Seeking Solutions:

Attributes of Effective Data Protection Authorities

U.S. CHAMBER OF COMMERCE

HUNTON& WILLIAMS

U.S. CHAMBER OF COMMERCE

HUNTON& WILLIAMS

The U.S. Chamber of Commerce is the world's largest business federation representing the interest of more than 3 million business of all sizes, sectors, and regions, as well as state and local chambers and industry associations.

Hunton & Williams is a global law firm with nearly 800 lawyers serving clients in the United States, Europe and Asia. The firm's Global Privacy and Cybersecurity practice is a leader in its field and has been ranked as a top practice globally for privacy and data security.

Acknowledgements: The authors of this report would like to thank the following for their country-specific contributions to this report: Rosario Mille of Estudio Millé, Susan Park and Taeuk Kang of Bae, Kim & Lee LLC, Haim Ravia and Dotan Hammer of Pearl Cohen Zedek Latzer, Kristin Wilson of Belly Gully, and Luis Burgueño and Roberto Rosas of Von Wobeser y Sierra S.C.

I. Introduction

In an increasing number of jurisdictions around the world, data protection authorities and other privacy regulators (collectively, "DPAs")[1] play a critical role in effectuating data protection governance and contributing to a more informed, privacy-centric culture. The manner in which DPAs carry out their duties reflects the underpinnings of privacy law in their jurisdictions. In some countries, privacy is viewed as a fundamental human right. In others, it is considered a consumer protection interest. A country's foundational principles with respect to data protection influence the role of the relevant regulator and result in varying practices, structures and values among DPAs. As privacy convergence increases across jurisdictions, and the role of DPAs evolve to adapt to changes in the legal landscape, the constitution of an effective DPA is ripe for review and consideration.

This report highlights the key attributes of DPAs that contribute to effective data protection governance, and explores how the level of effectiveness varies based on differences in the structure, roles and resources of a DPA. Among the virtues of the most effective DPAs is a proclivity to treat those it regulates as partners rather than adversaries. This trait is manifested in a commitment to promoting education, awareness and transparency, and soliciting feedback from and collaborating with, relevant stakeholders (including consumers, other regulators and the regulated community). Effective DPAs also demonstrate an understanding of, and ability to adapt to, the evolving business and technology landscape.

While all DPAs are tasked with the basic duty of protecting personal data, their methodologies, practices, and scope of authority vary greatly. In this report, we explore these differences and highlight commonalities across the most effective DPAs. The risks and challenges of data protection governance has grown in recent years with the ubiquity and increasing value of data in our global economy, making it imperative to understand how to effectively regulate data protection.

1 This report uses the term "DPA" to describe regulators that enforce laws governing privacy and data protection practices. As discussed in this paper, not all regulators that enforce privacy and data protection rules focus solely on those issues. The Federal Trade Commission, for example, is the primary regulator of privacy and data security practices in the U.S., and enforces a number of laws that protect consumers against a broad array of harmful practices, including anticompetitive, deceptive and unfair commercial practices. For consistency, this paper refers to both singularly-focused and multipurpose regulators as DPAs.

Seeking Solutions:

Key Attributes

Effective DPAs Promote Education and Awareness

Effective DPAs Seek Feedback

Effective DPAs Offer Guidance and Assistance

Effective DPAs Are Judicious

Effective DPAs Are Transparent

Effective DPAs Strive for Coordination and Cooperation

Effective DPAs Are Business and Technology-Savvy

II. Qualities of Effective DPAs

In conducting this study, we identified several key qualities of DPAs that contribute to effective data protection governance. The common thread among all the DPAs reviewed is that truly effective DPAs treat those they regulate as partners instead of adversaries. The most effective DPAs share a commitment to promoting education and awareness and to guiding and assisting the regulated community in a consistent manner, while exercising discretion and good judgment. They also possess a desire to improve through feedback and a willingness to act in a transparent manner. In addition, we found that DPAs that exhibited an aptitude for collaboration and gaining insight into the changing business and technology environments have a greater impact in their respective jurisdictions. This section explores these key qualities and other characteristics we found critical to a DPA's success.

A. Effective DPAs Promote Education and Awareness

To impart data protection values effectively, DPAs should be educators and privacy advocates that promote a culture of data protection both to the public and within the regulated community. In this capacity, DPAs should seek to instill accountability principles by educating, engaging and advising the regulated community on compliance with data protection laws. DPAs also should provide outreach services to the public, raising and informing individuals' awareness of their privacy rights.

DPAs serve an important role in teaching organizations about data protection practices and clarifying legal expectations. The need for education and awareness is driven by the reality that noncompliance is not always intentional, but rather is often caused by a lack of knowledge, understanding or awareness. The Institute for Research in the Social Sciences, for example, found that organizations' lack of awareness about data protection rights contributed to individuals facing difficulties in exercising their right of access.[2] Similarly, the European Union Agency for Fundamental Rights attributes the majority of noncompliance with registration obligations in EU member states to a lack of awareness and understanding.[3]

2 Information Commissioner's Office, *Data Protection Rights: What the Public Want and What the Public Want from Data Protection Authorities* (May 2015) at ¶ 106.

3 European Union Agency for Fundamental Rights, *Data Protection in the European Union: The Role of National Data Protection Authorities - Strengthening the Fundamental Rights Architecture in the EU II* (2010) at 42-43.

Seeking Solutions:

A DPA that takes a proactive approach toward data protection education and awareness helps maximize enforcement. DPAs do not have the resources to enforce every privacy right and police every action. To make efficient use of their finite staffing and financial resources, DPAs must be strategic about maximizing their ability to enforce data protection laws while at the same time reducing instances of noncompliance. For example, various DPAs have called on organizations to conduct regular privacy impact assessments ("PIAs") designed to help identify and mitigate privacy risks associated with their data handling practices. DPAs in the UK[4] and France[5], for instance, have published step-by-step guidance on how to conduct PIAs and advise on privacy risk management. DPAs also have encouraged organizations to implement privacy programs and employ privacy officers. Through these self-review mechanisms, organizations take it upon themselves to approach their data handling practices more thoughtfully and help reduce avoidable violations that present high risks to individuals' privacy[6]

The need for education and awareness is driven by the reality that noncompliance is not always intentional, but rather is often caused by a lack of knowledge, understanding or awareness.

There are many examples of DPAs launching campaigns designed to promote awareness and a deeper understanding of data protection rights. DPAs around the world commonly commission studies, publish reports, and issue white papers on data protection topics. Often these studies and reports are generated in connection with conferences and initiatives that add to the body of public knowledge regarding data protection rights. The most effective DPAs continue to innovate in encouraging organizations to adopt accountability mechanisms. For example, DPAs in some jurisdictions have administered contests designed to highlight best practices in data protection, and have awarded prizes to organizations that have employed them. The DPA in Slovenia, for instance, annually selects a private or public organization that

4 *See* Trilateral Research & Consulting, *Privacy Impact Assessment and Risk Management, Report for the Information Commissioner's Office* (May 4, 2013).

5 *See* Commission Nationale de l'Informatique et des Libertés, *Methodology for Privacy Risk Management* (2012 ed.) at 4.

6 A study commissioned by the UK Information Commissioner's Office found that the vast majority of large companies or data-intensive businesses in the UK voluntarily employ staff with a job position focused on data protection compliance. London Economics, *Implications of the European Commission's Proposal for a General Data Protection Regulation for Business: Final Report to the Information Commissioner's Office* (May 2013) at 10.

it considers most successful at personal data protection. The DPAs in France and Spain award annual monetary prizes to organizations that employ best practices in the field of data protection.[7] In Mexico, the DPA held the 2016 Innovation and Good Practices on Personal Data Protection Competition to recognize and advance both nationally and internationally best practices for data protection developed by both the public and private sectors.[8]

Other DPAs hold formal and informal events to spread data protection awareness to the public and regulated community. For example, New Zealand's DPA runs a Privacy Week, which features various forums, speakers and an art exhibition aimed at increasing public knowledge and debate over privacy and data protection issues.[9] The New Zealand DPA also occasionally hosts free lunchtime forums in major cities to discuss privacy risks associated with emerging technologies. In Hong Kong and Singapore, the DPAs host education and training workshops and conferences that introduce attendees to new privacy-related topics and help guide them in complying with new privacy obligations.[10] Hong Kong's DPA also sends exhibition vehicles to local communities where the public can explore and interact with informative display panels to learn more about protecting their privacy.[11]

B. Effective DPAs Seek Feedback

DPAs that seek feedback from the regulated community and public are better equipped to understand and enhance their governance abilities. In many jurisdictions, DPAs convene multi-stakeholder meetings with representatives from the public and private sectors or conduct national surveys on data protection issues to help gauge public opinion and the effectiveness of their

7 European Union Agency for Fundamental Rights, *supra* note 3 at 48-49.

8 The 2016 Innovation and Good Practices on Personal Data Protection Competition, *at* http://premioinnovacionpdp.inai.org.mx/Pages/Bienvenida.aspx (last visited Sept. 14, 2016).

9 *See* https://www.privacy.org.nz/forums-and-seminars/privacy-week.

10 *See* https://www.pcpd.org.hk/english/education_training/organisations/workshops/workshop.html; https://www.pdpc.gov.sg/news/Events/page/0/year/2016/month/All/personal-data-protection-seminar-2016; https://www.pdpc.gov.sg/news/Events/page/1/year/2015/month/All/personal-data-protection-seminar-2015; and https://www.pdpc.gov.sg/news/Events/page/2/year/2014/month/All/personal-data-protection-seminar-2014.

11 *See* https://www.pcpd.org.hk/english/news_events/events_programmes/roadshow/index.html; https://www.pcpd.org.hk/english/news_events/media_statements/press_20151221a.html; and https://www.pcpd.org.hk/english/news_events/media_statements/press_20131129.html.

regulations. They also solicit public comments on their work to help guide policymaking activities. For example, in France, prior to enacting a new registration procedure for French affiliates of groups that had implemented Binding Corporate Rules ("BCRs"), the French DPA contacted more than 60 multinational companies with BCRs to discuss the DPA's proposed procedure.[12]

The UK Information Commissioner's Office ("ICO") has been particularly focused on soliciting public feedback, informing its strategy and policymaking through a combination of studies and public comment periods. For example, in 2014, the UK ICO published a consultation on the framework criteria for selecting providers for its privacy seal scheme and gave organizations the opportunity to provide recommendations for the relevant framework criteria.[13] The U.S. Department of Commerce has established several collaborative processes that provide a forum for industry, civil society and academia representatives to discuss privacy issues associated with new technologies. These collaborative processes often result in a consensus over privacy best practices and codes of conduct that influence state and federal regulators' interpretation of privacy laws.

The U.S. Department of Commerce has established several collaborative processes that provide a forum for industry, civil society and academia representatives to discuss privacy issues associated with new technologies.

In addition to soliciting public feedback, the complexity of the technologies, business practices and civic issues implicated by data protection has increasingly led DPAs to seek training and advice from experts, including academics, technologists, consultants, economists and research organizations. In the summer of 2012, as part of its initiative to improve the country's focus on data protection, Serbia's DPA invited experts to conduct a seminar for its staff on data protection issues. The Serbian DPA acknowledged that, to kick-start a strong approach to data protection, it would focus on educating the public and businesses.[14]

12 *See* http://www.cnil.fr/linstitution/actualite/article/article/bcr-la-cnil-facilite-les-formalites-liees-aux-transferts-internationaux-de-donnees.

13 Information Commissioner's Office, *Framework Criteria for an ICO Endorsed Privacy Seal Scheme* (draft for consultation v1.3), *available at* https://ico.org.uk/about-the-ico/consultations/privacy-seals-draft-framework-criteria.

14 *See Training About Personal Data Protection by World and European Experts* (July 9, 2012), *available at* http://www.huntonprivacyblog.com/wp-content/files/2012/07/Serbia-Commissioners_Statement.pdf.

C. Effective DPAs Offer Guidance and Assistance

DPAs that offer guidance and assistance improve compliance by helping to decrease uncertainty in the marketplace. The evolving regulatory environment calls for DPAs to clarify interpretations of novel or nebulous legal questions, address obscure issues, and share their opinions on new practices and technologies. Their guidance provides direction to regulated businesses, which enables organizations to assess and adjust their practices accordingly. DPAs can provide such guidance when new laws are enacted or become effective,[15] after courts issue important opinions,[16] when problematic areas have been identified, and as emerging or evolving technologies and business practices arise.[17]

15 For example, less than a month before a new law became effective in January 2016 that expanded the country's data breach notification obligation to all data controllers, the Dutch DPA published a practical guidance to help organizations identify instances in which data security breaches must be reported to the DPA and data subjects. *See The Obligation to Report Data Breaches in the Data Protection Act (PDPA), Policy Rules for Applying Article 34a of the PDPA* (Dec. 8, 2015), *available at* https://www.huntonprivacyblog.com/files/2016/01/beleidsregels_meldplicht_datalekken.pdf. Similarly, in response to a new obligation under French data protection law to obtain prior consent before placing or accessing cookies on web users' devices, the French DPA released a set of FAQs, technical tools and relevant source code that provided guidance on how to obtain consent for the use of cookies and similar technologies in compliance with EU and French data protection requirements. *See* http://www.cnil.fr/vos-obligations/sites-web-cookies-et-autres-traceurs/. The guidance clarified which cookies are exempt from the consent requirement under French data protection law. Following the enactment of the Personal Information Protection Act and the IT Network Act in South Korea, the MOI and the Korea Communications Commission respectively released practical manuals for compliance with the two laws.

16 For example, a month after the Court of Justice of the European Union ("CJEU") invalidated the European Commission's decision on the adequacy of the protection provided by the Safe Harbor, certain DPAs published guidance on the legal mechanisms for cross-border data transfers to assist companies in legally transferring personal data to the U.S. *See*, *e.g.*, Commission Nationale de l'Informatique et des Libertés, *Safe Harbor: What Should Companies Do?* (Feb. 8, 2016), *available at* http://www.cnil.fr/linstitution/actualite/article/article/safe-harbor-que-doivent-faire-les-entreprises; and https://www.datenschutz.hessen.de/ft-europa.htm#entry4521.

17 For example, numerous DPAs have issued guidelines that address online purchases, direct marketing, contests and sweepstakes, and consumer tracking to increase merchant and consumer awareness and to help all parties understand their respective rights and obligations under data protection law. In 2014, the Israeli DPA hosted a conference for public transportation companies on privacy issues related to a new electronic transportation smartcard system deployed in Israel. Before the 2015 national election in Israel, the Israeli DPA also issued guidance to political parties on safeguarding the Voters' Roll.

Seeking Solutions:

DPAs can share guidance in different ways. Among other mechanisms, DPAs issue guidelines, draft guidance letters, author position papers and develop FAQs to convey their views on certain practices, shed light on the legal issues and the state of the law, and pose questions to the regulated community. This can be aimed at a particular entity, sector, business practice or technology. There are also more informal ways to convey guidance to the general public, such as through speeches, public workshops, interviews and press conferences. In addition, many DPAs field questions directly from businesses and individuals, either by receiving written inquiries by mail or email, or offering online and in-person question-and-answer sessions.

In addition to counseling regulated entities, DPAs can assist in their compliance efforts. Many DPAs provide assistance in the form of voluntary data protection audits or advisory visits at the request of regulated entities. These assessments result in the DPA providing practical advice and recommendations on improving data protection practices. There are no enforcement consequences associated with this assistance.

Many DPAs provide assistance in the form of voluntary data protection audits or advisory visits at the request of regulated entities.

Faced with the rapid growth of personal data feeding organizational initiatives across the private and public sectors, DPAs are finding new ways to scale their advice and assistance to organizations. Many DPAs have issued step-by-step guidance, self-assessment tools, template forms and toolkits to assist organizations in helping to ensure their business practices comply with applicable data protection laws. In the UK, for example, the ICO attempted to reach a broader audience by releasing a tool for organizations to help them remind and train their staff on data protection issues, including training videos, e-learning modules and promotional posters and checklists.[18] The ICO also developed an online data protection Self-Assessment Toolkit for small and medium-sized organizations to use in self-evaluating and benchmarking their data protection compliance.[19] Similarly, the U.S. Department of Health and Human Services, the primary federal regulator of health information privacy in the U.S., published a risk assessment tool that assisted regulated entities in evaluating their information security practices

18 Information Commissioner's Office, *supra* note 2, at ¶¶ 106-107.

19 *Id.*

for compliance with U.S. health privacy law. In Mexico, the DPA introduced an online interactive training center for businesses, the public and the government, where individuals can participate in courses related to different aspects of data protection.[20] Further, as part of these efforts, many DPAs have shown a penchant for helping develop codes of conduct, certification programs and other voluntary self-governance frameworks to provide assistance with compliance to a broader audience.[21]

In providing guidance and assistance, DPAs should be mindful that their positions create legitimate expectations in the regulated community. Consistency therefore is essential. It also is important for DPAs to be cognizant of the potential effect and legal consequences of their statements given that others may rely on them as a representation of the DPA's position, particularly in light of the fact that their guidance typically is not subject to the same level of judicial oversight and scrutiny as more formal decisions. Therefore, DPAs should take care to avoid imposing new legal obligations on regulated entities through guidance or unorthodox legal interpretations that find little support in the legal standards or case law. To the extent guidance creates more legal uncertainty, the DPA may be doing more harm than good.

D. Effective DPAs are Judicious

A key attribute of a DPA is its ability to be judicious and exercise discretion. After all, there is much at stake when enforcing data protection rights. Innovative technologies may be stifled, commerce depressed, and social welfare reduced by ineffective or inefficient enforcement that produces only meager benefits. Thus, the most effective DPAs understand that when it comes to enforcing data protection laws, the old adage "quality over quantity" holds true. They prioritize their enforcement objectives by taking into account which businesses and practices trigger the most complaints, carry the greatest potential risk, and are likely to result in the most significant harm.[22] Through this strategy, DPAs can make the biggest impact.

20 The "CEVINAI" platform, *at* http://cevifaiprivada.ifai.org.mx/swf/cevinaiv2/cevinai/campus.php (last visited Sept. 14, 2016).

21 For example, Mexico has implemented a self-regulation scheme referred to as the Binding Self-Regulation Parameters, with the national DPA authorizing, overseeing and revoking the certifying entities that enforce the system.

22 Information Commissioner's Office, *supra* note 2, at ¶¶ 116-117.

Seeking Solutions:

To implement this approach in practice and maximize the effectiveness of their enforcement actions, DPAs have found success using a risk-based approach to conducting audits, performing investigations, initiating enforcement actions and legal proceedings, and imposing fines and other sanctions. This risk-based approach requires DPAs to evaluate the benefits that will result from bringing enforcement actions and compare them to the opportunity costs associated with their actions. Through this process, DPAs may thoughtfully choose which sectors, businesses, activities and technologies to target based on a calculus of the potential magnitude and likelihood of harm associated with the data practices at issue. Indeed, this approach is consistent with many laws. Section 5 of the FTC Act, which is the principal law used to regulate privacy in the U.S., prohibits unfair trade practices. For a practice to be unfair, the FTC must establish that: (1) the act or practice causes, or is likely to cause, substantial injury; (2) the injury is not outweighed by countervailing benefits to consumers or competition; and (3) the injury was not reasonably avoidable by the consumers themselves. Accordingly, the FTC must balance both "injuries" and "benefits."[23]

DPAs have found success using a risk-based approach to conducting audits, performing investigations, initiating enforcement actions and legal proceedings, and imposing fines and other sanctions.

In addition, the most effective DPAs do not subscribe to a one-size-fits-all approach to enforcement, but rather react to the situation at hand. Rather than treating all organizations and violations exactly the same way, DPAs are most effective when they adjust their response to the relevant circumstances. Being responsive means formulating an enforcement strategy that accounts for the conduct, history and industry norms associated with the particular organization with which they are dealing, as well as the gravity of the situation. The organization's history of compliance (i.e., isolated or repeat violations) and cooperation (i.e., accommodating or uncooperative) should be factored into the DPA's decision. Another factor to consider is the intent of the violators, which may range from entities that willfully ignored well-known data protection responsibilities to those that made a reasonable decision in a situation that involved an unsettled or new application of data protection law. This tailored approach to enforcement results in DPAs making more impactful decisions on when to conduct audits, initiate investigations and

23 *See* FTC Policy Statement on Unfairness (Dec. 17, 1980), *appended to In re International Harvester Co.*, 104 F.T.C. 949, 1070 (1984), *available at* http://www.ftc.gov/bcp/policystmt/ad-unfair.htm.

bring enforcement actions. DPAs also take these considerations into account when determining whether to levy sanctions for violations and the amount of sanctions necessary (for example, whether to issue a warning, issue monetary penalties or impose equitable sanctions).

By taking a more tailored approach to enforcement, DPAs provide strong incentives to the regulated community by differentiating among organizations based on their behavior and circumstances. In this sense, the approach tends to reward organizations that have a history of compliance and have shown respect for privacy rights in the past, while providing enhanced scrutiny and offering less leniency to repeat offenders that have committed systematic violations. This approach benefits all stakeholders. It gives the regulated community an incentive to improve compliance and cooperate with regulators in return for less burdensome oversight, while promoting self-governance and enabling DPAs to more efficiently allocate their resources.

This approach also promotes administrative efficiency. As indicated above, it is routine matter for DPAs to field complaints and inquiries alleging violations of personal data rights. They also commonly initiate investigations or audits on their own accord. Given their scarce compliance and enforcement resources, DPAs that prioritize their enforcement efforts advance their compliance goals more effectively. In pursuing cases of noncompliance, DPAs have found the need to be "selective to be effective," or risk exhausting their scarce resources and producing diminishing returns from their actions.[24] As a result, it is important for DPAs to focus on serious, not trivial issues. As an example, in 2014, the UK implemented a new strategy for handling complaints that focused the ICO's efforts on the investigation of serious and repeat violations of data protection laws.[25] Under this approach, the ICO does not investigate every complaint it receives, and instead takes a more selective approach to investigations and working to resolve disputes between organizations and individuals. The ICO has noted that "[t]oo often we are drawn into adjudicating on individual disputes between organizations and their customers or clients, particularly where the legislation we oversee may only be a peripheral part of the matter being disputed. We want to focus on those who get things wrong repeatedly, and take action against those who commit serious contraventions of the legislation."[26]

24 Information Commissioner's Office, *supra* note 2, at ¶ 117.

25 *See* Information Commissioner's Office, *Consultation: Our New Apprach to Data Protection Concerns* (Start Date Dec. 18, 2013), *available at* https://www.huntonprivacyblog.com/files/2014/01/A-new-approach-consultation.pdf.

26 *Id.*

Seeking Solutions:

E. Effective DPAs Are Transparent

DPAs should act transparently so they can be held accountable by their various stakeholders, including the public and regulated community. It is important for stakeholders to understand DPA decisions and the reasons they brought enforcement actions or launched policy initiatives. Without transparency, it is difficult to predict how compliance will be judged, understand DPA decisions, comply with them or challenge them. Murky enforcement actions, theories of law, policy objectives and other important regulatory considerations also make it difficult to hold DPAs accountable for their decisions. Transparency helps build trust in DPA decisions and actions, preventing DPAs from being viewed as arbitrary and capricious.

There are several ways in which DPAs should strive to be transparent. First, DPAs should, from the outset, have a clearly defined mission and scope of authority. Preferably, these parameters of authority should be codified in law. DPAs with codified missions and scopes of authority are less likely to arbitrarily regulate new technologies or industries, or independently expand their authority. Second, DPAs should establish evaluation mechanisms, including annual reports or audits, to ensure that stakeholders can assess whether DPAs are acting effectively, fairly and efficiently, and are meeting their objectives.

Transparency helps build trust in DPA decisions and actions, preventing DPAs from being viewed as arbitrary and capricious.

Third, DPAs should set and communicate clearly articulated objectives and priorities for interpreting and enforcing laws. Setting priorities and objectives provides stakeholders with a better idea of what is expected of them and signals where they should focus their compliance efforts for improvement. For example, to help guide its enforcement decisions, the Office of the Privacy Commissioner ("OPC") in Canada sets strategic priorities to focus resources on the privacy challenges identified by the DPA as most pressing at the time. These priorities help inform the OPC's priorities when it comes to education and outreach efforts, investigations and audits, court actions, guidelines or studies, and research projects.[27]

27 Office of the Privacy Commissioner of Canada, *The OPC Privacy Priorities 2015-2020: Mapping a Course for Greater Protection* (2015) at 2, *available at* http://publications.gc.ca/site/eng/9.801466/publication.html.

Fourth, DPAs should accompany their decisions with meaningful explanations of the factors that led them to their judgments. Many DPAs make publicly available the criteria they use to make decisions, give reasons and explanations for their views, and reveal the evidence and empirical basis upon which they relied. In addition, DPAs regularly publish transparency reports containing information about their enforcement activities and bulletins regarding recent decisions and adopted regulations. Pursuant to Article 28(5) of the Data Protection Directive, all DPAs in the EU publish annual reports on the status of the protection of privacy rights in their jurisdictions.[28] In Mexico, the public can review the Treasury Secretary's Annual Federation Expenses Budget, which among other details, provides information about the Mexican DPA's allocation of public resources, objectives, investment programs and initiatives.[29] In addition, the Mexican DPA is required to issue an annual report in which it details its accomplishments during the preceding year and relevant statistics.[30] Likewise, the New Zealand Privacy Commissioner must prepare and publish an annual report at the end of each financial year.[31] New Zealand's DPA also is audited each year by the Auditor-General.[32] In South Korea, government agencies are required to submit to the DPA an annual data protection plan for their relevant industry area, while the DPA is required to submit to the National Assembly an annual report detailing the planning and execution of its data protection programs.[33] In Israel, the DPA is required to publish annual reports regarding the previous year's enforcement and supervisory activities.[34] Furthermore, Israel's Public Commission for the Protection of Privacy, an independent body whose members are professors and privacy practitioners, issues its own commentary to the DPA's annual report, with recommendations and calls for action.[35] Additionally, the Israeli DPA is subject to parliamentary oversight by the Constitution, Law and Justice Committee, which typically dedicates one of its sessions to deliberate on the

28 European Union Agency for Fundamental Rights, *supra* note 3, at 28.

29 The 2016 Annual Federation Expenses Budget (July 5, 2016); Annex 23.13, *available at* http://www.diputados.gob.mx/LeyesBiblio/pdf/PEF_2016.pdf.

30 INAI, *Work Report 2015* (April 2016 ed.), *available at* http://inicio.ifai.org.mx/nuevo/Informe%20de%20Labores%202015%20Ok_Med.pdf.

31 Section 150 of the Crown Entities Act 2004 (N.Z.).

32 Section 156 of the Crown Entities Act 2004 (N.Z.).

33 Personal Information Protection Act, Mar. 29, 2011, art. 67 (S. Kor.).

34 Protection of Privacy Law, 5741–1981, Section 10A (Isr.).

35 *Id.*

DPA's annual report and the Public Commission's commentary.[36] More active DPAs provide more frequent updates through blog posts, press releases and bulletins. Italy's DPA, for example, distributes monthly bulletins with the most up-to-date decisions or regulations adopted.[37]

Effective DPAs also provide entities with notice to help improve their transparency. As an active auditor, the French DPA provides advance warning of its audit plans and priorities each year through its annual inspection program alert.[38] In 2015, the French DPA announced its plans to conduct 550 inspections in 2015, including 350 onsite inspections, document reviews or hearings, and 200 online inspections. The DPA warned that a quarter of the onsite inspections would focus on closed-circuit television monitoring, and provided a list of technologies or data processing operations on which other inspections would focus.

F. Effective DPAs Strive for Coordination and Cooperation

DPAs that cooperate and work jointly with other regulators within and outside of their respective countries increase their efficiency and consistency globally. Coordination might involve (1) bringing joint enforcement actions, (2) informing each other of upcoming complaints and sharing relevant information about them, (3) facilitating joint research and education programs, (4) aiding the mutual exchange of knowledge and expertise between the entities via training programs and staff exchanges, (5) promoting an understanding of economic and legal conditions and theories that impact the enforcement of applicable privacy laws, and (6) informing each other of privacy-related developments in their respective countries. Coordination can benefit DPAs by saving them resources and avoiding duplicative work. Redundant

Redundant enforcement, such as overlapping investigations and audits, not only leads to the risk of inconsistent enforcement and an increased compliance burden on the regulated community, but also can result in wasteful use of public funds.

36 *Id.*

37 European Union Agency for Fundamental Rights, *supra* note 3, at 28.

38 *See* http://www.cnil.fr/linstitution/actualite/article/article/programme-des-controles-2015.

enforcement, such as overlapping investigations and audits, not only leads to the risk of inconsistent enforcement and an increased compliance burden on the regulated community, but also can result in wasteful use of public funds. Coordination facilitates enforcement by allowing regulators to pool their resources and reduce waste.[39]

There are numerous examples of initiatives that foster cooperation among DPAs and increase consistency in enforcement and regulation. Among the most important is the Global Privacy Enforcement Network ("GPEN"), which was established in 2007 at the behest of the member countries of the Organization for Economic Co-operation and Development. GPEN is "a network [of over 50 countries] designed to facilitate cross-border cooperation in the enforcement of privacy laws."[40] Among other activities, GPEN encourages the sharing of "best practices in addressing cross-border challenges" and the development of "shared enforcement priorities."[41] GPEN also conducts an annual privacy enforcement sweep, in which DPAs participate cooperatively in searching websites and apps to assess privacy practices and compliance with privacy laws.[42] DPAs in the Asia-Pacific region have in place a similar data protection cooperation arrangement within the context of the Asia-Pacific Economic Cooperation forum.[43]

39 In some jurisdictions, multiple regulatory agencies enforce privacy and data protection rights simultaneously, often under different regulations. Each year, for example, the German federal and state DPAs hold a biannual conference called the Conference of the German Data Protection Commissioners, which provides a private forum for all German state DPAs and the Federal Commissioner for Data Protection and Freedom of Information to share their views on current data protection issues, discuss relevant cases and adopt resolutions aimed at harmonizing how data protection law is applied across Germany. During the conference, the German DPAs typically adopt several resolutions concerning data protection including, for example, privacy issues associated with connected cars, DPA cooperation with competition authorities, facial recognition technology, employee privacy, end-to-end encryption and health data privacy.

40 Paul de Hert and Vagelis Papakonstantinou, *Three Scenarios for International Governance of Data Privacy: Towards an International Data Privacy Organization, Preferably a UN Agency?*, 9 ISJLP 271, 294-296 (2013).

41 *Id.*

42 Information Commissioner's Office, *supra* note 2, at ¶ 115.

43 *See* http://www.apec.org/Groups/Committee-on-Trade-and-Investment/Electronic-Commerce-Steering-Group/Cross-border-Privacy-Enforcement-Arrangement.aspx.

Many DPAs also enter into memoranda of understanding ("MOUs") to promote increased cooperation and information sharing. MOUs do not create legally binding obligations on DPAs to provide assistance to one another, but instead memorialize their commitment to cooperation and mutual assistance. MOUs typically set forth cooperation objectives, and describe procedures for collaboration in the areas of enforcement, education and research. In addition, many DPAs participate in joint awareness initiatives held each year, such as International Data Privacy and Protection Day, Asia-Pacific Privacy Awareness Week, Safer Internet Day, and Data Protection Day of the European Union.[44]

DPA collaboration is particularly important in Europe, where DPAs of EU member states share a common data protection framework. In the EU, the Article 29 Working Party helps EU countries develop a shared interpretation of the Data Protection Directive. The Working Party provides a formal forum within which EU DPAs "can harmonize the application of their respective laws," debate the passage and implementation of new regulations and policies, and work to ensure that data protection principles are applied consistently within the Member States.[45] Such cooperative meetings do not necessarily have to be formal to have a positive impact. For instance, the Portuguese DPA holds an informal meeting annually with the Spanish DPA to discuss key developments in the world of data protection.[46] Formal and informal joint case-handling workshops also allow DPAs to share their experiences and expertise, and promote consistency of action.[47]

In April 2016, after four years of drafting and negotiations, the long awaited EU General Data Protection Regulation (the "GDPR") was adopted, replacing EU and national data protection legislation with a single regulation that applies in all EU countries. Among other initiatives, the GDPR establishes the policy of a One Stop Shop to ensure cooperation and uniformity among EU DPAs regarding data protection enforcement. The One-Stop-Shop concept dictates that, where a business is established in more than one EU Member State, the DPA of the main establishment of the business will act as the lead authority for the business' cross-border processing. This policy does away with the EU's previous approach under

44 International Association of Privacy Professionals, Data Protection Authorities 2011 Global Survey (2011) at 27.

45 European Union Agency for Fundamental Rights, *supra* note 3, at 47.

46 *Id.*

47 Information Commissioner's Office, *supra* note 2, at ¶ 114.

Directive 95/46/EC, in which businesses were subject to the authority of the DPAs in all countries in which they were established – which often has led to inconsistent and unpredictable enforcement.

The GDPR will provide for mandatory cooperation between EU DPAs and a mechanism to help ensure consistent application of the new regime. Specifically, where an EU DPA takes an action or drafts a measure that has an EU-wide impact, the case must be referred to the newly created European Data Protection Board (the "Board") (and sometimes the European Commission), which has the power to issue a non-binding opinion that must be taken into account by the relevant DPA in trying to reach a consensus decision on the issue. This is meant to help ensure that the GDPR is consistently applied and that DPAs work together and learn from each other to reach the right decision. In certain situations, the European Commission may require the DPA to suspend the draft measure for a period of time to reconcile diverging positions between the relevant DPA and the Board. According to the European Commission, "[t]he consistency mechanism . . . preserves the role of national DPAs, ensures cooperation between DPAs within the [Board] and gives the Commission a role as a backstop."[48]

G. Effective DPAs Are Business and Technology-Savvy

In today's digital economy, the most effective DPAs are business and technology-savvy. On the business front, they should understand and incorporate into their decision-making processes, policies and regulations (1) changing business models that rely more and more on consumer data for economic growth, (2) the challenges of the competitive business environments they regulate, and (3) the intricacies of the ever-evolving global marketplace.

With respect to technology, DPAs' responsibilities are twofold. First, they must stay ahead of emerging technologies and the challenges posed by these technologies to make informed decisions and modify their policies and regulations accordingly. At the same time, they must be careful not to make decisions or impose burdens on businesses that are grounded in futuristic possibilities rather than the current state of technology. DPAs also should

48 *See* European Commission, *The Proposed General Data Protection Regulation: The Consistency Mechanism Explained* (Jun. 2, 2013), *available at* http://ec.europa.eu/justice/newsroom/data-protection/news/130206_en.htm.

take care to create technology-neutral policies that do not overly encourage or hinder the use of certain technologies. To become more technologically proficient, DPAs increasingly are hiring employees with technical capabilities, teaming up with outside experts and inviting in organizations and agencies to educate them on technology. For example, in March 2015, the FTC created an office devoted to technology research and investigation, which conducts research on technology issues including privacy, data security, connected cars, smart homes, algorithmic transparency, emerging payment methods, big data, and the Internet of Things.[49]

Second, DPAs should use the latest technologies to enhance their efficiency, effectiveness and transparency. They might publish blog posts and newsletters, host webinars or use social media platforms to raise awareness, such as by hosting pages and videos on YouTube, Twitter and Facebook, enabling them to informally interact with the public and regulated community to raise awareness about data protection issues. In Hong Kong, the DPA takes a unique approach by charging a nominal annual fee to join its Data Privacy Officer's Club, which is an organization that entitles individuals and businesses to obtain electronic newsletters that contain such items as newly-issued DPA press releases and guidance materials.[50]

To become more technologically proficient, DPAs increasingly are hiring employees with technical capabilities, teaming up with outside experts and inviting in organizations and agencies to educate them on technology.

It has become essential for effective DPAs to have a strong online presence. DPAs should maintain user-friendly and technologically up-to-date websites where relevant resources can be found. A highly-effective search function is a must.[51] Effective DPAs post information and guidance documents on data protection rights and obligations, and links to summaries of legislation, opinions and agency decisions concerning data protection, preferably in

49 *See* FTC, *BCP's Office of Technology Research and Investigation: The Next Generation in Consumer Protection* (Mar. 23, 2015), *available at* https://www.ftc.gov/news-events/blogs/business-blog/2015/03/bcps-office-technology-research-investigation-next.

50 *See* https://www.pcpd.org.hk/misc/dpoc/about.html.

51 In Israel, the DPA's website has an online search tool that allows users to find which companies' databases are registered.

multiple languages.[52] To ease the regulatory burden on businesses, DPAs should allow businesses to electronically (1) submit official documents, (2) register or notify the DPA of the processing of personal data, and (3) request and receive advice and information. Israel, Poland and Spain's DPA websites, for example, allow businesses to register with their respective DPAs online, while Belgium and Ireland's websites allow businesses to submit data breach notifications online. The Israeli DPA's website allows most forms and documents relating to databases to be submitted via email and allows database owners to pay applicable registration fees online. Some DPA websites also provide mechanisms for individuals to file complaints electronically.[53] For example, the ICO updated its website to provide a guided user journey that assists people in reporting concerns.[54] The Israeli DPA's website also allows individuals to file complaints through an online form. In New Zealand, individuals can input information regarding their complaints in an online form that generates an email request to the DPA.[55] In South Korea, the DPA even allows data protection dispute resolution through online arbitration, and individuals and businesses can request online settlements of their disputes.[56]

DPAs should also use technology to increase their own internal efficiency and effectiveness, such as by building digital databases to store, organize and easily access vital information (e.g., recordings of findings, data analysis and court documents). More effective use of technology for these purposes also will allow DPAs to more easily share relevant information with other agencies inside and outside of their countries to promote cooperation and reduce redundancies.

52 DPAs often make their websites and corresponding online resources available in multiple languages. These include among others, France, Italy, Latvia, the Netherlands and Switzerland. In Spain and Sweden, the DPAs' websites and some of their online resources are available in 6 and 10 languages, respectively.

53 European Union Agency for Fundamental Rights, *supra* note 3, at 48-49.

54 Information Commissioner's Office, *supra* note 2, at ¶¶ 117-118.

55 https://www.privacy.org.nz/your-rights/complaint-form.

56 http://www.ecmc.or.kr.

III. Organizational Attributes of DPAs

In addition to a DPA's practices and skills, the organizational attributes of a DPA contribute to the success of a DPA. The funding, autonomy, responsibility and authority of a DPA are some of the organizational attributes that vary by legal system. This section explores how the structure, roles and resources of a DPA can impact the DPA's effectiveness.

A. Roles of a DPA

While all DPAs are tasked with the basic duty of protecting personal data, the methods, legal authority, and scope of their work vary greatly. Depending on the jurisdiction, the DPA may serve as a supervisor, investigator, adjudicator, educator or policy maker – or all of these. To be effective, DPAs should strive to embody the qualities discussed in Section II above, regardless of their precise roles and duties. The subsections below provide an overview of the various roles that DPAs serve and the legal powers afforded to them under their respective governance frameworks.

Depending on the jurisdiction, the DPA may serve as a supervisor, investigator, adjudicator, educator or policy maker – or all of these.

1. Supervision

In many jurisdictions, DPAs supervise companies' compliance with data protection laws on a proactive basis. DPAs use different mechanisms to oversee compliance, including audits, registration and notification regimes designed to apprise the DPA of higher risk practices.

To keep the DPA informed, some countries' rules require that organizations notify the DPA of certain data protection issues, such as when transferring data outside the country, processing sensitive data or experiencing a data breach. In other jurisdictions, the DPA maintains a public registry of all processing operations based on submitted notifications and registrations. In other jurisdictions, the DPA serves as a gatekeeper, requiring organizations to seek approval before engaging in certain types of data processing activities. The DPA in these jurisdictions may be responsible for authorizing the processing of sensitive personal data or approving the transfer of personal data to other countries based on applicable legal restrictions.

As supervisors, DPAs also take a proactive role in performing audits and inspections to monitor and assess legal compliance. In this role, the DPA can review compliance without needing any indication or suspicion of infringement or misconduct. For example, many DPAs in the EU have the legal authority to audit or examine operators involved in data processing regardless of whether there is a basis to believe that illegality or misconduct has occurred or is likely to occur.[57] The DPA's authority to examine legal compliance proactively, without cause, varies by jurisdiction. They may be able to conduct: (1) onsite inspections during which the DPA may visit a company's facilities and access anything that stores personal data (e.g., servers, computers and applications);[58] (2) document reviews in which an entity under review sends documents or files upon written request; (3) hearings in which the DPA may summon representatives of organizations to appear for questioning and provide the DPA with necessary information; and (4) online inspections during which the DPA may remotely inspect an organization's website and other online services.

2. Investigation

DPAs generally are tasked with investigating potential violations of privacy and data protection laws and infringements of privacy rights based on alleged noncompliance or misconduct. For example, the Argentine Privacy Commissioner is empowered to inquire into any matter in which it is believes an individual's privacy is likely to have been infringed. In their investigative role, DPAs may initiate reviews on their own accord based on an indication of noncompliance (such as from issues discovered during proactive audits) or field complaints from individuals, civil society and governments related to data protection grievances. In Hong Kong, for example, the Privacy Commissioner initiates investigations on its own in some cases based on its proactive monitoring and assessment efforts, while also responding to a significant volume of complaints from the general public.[59]

To help DPAs carry out this investigative role, many jurisdictions provide their DPAs with robust authority to gather information through information

57 European Union Agency for Fundamental Rights, *supra* note 3, at 22.

58 For example, the Korea Internet & Security Agency ("KISA"), a subsidiary of the Korea Communications Commission, conducts onsite inspections for violations of data protection laws.

59 *See* Privacy Commission for Personal Data, Ann. Rep. 48-77 (2014-15), *available at* https://www.pcpd.org.hk/misc/annual_reports/ar2014_15/ar2014_15/index.html.

requests, production demands and access requests.[60] DPAs may, for example, be entitled to obtain access to personal data processed by entities, discover documents regarding such processing, and compel relevant testimony (e.g., in Hong Kong, Canada, Mexico and the U.S.).[61] Furthermore, some DPAs are empowered to enter and search premises where data processing is performed and seize evidence, in certain circumstances, without the consent of the owner or prior authorization from the courts.[62] Singapore's Personal Data Protection Commission, for example, is authorized to enter an organization's premises without a warrant so long as it gives two days' notice (but the DPA must obtain a search warrant for unannounced visits or when seizing information).[63] Israel's DPA has the right to conduct unannounced audits and inspections of premises where databases are maintained, and collect evidence and seize computers.

Similarly, the Belgian Privacy Commission may formulate non-binding recommendations, but must submit a criminal complaint to the Public Prosecutor's Office for criminal violations or file a civil action before the Tribunal of First Instance.

3. Adjudication

DPAs play an important role in enforcing the data protection rights of individuals. Depending on the jurisdiction, the DPA may function as a prosecutor who seeks redress for privacy incursions or as an arbiter who mediates or adjudicates disputes involving privacy infringements within the relevant legal framework. Because these roles vary by jurisdiction, DPAs typically are granted a range of legal authorities to pursue their designated responsibilities.

Many legal systems provide DPAs with the ability to prosecute alleged privacy violations. These DPAs may bring enforcement actions before a tribunal either independently or at the request of a third party. They are responsible for presenting the case against the individual or organizations suspected of violating the data protection law. By contrast, other jurisdictions entrust their DPAs to adjudicate data protection laws

60 *See* European Union Agency for Fundamental Rights, *supra* note 3.

61 *Id.* at 22.

62 *Id.*

63 ROSEMARY P. JAY, DATA PROTECTION & PRIVACY 2015 138 (3d ed. 2014).

directly. In this capacity, a DPA has quasi-judicial powers that allow it to hear complaints, decide the merits of the case brought by a claimant (as an alternative forum to judicial authorities), issue declarations of fault and resolutions, and impose a duty to take provisional or correctional measures.[64] Nevertheless, the administrative decisions made by the DPA may be appealed to the courts through the judicial system.[65] Certain jurisdictions limit DPAs' adjudicatory authority to a more passive role in which they refer claims to the courts or law enforcement authorities, or facilitate or enable settlement of complaints through the use of alternative dispute resolution processes. These DPAs typically issue non-binding decisions and enter into settlements with interested parties, but are required to initiate a lawsuit or hand over disputes to other law enforcement agencies that will enforce the law through the judicial system if no agreement can be reached. In Switzerland, for example, the Federal Data Protection and Information Commissioner has no direct enforcement powers against private or public organizations, and instead may issue non-binding recommendations to the organization and submit the matter to the Federal Administrative Court and the Federal Supreme Court for a decision if the recommendations are rejected or ignored.[66]

Depending on the jurisdiction, the DPA may function as a prosecutor who seeks redress for privacy incursions or as an arbiter who mediates or adjudicates disputes involving privacy infringements within the relevant legal framework.

Similarly, the Belgian Privacy Commission may formulate non-binding recommendations, but must submit a criminal complaint to the Public Prosecutor's Office for criminal violations or file a civil action before the Tribunal of First Instance.[67] The Argentine Privacy Commissioner may refer matters that cannot be resolved to the Director of Human Rights Proceedings, who may in turn refer the matter to the Human Rights Review Tribunal, which can issue binding decisions and award various remedies. In Hong Kong, the DPA can

64 European Union Agency for Fundamental Rights, *supra* note 3, at 26.

65 On the other hand, in Mexico, the DPA is empowered under the Mexican Constitution to issue binding, final and *incontestable* decisions, and impose fines and sanctions for privacy infringements.

66 Jay, *supra* note 63, at 178.

67 *Id.* at 24.

issue only non-binding "enforcement notices" after finding a violation of the data protection law; these enforcement notices give the violator an opportunity to correct its conduct, but the courts, rather than the DPA, have the power to impose penalties for noncompliance.[68] In South Korea, both the Ministry of the Interior and the Korea Communications Commission may issue corrective orders and administrative fines.[69]

DPAs often have certain remedies available to them to address violations of law. Depending on the jurisdiction, the DPA may have the authority to issue a warning or reprimand, enter into a settlement agreement, award indemnity, impose sanctions or order redress. Certain DPAs in the EU have the legal authority to levy administrative fines, which are subject to judicial review. In other jurisdictions, DPAs can negotiate settlements, but do not have the authority to fine violators,[70] while other DPAs are empowered to order monetary or equitable redress. In the UK, for example, the Information Commissioner's Office may issue certain types of administrative fines, but it is not empowered to order violators to provide redress to individuals who seek compensation for harm.[71] In the U.S., the FTC has the ability to enter into settlement agreements with companies.[72] A number of these settlements have obligated businesses to implement comprehensive privacy and security programs, engage independent experts to perform biennial assessments, provide monetary redress to consumers, repay ill-gotten gains, delete unlawfully obtained consumer information, and provide robust notice and choice mechanisms to consumers. The Israeli DPA can issue declarations of fault and fines. It also can suspend or revoke database registrations, which can be appealed to a court.[73] The Philippine Privacy Commissioner is empowered to award indemnity on matters affecting any personal information.[74]

68 *See* Personal Data (Privacy) Ordinance, (2012-13) Cap. 486, §§ 50, 50A (H.K.).

69 *See* Personal Information Protection Act, Mar. 29, 2011 (S. Kor.).

70 European Union Agency for Fundamental Rights, *supra* note 3, at 35.

71 Jay, *supra* note 63, at 206.

72 Although the FTC may not levy civil monetary penalties for violations of Section 5 of the FTC Act, it may issue fines for violations of certain privacy statutes, such as the Children's Online Privacy Protection Act, the Fair Credit Reporting Act, and Do Not Call. Furthermore, if a company violates a settlement order, the FTC may seek civil monetary penalties for the Section 5 violations.

73 Protection of Privacy Law, 5741–1981, Section 10(3)(f) (Isr.).

74 *See* Data Privacy Act of 2012, Rep. Act No. 10173, § 7(b) (2011) (Phil.).

In carrying out their enforcement responsibilities, DPAs also may have the equitable power to intervene in data processing practices to prevent or mitigate the risk of a violation. This includes the authority to (1) approve a processing operation on sensitive data before it may be carried out; (2) order the discontinuation of a processing activity or the modification, deletion or destruction of data being processed; (3) temporarily or permanently ban or block data processing activities;[75] and (4) require the registration of certain processing and implementation of specific safeguards to prevent unlawful data processing or compromise of data.[76] The vast majority of DPAs in the EU have some form of such authority, including the ability to issue a prohibition notice or a mandatory injunction against data processing in violation of data protection law.

4. Outreach

In a majority of jurisdictions, the job responsibilities of the DPA include providing recommendations, advice and guidance to the regulated community, the public and government officials. For example, DPAs often inform data subjects of their rights, advise entities of their obligations, answer questions about data protection laws and issue opinions on the meaning of existing rules. Some countries split advisory duties. In Mexico, for example, the Ministry of Economy is tasked with educating national and international corporations about their data protection obligations under Mexican data protection law, and working in cooperation with the national DPA to, among other activities, issue relevant guidelines for the content and scope of privacy notices.[77] In Russia, while the Roskomnadzor is the federal authority responsible for protecting individuals' personal data rights, another agency, known as FSTEK, is charged with developing technical regulations on data processing (e.g., requirements for IT systems used to carry out the

DPAs often inform data subjects of their rights, advise entities of their obligations, answer questions about data protection laws and issue opinions on the meaning of existing rules.

75 For example, the Philippine Privacy Commissioner may impose a temporary or permanent ban on processing of personal information, upon finding that the processing will be detrimental to national security and the public interest.

76 European Union Agency for Fundamental Rights, *supra* note 3, at 22-24.

77 Jay, *supra* note 63, at 116.

processing and measures required for legitimate data transfers).[78] FSTEK also is often involved in the inspections carried out by Roskomnadzor.[79]

5. Policymaking

Many DPAs serve as policymakers in some capacity, whether informing those with policymaking power or developing policies themselves. In either case, DPAs regularly are consulted as a matter of practice.[80] Given their expertise in data protection law and familiarity with the regulated community, DPAs can help enlighten policy makers and make data protection legislation more effective and responsive to changes in the regulatory environment.

With respect to advising policymakers, in certain jurisdictions, the DPA's advisory role is well-established and formalized by statute. In such jurisdictions, the executive and legislative branches are required to consult the DPA prior to the enactment of relevant legislation or regulations. For example, Article 28(2) of the Data Protection Directive calls for supervisory bodies to be consulted by national legislatures when drafting administrative measures or regulations relating to the protection of individuals' rights and freedoms with regard to the processing of personal data. In other jurisdictions, the DPAs' advisory activities are optional and conducted on a more ad hoc basis. The FTC, for example, frequently testifies before the U.S. Congress about data privacy and consumer protection issues.[81] DPAs also may advise the executive and legislative branches on relevant draft legislation and provide comments on privacy-related legislative and regulatory proposals.

Given their expertise in data protection law and familiarity with the regulated community, DPAs can help enlighten policy makers and make data protection legislation more effective and responsive to changes in the regulatory environment.

In addition to advising policymakers, DPAs also might have quasi-legislative power to promulgate regulations, supervise the development

78 *Id.* at 132.

79 *Id.*

80 European Union Agency for Fundamental Rights, *supra* note 3, at 26. In France, Italy, Germany, Austria and Greece, consultation with the DPA is legally required in the elaboration of executive regulations. *Id.* at 28.

81 FTC, *2014 Privacy and Data Security Update* (2015).

of private codes of conduct and issue binding opinions for the regulated community.[82] France's DPA, for example, is empowered to establish procedures and standards for personal data processing, and has issued codes of conduct for compliance.[83] In Hong Kong, the Privacy Commissioner is authorized to approve and issue codes of practice that offer practical guidance for complying with the provisions of the data protection law. Pursuant to UK law, the Information Commissioner has the authority to issue industry codes of practice. Similarly, Ireland's DPA has the authority to propose and prepare codes which, if approved by the legislature, have binding legal effect.[84] In New Zealand, the DPA has the power to issue codes of practice for specific industries, including credit reporting agencies and telecommunications providers. In Israel, although guidelines issued by the DPA are not legally binding per se, they effectively serve as guiding principles for the DPA's exercise of enforcement powers. In addition, some DPAs may propose legislative and regulatory reforms relevant to data protection law to address emerging issues.[85] In the U.S., the Department of Commerce has convened several multistakeholder processes concerning privacy issues associated with new technologies, including unmanned aircraft systems, mobile applications and facial recognition technologies. These processes bring together stakeholders from industry, civil society and academia to develop voluntary codes of conduct, bills of rights, lists of best practices and other types of guidelines related to data privacy issues.

B. Structural Attributes of a DPA

The governance framework of a DPA is an important feature to consider when assessing the qualities of an effective DPA. A DPA's structure can be broken down into four key elements: (1) the DPA's source of financial funding; (2) the system for appointing and removing DPA officials; (3) the DPA's decision-making authority and autonomy; and (4) the DPA's jurisdictional and subject matter scope.

82 European Union Agency for Fundamental Rights, *supra* note 3, at 28.

83 *Id.* at 44.

84 Data Protection Acts of 1988 and 2003 (Acts No. 25/1988, 6/2003) § 13 (Ir.), *available at* https://www.dataprotection.ie/docs/Law- On-Data-Protection/m/795.htm.

85 *See* European Union Agency for Fundamental Rights, *supra* note 3, at 24.

Seeking Solutions:

1. Financial Funding

The source and adequacy of a DPA's funding can have a significant impact on the DPA's autonomy, incentives and effectiveness. Below are examples of the various ways in which DPAs can receive funding.

- Some DPAs are fully financed by their respective governments and are not funded at all through their enforcement activities (e.g., registration fees or sanction revenues). Most EU Member States' DPAs are fully funded by their nation's governmental budgets. This includes, for example, the DPAs in Estonia, France, Italy and the Netherlands.[86] Outside of Europe, the DPAs in Argentina, Mexico, New Zealand and South Korea, for example, are fully funded by their national governments.

- Other DPAs are financed by their respective governments and through their enforcement activities. These DPAs may be incentivized to increase their enforcement activities to boost their resources. Examples include Hong Kong, Israel, Luxembourg and Malta.[87]

- Other DPAs are financed solely through their enforcement activities. One notable example is the UK, in which registration fees provide the sole source of funding for the country's DPA.[88] DPAs that are funded solely through enforcement activities may have an even greater incentive to increase such activities.

Regardless of the source of funding, many DPAs do not receive sufficient resources to allow them to be as autonomous and effective as they otherwise might be.

Regardless of the source of funding, many DPAs do not receive sufficient resources to allow them to be as autonomous and effective as they otherwise might be. A study conducted by the UK ICO highlighted this issue: "As public sector budgets remain under pressure DPAs are likely to continue to face the prospect of financial restraints which means that it could be problematic in the future for DPAs to properly resource all the work they would ideally like to do. [R]esearch [also has] found that in several DPAs understaffing and a lack of adequate financial resources was a relevant element in ensuring the autonomy of DPAs."[89]

86 *Id.* at 20.

87 *Id.*

88 *Id.*

89 Information Commissioner's Office, *supra* note 2, at ¶¶ 88-89.

The study determined that a lack of resources "may present a barrier to how effectively DPAs can respond to the data protection challenges which new technologies bring."[90] DPAs in countries such as Austria, Bulgaria, Romania, Cyprus, France, Greece, Italy, Latvia, the Netherlands, Portugal and Slovakia have all reported being hampered by inadequate funding and staffing.[91]

There is some risk that the sources and adequacy of funding may improperly influence the decisions and actions of a DPA, and ultimately hinder its ability to meet its regulatory goals. To reduce this risk, funding sources and sufficiency of funding should be transparent so the public and regulated community have confidence that the DPA is acting independently and effectively. As an additional control, DPAs' budgets also should be subject to periodic governmental review to ensure that they are adequate and the funds are being used effectively and efficiently.

2. Tenure of a Data Protection Official

Although a DPA's independence from government can never be absolute, for a DPA to be more structurally autonomous (and viewed by the public and regulated community as such), the processes for appointing and removing DPA officials must be transparent, fair and unbiased. As one study suggested, structural autonomy is, "in fact, primarily assured by the procedure of nomination and removal of [DPA] officers."[92]

To be effective, DPAs should be seen as credible regulators that are not beholden to outside influences and political agendas. The UK ICO study found that a vast majority of the public "believed it was important that [DPAs be] independent of government and business."[93] The same study also found that "[t]he independence of some DPAs has been called into question by the public and . . . by the European Commission. There have been concerns that DPAs' governing staff are appointed by political bodies, or that [they are] supervised by a specific government ministry, or appear to take limited action against other public institutions where there has been a data protection breach."[94] The Court of Justice of the European Union also has indicated that DPAs must remain free from external

90 *Id.* at ¶ 130.

91 European Union Agency for Fundamental Rights, *supra* note 3, at 42.

92 *Id.* at 19.

93 Information Commissioner's Office, *supra* note 2, at ¶ 84.

94 *Id.* at ¶ 85.

influences, including direct and indirect State influence. "The mere risk of political influence through the State is sufficient to hinder the independent performance of the DPA's tasks."[95] Transparent and fair appointment and removal processes also help ensure that DPAs are structurally autonomous and trusted by the various stakeholders. Below is a summary of the various ways in which DPA officials are appointed to and removed from office.

i. Appointment Options

In many EU countries (e.g., Germany, Slovenia and Greece), DPA officers are elected by legislative assemblies.[96] Some countries do more than others to ensure that appointments are fair and lead to an autonomous and independent DPA. Greece, for example, requires a consensus between the majority and opposition parties before a DPA official may be appointed.[97]

On the other end of the spectrum are countries such as Hong Kong, Ireland, Israel, Luxembourg, Philippines, the UK, Lithuania and Estonia, in which DPA officials are directly appointed by their respective governments without giving opposing voices in the legislature an opportunity to object to the appointment.[98] In other countries, such as Argentina, Denmark and Latvia, DPAs are connected to their respective country's Ministry of Justice.[99] In these cases, there often is doubt as to whether the appointed DPA officials truly can be autonomous and not beholden to the politicians who placed them in office.[100]

Transparent and fair appointment and removal processes also help ensure that DPAs are structurally autonomous and trusted by the various stakeholders.

Some countries involve a combination of various government branches (i.e., executive, legislature and judiciary) and public organizations in the

95 *Id.* at ¶¶ 83-91.

96 European Union Agency for Fundamental Rights, *supra* note 3, at 19.

97 *Id.*

98 *Id.*

99 *Id.* at 8.

100 *Id.*

DPA nomination and appointment process.[101] These countries include Argentina, France, Mexico, Spain, Portugal and Belgium. An example of this process also can be found in the U.S., where the President nominates an individual to be an FTC Commissioner and the nomination must be confirmed by the Senate before the individual takes office.[102] In Mexico, the Chamber of Senates of the Mexican Legislative Branch appoints the DPA's seven commissioners, which can be vetoed by the Mexican President within ten days of appointment.[103] In South Korea, there are different appointment processes for the different data protection regulators. The National Assembly and Chief Supreme Court Justice nominate the members of the Personal Information Protection Commission, who are then considered and appointed by the President.[104] For the Korea Communications Commission, two members are appointed by the President and three members are appointed upon the recommendation of the National Assembly (of these latter three members, the ruling political party recommends one member and the opposition party recommends the other two members).[105] In Argentina, the DPA is appointed by the President and submitted to the National Congress for approval.

The more entities that play a role in the DPA selection process, the more likely the DPA will have the ability and incentive to act fairly and independently. When DPAs are appointed solely by one government entity or politician, there is a risk that those DPAs will not be as autonomous as the public and the regulated community would hope.

ii. Removal Options

Fair removal procedures and term limits help ensure that DPAs remain autonomous and independent once they take office. DPA officials should neither remain in power once they are no longer effective nor be arbitrarily removed from power for political reasons. To help ensure fair processes, the procedures and grounds for removal should be codified in law.

101 *Id.*

102 Daniel J. Solove and Woodrow Hartzog, *The FTC and the New Common Law of Privacy*, 114 Colum. L. Rev. 583, 608 (2014).

103 Constitución Política De Los Estados Unidos Mexicanos [C.P.], *as amended,* Diario Oficial de la Federación [DO], 5 de Febroro de 1917 (Mex.), art. 6, section A, subsection VII, paragraphs 8, 9 and 10 (2016), *available at* http://www.diputados.gob.mx/LeyesBiblio/htm/1.htm.

104 Personal Information Protection Act, Mar. 29, 2011, art. 7 (S. Kor.).

105 Act on the Establishment and Operation of Korea Communications Commission, Mar. 23, 2013, art. 5 (S. Kor.).

In the U.S., for example, FTC Commissioners serve staggered seven-year terms and cannot be removed from office except for "inefficiency, neglect of duty, or malfeasance in office."[106] Further, no more than three FTC Commissioners may be members of the same political party.[107] In Mexico and Italy, DPA officials may serve only one term of seven years. In New Zealand, the Privacy Commissioner can serve multiple five-year terms.[108] In the Philippines, DPA officials can serve two three-year terms. In countries such as Slovenia and Poland, DPA officials can be removed only for specific types of misconduct pursuant to the same procedures used to appoint them.[109] In Israel, DPA officials may be removed in accordance with the general dismissal procedures of the Israeli civil service.[110] In Hong Kong, the Privacy Commissioner can only be removed from office by the Chief Executive with the approval by resolution of the Hong Kong Legislative Council on the grounds of inability to perform the functions of the office or misbehavior.[111] Such removal practices and term limits may help reduce political influence and pressure and foster a more independent DPA. In countries like Ireland and New Zealand, however, the government can itself directly remove DPA officials, which raises concerns about whether such DPA officials can be truly independent, especially when monitoring the government's compliance with data protection laws.[112]

To help ensure fair processes, the procedures and grounds for removal should be codified in law.

Removal procedures are more likely to be fair when they (1) are clearly codified in law and (2) include safeguards designed to prevent the removal of DPA officials for arbitrary or political reasons. To promote

106 Daniel J. Solove and Woodrow Hartzog, *supra* note 102, at 608.

107 *Id.*

108 European Union Agency for Fundamental Rights, *supra* note 3, at 20.

109 *Id.*

110 Israeli government executive decision number 2464 dated March 8, 2015; "Rotation and Tenure Arrangements for Senior Officials", Commissioner of Public Service (Directive 1.6 dated February 8, 2016) (in Hebrew), *available at* http://www.csc.gov.il/DataBases/CommissionGuidelines/Documents/GuideLine16.pdf.

111 *See* Personal Data (Privacy) Ordinance, (2012-13) Cap. 486, §§ 5(3), 5(4), 5(5) (H.K).

112 European Union Agency for Fundamental Rights, *supra* note 3, at 20.

an effective, fair and independent DPA, DPA officials need to know that they will be removed from power when they are no longer effective or act in a way that is opposed to the societal interests and will not be removed from power based on political whims.

3. Decision-Making Authority and Autonomy

In addition to adequate funding and appropriate appointment and removal procedures, a DPA's decision-making authority and autonomy are key structural elements to consider when analyzing the qualities of an effective DPA. In some jurisdictions, the DPA's powers are prescribed by law. For instance, the constitutions of Mexico, Portugal and Greece explicitly recognize and codify the existence and powers of their respective DPAs, which are given the authority to oversee the creation of data protection legislation.[113] In Malta and Spain, the DPAs are given distinct legal personalities under the law, and in Slovenia the DPA is given the right to commence legal proceedings and challenge the constitutionality of legislation before the national Constitutional Court.[114]

In the U.S., the FTC, which is considered the country's de facto federal DPA, has been steadily given more and more decision-making authority and autonomy. Over the years, for example, Congress has given the FTC (1) the power to enforce the Fair Credit Reporting Act (which ensures that consumer reporting agencies respect consumers' privacy); (2) rulemaking and enforcement powers under the Children's Online Privacy Protection Act; and (3) the authority under the Gramm–Leach–Bliley Act to establish safeguards rules for financial institutions to follow for securing customer records and information.[115] Under Section 5 of the FTC Act, the FTC also has broad authority to bring enforcement actions against companies for unfair or deceptive acts or practices relating to privacy and data security. The FTC's decision-making authority and autonomy have grown to such a large extent that the Third Circuit Court of Appeals confirmed that the FTC may bring lawsuits

A DPA's decision-making authority and autonomy are key structural elements to consider when analyzing the qualities of an effective DPA.

113 *Id.*

114 *Id.*

115 Daniel J. Solove and Woodrow Hartzog, *supra* note 102, at 603-604.

against companies for insufficient or unreasonable data security practices, despite having no obligation to publish rules or regulations regarding what constitutes reasonable security standards.[116]

With great authority and independence, however, comes great responsibility. The more independent and powerful a DPA is, the more it should be held accountable and its actions should be transparent to the various stakeholders, including the public, the regulated community and the legislature. Evaluation mechanisms, such as annual reports and audits, may be established to help ensure that relevant stakeholders can evaluate whether DPAs are acting effectively, fairly and efficiently, and are meeting their objectives. To further ensure that DPAs do not abuse their authority and independence, and maintain the trust of the public and the regulated community, DPAs should allow challenges to their decisions and actions. This may include (1) channels for complaint and redress regarding enforcement actions and existing regulations; (2) notice and comment periods whereby the public and regulated community can voice their opinions regarding proposed policies and regulations; and (3) legislative hearings in which DPAs can be questioned about and be required to explain certain major decisions they have made.

4. Jurisdictional Scope

DPAs in different countries have varied jurisdictional scopes of power. For instance, some DPAs focus solely on data protection, while other DPAs have a wide range of responsibilities, from processing "freedom of information" requests to overseeing environmental information. In the U.S., for instance, the FTC handles data protection regulation and enforcement, and also protects consumers more generally against anticompetitive, deceptive and unfair commercial practices. In Mexico, the DPA focuses on both data protection issues and those related to public access to information.[117] In Israel, the DPA is part of the Ministry of Justice, and has responsibility over such issues the Israeli electronic signature regime and credit reporting.[118]

116 *FTC v. Wyndham Worldwide Corp.*, 799 F.3d 236 (3d Cir. 2015).

117 Constitución Política De Los Estados Unidos Mexicanos [C.P.], *as amended,* Diario Oficial de la Federación [DO], 5 de Febroro de 1917 (Mex.), art. 6, section A, subsection VII, paragraphs 1 and 2, *available at* http://www.diputados.gob.mx/LeyesBiblio/htm/1.htm.

118 Israeli Electronic Signature Law, 5761–2001, Section 9 (Isr.) (unofficial translation), *available at* https://www.law.co.il/media/e-sig/Israeli_didsig_law_english.pdf.

Some DPAs focus solely on either the public or private sector, while other DPAs focus on both. A 2011 survey of 32 countries conducted by the International Association of Privacy Professionals found that "the widespread norm among jurisdictions is to endow their DPAs with a broad scope of authority, with over 90 percent of . . . respondents indicating their areas of focus include both the public and private sectors."[119] The study also found that "DPA responsibilities range from privacy enforcement to legislative advocacy to mediation, to name a few, with the vast majority of respondents reporting oversight responsibilities for public- and private-sector organizations as well as individuals."[120]

Some countries provide data protection powers to different agencies based on the types of businesses or practices the agencies typically regulate. For instance, in the U.S., although their data protection enforcement powers may at times overlap, the Department of Health and Human Services, the Federal Communications Commission, the FTC and the Securities and Exchange Commission all have jurisdictional scope over the particular types of businesses or practices they typically regulate (i.e., health and medical, communications, unfair or deceptive trade practices, and financial institutions, respectively). In Germany, the Federal Commissioner for Data Protection and Freedom of Information has a special department that is responsible solely for data protection in telecommunications and postal services.[121] In South Korea, there are four entities that have data protection-related powers: (1) the Personal Information Protection Commission; (2) the Ministry of the Interior, which governs general data protection issues under the Personal Information Protection Act; (3) the Korea Communications Commission which governs privacy issues related to online service providers; and (4) the Financial Services Commission, which governs privacy issues related to the financial services industry.

DPA responsibilities range from privacy enforcement to legislative advocacy to mediation, to name a few, with the vast majority of respondents reporting oversight responsibilities for public- and private-sector organizations as well as individuals.

119 International Association of Privacy Professionals, *supra* note 44, at 6.

120 *Id.*

121 *Id.* at 9.

IV. Conclusion

In an increasingly data-driven global market, effective data protection governance promotes accountability among relevant stakeholders, while enhancing the privacy compliance posture of the regulated community. A measured DPA that educates and supports the individuals and businesses it governs is well-situated to strike the appropriate balance between promoting sound data privacy practices and providing the regulated community with the tools to self-govern and thrive in the digital economy.

As the role of the DPA evolves with changing business and legal landscapes, the discourse around the characteristics and qualities of an effective DPA must consider the underlying principles of fairness, transparency, collaboration and consistency. These principles inevitably will serve as the foundation for a successful data governance framework, regardless of the divergent data privacy cultures around the world.

U.S. CHAMBER OF COMMERCE

1615 H Street, NW | Washington, DC 20062-2000
www.uschamber.com