Organizational Accountability in Data Protection Enforcement

How Regulators Consider Accountability in their Enforcement Decisions

October 6, 2021

A CIPL White Paper written in collaboration with Professor Christopher Hodges

20 CIPL
CIPL AT 20 — SHAPING DATA POLICY FOR TOMORROW
HUNTON ANDREWS KURTH

Table of Contents

Recommendations for Data Protection Authorities **3**

I. Executive Summary **4**

II. Background **6**

III. The Shift Towards an Outcomes-Based Approach to Regulatory Oversight **8**

IV. Results and Takeaways from CIPL's Regulator (Including DPAs) Survey **11**

A. Responses from Non-DPA Regulators on Approach to Enforcement and Consideration of Accountability Practices 11

B. Responses from DPAs 12

1. Responses to Questions on Accountability as a Mitigating/Aggravating Factor 12
2. Lack of Consistency in Using Accountability as Mitigating or Aggravating Factor Among EU DPAs 13
3. DPAs' Transparency About their Approach to Enforcement 15

C. Conclusion and Recommendations 18

Appendix **23**

RECOMMENDATIONS FOR DATA PROTECTION AUTHORITIES

- DPAs should continue to align their approach to regulatory oversight and enforcement with the global trend in other regulatory areas towards an outcomes-based approach that emphasizes ex ante engagement, guidance and encouragement of accountable practices.
- DPAs that are able under their laws to consider and give credit for organizational accountability measures in their enforcement actions should recognize as mitigating factors all of the accountability measures that we identified in our survey—e.g., privacy programs, certifications/codes, the effectiveness of any accountability mechanisms, transparency about accountability mechanisms, and cooperation in investigations.
- DPAs should publish externally-facing regulatory strategy documents about their enforcement practices and priorities that clarify the role and value of organisational accountability as a mitigating or aggravating factor, and update them as appropriate.
- DPAs should be transparent to organizations about whether and how they consider demonstrable accountability as a mitigating or aggravating factor, and, at the conclusion of an enforcement matter, inform organizations and the broader public specifically about what accountability measures were considered as mitigating or aggravating factors in determining the course of the enforcement action and any sanctions and fines.
- DPAs should strive to achieve a globally consistent approach to the consideration of accountability mechanisms in enforcement actions.
- Global DPAs, or groupings of DPAs like the European Data Protection Board (EDPB), Global Privacy Assembly (GPA), Asia Pacific Privacy Authorities (APPA) or the Global Privacy Enforcement Network (GPEN), should issue relevant guidelines or best practices for DPAs on the role and use of accountability measures as mitigating and aggravating factors in enforcement.
- Specifically, the EDPB should update the Article 29 Working Party's 2010 Opinion on accountability to provide best practices for how DPAs should consider the use of accountability mechanisms as mitigating factors in enforcement. Similarly, the GPA should adopt guidelines on the operationalization of the Accountability Principle from its 2009 Madrid Resolution that includes how DPAs should consider accountability mechanisms as mitigating factors in enforcement.
- DPAs should also encourage organisational accountability by publishing guidance on best practices for implementing organizational accountability frameworks through privacy management programs, certifications and other mechanisms. Additionally, EU DPAs should link to relevant EDPB and Article 29 Working Party guidance on their websites, as the EDPB needs to play a key role in promoting harmonization in enforcement, and DPAs should recognize its role.
- When drafting or amending data protection laws, law and policy makers should specifically provide that the existence and ability to demonstrate effective organizational accountability measures and frameworks will be considered as mitigating factors in enforcement actions and fining decisions.

I. EXECUTIVE SUMMARY

Promoting organizational accountability among all organizations that process personal data has been one of the Centre for Information Policy Leadership's (CIPL) main areas of focus. An important component of our work on that front has been to identify ways in which data protection laws, public policy, and approaches to enforcement can encourage and incentivize organizational accountability. This paper elaborates specifically on the enforcement component of our previous policy work on accountability.

There is a perception among private sector organizations that global data protection authorities (DPAs) generally do not sufficiently consider in their enforcement and fining decisions, the specific accountability measures that organizations have put in place to prevent violations and harm to individuals. This perception prompted us to reiterate and further elaborate upon a key policy recommendation we made in our 2018 white paper "Incentivising Accountability: How Data Protection Authorities and Law Makers Can Encourage Accountability"—that DPAs should use demonstrable accountability measures that organizations have put in place as mitigating factors in their enforcement and fining decisions. Doing so would clarify to organizations the value of implementing coherent and comprehensive privacy compliance programs and other accountability measures.

To gain a deeper understanding of this particular issue, we also examined what DPAs are actually doing in that regard by trying to answer some of the following questions:

- Apart from any legal requirements to do so, do they have a policy to consider accountability in an enforcement context?
- Are they, in fact, considering accountability in their enforcement actions?
- Are they, like other global regulators in other fields, adopting a more outcomes-based approach to regulatory oversight that includes *ex ante* engagement and encouragement of best practices?
- Are they giving organizations credit for their good faith efforts to implement accountability when establishing fines for privacy violations?
- Are DPAs following a consistent approach globally and across regions, thereby facilitating globally consistent compliance and accountability measures (a critical issue for organizations operating in multiple jurisdictions under a single global privacy compliance and accountability program), or are their approaches to accountability variable and discrepant?
- Do DPAs clearly state their expectations with respect to accountability?

CIPL believes these issues are important. In fact, an increasing number of data protection laws codify the use of demonstrable accountability as mitigating factor in enforcement. This, of course, makes sense, because it encourages accountability. But to build effective compliance and accountability programs, organizations have to know what exactly is being considered as a mitigating factor, how it is being considered and whether DPA expectations are similar across jurisdictions.

To find out how DPAs are using accountability as a mitigating factor, and to better illustrate our longstanding policy argument that accountability can and should be incentivized in this fashion, CIPL partnered with Professor Christopher Hodges of Oxford

University, who has been studying effective regulatory approaches in many other regulatory areas for a long time. Specifically, in late 2020, we decided to jointly collect insights and examples through a survey asking how different national regulators, including DPAs, consider organisations' accountability and compliance frameworks, programs, tools and measures in their enforcement practices. Sixty-five regulators around the world from a variety of fields and sectors (41 DPAs and 24 non-DPAs) responded to our survey asking them about their policies and practices on accountability in enforcement. At a very high level, the survey confirmed the following:

a) many national regulators in other, more established regulatory fields, are recognising accountability as a mitigating factor in their enforcement actions; and

b) DPAs, too, are starting to trend in that direction, but have not yet universally adopted this practice consistently or explicitly articulated it as their regulatory policy.

This white paper elaborates on these conclusions, explains what we learned from the survey, and makes a number of recommendations based both on CIPL's earlier policy work on accountability and the responses to the survey.

II. BACKGROUND

For many years, CIPL has promoted the concept of organizational accountability as an essential building block of effective privacy and data protection. The concept of accountability means that organizations should adopt measures that implement applicable privacy legal requirements and that they should be able to demonstrate the existence and effectiveness of such measures both internally and externally upon request. Effectively, this means that organizations should implement comprehensive data privacy and security programs that cover all aspects of data processing, including collection, use, transfer to third parties and disposal.

Having a comprehensive privacy program in place enables compliance with applicable legal obligations. However, accountability is not only about compliance. An organization's privacy program can often go above and beyond what is required by law. In order to be effective, a privacy program must be operated in such a way as to have the active support of all staff and be fully legitimized within the organization by the most senior leadership and embedded within the organization's ethical culture and values. Organizational accountability provides significant benefits to all stakeholders—the organizations themselves, individuals and regulators. It enables compliance with legal requirements and confers trust and competitive advantages on businesses, provides for consistent and effective protection for individuals and their data, and makes regulators' jobs easier by simplifying investigations and increasing organizational transparency. As such, there are multiple public policy reasons for regulators to encourage organizations to adopt comprehensive privacy programs and all of their constituent accountability measures, controls and tools.

As noted, CIPL previously addressed the issue of how regulators can encourage a more robust uptake of organizational accountability measures in its paper "Incentivising Accountability: How Data Protection Authorities and Law Makers Can Encourage Accountability." In that paper, we discussed the possibility of DPAs using demonstrated accountability as a mitigating factor in enforcement actions as one possible incentive for organizations to adopt accountability practices, even above and beyond what is strictly required by law. The paper also argued that DPAs should formally communicate and be transparent about their policies regarding using accountability as a mitigating factor and specifically refer to them in enforcement cases.

Organizational accountability can be used by DPAs as evidence of good-faith efforts by organizations to comply with relevant legal requirements, and, more broadly, as evidence that an organization is serious about its commitment to privacy protection and responsible data stewardship and has made substantial investments into privacy compliance. The EU's General Data Protection Regulation (GDPR), the Brazilian General Law for the Protection of Personal Data (LGPD), and Singapore's Personal Data Protection Act (PDPA) contain examples of that approach, as they have codified to some extent certain elements of accountability as mitigating factors in an enforcement context (see discussion in Section III below). Additionally, Canada's Office of the Privacy Commissioner and Hong Kong's Privacy Commissioner for Personal Data have both issued guidance on privacy management programs.

In furtherance of this aspect of CIPL's work on organizational accountability, we partnered with Professor Christopher Hodges to determine how and whether regulators are considering accountability measures and the existence of compliance programs in

their enforcement practices. To that end, we conducted a survey of global regulators from a variety of regulatory areas, including DPAs, concerning various aspects of their enforcement policies and practices, including how they were using organizational accountability as a mitigating factor in their fines and sanctions.

Particularly with respect to global DPAs, the purpose of this inquiry was fourfold to:

(1) undergird CIPL's longstanding effort to promote organizational accountability with **empirical data on whether and how DPAs currently encourage its use;**

(2) respond to a general desire among regulated organisations **to understand the current expectations of DPAs** with respect to organizational accountability;

(3) **compare regulatory and oversight practices in data protection and other regulated fields;** and

(4) consider data protection accountability within the broader context of an ongoing **regulatory paradigm shift towards an outcomes-based approach** that prioritizes *ex ante* guidance, engagement and incentives, including encouraging accountability-based compliance, over ex post enforcement and punishment.

The core question at issue in this paper—whether regulators (including DPAs) consider various demonstrable accountability measures in their enforcement decisions—was articulated in the survey as follows:

> [t]o understand the extent to which regulators take into account in their enforcement, sanctioning and fining decisions any frameworks, systems, programs, practices, processes, policies and procedures, measures or tools (collectively "mechanisms") that organizations have put in place to comply with legal requirements or other external standards, or to implement their own internal behavioural objectives, corporate ethics requirements, goals and public promises. Such mechanisms are sometimes referred to as compliance mechanisms, and, in the data protection context, as **accountability mechanisms**.

In the following sections of the paper, we:

a) situate the current issue within the broader context of an ongoing regulatory paradigm shift beyond the area of data protection towards an accountability- and outcomes-based approach to regulatory oversight;

b) summarize and discuss the survey responses from regulators and global DPAs; and

c) make specific recommendations based on our findings.

III. THE SHIFT TOWARDS AN OUTCOMES-BASED APPROACH TO REGULATORY OVERSIGHT

At a high level, the goal of regulatory oversight is to achieve a specific outcome, for example, the protection of personal data. Historically, this has been done through deterrence by enforcing legal requirements through sanctions or punishment, with the idea that the fear of adverse consequences will help to prevent future wrongdoing.

However, deterrence-only regulatory approaches have been subject to extensive criticism. There is considerable evidence showing that, in many cases, deterrence alone may do little to achieve compliance, and thus fails to help regulators accomplish their desired outcomes. Countless studies have found that the threat of sanctions or punishment often have little effect on the decisions an individual makes. And deterrence has been shown to be even less effective when used to regulate organizations, as opposed to individuals. Organizations cannot be treated as if they are a singular entity which make rational decisions in the same way an individual might, and thus deterrence may not reliably impact future corporate behaviour. Nevertheless, many enforcement authorities continue to use deterrence as their primary method of enforcement.

It is simplistic to believe that every action or decision within a company results from either a calculation of costs and benefits, or is governed solely by maximisation of profits. Events can result from mistakes, accidents, confusion, poor judgment on prioritization, and especially from the complexity that arises from integrating multiple people and systems. Thus, the idea of imposing a financial penalty on "the organisation" in the belief that "it" will respond as a single integrated organism and avoid some future actions that result in breaches of a rule simplistic and may not always prove true. Many organisations even treat regulatory fines as an operating cost to be accommodated and prioritized amidst other costs, and as a result, fines do not necessarily lead to the implementation of changes or specific measures that reduce future risk of violation. Effective regulators (and managers) understand this—enforcers often do not.

In recent years, there has been an evolution in regulatory practice away from an enforcement approach based on deterrence towards more of an outcomes-based approach. The OECD defines enforcement as "promoting compliance and reaching regulations' outcomes—e.g., lowering risks to safety, health and the environment, ensuring the achievement of some public goods." This outcomes-based approach focuses on *ex ante* engagement, support and encouragement of organizations to achieve desired outcomes and compliance, for example, through organizational accountability frameworks and measures. The reasoning behind the adoption of this outcomes-based approach is that it is more effective in actually achieving the goal of regulatory enforcement and oversight: getting organizations to comply with the law and to otherwise proactively behave responsibly and ethically. And one of the primary ways to achieve these outcomes has been to encourage and incentivize organizations to implement internal mechanisms that enable these outcomes.

The idea to require companies to have internal compliance and accountability programs largely began in the US, where enforcement agencies were given the ability to lower fines for organizations that had compliance mechanisms in place. CIPL's white paper "Organizational Accountability–Existence in US Regulatory Compliance and its Relevance for a US Federal Privacy Law" looked at several examples of how accountability is ingrained in the US legal system, dating back to the Foreign Corrupt Practices Act

in the late 1970s. Other US examples include the United States Department of Justice's Guidance on *Evaluation of Corporate Compliance Programs*, which lays out criteria for what a corporate compliance program should seek to achieve and contain, and the Sarbanes-Oxley Act, which created a framework for an effective compliance program that has been adapted in other US laws. The approach has also been embraced by enforcement authorities outside the US, like the Australian Competition & Consumer Commission's compliance objectives, which lay out a set of strategies for meeting those objectives, France's anti-corruption agency, which promotes good practices that include elements of accountability and that may be taken into account in case of infringement, and the UK Bribery Act guidance, which includes principles aligned with organisational accountability.

The trend towards an outcomes-based regulatory approach can be seen particularly in regulatory regimes that focus on specific industries and issue areas. Regulators in these sectors typically achieve a detailed understanding of the businesses they are regulating and how they operate. They may also engage with companies about how they operate and perform internally, including relating to their compliance systems. This level of understanding helps regulators target their approach towards regulatory actions that actually can reduce future risk. Indeed, our survey responses indicate that there is a trend among many regulators, including DPAs, towards adopting this outcomes-based approach within the areas of their competence and expertise.

In CIPL's white paper "Regulating for Results: Strategies and Priorities for Leadership and Engagement," we supported such an outcomes-based approach to data protection regulation and enforcement because it provides benefits to individuals, DPAs and regulated organizations. This approach helps individuals by ensuring organizations are proactive in protecting their data, helps DPAs by maximizing use of their often-limited resources to achieve their goals, and provides organizations with clarity as to what is expected of them. Ultimately, the approach serves to achieve the key aims of data protection regulations, which are the protection of personal data, and also to enable the effective use of data for the benefit of society. The OECD's best practice principles for regulatory agencies encourage compliance promotion, including through the use of appropriate materials such as regulatory guidance and compliance toolkits.

As will be discussed below, many DPAs have begun to embrace this approach and consider an organization's efforts to comply with a law through accountability practices, such as privacy programs and certifications, as mitigating factors in enforcement actions. DPAs are also starting to consider and give weight to when organisations' data protection and governance practices go above and beyond compliance with the relevant standards. Some DPAs are even seeking to identify innovative and better solutions to encourage and reward such accountability.

Article 83.2 of the GDPR demonstrates an embrace of the outcomes-based approach, as it specifically directs DPAs to consider certain accountability measures when determining whether to impose an administrative fine and when deciding on the amount of a fine. Those factors include:

- any action taken by the controller or processor to mitigate the damage suffered by data subjects;
- the degree of responsibility of the controller or processor, taking into account technical and organisational measures implemented by them pursuant to Articles 25 and 32;
- the degree of cooperation with the supervisory authority, in order to remedy the infringement and mitigate the possible adverse effects of the infringement;
- adherence to approved codes of conduct pursuant to Article 40 or approved certification mechanisms pursuant to Article 42; and
- any other aggravating or mitigating factor applicable to the circumstances of the case, such as financial benefits gained, or losses avoided, directly or indirectly, from the infringement.

The Brazilian LGPD goes a step further than the GDPR. In addition to incorporating a similar list of mitigating accountability factors in Article 52, it also includes "adoption of policies related to good practice and governance," which is a reference to organizations having comprehensive data governance programs. Similarly, Singapore's PDPA directs its enforcement authority to consider whether an organisation "implemented adequate and appropriate measures for compliance with the requirements under this Act" as a factor in determining a financial penalty for a violation of the Act.

The GDPR's list of possible mitigating factors could have been more explicit that comprehensive privacy management and compliance programs, as well as individual compliance mechanisms, could be mitigating factors. But clearly that is implied in the list, or, at a minimum, not precluded. Most importantly, however, the GDPR, LGPD and PDPA are good examples of taking steps to codify accountability as mitigating factors that DPAs must take into consideration when sanctioning and fining organizations, a practice that squarely reflects an outcomes-based approach to regulatory oversight.

IV. RESULTS AND TAKEAWAYS FROM CIPL'S REGULATOR (INCLUDING DPAS) SURVEY

CIPL and Professor Christopher Hodges surveyed various regulators in fields such as banking/finance, consumer protection, food safety, and telecommunications, as well as DPAs around the world asking about various aspects of their enforcement practices. The survey, among other things, asked specifically about how non-data protection regulators and DPAs take organizational accountability into account in their enforcement actions as mitigating or aggravating factors, as well as about transparency around such practices. The discussion in this Section focuses on the answers to these particular questions.

A. Responses from Non-DPA Regulators on Approach to Enforcement and Consideration of Accountability Practices

We received responses from three governmental agencies, and 21 non-DPA authorities from around the world covering a wide range of sectors. These confirm the conclusions of previous evidence on enforcement policy, notably OECD papers and academic studies, which indicate that there have been a series of linked evolutions in the practice of regulation and enforcement, notably the following:

- The **concept of enforcement** has expanded to include aiming to promote evidence-based and risk-based achievement of regulatory purposes and outcomes (based on desired levels of protection).
- There has been an **expansion in the tools used** by regulators beyond simply prosecution and imposing fines, and regulators are now including the use of soft intervention and tools to achieve compliance.
- There has been an **expansion in the factors taken into account** in both deciding: (a) what action to take and (b) what level of sanction to impose. This has shifted from basing fines essentially on a small number of considerations covering historical (severity of the violation and harm caused) and future (deterrence) elements, to taking a far wider list of relevant factors into account, including accountability factors.
- The **wider list of factors** that regulators take into account generally fall into one of four broad categories:
  - factors relating to the violation and/or harm caused (severity, nature of harm, duration, number of people/organisations harmed);
  - factors relating to actions by the infringer *before* or *at the time of* commission of the infringing act (e.g., previous record of compliance or infringement; preventative steps and systems taken (such as implementing compliance and accountability programs, tools and measures), adherence to approved codes or certifications; motivation, intention, negligence, recklessness, degree of responsibility);
  - factors relating to the infringer's behaviour *after* the infringement (e.g., action taken to cease or mitigate breach/harm; speed of reaction; actions taken to inform those harmed, the authority and relevant others; degree of cooperation with the authority and others); and
  - factors of *general application* (e.g., whether there are any other aggravating or mitigating factors; extent of any financial benefits gained, or losses avoided, from the infringement).

- Almost all of the non-DPA authorities that responded to this study take aggravating and mitigating factors into account in enforcement and almost all of them consider accountability factors specifically. They also consider a broad range of factors and usually all the factors included in Article 83.2 of the GDPR (or equivalent). Only one respondent reported that it takes no mitigating factors into account, and three appeared to take no or limited aggravating factors into account.
- A clear trend towards **greater transparency** on the approach taken to enforcement. Only one of the non-DPA authorities in this study had not published information on its approach to fines or enforcement.

In conclusion, almost all the non-DPA authorities who responded to this survey are taking organizational accountability measures into account in their enforcement actions, albeit to varying degrees and with varying levels of transparency as to which specific accountability measures.

B. Responses from DPAs

1. Responses to Questions on Accountability as a Mitigating/Aggravating Factor

As part of the survey, we asked DPAs if they were considering the following accountability mechanisms as mitigating or aggravating factors:

- existence of frameworks, programs, processes, measures or other tools that organizations have put in place to comply with legal requirements;
- having a relevant certification or participation in a code of conduct;
- the effectiveness of an organization's accountability mechanisms;
- an organization's transparency about its accountability mechanisms; and
- an organization's current or historic cooperation in an investigation or enforcement context.

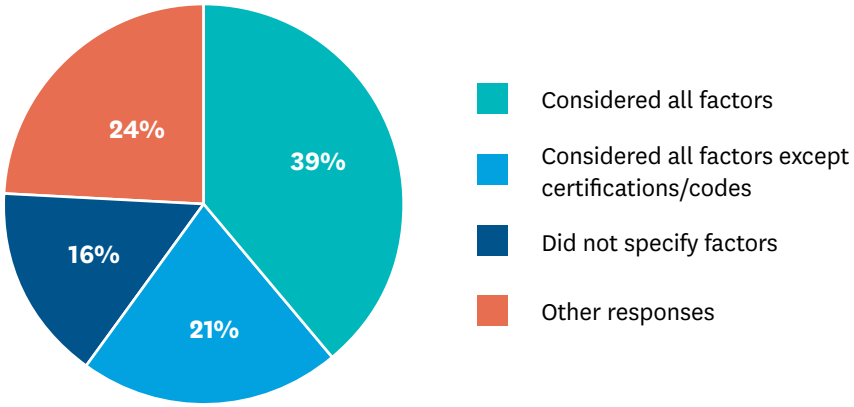
We sent the survey to 59 DPAs worldwide and received responses from 41 of them, the majority of which came from Europe, but also from DPAs in North America, South America, and the Asia-Pacific region. The vast majority of DPAs responded that they take at least some elements of organizational accountability into account as either mitigating or aggravating factors in enforcement actions. In fact, only three of the 41 respondents did not clearly state that they take at least one of these factors into account, and those three respondents either did not provide clear answers to the survey questions, or noted that the questions were not relevant to their authority as they did not levy fines. Additionally, one of the respondents is a new DPA that is not yet fully operational, but indicated its intent to consider these factors in the future. This result, in and of itself, reflects that DPAs are embracing an outcomes-based approach to enforcement rooted in organizational accountability. A large majority of DPAs are taking into account, and, therefore, indirectly encouraging and rewarding, elements of organizational accountability in the context of their enforcement actions.

Of the 38 DPAs that responded that they consider (or will consider in the future) at least one of the accountability factors from our survey in their enforcement actions, the responses broke down as follows:

- 39% of DPAs responded that they take all of the mitigating and aggravating factors into account, although some specifically noted that they make such decisions on a case-by-case basis;
- 21% of DPAs, most of which are based in the EU, responded that they take all of the factors into account except for "having/not having a relevant certification, label, or participating/not participating in a relevant code of conduct" as a mitigating and/or aggravating factor. Many of them noted that they did not do so because certifications and codes of conduct under the GDPR were not yet available (at the time of the survey);

- 16% of DPAs responded that they take (or will take) some of the mitigating and aggravating factors into account, but did not specify which ones; and
- The remaining 24% of DPAs all responded that they take some of the factors into account, and do not consider other factors, but there was no consistent theme among them on which factors they did or did not consider. Interestingly, a majority of these DPAs considered different sets of factors despite being subject to the same rules in the GDPR.

All DPA Responses on Accountability in Enforcement

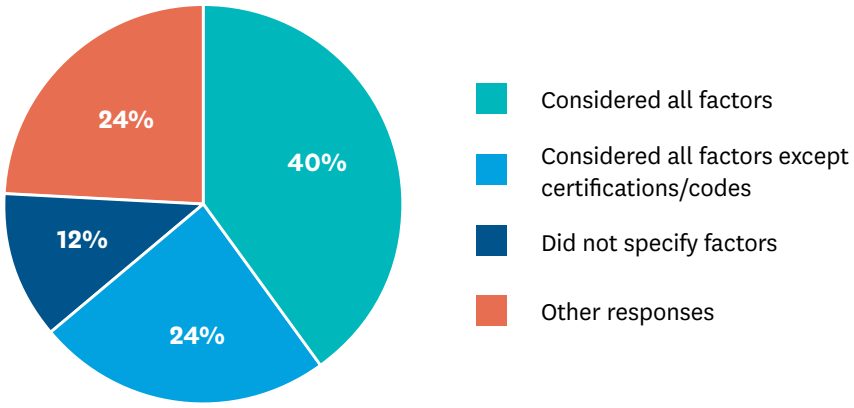


Thus, based on their survey responses, DPAs clearly are taking organizational accountability measures into account in their enforcement actions, albeit to varying degrees. We note, however, that there is room for greater consistency among the DPAs' practices. This is particularly true in the case of EU DPAs, all of which enforce the same regulation—the GDPR—including Article 83.2. Based on their shared law and due to their similar approaches to oversight and enforcement, EU DPAs could have been expected to have more consistent responses to the survey.

2. Lack of Consistency in Using Accountability as Mitigating or Aggravating Factor Among EU DPAs

Of the 41 responses we received, 61% were from DPAs subject to the GDPR. Among these, there was a sizeable disparity in their responses about which particular accountability measures they consider in their enforcement actions.

EU DPA Reponses on Accountability in Enforcement



On a positive note, we noticed some consistency in the accountability factors that a majority of EU DPAs are considering. 40% of EU DPAs responded that they do or would consider taking all of the specified mitigating and aggravating factors into account. Another 24% of EU DPAs considered all factors except for certifications as aggravating or mitigating factors. However, given that GDPR certifications and codes of conduct under the GDPR were not yet available at the time of the survey, and that several of the DPAs cited that as the reason they did not include them as mitigating or aggravating factors, it is probably fair to say that there is strong consistency in considering organizational accountability in enforcement among those 64% of DPAs.

The remaining DPAs, however, illustrate the lack of consistency referred to above, and can be categorized as follows:

- Three DPAs simply cited to Article 83.2 of the GDPR in response to the questions about accountability, but did not specify which of the factors from the questionnaire they considered as mitigating or aggravating factors. While these DPAs did recognize that organizational accountability is addressed by Article 83.2, it is difficult to know how to interpret these responses and what they actually mean for how these DPAs are considering accountability in their enforcement actions.

  The remaining six DPAs' responses all answered the questions directly, but specifically omitted one or more of the other mitigating or aggravating factors:

- One DPA responded that the existence of accountability frameworks and cooperation in an investigation were the only factors it might consider as mitigating factors, though it had not yet established a practice of considering accountability frameworks. This DPA also responded that it would consider lack of implementation, transparency or demonstrability of accountability mechanisms and misrepresentation as aggravating factors.

- Another DPA responded that they do not consider the effectiveness of an organization's accountability mechanisms or its transparency around its accountability mechanisms as mitigating or aggravating factors in enforcement actions.

- Another DPA took all stated factors into account as mitigating factors except for transparency concerning the existence of relevant compliance mechanisms and the level of cooperation with the DPA, because both of these items are required under their data protection law. However, that DPA does take into account the effectiveness of such mechanisms as a mitigating factor. Further, that DPA may possibly take into account not having a relevant certification or not participating in a code into account as an aggravating factor on a case-by-case basis.

- Another DPA responded that they considered all mitigating factors to the extent they exceed what is legally required. If the stated accountability measures are not legally required, they are not considered as aggravating factors. However, if an organization commits to voluntary accountability tools but fails in that commitment, it can be an aggravating factor.

- Another DPA responded that they do not take transparency about accountability mechanisms into account as a mitigating factor, but did not provide an explanation as to why.

- Another DPA responded that they do not consider a misrepresentation of accountability mechanism as an aggravating factor.

Ultimately, there is a lack of consistency with which accountability factors EU DPAs are considering as mitigating or aggravating factors.

Consistency from DPAs regarding which accountability practices are considered in enforcement is incredibly important for organisations that operate across multiple jurisdictions, or even globally, because they often have a single privacy compliance

and management program for their entire organization. Such unified programs significantly improve their effectiveness and efficiency, but regulatory inconsistencies around basic concepts, such as accountability, undermine these goals. The greater the agreement on this issue across regulators, the better organizations can implement effective and consistent accountability measures, controls and tools across their national operations. The apparent lack of consistency with which accountability factors EU DPAs are considering sends a confusing message to organisations about what proactive steps they should be taking. It also creates uncertainty regarding whether having particular accountability measures in place, such as comprehensive privacy compliance programs, will earn organizations some credit in an enforcement context.

Of course, some inconsistencies among EU DPAs on how to apply accountability measures as a mitigating factor are also understandable. The GDPR is still new, and data protection regulation and the necessary DPA oversight, supervision and responses are a rapidly evolving space. Further, national administrative procedures have not been aligned as part of the effort to harmonise data protection laws. Hence, it is perhaps unsurprising that DPAs, at this stage, may not yet have the same ideas about how to consider, acknowledge and reward accountability.

However, CIPL believes that consistency in considering accountability measures in GDPR enforcement must be a top priority for EU DPAs and the EDPB, given that one of the primary purposes behind the passage of the GDPR was to harmonize data protection regulation across the EU. While this lack of consistency may simply be due to differences in maturity among DPAs and may improve over time, any lack of consistency in enforcement threatens the goal of harmonization, and must be addressed promptly. It also misses an opportunity to specifically encourage and reward organizational accountability as one of the cornerstone requirements of the GDPR under Articles 5.2 and 24 by way of giving it "due regard" in an enforcement context under Article 83.2. The EDPB should work with DPAs to improve their practices so that accountability mechanisms are considered consistently across the EU.

3. DPAs' Transparency About their Approach to Enforcement

In addition to the questions about accountability mechanisms as mitigating/aggravating factors, we also asked DPAs three questions about their transparency regarding enforcement practices and accountability mechanisms:

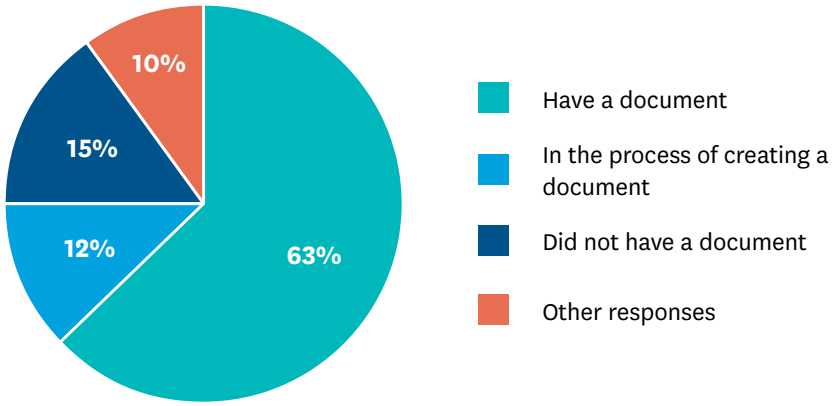
- Whether they had an externally-facing policy or document establishing or describing their enforcement approach and priorities;
- Whether they had examples of cases where they used accountability mechanisms as a mitigating/aggravating factor; and
- Whether they or another relevant authority had published precedents, guidelines, or requirements on best practices with respect to such accountability mechanisms.

Transparency from DPAs regarding their enforcement practices is an essential component of a results-based approach to data protection regulation. It is important for organizations to understand how regulators value (or don't value) particular accountability measures in an enforcement context. Clarity on what is expected can encourage a race to the top among organizations. The responses to our transparency questions indicate that many DPAs around the world are demonstrating strong transparency practices regarding their enforcement practices generally. Yet it is not clear that DPAs are effectively and consistently communicating to organizations and the wider public specifically about how accountability is being considered in enforcement.

In response to the question on whether they have an externally-facing policy or document describing their enforcement approach and priorities, of the 41 DPAs that responded to the survey:

- 63% of DPAs responded that they did, in fact, have such a policy or document;
- 12% of DPAs said that, while they do not currently have such a document, they are in the process of creating one;
- 15% of DPAs said that they did not have such a document at all; and
- The remaining 10% of DPAs either did not directly answer the question, or mentioned documents or websites that did not appear to directly meet the criteria of the question.

DPA Responses on Externally-Facing Enforcement Documents

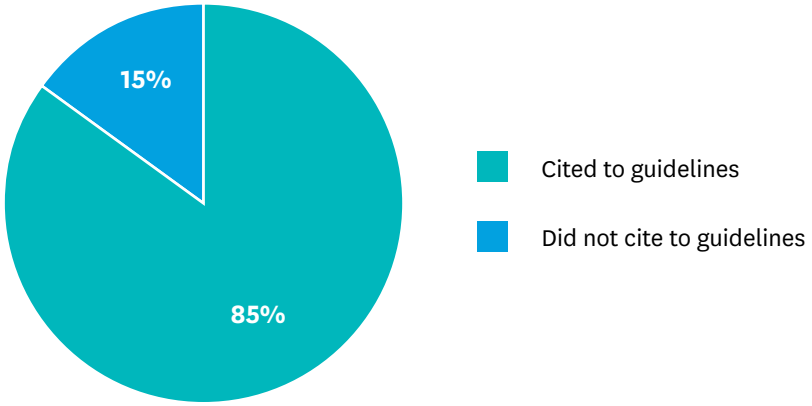


Generally, the responses to this question portrayed a fairly positive outlook globally, as 75% of respondents, including all 16 non-EU respondents, either have such a document describing their enforcement approach and priorities or will have one soon.

However, it is noteworthy that the 25% of respondents who either did not have such a document or did not provide a clear answer to the question are *all* located within the EU and are charged with enforcing the GDPR. While the GDPR does not provide for an obligation for DPAs to publish such document, failing to publish one is a missed opportunity from DPAs to provide transparency on their enforcement strategy, as well as how they consider elements of accountability as mitigating or aggravating factors. This lack of transparency, as with the lack of consistency, hinders the encouragement of accountability under the GDPR. However, it should be noted that the responses to this question may be the result of EU DPAs choosing different priorities among the sheer number of competing GDPR upstart issues that they must grapple with.

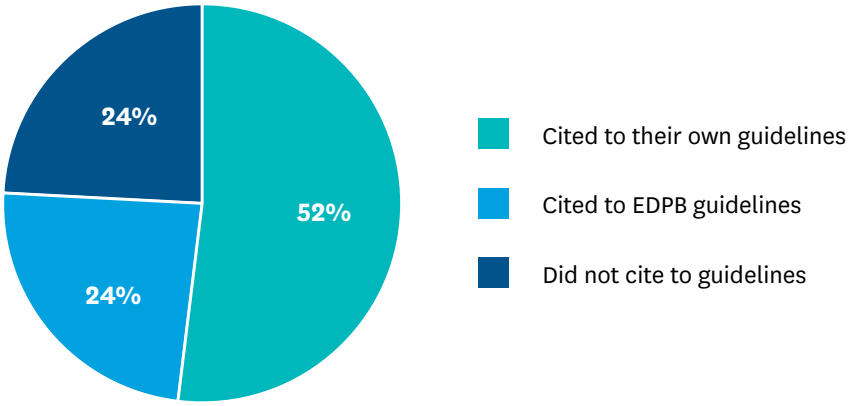
In response to the question regarding publishing precedents, guidelines or requirements on best practices with respect to accountability mechanisms, 85% of DPAs responded that either they or the EDPB had published such guidelines, or that they plan to issue these guidelines in the near future. These responses generally indicate that DPAs understand the importance of both transparency around their own enforcement practices, and are promoting the use of accountability mechanisms by organisations.

DPA Responses on Guidelines on Accountability Best Practices



However, while a majority of EU DPAs cited to guidelines on best practices (or indicated plans to issue such guidance), with some citing to their own guidance and others citing to EDPB guidance in response, 24% of EU DPAs responded that neither they nor another relevant authority had published such guidelines.

EU DPA Responses on Guidelines on Accountability Best Practices



Based on these responses, it is fair to ask why some EU DPAs cited to EDPB guidelines and others did not. While this could just be an oversight by these DPAs or based on a misunderstanding or narrow reading of the survey question, one possibility is that despite the EDPB's guidance on considering compliance mechanisms when determining fines, some or all of these DPAs may not have the guidance at the top of their mind in their activities. Alternatively, it could mean that these DPAs understood the question concerning published precedents, guidelines or requirements on best practices for accountability mechanisms not to cover how these mechanisms are considered in an enforcement context. The more likely explanation, we believe, is that DPAs have been busy with the many GDPR-related implementation issues they are faced with and that they simply have not been able to do everything at once. Regardless of the reason, these responses show that DPAs may be overlooking important mitigation factors that the GDPR would allow them to consider. As such, a fair takeaway is that work remains to be done for DPAs around clarifying their expectations with respect to implementing accountability measures, as well as their practices with respect to considering accountability as a mitigating and aggravating factor in enforcement.

On the other hand, a few of the DPAs who responded to our survey provided outstanding examples of this practice, and these should serve as models for other DPAs:

- One DPA publishes all of its enforcement decisions on its website and indicated it was standard practice, when relevant, to walk through the mitigating/aggravating factors laid out in its privacy law to illustrate how it came to the penalty it ultimately imposed.
- Other DPAs provided specific examples in their responses, such as how one DPA decided to issue a correction order instead of a fine when an organization proved that it was in compliance with a demonstrated certification.
- Another DPA levied a higher fine because an organization's internal processes were not adequately aligned with the risk posed by its processing, and noted that they specifically walk through this analysis in their published decisions.

DPAs should universally adopt such practices to help organizations understand how their accountability measures are being taken into account in particular enforcement actions. These practices help to illustrate regulators' priorities so that peer organisations who are following regulatory action against other organizations may correct their own accountability controls and tools as a result of these enforcement action. Indeed, some organisations report being unaware of how their accountability practices have been considered as mitigating factors in particular enforcement matters. This may demonstrate an absence of transparency by DPAs around the mitigating role of accountability in particular enforcement cases. However, transparency about DPA expectations with respect to the *ex ante* implementation of accountability measures, and about how such measures are being considered *ex post* in an enforcement context, are key pieces of an outcomes-based approach to regulation.

C. Conclusion and Recommendations

Nearly all of the DPAs who responded to our questionnaire are considering accountability mechanisms in their enforcement practices in some capacity, and thus are at least partially aligned with an outcomes-based approach to regulation and oversight. Indeed, it is encouraging that such a large percentage of the respondents are considering organizational accountability in their enforcement decisions. Yet, there is a lack of consistency in the accountability mechanisms that they are considering, particularly among the EU DPAs. Moreover, DPAs are not clearly and consistently communicating and being transparent about the types of accountability measures they consider and whether they use them as mitigating or aggravating factors in their enforcement decisions. Improving DPA practices and transparency with respect to these issues will go a long way towards promoting and encouraging organisations to adopt accountability practices, which in turn will help DPAs achieve their goal of ensuring that organisations are sufficiently protecting individuals' data.

CIPL recommends the following:

- DPAs should continue to align their approach to regulatory oversight and enforcement with the global trend in other regulatory areas, towards an outcomes-based approach that emphasizes *ex ante* engagement, guidance and incentives for accountable practices.
- All DPAs that are able, under their laws, to consider and give credit for organizational accountability mechanisms in their enforcement actions, should embrace all the factors we included in our survey as mitigating (or aggravating) factors:

  a) **existence** of any frameworks, systems, programs, processes, practices, policies and procedures, measures or tools that organizations have put in place to comply with legal requirements or other external standards, or to implement their own internal behavioural objectives, corporate ethics requirements, goals and public promises;

  b) **having** a relevant certification, label, seal, or **participating** in a code of conduct;

c) the **effectiveness** of an organization's current accountability mechanism(s) and instruments set forth in a) and b) above, and how they are operated;

d) an organization's **transparency** around the existence of the mechanisms or instruments described in a) and b) above, and the organization's ability to demonstrate their existence and effectiveness;

e) an organization's **current or historic cooperation** with the DPA in an investigation or enforcement context, including in connection with questions around the existence or effectiveness of any mechanisms or instruments described in a) and b) above; and

f) other relevant factors.

- Every DPA should publish an externally-facing document regarding its enforcement practices and priorities which includes information about how it is considering accountability mechanisms as a mitigating or aggravating factor in its enforcement actions, and what such accountability mechanisms might include and look like. This document should be updated regularly and published on the DPA's website.
- In the context of specific enforcement proceedings, DPAs should advise organizations whether and how they are considering demonstrable accountability measures that organisations had put in place as a mitigating factor in setting a fine. At the conclusion of an enforcement matter, DPAs should inform organizations, and the broader public specifically, about what accountability measures were considered as mitigating or aggravating factors in determining the course of the enforcement action and any sanctions and fines. Also, they should advise organisations whether and how they are using the absence of relevant accountability measures as an aggravating factor.
- All DPAs (particularly if enforcing the same law(s)) should develop a globally consistent approach to their consideration of accountability mechanisms as mitigating or aggravating factors in their enforcement actions.
- Global DPAs, or groupings of DPAs, like the European Data Protection Board (EDPB) or Global Privacy Enforcement Network (GPEN), should publish relevant guidelines or best practices on the role and use of accountability measures as mitigating and aggravating factors in enforcement.
- Specifically, the EDPB should update the Article 29 Working Party's 2010 Opinion on accountability to provide best practices for how DPAs should consider the use of accountability mechanisms as mitigating factors in enforcement. Similarly, the GPA should adopt guidelines on the operationalization of the Accountability Principle from its 2009 Madrid Resolution that includes how DPAs should consider accountability mechanisms as mitigating factors in enforcement.
- All DPAs should encourage organisational accountability by publishing their own guidance on best practices for implementing organisational accountability frameworks through privacy management programs, certifications and other mechanisms. Additionally, EU DPAs should clearly endorse and link to relevant EDPB and Article 29 Working Party guidance on their websites.
- When drafting or amending data protection laws, law and policy makers should codify the use of organizational accountability measures as mitigating and aggravating factors, specifically providing that the existence and ability to demonstrate organizational accountability measures and frameworks will be considered as mitigating factors in the context of enforcement actions and fining decisions.

If you would like to discuss any of our comments in this paper, or require additional information, please contact Bojana Bellamy, bbellamy@HuntonAK.com; Markus Heyder, mheyder@HuntonAK.com; or Sam Grogan, sgrogan@HuntonAK.com.

1 CIPL is a global privacy and data policy think tank in the law firm of Hunton Andrews Kurth LLP and is financially supported by the law firm and 80 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/.

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

3 See CIPL white papers on "The Case for Accountability: How it Enables Effective Data Protection and Trust in the Digital Society," July 23, 2018, available at https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_accountability_paper_1_-_the_case_for_accountability_-_how_it_enables_effective_data_protection_and_trust_in_the_digital_society.pdf; CIPL Accountability Q&A, July 3, 2019, available at https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_accountability_q_a__3_july_2019_.pdf; and "What Good and Effective Data Privacy Accountability Looks Like: Mapping Organizations' Practices to the CIPL Accountability Framework," June 3, 2020, available at https://www.informationpolicycentre.com/organizational-accountability.html.

4 *See* endnote 2 above.

5 Examples from the "Incentivising Accountability" paper of how accountability can be used by DPAs as a mitigating factor in an investigation or enforcement context include: (a) as one of the discretionary factors in considering whether to initiate an enforcement action; (2) as a mitigating factor in assessing the types of sanctions and levels of fines; or (3) as a mitigating factor in case of an individual failure or human error, where the organization is able to demonstrate that it took the reasonable precautions to prevent the failure or error.

6 GDPR, Art 83.2.

7 LGPD, Article 52, §1, I-IX (e.g., IX provides for consideration of "adoption of policies related to good practice and governance" which is an express reference to organizational data protection programs).

8 Singapore Personal Data Protection Act 2012, Sec. 11-12 & Sec. 48J(6)(e). Singapore's Personal Data Protection Commission also issued a "Guide to Accountability under the Personal Data Protection Act" in March, 2020, available at https://www.pdpc.gov.sg/-/media/Files/PDPC/PDF-Files/Other-Guides/Guide-to-Accountability.pdf?la=en.

9 Similarly, the US Federal Trade Commission (FTC) has required organizations to implement such comprehensive accountability and privacy compliance programs in many of its privacy consent orders. This reflects the premium the FTC places on organizations having such programs and indicates that it will treat their pre-enforcement existence as a mitigating factor. See CIPL white paper on "Organizational Accountability in Light of FTC Consent Orders," November 13, 2019, available at https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_white_paper_-_organizational_accountability_in_light_of_ftc_consent_orders__13_november_2019_.pdf. Additionally, Canada's proposed Consumer Privacy Protection Act, which updates and amends its Personal Information Protection and Electronic Documents Act, contains a requirement for organizations to "implement a privacy management program that includes the organization's policies, practices and procedures put in place to fulfil its obligations under [the] Act," available at https://parl.ca/DocumentViewer/en/43-2/bill/C-11/first-reading.

10 Office of the Privacy Commissioner of Canada, "Getting Accountability Right with a Privacy Management Program," April 2012, available at https://www.priv.gc.ca/media/2102/gl_acc_201204_e.pdf.

11 Privacy Commissioner for Personal Data, Hong Kong, "Privacy Management Programme, A Best Practice Guide," August 2018, available at https://www.pcpd.org.hk/pmp/files/pmp_guide2018.pdf.

12 See Appendix A for the Questionnaire for "Joint Project on Regulatory Enforcement Policy and Practice by the Centre for Information Policy Leadership (CIPL) and Professor Christopher Hodges."

13 "A common theme in these discussions [of the UK finance industry sponsored by the FCA] was fear. Fear of the short-term focus on profit and expectations of shareholders, elevated in importance by financial KPIs and short time horizons for reporting. Fear of regulators, and the potential for inadvertently breaching an obscure rule, making regulation a distraction. And fear of being the first mover to do the right thing and getting left behind a pack not yet willing to make a collective bold and purposeful move.": *Transforming culture in financial services. Driving purposeful cultures. Discussion paper* (Financial Conduct Authority, March 2020), DP20/1.

14 E. Soltes, *Why do they do it: Inside the Mind of the White-Collar Criminal* (Public Affairs, 2016); D. Gentilin, *The Origins of Ethical Failures. Lessons for Leaders* (Routledge, 2016); D. Beunza, *Taking the Floor. Models, Morals, and Management in a Wall Street Trading Room* (Princeton University Press, 2019).

15 The OECD considers that many errors result from lack of awareness, motivation or capacity: *reducing the Risk of Policy Failure: Challenges for Regulatory Compliance* (OECD, 2000). An extensive empirical study into major examples of corporate wrongdoing found that in post-1970 common law countries, corporate regulation is reactive in nature, and has little role to play in moderating future compliance behaviour. L. Hail, A. Tahoun and C. Wang, "Corporate Scandals and Regulation" (2018) 56(2), *Journal of Accounting Research* 617-671.

16 C. Hodges and R. Steinholtz, *Ethical Business Practice and Regulation: A Behavioural and Values-Based Approach to Compliance and Enforcement* (Hart, 2017); Y. Feldman, *The Law of Good People. Challenging States' Ability to Regulate Human Behaviour* (Cambridge University Press, 2018).

17 *Regulatory Enforcement and Inspections*, OECD Best Practice Principles for Regulatory Policy (OECD, 2014). Achieving desired outcomes is also an issue recommended to be used in evaluation of the performance of regulators: *OECD Regulatory Enforcement and Inspections Toolkit* (OECD, 2018), 15.

18 A leading example is *Evaluation of Corporate Compliance Programs. Guidance Document* (US Department of Justice, updated April 2019).

19 See CIPL white paper on "Organizational Accountability—Existence in US Regulatory Compliance and its Relevance for a US Federal Privacy Law," July 3, 2019, available at https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_white_paper_on_organizational_accountability_-_existence_in_us_regulatory_compliance_and_its_relevance_for_a_federal_data_privacy_law__3_july_2019_.pdf.

20 Public Law 95-213: Foreign Corrupt Practices Act of 1977 (91 Stat. 1494; 1977), available at https://www.govinfo.gov/content/pkg/STATUTE-91/pdf/STATUTE-91-Pg1494.pdf.

21 D. Tokar, "How the Justice Department Incentivizes Companies to Invest in Compliance," The Wall Street Journal, Dececember 24, 2019, https://www.wsj.com/articles/how-the-justice-department-incentivizes-companies-to-invest-in-compliance-11577183403.

22 Public Law 107-204: Sarbanes-Oxley Act of 2002. (116 Stat. 745; 30 July 2002), available at https://www.congress.gov/107/plaws/publ204/PLAW-107publ204.pdf.

23 For a broader discussion on global laws that have embraced accountability, see CIPL White Paper on Organisational Accountability — Past, Present and Future, 30 October 2019, available at https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_white_paper_-_organisational_accountability_%E2%80%93_past_present_and_future__30_october_2019_.pdf.

24 *2020 Compliance and Enforcement Policy and Priorities* (ACCC, 2020).

25 These include: senior management commitment to implementing a culture of integrity, transparency and compliance; the adoption of internal codes of conduct implementation of whistle-blowing systems; mapping risks and implementing internal controls and audits; and the training of staff on corruption risks. Available at https://www.vie-publique.fr/en-bref/19802-lutte-anticorruption-publication-du-referentiel-francais.

26 These include proportionate procedures, top-level commitment, risk assessment, due diligence, communication and training, monitoring, and review. Available at https://www.justice.gov.uk/downloads/legislation/bribery-act-2010-guidance.pdf.

27 See CIPL White Paper on "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.

28 *Regulatory Enforcement and Inspections, OECD Best Practice Principles for Regulatory Policy* (OECD, 2014).

29 GDPR, Art 83.2.

30 Brazil Law No. 13.709 of 14 August 2018, General Personal Data Protection Law (as amended by Law No. 13.853 of 8 July 2019) (LGPD), Article 52 § 1. Notably, Article 50 of the LGPD also explicitly requires the implementation of a comprehensive privacy program, which the GDPR does not require.

31 Singapore Personal Data Protection Act 2012, Sec. 48J(6)(e).

32 The survey was distributed to non-DPA regulators through the International Network for Delivery of Regulation (INDR) Non-DPA regulators. The same survey was sent directly to 42 DPAs in Europe, the Asia-Pacific region, and the Americas. 41 DPAs Responded. A deeper analysis of all responses to the questionnaire, from both DPAs and other global regulators, will be published by Professor Hodges at a later date.

33 Australian Competition and Consumer Commission (ACCC); Australian Financial Security Authority (AFSA); Belgian Institute for Postal Services and Telecommunications (BIPT), Belgium; the Central Bank of Brazil; Brazilian National Telecommunications Agency (ANATEL); Administrative Council for Economic Defence (CADE), Brazil; National Civil Aviation Agency (ANAC), Brazil; Safety and Chemicals Agency (TUKES), Finland; the Federal Financial Regulatory Authority (BaFin), Germany; Banca d'Italia; the Regulatory Authority for Energy, Networks and Environments (ARERA), Italy; Inspectorate for Education, The Netherlands; the Authority for Consumers and Markets (ACM), the Netherlands; the Radiocommunications Agency, the Netherlands; the National Regulatory Authority for Communications (NRA), Malta; the Office of Electronic Communication (UKE), Poland; Financial Supervision Authority (KNF), Poland; the Monetary Authority of Singapore; the National Competition Authority and Regulatory Authority for Telecommunications, Energy, Postal Services, Railway Infrastructure, Airport Tariffs and Media (CNMC), Spain; Food Standards Agency (FSA), UK; Solicitors Regulatory Agency (SRA), UK; Office for Product Safety and Standards (OPSS), UK.

34 *OECD Best Practice Principles for Regulatory Policy: Regulatory Enforcement and Inspections* (OECD, 2014); *OECD Regulatory Enforcement and Inspections Toolkit* (OECD, 2018); *Better Regulation Practices across the European Union* (OECD, 2020).

35 C. Hodges, *Law and Corporate Behaviour: Integrating Theories of Regulation, Enforcement, Culture and Ethics* (Hart Publishing, 2015).

36 An example of evolution in an already sophisticated and wide-ranging approach can be seen by comparing *Enforcement Policy* (Department for Business, Energy & Industrial Strategy, Office for Product Safety and Standards, 2018) with *Enforcement Policy* (Department for Business, Energy & Industrial Strategy, Office for Product Safety and Standards, 2021), section 3.

37 Among various examples of the wider approach are those in financial services: *FCA Mission: Approach to Enforcement* (UK Financial Conduct Authority, 2019); *Enforcement* (Monetary Authority of Singapore, 2018).

38 Examples are using advice, recommendations and requests (TUKES, Finland; many UK authorities; the Education Inspectorate in the Netherlands) and achieving redress of consumer harm (numerous authorities in Nordic states and UK, the Australian AICO, and others).

39 It is not our purpose to match the practice of considering accountability as a mitigating factor to the relevant governing laws in the various jurisdictions. Some global regulators, DPAs and non-DPAs, have historically considered mitigating factors on the basis of their enforcement or prosecutorial discretion with or without statutory authority to consider specific mitigating factors. Our purpose is mainly to consider whether there is a trend globally towards more outcomes-based enforcement practices. Laws, like the GDPR and LGPD that explicitly incorporate such practices are valuable evidence of the trend towards an outcomes-based approach, but the trend may not necessarily depend on them alone.

40 Albania's Information and Data Protection Commission, Australia's Office of the Australian Information Commissioner, Austria's Data Protection Commission, Brazil's ANPD, Bulgaria's Commission for Personal Data Protection, Canada's Information and Privacy Commissioner of Ontario, Canada's Office of the Privacy Commissioner, Croatia's Data Protection Agency, Czech Republic's Office for Personal Data Protection, Finland's Data Protection Ombudsman, France's CNIL, Germany's Federal Data Protection Commissioner, Gibraltar Regulatory Authority, Greece's Hellenic Data Protection Authority, Guernsey's Office of the Data Protection Authority, Hong Kong's Office of the Privacy Commissioner for Personal Data, Hungary's Parliamentary Commissioner for Data Protection and Freedom of Information, Iceland's Data Protection Authority, Ireland's Data Protection Commissioner, Israel's Privacy Protection Authority, Japan's Personal Information Protection Commission, Jersey Office of the Information Commissioner, Latvia's State Data Inspectorate, Lithuania's State Data Inspectorate, Malta's Office of the Information and Data Protection Commission, Mexico's INAI, Mexico's INFOEM, Netherlands' Data Protection Commission, New Zealand's Privacy Commissioner's Office, Philippines' National Privacy Commission, Poland's Personal Data Protection Office, Portugal's National Data Protection Commission, Romania's National Supervisory Authority for Personal Data Protection, Serbia's Commissioner for Information of Public Importance and Protection of Personal Data, Singapore's Personal Data Protection Commission, Slovakia's Office for Personal Data Protection of the Slovak Republic, Slovenia's Information Commissioner of the Republic of Slovenia, Sweden's Data Inspection Board, Switzerland's Federal Data Protection and Information Commissioner, UK's Information Commissioner's Office, United States' Federal Trade Commission.

41 The subsequent analysis in this paper is based *only* on the self-reported responses to our survey, which was conducted in late 2020, and does not consider any known or unknown contrary practices of the surveyed DPAs.

42 An important caveat to the conclusions drawn from the DPAs' self-reported approach on this matter is (limited) anecdotal information from organizations that have been subject to enforcement actions. These organizations have said that some DPAs that claim to use demonstrated accountability as a mitigating factor have not, in fact, inquired into, or noticeably relied upon as a mitigating factor, any demonstrable accountability measures the organizations had put in place in the DPAs' enforcement actions against the organization. This may suggest that (a) there is a disconnect between such DPAs' stated enforcement policies and actual enforcement practices, or (b) such DPAs have not been sufficiently transparent in their enforcement and fine setting approach, or clearly articulated the role of accountability as a mitigating (or aggravating factor).

43 The EDPB has acknowledged that the differing approaches in enforcement between DPAs stem, in particular, from the lack of harmonized procedures and administrative laws, and is currently working to address this. See EDPB Programme 2021-2022.

44 For the purposes of this paper, the UK was considered a "DPA subject to the GDPR" and part of the EU, as the survey was sent to DPAs in 2020.

45 Spain and the Netherlands have already approved national codes of conduct, however. Belgium and France have also approved codes of conduct for cloud service providers since the survey was conducted.

46 These DPAs all cited generally to the EDPB's GDPR Guidelines, Recommendations and Best Practices, but only one of them named a specific document. The guidance that appears to be most relevant, and which one country named, is the Article 29 Working Party's WP 253/17: "Guidelines on the application and setting of administrative fines for the purposes of the Regulation 2016/679," which were adopted on 3 October 2017. However, other potential relevant EDPB guidelines include: "Guidelines 1/2018 on certification and identifying certification criteria in accordance with Articles 42 and 43 of the Regulation," Version 3.0, 4 June 2019, p. 6, which mentions certifications as a mitigating or aggravating factor when deciding when to impose a fine and when deciding on the amount of the fine; and "Guidelines 1/2019 on Codes of Conduct and Monitoring Bodies under Regulation 2016/679," Version 2.0, 4 June 2019, p. 11, which mentions that adherence to an approved code of conduct will be considered by supervisory authorities when imposing an administrative fine. One country mentioned that the EDPB had issued three guidelines in relation to such mechanisms, but again did not specify to which three they were referring.

47 See, e.g., endnote 41.

48 Article 29 Working Party, WP 173: "Opinion 3/2010 on the principle of accountability," 13 July 2010.

49 International Conference of Data Protection and Privacy Commissioners, The Madrid Resolution: International Standards on the Protection of Personal Data and Privacy, 5 November 2009, p. 15.

APPENDIX

JOINT-PROJECT ON REGULATORY ENFORCEMENT POLICY AND PRACTICE by the CENTRE FOR INFORMATION POLICY LEADERSHIP (CIPL) and PROFESSOR CHRISTOPHER HODGES

The Objectives of this Research Project

CIPL, the International Network for Delivery of Regulation (INDR) and Professor Christopher Hodges are pursuing a new research project on regulatory enforcement policy and practice in the area of privacy and data protection. To broaden the scope of relevant and useful information, the project will explore and draw from other regulatory areas as well. This questionnaire is part of this project. It is directed to a broad scope of regulators and enforcement authorities, including privacy and data protection regulators.

This project builds upon previous work by CIPL and Professor Hodges on innovative strategies and methods that regulators can use to improve organizational behaviours and promote corporate social responsibility, accountability and compliance. In the privacy and data protection arena, this includes ways in which organizations can be made more accountable and responsible in using and protecting personal data.

The specific objective of this phase of the project is to understand the extent to which regulators take into account in their enforcement, sanctioning and fining decisions any frameworks, systems, programs, practices, processes, policies and procedures, measures or tools (collectively "mechanisms") that organizations have put in place to comply with legal requirements or other external standards, or to implement their own internal behavioural objectives, corporate ethics requirements, goals and public promises. Such mechanisms are sometimes referred to as compliance mechanisms, and, in the data protection context, as accountability mechanisms.

Are the existence of such mechanisms used as a mitigating factor (or their absence as an aggravating factor) when making decisions on sanctions and fines?

QUESTIONNAIRE

- Please send us answers to the following questions
- Please provide details of sources for each answer that may be useful, such as relevant legislation, regulatory guidance and policy documents
- Please feel free to explain the background to any answers

---

1. What is your role in enforcing laws and what enforcement tools do you have (e.g., warnings, undertakings, injunctions, bans on activities, consent orders, consumer redress, fines)? Do you enforce them yourselves or do you refer enforcement matters to prosecutors or another authority?

[please type your response here]

2. Do you have an externally-facing policy or document establishing or describing your enforcement approach and priorities in your area of competence?

[please type your response here]

3. Are there any mandatory or advisory guidelines you refer to when calculating sanctions and fines?

[please type your response here]

4. Do you have the power to make decisions (i.e. have discretion) on:

a) which circumstances or cases are referred to another department or authority for enforcement?

[please type your response here]

b) whether you may yourself investigate a matter and impose fines or other sanctions?

[please type your response here]

c) choosing the enforcement tool (e.g., warnings, undertakings, injunctions, bans on activities, consent orders, consumer redress, fines), and/or deciding on how much the fine might be?

[please type your response here]

5. If you make any decisions on enforcement, sanctions or fines, do you take the following factors into account as mitigating factors?

a) Existence of any frameworks, systems, programs, processes, practices, policies and procedures, measures or tools that organizations have put in place to comply with legal requirements or other external standards, or to implement their own internal behavioural objectives, corporate ethics requirements, goals and public promises;

b) Having a relevant certification, label, seal, or participating in a code of conduct;

c) The effectiveness of an organization's current accountability mechanism(s) and instruments set forth in (a) and (b) above and how they are operated;

d) An organization's transparency around the existence of the mechanisms or instruments described in (a) and (b) above and the organization's ability to demonstrate their existence and effectiveness;

e) An organization's current or historic cooperation with you in an investigation or enforcement context, including in connection with questions around the existence or effectiveness of any mechanisms or instruments described in (a) and (b) above; or

f) Other factors relating to the scope of this study.

[please select in the Yes/No options above which elements you take into account, and type here any further comments you may have]

6. Do you take the following factors into account as aggravating factors if and when making decisions on enforcement, sanctions and fines? ?

a) The absence of any frameworks, systems, programs, processes, practices, policies and procedures, measures or tools to comply with legal requirements or other external standards, or to implement an organization's own internal behavioural objectives, corporate ethics requirements, goals and public promises;

b) Not having a relevant certification, label, seal, or not participating in a relevant code of conduct;

c) Where the mechanisms set forth in (a) do exist within an organization, or an organization has or participates in the instruments set forth in (b), the lack of effective implementation, transparency or demonstrability of any such mechanisms or instruments.

d) The fact that an organization may have misrepresented that it has implemented or participates in such mechanisms or instruments;

e) An organization's lack of current or historic cooperation with you in an investigation or enforcement context, including in connection with questions around the existence or effectiveness of any mechanisms or instruments described in (a) and (b) above

f) Other factors relating to the scope of this study.

[please select in the Yes/No options above which elements you take into account, and type here any further comments you may have]

7. Can you share examples of cases where you used such compliance mechanisms or instruments as a mitigating or aggravating factor?

[please type your response here]

8. Does your law or applicable regulatory guidance (including guidance from you) include a requirement or recommendation to build and implement frameworks, systems, programs, processes, practices, policies and procedures, measures or tools that help organizations comply with legal requirements and/or other standards? If yes, what specific actions do they require or suggest?

[please type your response here]

9. Have you or another relevant authority published precedents, guidelines or requirements on best practice with respect to such compliance mechanisms or instruments??

[please type your response here]

About the Centre for Information Policy Leadership

CIPL is a global data privacy and data policy think tank in the law firm of Hunton Andrews Kurth LLP and is financially supported by the law firm and 80 member companies that are leaders in key sectors of the global economy. CIPL's mission is to engage in thought leadership and develop best practices that ensure both effective privacy protections and the responsible use of personal information in the modern information age. CIPL's work facilitates constructive engagement between business leaders, privacy and security professionals, regulators and policymakers around the world. For more information, please see CIPL's website at **http://www.informationpolicycentre.com/.**

If you would like to discuss any of our comments or require additional information, please contact Bojana Bellamy, bbellamy@HuntonAK.com; Markus Heyder, mheyder@HuntonAK.com; or Sam Grogan, sgrogan@HuntonAK.com

CIPL AT 20 — SHAPING DATA POLICY FOR TOMORROW

HUNTON ANDREWS KURTH

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

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

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