of internal incentives to implement accountability of any degree along the spectrum. In many cases "enlightened self-interest" can provide the necessary motivation for organisations to place at the high end of the accountability spectrum. Some of these incentives are increasingly recognised and also formally incentivised by law makers, including in the GDPR. Nevertheless, the more accountability aims beyond what is required, the more it would be helpful to support it through additional "external incentives." As organisations increasingly face competing (and sometimes conflicting) regulatory priorities coupled with market pressures to drive value for shareholders, providing organisations a figurative "return on investment" on data privacy compliance and accountability would be advantageous for any DPA and law and policy maker.

2. Benefits to individuals and DPAs that warrant external incentives

Table 1 above sets forth significant benefits of accountability to individuals and DPAs. Benefits to individuals centre on improved privacy protections, increased individual empowerment, heightened trust in the digital economy and more effective redress. The benefits to the DPAs boil down to a significant augmentation of their limited enforcement and oversight resources

through better actual compliance by organisations and better ability to demonstrate such compliance, which streamlines investigations and enforcement; assurance that organisations are engaged in a risk-based approach to data protection; involvement of third-party certification bodies that provide front-line oversight, "enforcement" and complaint-handling in the context of formal accountability schemes such as privacy certifications and codes of conduct; and improved cross-border enforcement in the context of such accountability schemes.

Given these wide-ranging benefits to individuals (whose collective interests DPAs represent) and to the DPAs themselves, accountability should not be left solely to the threat of sanctions under the applicable law or to the enlightened self-interest of the organisation. It should also be actively promoted through "external incentives." This is particularly important in connection with non-mandatory heightened accountability. From an organisation's perspective, particularly at the highest level of management, investing in levels of accountability that exceed what is required begs the question of justification, especially where the internal incentives are perceived as sufficiently realised. This is where external incentives have a crucial role to play. Such incentives will, in effect, function as an additional "return on investment" on any heightened accountability the organisation implements and thus will help drive corporate best practices in responsible data use and management.

III. Who Should Incentivise Accountability

External incentives for accountability should come primarily from DPAs and law makers.

A. DPAs

As noted in CIPL's Regulating for Results discussion paper,[9] the DPAs' leadership role should include encouraging and incentivising organisations to adopt accountability frameworks, particularly the kinds that go above and beyond what is minimally required.[10] Indeed, DPAs have become de facto data regulators and society's arbiters of responsible use of personal data in the modern information age. As such, they have a particular responsibility to find ways to incentivise the broad-scale implementation of accountability.

B. Law and Policy Makers

Law and policy makers too must be concerned about accountability and individuals' trust in the digital society as this is crucial for reaping the benefits of the fourth industrial revolution. Only accountability can deliver that, coupled with sensible regulation. Accordingly, law and policy makers in jurisdictions that have not yet done so should specifically incentivise accountability through any new or updated data protection laws and regulations to enable the trusted information age.

IV. How Accountability Should be Incentivised

Incentivising accountability could be viewed as a core component of a results-based approach by DPAs to data protection oversight and enforcement. As CIPL has advocated over the past year and as further described in CIPL's Regulating for Results discussion paper,[11] the results-based approach relies to a significant extent on constructive engagement between DPAs and accountable organisations. Prioritising the encouragement and incentivising of desired conduct over penalising undesirable conduct is a core principle of constructive engagement.

There is a broad range of incentives that could be deployed to encourage broader implementation of accountability. As further discussed below, some laws already include, and some DPAs already pursue policies that provide, relevant incentives in this context. Some potential incentives have never been tried in the data protection context, as far as we know.

For example, perhaps the most impactful incentive would be to allow controllers that can effectively demonstrate accountability beyond pure legal compliance to pursue a broader range of reasonable and beneficial uses of personal data. Such broader range of uses could occur in the context of participation in "regulatory sandboxes" specially designed for this purpose.[12] A regulatory sandbox allows qualifying (here accountable) businesses to test innovative products, services, business models and delivery mechanisms in the real market, with real consumers. In the data protection context, this could include testing new data processing activities, data collection methods, or the offering of new information services with appropriate regulatory safeguards and oversight. Of course, given that they permit the processing of real consumers' data and that statutory data protection requirements will still apply to such data processing, further thinking on how such sandboxes would work will be required.

Another impactful incentive could be interpreting data protection principles and requirements (e.g., compatible purposes and fair processing) through the lens of risk and more flexibly for organisations that demonstrate heightened accountability. This would be consistent with the GDPR, which allows for the risk-based calibration of organisations' compliance measures and mitigations. It would be useful to conduct further work on such risk-based and flexible interpretation of data protection principles in the future.

Other incentives include formally recognising demonstrated or certified accountability (e.g., codes and certifications) as:

1) a mitigating factor in enforcement actions and in assessing sanctions and/or levels of fines;

2) evidence of due diligence when selecting data processors or service providers; and

3) a formal cross-border data transfer mechanism.

Again, some legislators have already taken some steps to provide these incentives, such as in the GDPR and several other national data protection laws.

An important initial step on the issue of incentives generally would be for DPAs to formally express their support for verified or certified accountability schemes, such as future GDPR codes of conduct and certifications, BCR, APEC CBPR and PRP, the Privacy Shield or similar mechanisms. It has been the practice of some DPAs to state informally that they take participation in accountability mechanisms such as CBPR or BCR and other certifications into account when making enforcement-related decisions and that they can be used as evidence of reasonable and good-faith efforts to comply with relevant requirements. However, informal statements to that effect do not provide sufficient assurances to organisations and their Boards that the advantages of doing more than necessary are sufficiently predictable and tangible. Thus, any support for accountability and any articulation of specific incentives should as much as possible be codified by law (as has been done in the GDPR to some extent; see below). If that is not possible, or as an interim measure, such articulation of incentives should take the shape of official policy positions by DPAs in jurisdictions where the law is silent on this issue but the DPAs may, in their discretion, consider participation in formal accountability schemes as mitigating factors in their enforcement decisions.

As stated, the GDPR has started to codify possible incentives to participate in such accountability schemes. For example, Article 83(2)(j) provides that "in deciding whether to impose an administrative fine and deciding on the amount [...] due regard shall be given to [...] adherence to approved codes of conduct [...] or approved certification mechanisms [...]." Discussing that provision, the WP29 guidelines on administrative fines[13] note that "[i]n case of a breach of one of the provisions of the Regulation, adherence to an approved code of conduct might be indicative of how comprehensive the need is to intervene with an effective, proportionate, dissuasive administrative fine or other corrective measure from the supervisory authority."[14]

Further, the WP29 guidelines on administrative fines also state that

> [w]here the controller or processor has adhered to an approved code of conduct, the supervisory authority may be satisfied that the code community in charge of administering the code takes the appropriate action themselves against their member, for example through the monitoring and enforcement schemes of the code of conduct itself. Therefore, the supervisory authority might consider that such measures are effective, proportionate or dissuasive enough in that particular case without the need for imposing additional measures from the supervisory authority itself. Certain forms of sanctioning non-compliant behaviour may be made through the monitoring scheme, according to article 41 (2) c and 42 (4), including suspension or exclusion of the controller or processor concerned from the code community. Nevertheless, the powers of the monitoring body are "without prejudice to the tasks and powers of the

competent supervisory authority", which means that the supervisory authority is not under an obligation to take into account previously imposed sanctions pertaining to the self-regulatory scheme.[15]

Statements such as this are helpful in encouraging and incentivising participation in accountability schemes, particularly where they are reiterated with regard to specific codes and certifications as they become available.

In addition, the GDPR also provides in Article 28(5) that "adherence of a processor to an approved code of conduct as referred to in Article 40 or an approved certification mechanism as referred to in Article 43 may be used as an element by which to demonstrate sufficient guarantees as referred to in [Article 28(1) and (4)]." In jurisdictions where such use of verified or certified accountability as evidence of due diligence and compliance is not yet formally recognised by law (as it is under the GDPR), DPAs could nevertheless formally endorse such use in connection with their ability to make discretionary enforcement decisions.

A. Incentives for Implementing Accountability

As discussed in the first paper in this series and in the section on benefits of accountability, organisations have some internal incentive to deliver accountability and implement comprehensive privacy management programs (See discussion in Section II. B. 1. above). This section discusses how DPAs, law makers and policy makers can additionally encourage and incentivise companies to implement accountability beyond their own internal incentives to encourage more wide-spread adoption of accountability by organisations of all types, sizes and structures.

The following table sets forth some of the specific incentives DPAs and/or law and policy makers could provide to organisations[16] to encourage active implementation of accountability:

Using demonstrated accountability[17] as a differentiating or mitigating factor in investigation or enforcement contexts
For example: • As one of the discretionary factors in considering whether to initiate an investigation or enforcement action. • As a mitigating factor in assessing the type of penalties and levels of fines. • As a mitigating factor in case of an individual failure/human error, where the organisation is able to demonstrate that it took the reasonable precautions to prevent the failure or error. DPAs should communicate this policy regularly and refer to it in specific enforcement cases.
Using demonstrated accountability as a "licence to operate" and use data responsibly, based on organisations' evidenced commitment to data protection
As one of the bases for: • Facilitating responsible AI, machine learning, automated decision-making and other big data applications because of the risk assessment, mitigations and other controls in the accountability program. • Allowing broader use of data for social good and research. • Participation in relevant "regulatory sandbox" initiatives.

Publicly recognising best in class organisations and showcasing accountable "best practices" (including those that may be an aggregation of such best practices compiled and generalised by regulators)
• To promote reputation and trust of accountable organisations. • To promote healthy peer pressure and competition in the marketplace.
Supporting and guiding organisations (particularly small and emerging companies) on a path towards accountability, either individually or through association bodies
For example: • Compliance Agreements used by the Canadian Office of the Privacy Commissioner.
Co-funding between DPAs and industry for research into novel accountability tools
• Similar to proposals contained in the Privacy Bridges Report of 37th International Privacy Conference, Amsterdam 2015[18] (See Bridge 10 on Collaborating on and Funding for Privacy Research Programs). • Specific grants by regulators such as the UK ICO and Canadian Federal and Provincial regulators to fund research projects in accountability.
Offer to play proactive advisory role to organisations seeking to implement accountability
• In context of novel technology or business models. • Offer specific resources, including documentation and dedicated contact persons, to support the implementation of heightened accountability.
Using accountability as evidence of due diligence
For example: • In a selection process of processors and other vendors. • In M&A transactions.
Using formal accountability schemes as evidence of uniform and high level privacy protection to enable cross-border data transfers within the company group and to third parties
• APEC CBPR and PRP; EU BCR; GDPR certifications.
Articulate proactively the elements and levels of accountability to be expected
• For instance, at what point would expecting accountability measures constitute undue hardship to organisations?[19] • Based on the concept of proportionality and a risk-based approach to accountability measures.

Table 2 – Incentives for Implementing Accountability

Indeed, providing incentives along the lines of the above for the implementation of accountability is consistent with, and follows from, the explicit recognition by the WP29 and many other DPAs of the numerous benefits of accountability. As stated, organisations have choices for achieving compliance and implementing accountability. They range from bare bones compliance to gold plate corporate digital responsibility. The higher the aim, the stronger the need to justify the organisational resources required for the desired level of accountability. Clear and affirmative pronouncements by DPAs about the specific advantages of aiming high would go a long way to helping data protection officers and other relevant staff obtain the necessary buy-in and resources from their corporate leadership, particularly where the accountability measures exceed the legal requirements. Embedding such incentives in the law would help both DPAs and organisations.

B. Balancing Incentives with Enforcement Powers

When providing such incentives, DPAs must safeguard against any weakening of their legitimate data protection enforcement obligations or the appearance of such weakening. DPAs are functionally independent bodies and while they have an important role to play in supporting companies on the road towards implementing accountability, there is a fine line to draw between assistance and leniency. The incentives are intended to encourage the uptake of accountability rather than to downplay a DPA's prerogative to take appropriate action where necessary. Thus, for example, using demonstrated accountability as a mitigating factor in an enforcement context or as evidence of due diligence in a contracting context should occur within clearly articulated guidelines. Using demonstrated accountability as a basis for facilitating broader uses of data, such as in a regulatory sandbox setting, should be clearly defined and subject to appropriate oversight. And, when DPAs showcase accountability "best practices" as an incentive for more organisations to implement such practices, they must do so in a way that does not compromise the DPA's subsequent ability to enforce against organisations that purport to adhere to such best practices but failed to do so in practice. In short, any proactive incentivising of accountability, through whatever mechanism, must keep in mind one of the ultimate goals of accountability — enabling trust in the digital economy and society.

V. Conclusion

DPAs have been on the forefront of promoting accountability's broad global acceptance as a comprehensive and coherent framework for the responsible and beneficial use of data, including by advocating for its inclusion in data protection law. In so doing, they have helped to cement accountability's status as the cornerstone of modern data protection. The next chapter in the story of accountability is ensuring its broad-scale adoption and actual implementation across all industries, types and sizes of organisations and regions beyond what is merely required by law. Thus, the next frontier for accountability is for DPAs and law and policy makers to define clear incentives for implementing it. Such incentives will help organisations justify the resources and efforts necessary to maximise their accountability measures where they go beyond the requirements of the law. Taking accountability seriously and proactively incentivising it is essential to creating trust in the digital economy and society and, in fact, will be game-changing in that respect.

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] 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.

[3] 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.

[4] See APEC CBPR and PRP system documents, available at http://www.cbprs.org/GeneralPages/APECCBPRSystemDocuments.aspx.

[5] *Id*.

[6] See EU-US Privacy Shield Framework, available at https://www.privacyshield.gov/Privacy-Shield-Principles-Full-Text.

[7] For example, in the context of Anti-Bribery Legislation, Section 7 of the UK Bribery Act 2010 provides that a relevant commercial organisation is guilty of an offence if a person associated with it bribes another person intending to obtain or retain business or a business advantage. However, it is a defence for the organisation to prove it had "adequate procedures" in place to prevent those associated with it from undertaking such conduct. The UK Ministry of Justice provided guidance on what adequate procedures entail (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.gov.uk/government/uploads/system/uploads/attachment_data/file/181762/bribery-act-2010-guidance.pdf). Adequate procedures include a top-level commitment to preventing bribery; risk assessments of internal and external risks of bribery and due diligence procedures; policies and procedures proportionate to the bribery risks faced by the organisation; communication, including training of bribery prevention policies and procedures throughout the organisation; and monitoring and reviewing procedures designed to prevent bribery by persons associated with it and making improvements where necessary. Concurrently, the Director of Public Prosecutions and the Director of the Serious Fraud Office issued joint guidance for prosecutors setting out the Directors' approach to deciding whether to bring a prosecution under the Bribery Act 2010 (See Bribery Act 2010: Joint Prosecution Guidance of The Director of the Serious Fraud Office and The Director of Public Prosecutions, available at https://www.sfo.gov.uk/?wpdmdl=1456). The guidance notes that "Prosecutors must look carefully at all the circumstances in which the alleged bribe occurred including the adequacy of any anti-bribery procedures. A single instance of bribery does not necessarily mean that an organisation's procedures are inadequate. For example, the actions of an agent or an employee may be wilfully contrary to very robust corporate contractual requirements, instructions or guidance."

Implementing accountable anti-bribery procedures clearly acts as an incentive for organisations not only to achieve compliance with the law or providing a defence in a prosecution proceeding, but to avoid a prosecution altogether when an instance of bribery does occur by a person associated with the organisation. Similarly, in the U.S., the Criminal Division of the United States Department of Justice and the Enforcement Division of the United States Securities and Exchange Commission in their guidance on the U.S. Foreign Corrupt Practices Act, note that "[i]n appropriate circumstances, DOJ and SEC may decline to pursue charges against a company based on the company's effective compliance program, or may otherwise seek to reward a company for its program, even when that program did not prevent the particular underlying FCPA violation that gave rise to the violation." Additionally, the guidance notes that the "DOJ and SEC recognize that positive incentives can also drive compliant behavior. These incentives can take many forms such as personnel evaluations and promotions, rewards for improving and developing a company's compliance program, and rewards for ethics and compliance leadership." See A Resource Guide to the U.S. Foreign Corrupt Practices Act, November 2012, available at https://www.justice.gov/criminal/fraud/fcpa/guidance/guide.pdf at pages 56, 59 and 60.

[8] 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.

[9] *Supra* note 2.

[10] *Id*. at pages 6, 31, 35 and 38.

[11] *Supra* note 2.

[12] For example, the UK Financial Conduct Authority's regulatory sandbox model has supported 60 firms to test their innovations in financial services with real customers in the live market under controlled conditions. See https://www.fca.org.uk/firms/regulatory-sandbox/global-sandbox.

[13] See WP29's WP253 Guidelines on the application and setting of administrative fines for the purposes of the Regulation 2016/679, available at http://ec.europa.eu/newsroom/just/document.cfm?doc_id=47889 at page 15.

[14] *Id*.

[15] *Id*.

[16] In addition to providing specific incentives to organisations, DPAs and law and policy makers should also consider how to incentivise and encourage third-party certification bodies and "Accountability Agents" to become involved in delivering organisational accountability through formal accountability schemes such as certifications. The success of "heightened accountability" through formal accountability schemes such as certifications depends in no small part on the willingness of competent certification bodies and Accountability Agents of all sizes to enter the market.

[17] "Demonstrated accountability" includes all the essential elements of accountability (i.e., leadership and oversight, risk assessment, policies and procedures, transparency, training and awareness, monitoring and verification, and response and enforcement). Thus, the degree to which each of the accountability elements are demonstrably implemented within an organisation will impact the degree to which such implementation can serve as a mitigating factor.

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

[19] Some regulators, as a matter of their statutory duty, already consider the impact on organisations of adopting regulator recommendations as to best practices. Making these determinations for more of their recommendations and suggested best practices will include conducting more detailed impact assessments to measure the costs and benefits to organisations of adopting such practices.