

# **Data Protection Authorities**

## **2011 Global Survey**

International Association of Privacy Professionals





# Data Protection Authorities 2011 Global Survey

---

## Executive Summary and Findings

### International Association of Privacy Professionals



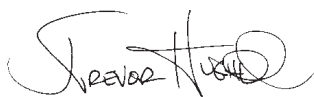
Dear Data Protection Professionals,

We are pleased to present the third edition of the IAPP's annual analysis of the work of data protection authorities (DPAs) from around the world.

The *Data Protection Authorities 2011 Global Survey* expands on the past two years to offer insights into the work of data protection regulators. This year's report provides a deeper understanding of key points of interest—from funding and structure to focus and enforcement. We have continued to build on last year's analysis of such topics as how DPAs are meeting the technological needs inherent in many aspects of data protection, while expanding our survey to explore new questions recommended by past survey participants and privacy experts. This year's report also features in-depth profiles on members of various DPA staffs and the varied areas of expertise that contribute to privacy protection.

Built upon three years of detailed responses from DPAs in every sector of the globe—including four new respondents from North America, South America and Europe—we hope you will find the report to be a valuable resource for exploring the ever-evolving nature of global data protection regulation.

Sincerely,



J. Trevor Hughes, CIPP  
President and CEO  
IAPP





# Table of Contents

<b>Introduction</b>	<b>4</b>
<b>I. Survey Methodology</b>	<b>5</b>
<b>II. Executive Summary</b>	<b>6</b>
<b>III. Survey Findings</b>	<b>8</b>
<b>DPA Leadership</b>	<b>8</b>
Profiles in Privacy: Dirk Hensel	9
<b>The DPA Office: Staff, Size and Allocation</b>	<b>10</b>
Profiles in Privacy: Anne-Marie Hayden	15
<b>Authority and Enforcement</b>	<b>16</b>
Profiles in Privacy: Mike Flahive	23
<b>Transborder Issues</b>	<b>24</b>
Profiles in Privacy: IFAI	28
<b>Appendices</b>	<b>31</b>
<b>APPENDIX A: Global DPA Audited Survey Results</b>	<b>31</b>
<b>APPENDIX B: Data Protection Offices and Officials</b>	<b>37</b>
<b>APPENDIX C: Appointing Bodies</b>	<b>39</b>
<b>APPENDIX D: DPA Concerted Efforts</b>	<b>40</b>

# Introduction

---

The International Association of Privacy Professionals' *Data Protection Authorities 2011 Global Survey* includes input from privacy offices and data protection authorities in 32 jurisdictions to examine the scope, authority and resources of DPAs.

A key purpose of this survey, which is now in its third year, is to assess the present state of data protection, privacy and information sharing while providing a reliable and useful platform for the continued exploration of these issues.

Among the points explored in this survey are DPAs' primary areas of focus and responsibilities; overall staffing and budgetary levels, as well as allocation of resources across different areas of responsibility, and the current status and future expectations of enforcement powers.

Our findings are based on the responses of DPAs in the following jurisdictions:

Argentina	Italy
Australia	Latvia
Bulgaria	Lithuania
Canada	Macao
Cyprus	Malta
Estonia	Mauritius
European Union	Mexico
Faroe Islands	New Zealand
Finland	Norway
Germany	Poland
Gibraltar	Serbia
Greece	Slovak Republic
Guernsey	Slovenia
Hong Kong	Spain
Hungary	Sweden
Ireland	United Kingdom

# I. Survey Methodology

---

The IAPP's *Data Protection Authorities 2011 Global Survey* was fielded to 64 federal offices overseeing privacy and data protection as well as the European Data Protection Supervisor (EDPS). In May, the IAPP sent individual e-mails to contacts at each DPA to invite their participation in the survey. Reminders were sent to DPAs prior to the survey's closing date in early June. A total of 32 DPAs fully completed the survey for inclusion in the 2011 report.

The following considerations should be noted when evaluating the results of this survey.

## ***Breadth of response***

This survey's findings are based on voluntary returns with a response rate of 50 percent. Based on the breadth of respondents, the data offered here provides insights on a range of DPAs; however, it is important to note that there may be substantial differences between respondents and those DPAs that chose not to participate in this year's survey. It is of interest that a small number of past participants did not return surveys for this year's report, while several new DPAs have provided data incorporated into these findings.

## ***Language***

The questionnaire was presented in English only, which may have had an impact on the response rate and/or caused confusion for some respondents.

## ***EDPS***

Although this survey primarily focuses on national data protection authorities, we have also included data pertaining to the EDPS, the European Union's DPA, which is devoted to promulgating best practices for protecting personal data and privacy in all EU institutions and serves as a model for DPAs in the EU and possibly beyond the region as well.

## ***Benchmarking***

With this third DPA survey, the IAPP seeks to provide not only a baseline for future surveys but also to collect information on current privacy challenges. Naturally, the questions we ask continue to vary as issues evolve and change over time. As was the case with our 2010 survey, this year's report contains the addition of several new questions that should be taken into account when analyzing the results for comparative purposes.

## II. Executive Summary

---

Building upon two prior years of data, the 2011 DPA survey reveals both new and continuing trends for data protection authorities and privacy commissioners. In analyzing these trends; however, it is important to note that this year's sample includes three DPAs that had not previously participated in the survey, bringing with them new information not assessed in last year's report. Conversely, some authorities that responded in 2010 did not return completed surveys in time for this year's report, so some points of comparison will not be identical from year to year.

The *Data Protection Authorities 2011 Global Survey* focuses on four data sets compiled from 32 DPAs that completed the survey, spotlighting trends in the areas of Leadership; the DPA Office: Staffing, Size and Allocation; Transborder Issues, and Authority, Compliance and Enforcement.

- **DPA Leadership**

Based on the responses to this year's survey, and on trends noted in our past studies, it is clear that the role of the data protection commissioner or supervisor is now *de rigueur* for protection of citizens' privacy at the national level. This year marks the first time that all jurisdictions reported having this role.

- **The DPA Office: Staffing, Size and Allocation**

Although budget allotments varied widely across jurisdictions, this year's survey results show a growing trend of increased DPA staff sizes, up about 14 percent over last year's survey. The primary areas of focus, however, were consistent. DPAs have once again reported that three activities—office administration, complaint management and enforcement—receive the greatest share of their annual budgets.

- **Transborder Issues**

In our 2011 survey, we take a closer look at issues affecting DPAs and individuals across jurisdictional lines. Among our findings, it appears that responding European DPAs handled a relatively small number of Binding Corporate Rules (BCRs) applications in the past year, with the vast majority approving five or fewer each year. We also asked our European respondents for their feedback on one transborder issue that has received significant attention in the past year—the EU-U.S. Safe Harbor agreement. None reported a “strongly negative” view of this framework, despite indications to the contrary in some media reports.

- **Authority and Enforcement**

Continuing a trend we spotlighted in last year's report, the widespread norm among jurisdictions is to endow their DPAs with a broad scope of authority, with over 90 percent of our respondents indicating their areas of focus include both the public and private sectors. This year's results also point to an increase in the number of DPAs with a focus on information access/freedom-of-information, from eight in 2010 to 11 this year. 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. In terms of enforcement, DPAs reported a variety of mechanisms, with all responding that they launched at least one privacy investigation in the past year. A total of 86 percent of respondents reported beginning more than 10, with half conducting upwards of 100 investigations in 2011. See *Figure 1*.



**Figure 1: Data protection/privacy (public sector)**

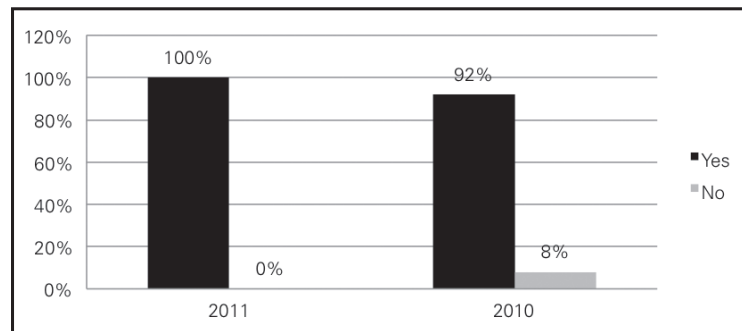
<b>Data protection/privacy (public sector)</b>	<b>Data protection/privacy (private sector)</b>	<b>Information access/freedom of information</b>
Argentina	Argentina	Australia
Australia	Australia	Cyprus
Bulgaria	Bulgaria	Germany
Canada	Canada	Hungary
Cyprus	Cyprus	Ireland
Estonia	Estonia	Mauritius
European Union	Finland	Mexico
Faroe Islands	Gibraltar	Serbia
Finland	Greece	Slovenia
Germany	Guernsey	United Kingdom
Gibraltar	Hong Kong	
Greece	Hungary	
Guernsey	Ireland	
Hong Kong	Italy	
Hungary	Latvia	
Ireland	Lithuania	
Italy	Macao	
Latvia	Mauritius	
Lithuania	Mexico	
Macao	New Zealand	
Mauritius	Norway	
Mexico	Poland	
New Zealand	Serbia	
Norway	Slovak Republic	
Poland	Slovenia	
Serbia	Spain	
Slovak Republic	Sweden	
Slovenia		
Spain		
Sweden		
United Kingdom		

### III. Survey Findings

#### DPA Leadership

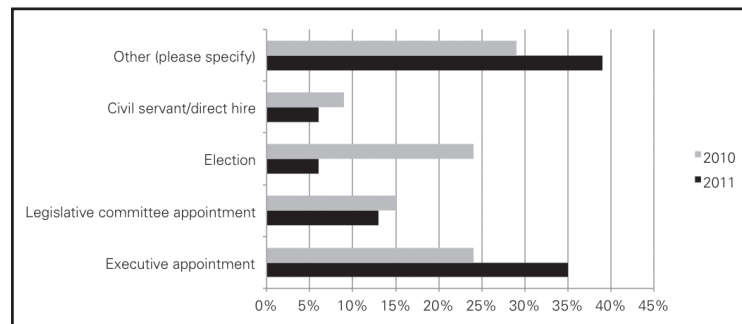
While having a data protection commissioner's (DPC) role—at least one dedicated official in charge of privacy and data protection efforts—has been the norm in our past surveys, this year the response was unanimous. While most reported one DPC, three of our responding DPAs have multiple individuals fulfilling the commissioner's role. In Australia, for example, while the privacy commissioner takes the lead on privacy and data protection matters, the country's information commissioners also have privacy/data protection functions. Mexico's DPA, meanwhile, is led by five commissioners, and in Bulgaria, the Commission for Personal Data Protection is a collective body consisting of five members.

**Figure 2: Prevalence of commissioners**

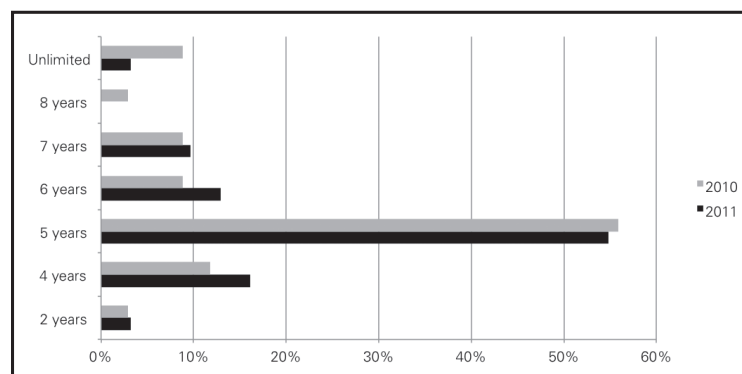


This year, 81 percent of respondents reported the DPC's appointment is reserved to executive officials or legislators, and DPC terms increased to an average of 4.9 years in 2011.

**Figure 3: Appointment process**



**Figure 4: Commissioner terms**



## Profiles in Privacy: Dirk Hensel

By Jedidiah Bracy, CIPP



Telecommunications and the delivery of information are undergoing a seismic shift into the digital realm, and technology is advancing at a rapid and unprecedented rate. Smartphones can track user locations, shopping preferences and Internet histories—often without the user knowing—and many companies

have the ability to store vast amounts of information for indeterminate amounts of time.

At the heart of these advancements is Germany's Federal Commissioner for Data Protection and Freedom of Information and the work of Dirk Hensel with the department responsible for data protection in the field of Telecommunication, Telemedia and Postal Services. Hensel's department must stay abreast of the rapid changes in telecommunications technology, deal with various data protection issues and work with a wide array of additional German supervisory authorities.

Multiple bodies have regulatory authority in Germany, and in the private sector, data protection supervision belongs to state authorities. The one exception to the rule is the supervision of telecommunications and postal services companies, which belongs to the federal authorities.

To describe his work, Hensel notes that his job is driven by current events, thereby making it "very diversified." He says his unit is "working within the legal field of creating codes—we don't make law—but we're involved whenever a law is drafted. We have an effect on data protection and do have influence on drafts."

Telecommunications legislation processed within Germany and the EU is also handled by Hensel's department, and with "more than 3,000 telecommunications providers and nine people in our unit," there is no shortage of work, he says.

Hensel's unit conducts onsite inspections to ensure compliance with data protection legislation. "Companies also come to us to ask for advice on projects," he says, "so we do a lot of consulting." His team also responds to citizens' complaints.

Hensel has been working in his current position for three years but began his internship in 2006. Before passing the bar, Hensel wanted to pursue copyright or media law, but one influential contact urged him to apply to the minister of the interior. Hensel helps brief his office on what to say to the media, acts as an expert witness in court and helps brief Data Protection Commissioner Peter Schaar. As with all employees on his team, Hensel says he reports to Schaar and works closely with him.

Hensel's office is working with several pressing issues in Germany and the EU, including the Federal Constitutional Court's overruling of the national implementation of the EU Data Retention Directive.

When asked about whether he is seeing any particular data protection trends in Germany, Hensel is optimistic.

"You have to differentiate between consumers and companies. I think that increased awareness in our population about data protection has resulted." Well-publicised data breaches "became more prominent in the press, so there was more awareness. People started to care about their data, and as a reaction, companies started to stress data protection."

There are, however, many issues causing concern. "Due to globalization and the Internet," he says, "you don't have national boundaries; you have worldwide accessibility to data on the one hand—which is good—but risks to privacy on the other."

With rapid changes in technology, it's also becoming more difficult to understand how things like cookies, geolocation and behavioural advertising work.

"Things need to be more transparent and everyone should have a choice," he says. "Transparency is one of the most crucial elements to give an individual the possibility to decide to what extent he or she wants to use privacy."

Though privacy is a global challenge, Hensel says each country's approach to privacy "is a question of cultural background of the nation and its people. There will be differences."

What is needed, he says, "would be to find a common basis for fundamental privacy rights. It's important to start the discussion."

## The DPA Office: Staff, Size and Allocation

### A. Overall Budget\*

Respondents reporting their DPA budgets varied widely in their allocations, with an average budget of €5.55 million. The Americas region boasts the most well-funded DPA—Mexico—and with Canada's Office of the Privacy Commissioner also in this region, includes two of the four top DPA budgets for an average regional allocation of €22.35 million. The European region follows, with four of the top six highest budgets and an average of €4,542,101 per DPA; however, it is important to note the absence of data from France, which last year reported one of the higher budget amounts. The Asia-Pacific region averaged €3,474,486 per DPA.

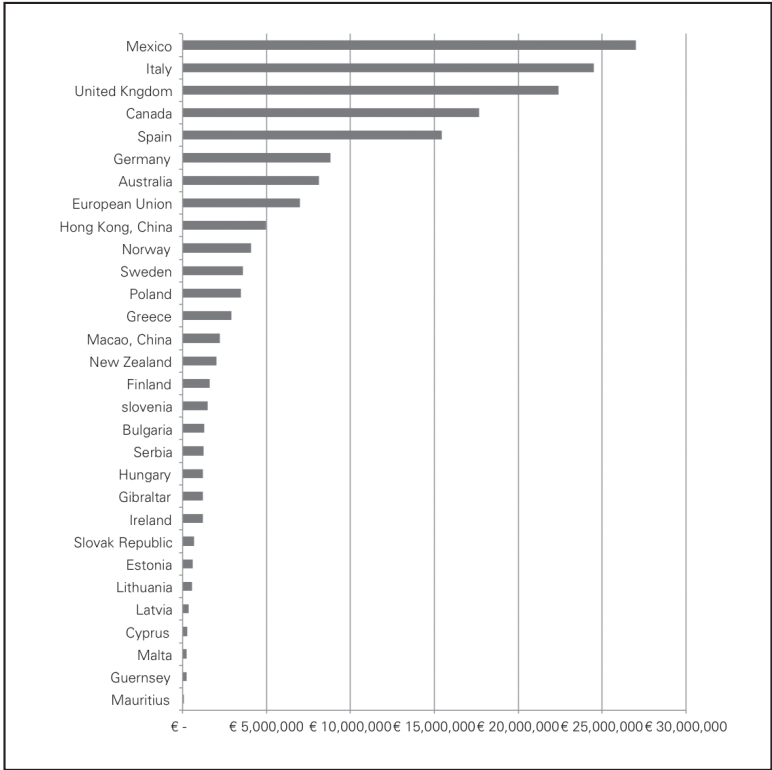
**Figure 5: Overall budget comparison**

<b>OVERALL BUDGET AVERAGE</b>	€ 5,551,327		
<b>AMERICAS AVERAGE</b>	<b>€ 22,349,533</b>	Poland	€ 3,475,126
Mexico	€ 27,012,414	Greece	€ 2,923,707
Canada	€ 17,686,651	Finland	€ 1,600,094
<b>ASIA-PACIFIC AVERAGE</b>	<b>€ 3,474,486</b>	Slovenia	€ 1,500,000
Australia	€ 8,118,257	Gibraltar	€ 1,201,000
Hong Kong	€ 4,975,212	Bulgaria	€ 1,308,871
Macao	€ 2,217,793	Serbia	€ 1,260,000
New Zealand	€ 1,999,396	Hungary	€ 1,215,454
Mauritius**	€ 61,770	Ireland	€ 1,200,000
<b>EUROPE AVERAGE</b>	<b>€ 4,542,101</b>	Slovak Republic	€ 684,349
Italy	€ 24,500,000	Estonia	€ 592,446
United Kingdom	€ 22,395,759	Lithuania	€ 546,667
Spain	€ 15,425,160	Latvia	€ 377,051
Germany	€ 8,798,253	Cyprus	€ 297,033
European Union	€ 7,000,000	Malta	€ 250,000
Norway	€ 4,093,416	Guernsey	€ 223,944
Sweden	€ 3,600,000		

\*Currencies were converted into euros between June 30 and July 8, 2011.

\*\*Mauritius is an island nation normally associated with the African continent, but because of the lack of other African respondents, we included it in the Asia-Pacific region.

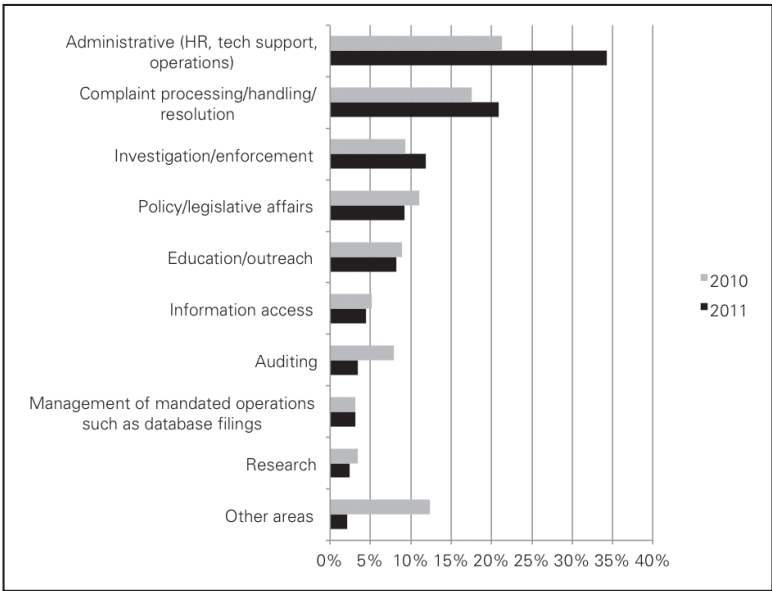
Figure 6: Annual budgets of data protection authorities



B. Funding Allocation by Activity

Consistent with past surveys, DPAs reported they allocate the greatest share of their annual budgets to three primary activities: Administrative, Complaint Processing and Investigation/Enforcement.

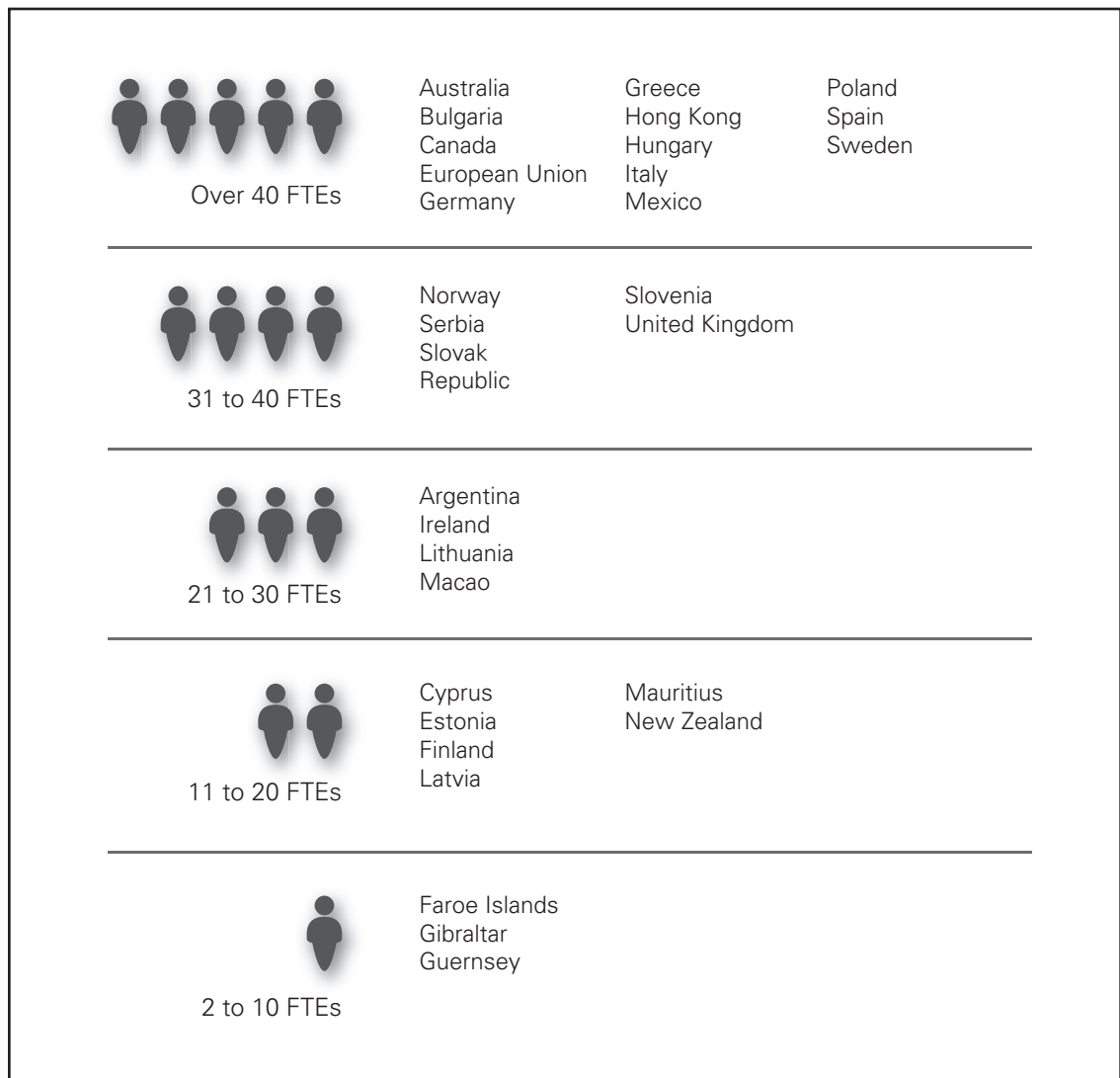
Figure 7: Budget allocation by activity



### C. Staffing

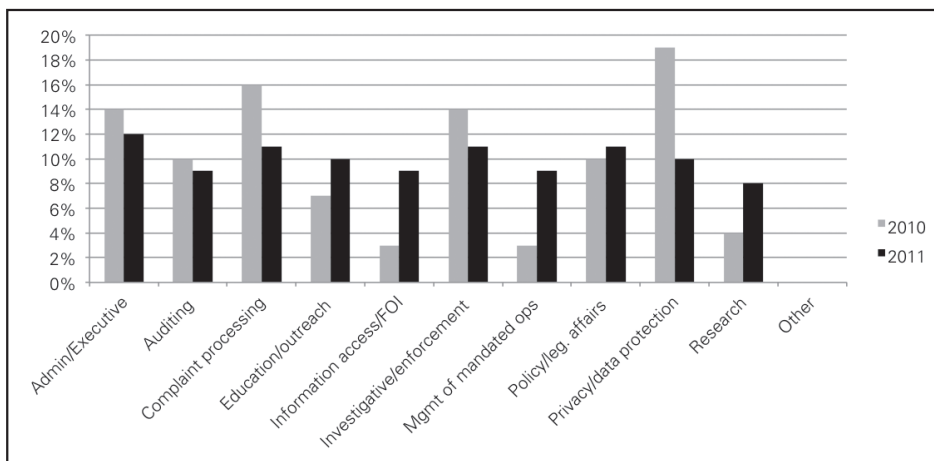
In spite of ongoing reports of widespread fiscal austerity, survey responses indicate that DPA staff sizes are growing. For 2011, 58 percent of responding DPAs listed 31 or more full-time employees (FTEs) in their central office, compared with 43 percent in 2010. On the other end of the spectrum, 10 percent of 2011 respondents said their office employs 10 or fewer FTEs, compared with 20 percent in 2010. Again this year, the survey indicates that maintaining regional offices is a rarity. Canada reports employing between two and five FTEs outside the central office; Germany, the United Kingdom and New Zealand were the only other DPAs listing regional offices, employing between 11 and 20 staff members outside the central office.

**Figure 8: Central office staff sizes**



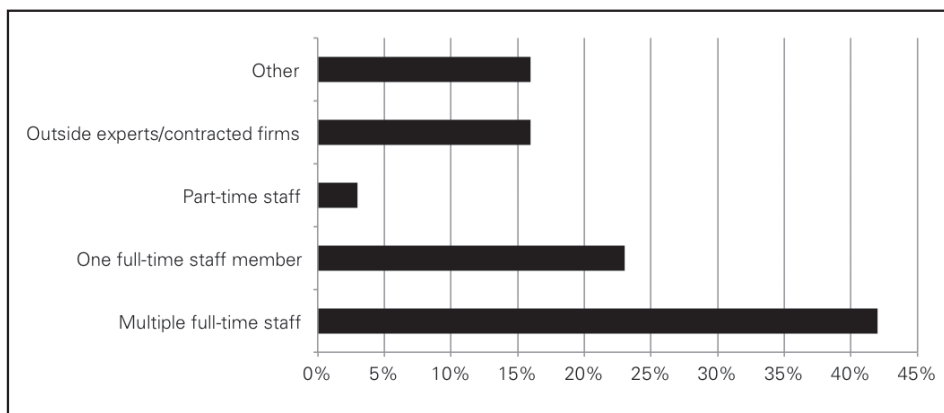
When it comes to DPA staff allotment by activity type, most fields were staffed with a similar number of employees to 2010, ranging between nine and 12 percent of total staff for each activity in 2011.

**Figure 9: Staff allocation by activity**



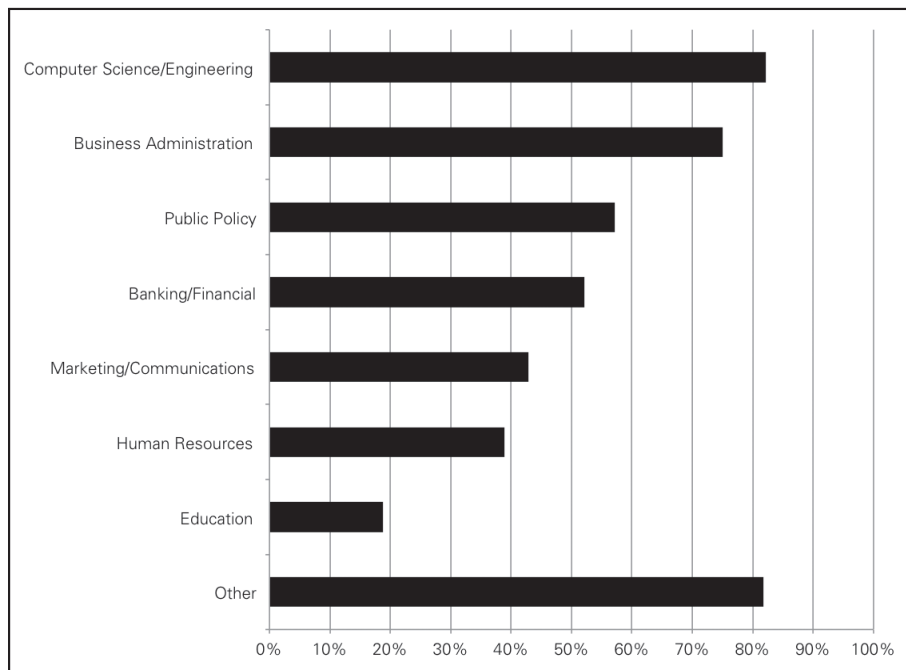
For operational technical support, such as would be required for investigations and complaint resolutions, the majority of DPA offices responded that they rely on internal full-time staff instead of outside contractors.

**Figure 10: Management of technological needs for investigations**



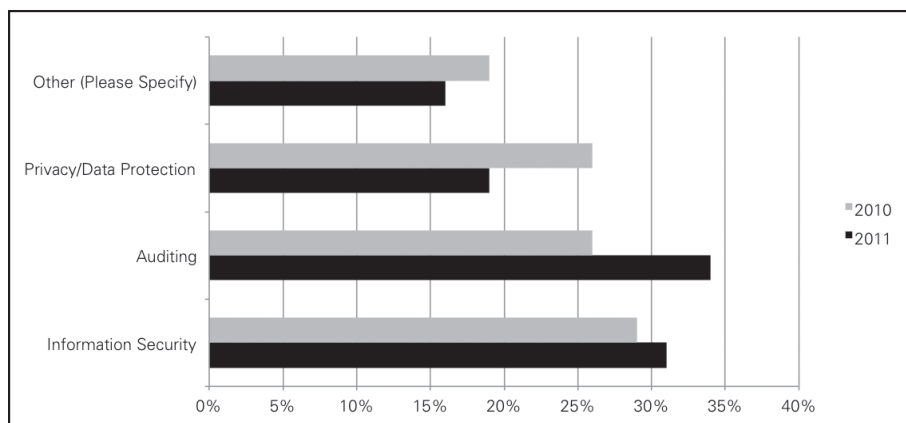
DPA offices employ staff with a wide variety of advanced degrees, the most prevalent areas being computer science and business administration; however, more than three-quarters reported employing staff with advanced degrees not listed on the survey. Based on the prevalence of responses, we will add the juris doctorate as a degree choice beginning with the 2012 survey.

**Figure 11: Staff with advanced degrees**



In looking at the number of DPA staff members holding professional certifications such as the CIPP, CISSP, CISA or CPA, a disparity seems to emerge between the number of IAPP members and the number of DPA staff holding a privacy certification. In 2010, 47 percent of members responding to IAPP surveys held a privacy certification, compared with 26 percent of DPA staff surveyed. This year, our annual surveys indicate that 66 percent of IAPP members hold a privacy certification, compared with 19 percent of DPA staff.

**Figure 12: DPA staff certifications**





## Profiles in Privacy: Anne-Marie Hayden

By Jennifer L. Saunders, CIPP



Facebook. Google. E-Harmony. Just three high-profile companies whose names come to mind when discussing the work of Canada's Office of the Privacy Commissioner (OPC). With the OPC the driving force behind enforcement and educational initiatives tied to some of the most well-known names in the

online world, a key role in the office is that of the OPC's communications team, led by Communications Director Anne-Marie Hayden.

The importance of communications in the broader picture of the work of data protection authorities like the OPC can perhaps best be illustrated by the 2010 mobilization of DPAs from around the globe to address online privacy concerns in the wake of issues with the introduction of one Internet giant's social networking feature.

Hayden notes that the effort, which was not an investigation but a call for improvements, "spoke to the power of communication for the issue of privacy."

By mobilizing DPAs and communicating with the press, the message that when it comes to privacy, the key is to "build it in rather than mop up the mess later" could be shared in a way that Internet users could immediately find accessible.

When asked what she perceives as the key to successful communication, Hayden answers at once.

"We hire writers," she says, pointing out that in a time when media has been changing drastically, former journalists—"super-smart people who understand complex issues and how to communicate them to the public"—have been seeking new lines of work and have brought broad perspectives to the OPC staff to support its communications efforts.

Like many privacy professionals, Hayden herself did not start out planning to pursue a career in the field of data protection. But, as is typical of so many of us who have found our way into this ever-evolving profession, Hayden describes her work as one of the most interesting careers imaginable.

After graduating from college, Hayden worked in public relations in the private sector, a career path that, she explains, provided her with exposure to significant issues as she handled account coordination and found herself doing a bit of everything—from public opinion research and media relations to production—learning the ins and outs of how such a firm works.

Those experiences taught Hayden a valuable skill that has served her well in her multifaceted role with the OPC—the ability to be nimble.

With Jennifer Stoddart's appointment as Canada's privacy commissioner in 2003, Hayden began to lead the OPC's communications more directly, developing and executing ideas and focusing on a team approach. Hayden explains that a key facet of her role is to pay attention to what is happening around her to best convey industry issues, policy guidance and best practices.

Today, the OPC has seen significant growth in its communications shop, Hayden notes, from about 10 staff members to between 20 and 25. As part of that growth, education and outreach has come under the communications umbrella.

Communications is now not only the first point of contact for many who are seeking information on the OPC, it is also a place for advice for organizations and individuals about rights and responsibilities, Hayden explains.

From a communications standpoint, the key is to "work on a very concrete, immediate strategy" when it comes to breaking news about data breaches, new social networking sharing options or other issues related directly to privacy, she says.

"The issues are increasingly complex. The need to synthesize them and make them easier to understand and meaningful to the general public is the challenge," she adds.

Looking forward, Hayden says, her team's goal is to build on past achievements; continually improve and coordinate communication, and build momentum.

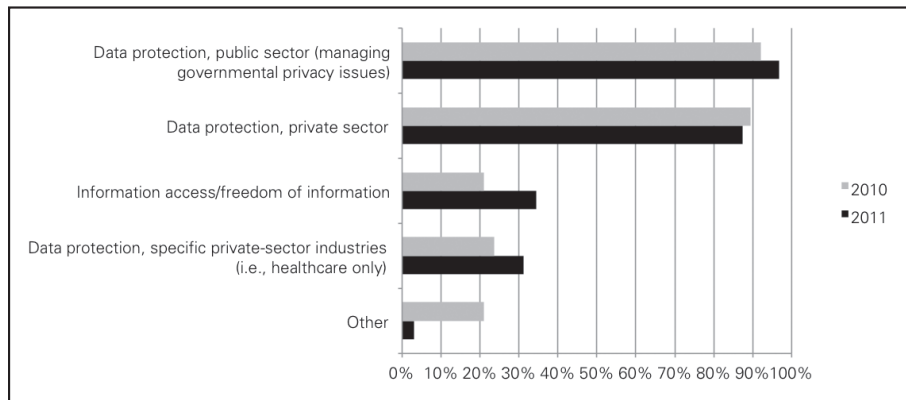
From a personal standpoint, she says, when it comes to overseeing communication and education aspects of the ever-changing privacy landscape, "Show me a job more interesting."

## Authority and Enforcement

### A. DPA Responsibilities

Respondents this year indicate it is the norm for jurisdictions to endow their DPAs with a broad scope of authority, with the vast majority of DPAs reporting their authority extends to both the public and private sectors.

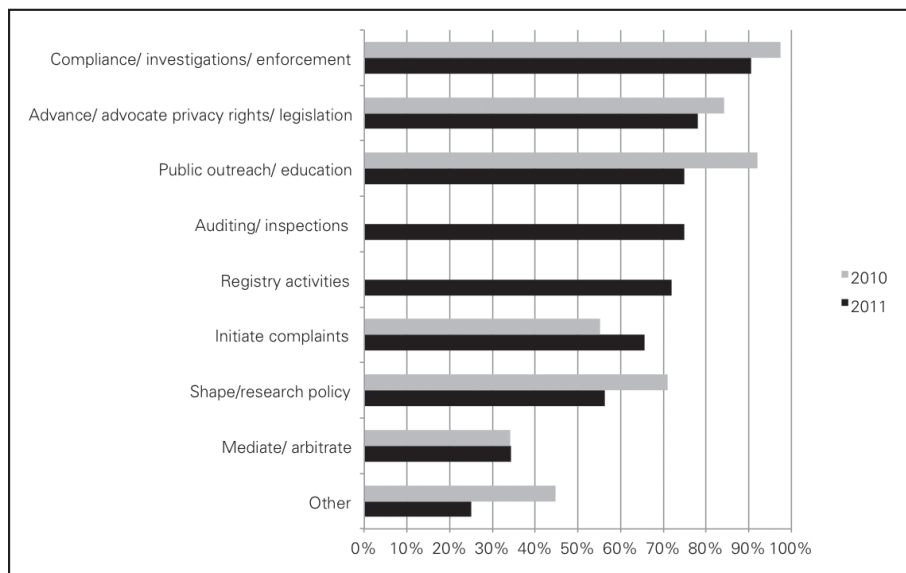
**Figure 13: DPA scope of authority**



DPAs typically have a broad range of responsibilities, including not only privacy enforcement but also legislative advocacy and mediation.

It is interesting to note that while the majority of DPAs still reported involvement in public outreach, significantly fewer reported such responsibilities this year—68 percent compared with 92 percent in 2010. A similar drop occurred in the policy-research responsibility.

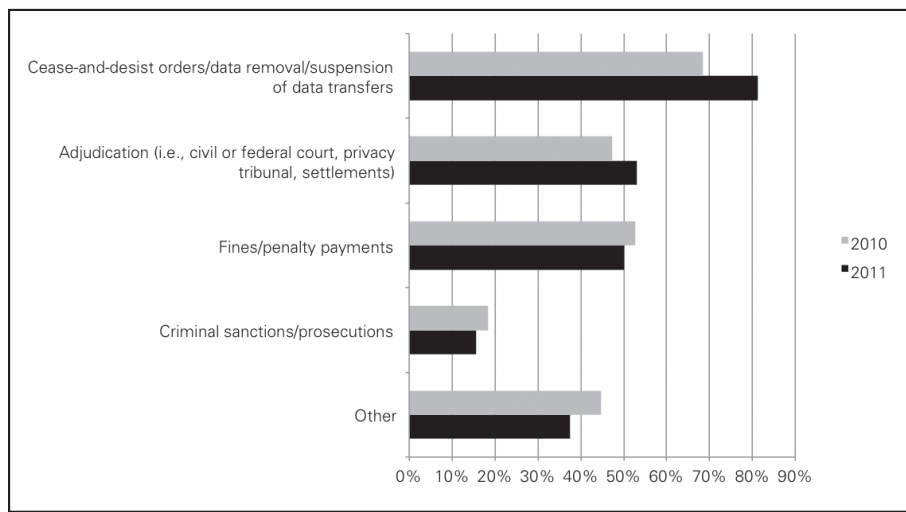
**Figure 14: DPA responsibilities**



## B. Enforcement Overview

About 81 percent of respondents said they oversee individuals as well as private- and public-sector organizations—84 percent specifically reporting private-sector organizations and 91 percent public-sector organizations. Most DPAs also reported that they have a variety of enforcement mechanisms at their disposal, with authority to block errant data practices topping the list at 74 percent.

**Figure 15: DPA enforcement powers**



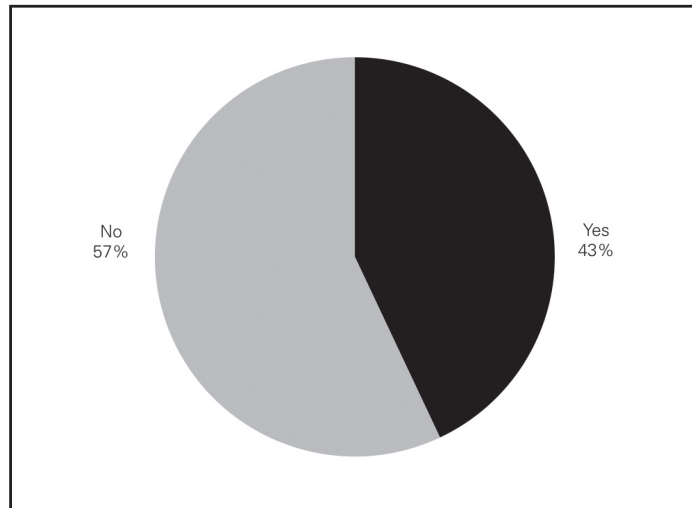
Several DPAs—Faroe Islands, Finland, Gibraltar, Guernsey, Ireland, Mauritius, Mexico and Serbia—also reported having the authority to pursue criminal sanctions/prosecutions or advise police and prosecutors as part of their enforcement powers.

**Figure 16: Countries reported to have the authority to pursue criminal sanctions/prosecutions or advise police and prosecutors**



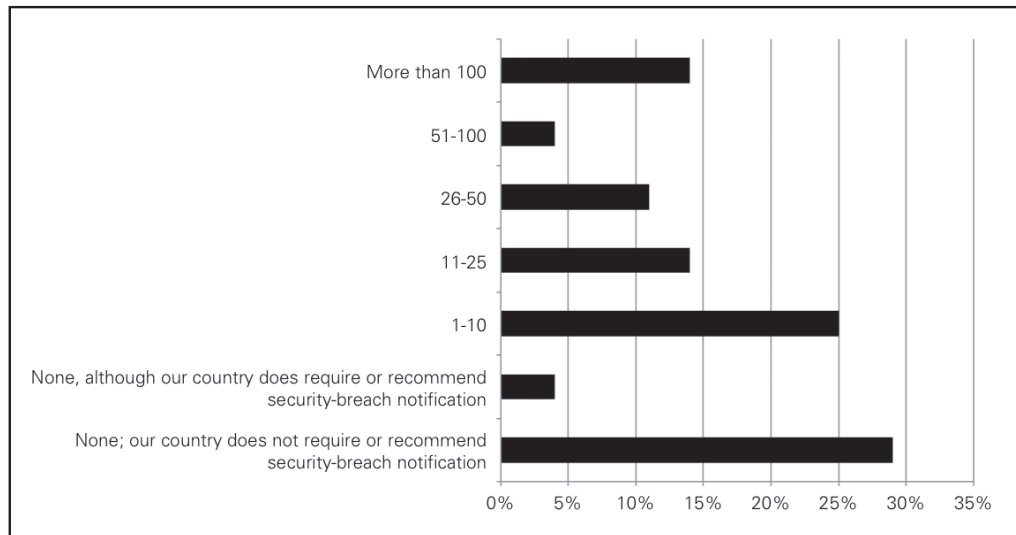
This year's survey indicates that more jurisdictions are enforcing data breach notification, up from one-third of respondents in 2010 to 43 percent in 2011.

**Figure 17: Security breach notification enforcement**



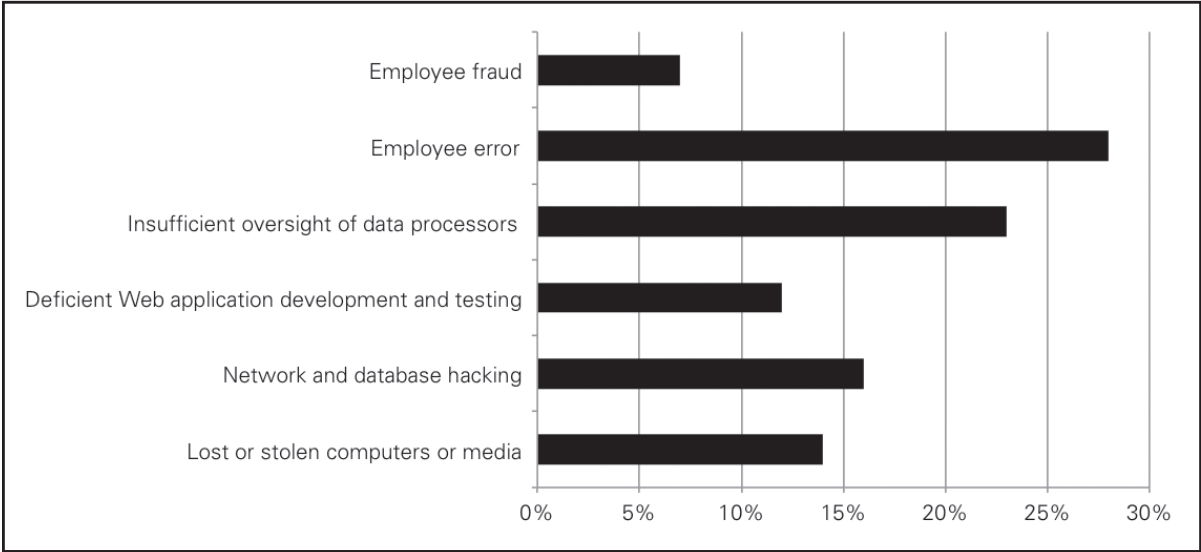
Responding DPAs reported a variety of experiences with security breach notification. Roughly one-third did not handle any reported breaches; 42 percent processed more than 10, and 14 percent managed more than 100.

**Figure 18: Prevalence of breach notifications**



Insider threats or errors were listed as the primary causes of data security breaches reported to DPAs in the past year, with nearly half of all incidents directly attributable to employee acts and omissions.

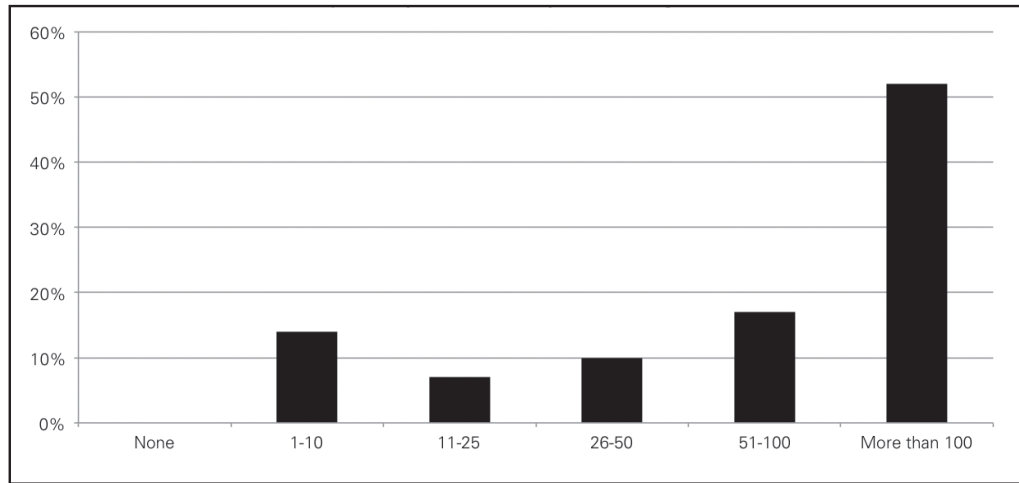
**Figure 19: Cause of breach notifications**



Roughly one-fourth of breaches were caused by vendors and business partners, and another 16 percent were reported to be the result of external hackers.

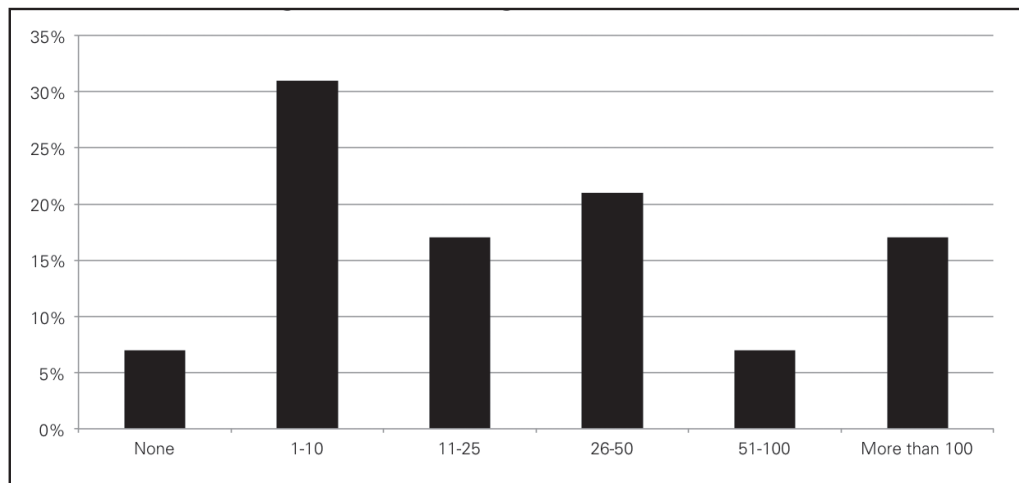
DPA's were very active in launching privacy investigations in 2011, with more than half of all respondents conducting more than 100 investigations in the past year.

**Figure 20: Frequency of privacy investigations**



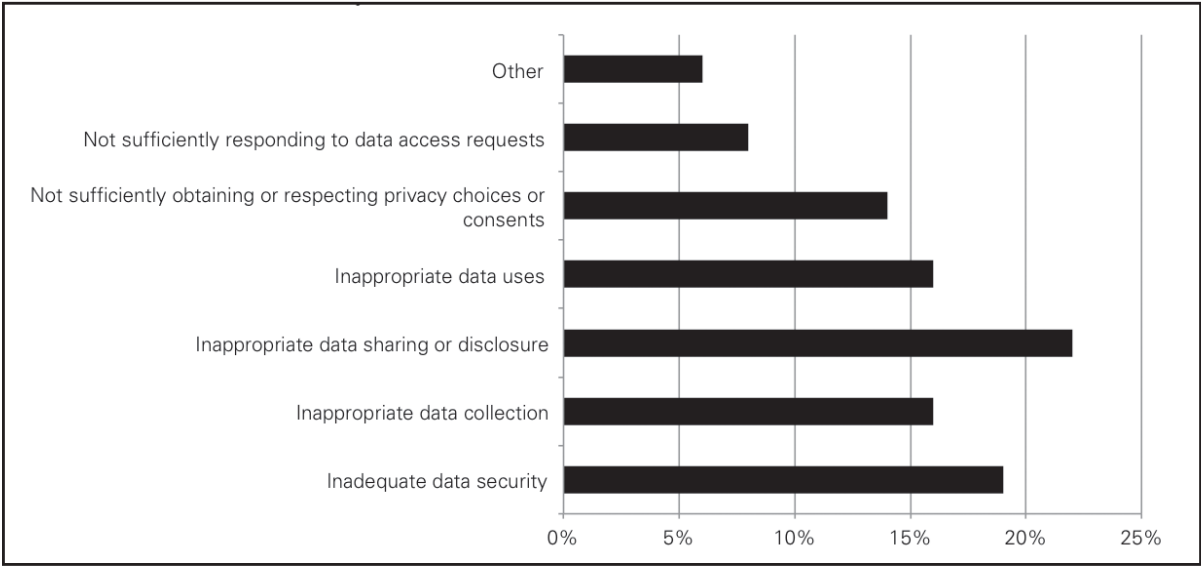
A smaller—but still significant—number of those privacy investigations resulted in enforcement actions.

**Figure 21: Investigations resulting in enforcement actions**



DPA's did not focus their enforcement actions on violations of any one particular privacy principle. While 22 percent reported inappropriate data sharing or disclosure as the primary cause of enforcement actions, the areas of security, collection and insufficiently obtaining consent or respecting privacy choices received between 14 percent and 19 percent of responses. Less than 10 percent of enforcement actions focused on insufficient responses to data access requests.

Figure 22: Key causes of enforcement actions

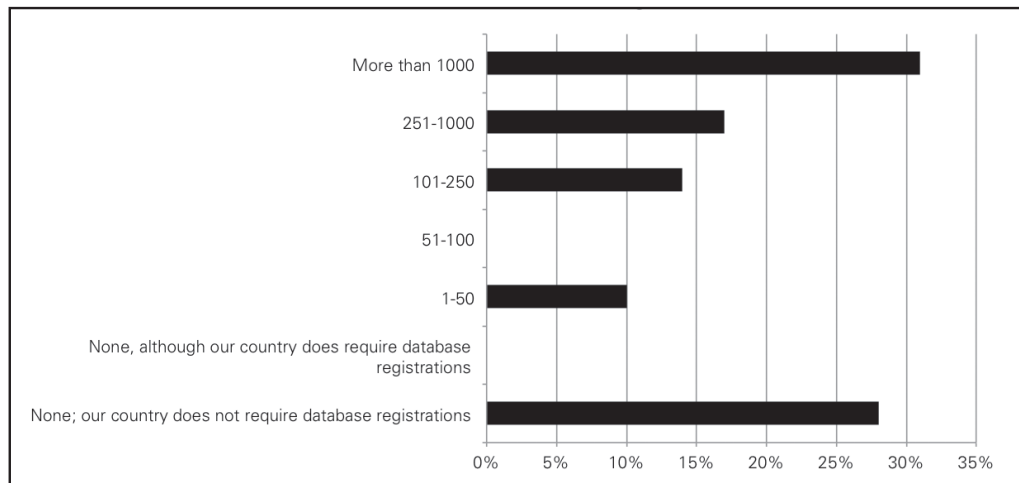


Of the 16 DPA's that reported collecting fines through their enforcement actions, Spain led the way at nearly €17.5 million, followed by Italy at €4 million and the UK at approximately €353,796.

### C. Database Registrations to DPAs

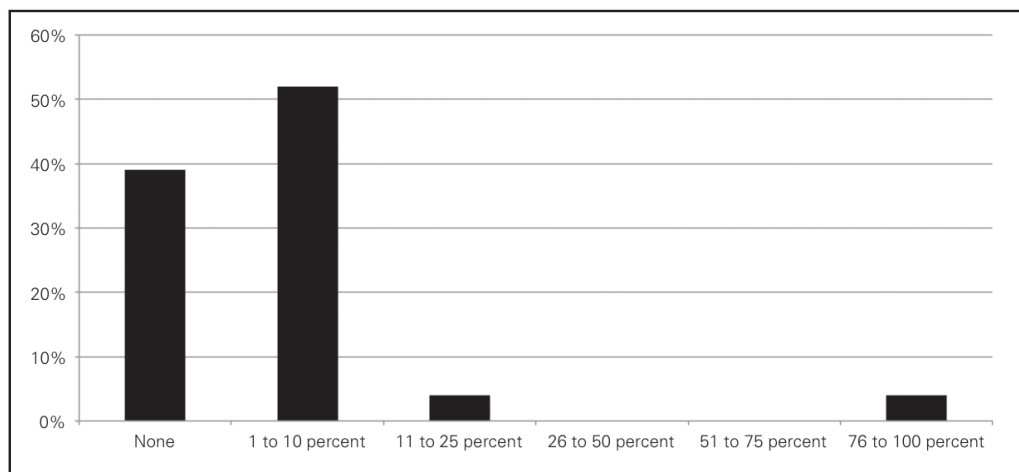
Database registration—a European innovation—is implemented to varying degrees among DPAs; in 2011, 38 percent processed fewer than 100 registrations, while roughly one-third of respondents handled more than 1,000.

**Figure 23: Prevalence of database registrations**



Among the DPAs responding, the burden of database registration falls primarily on domestic companies, with 92 percent of respondents indicating that 10 percent or fewer of their database registrations originated from foreign organizations.

**Figure 24: Foreign database registrations**





## Profiles in Privacy: Mike Flahive

By Angelique Carson, CIPP



Privacy, as a concept, has exploded.

That's according to Assistant Commissioner—Investigations Mike Flahive at New Zealand's Office of the Privacy Commissioner (OPC), who reports that the number of complaints his office receives has nearly doubled since the day he

took his job alongside privacy regularly making newspaper headlines.

"It's very rare for a week to go by without a national newspaper reporting some aspect of privacy," he says, "so I think it's a heightened topic of much interest in the community at the moment."

Flahive joined the OPC five years ago. Before that, he worked as a lawyer in both private practice and for the local government. He also spent 22 years as a senior detective in the police force. In his current position as an investigator and mediator, Flahive manages a team of 12, most of whom are lawyers, with offices in Auckland and Wellington. The team's main function is to serve as an alternative dispute resolution service, receiving complaints, determining whether the complaint is substantive and then whether the complaint should be referred to the court—the Human Rights Tribunal in this case—or mediated and settled.

A complaint is considered legitimate if it can be proven that at least one of the principles in the Privacy Act has been breached and that harm—such as humiliation, economic damage or loss of benefit—was suffered as a result.

"Most people are left with only injury to feelings, and that can be very difficult to prove," says Flahive. "And the law here says it's got to be significant, so more than the ordinary. You have to have been significantly embarrassed. It's not uncommonly proved, but it is a difficult hurdle."

Settled cases may result in an apology or payment of money equivalent to damages to the complainant and an agreement to comply with OPC recommendations for improvement. The OPC then informally monitors the organization for compliance. Flahive says in a country as small as New Zealand, it's "quite easy to pick out those agencies that are constantly offending and attempt to move them towards compliance."

Complaints that cannot be resolved are referred to the Human Rights Tribunal via a director of proceedings—a prosecutor, essentially—who is independent of the OPC but works closely with the office.

The OPC does not have fining powers, but a New Zealand Law Commission discussion paper about potential changes to the Privacy Act has included mentions of a more formal regime. Even without fines, "99 percent of the time, agencies will comply with our suggestions, even the big public- or private-sector organizations," Flahive says. "We're cautious that we're not making recommendations that will cost the organization a huge amount of money. Or, if there is potential for them to be spending a lot of money, then we'll accept that it's going to take some time to acquire the budget and resources."

The office aims to resolve about 30 percent of the complaints it receives, recognizing that many reported cases won't have a legitimate claim. Flahive says the number of complaints received has certainly increased, now nearing 1,000 compared with 500 to 600 per year five years ago. Flahive attributes that increase to more sophisticated technology and consumer understanding.

"In my job, we get a constant diet of privacy, and sometimes if you don't look up from your desk, you might be falsely thinking that privacy is huge," Flahive says, "so I'm constantly testing myself against my friends and colleagues outside work to see if it's just me looking at the thin blue line. But, I think it's really an explosion."

Asked what privacy advice he'd give to organizations, Flahive stresses that ignorance of the law is no excuse.

"I often find myself in that role of encouraging people to get a good grasp of the Privacy Act, which they may never have read. But it's been in effect for nearly 20 years now, so it's shameful that organizations that deal with personal information aren't aware of their obligations."

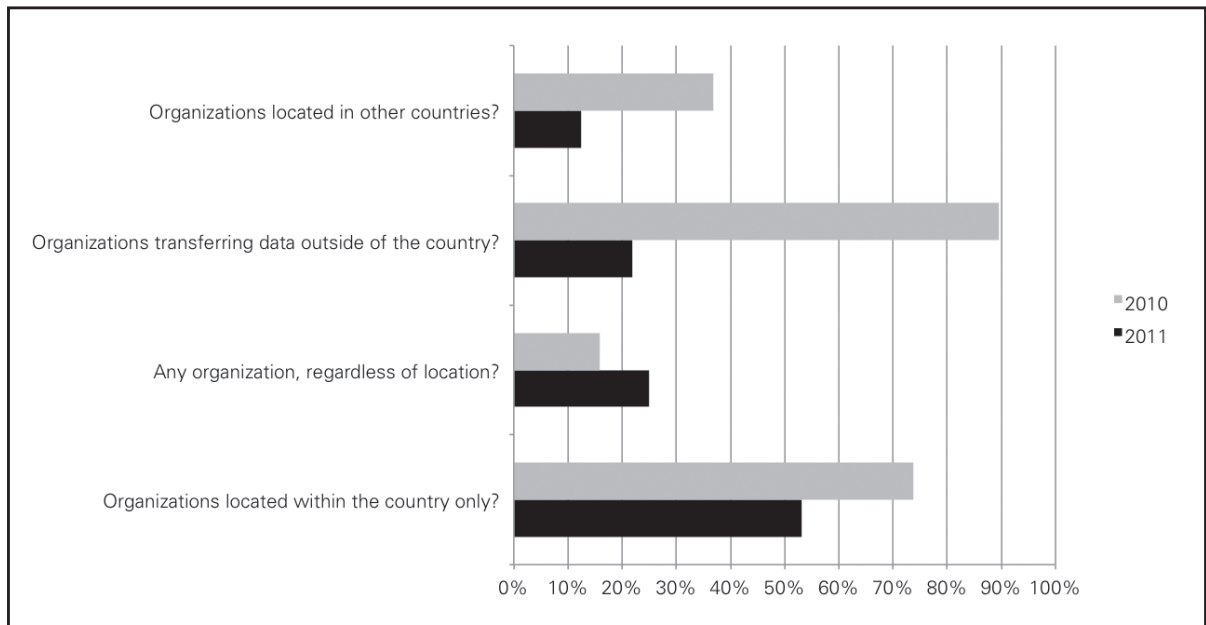
Flahive encourages organizations that may lack knowledge on the Privacy Act to put in place a privacy officer that has an idea of the rules and obligations.

"If you want to ensure that people have trust and confidence in your business, one key thing you need to do is not offend your business community," he says. "And if you breach the Privacy Act, you may offend not only one person but many—and that might affect the company bottom line."

## Transborder Issues

In examining transborder issues, it is interesting to note that many DPAs have indicated they enforce laws protecting citizens from the misuse of their data not only by domestic organizations but by those that either transfer data outside the jurisdiction or, in some cases, are located entirely outside the DPA's country or jurisdiction.

**Figure 25: DPA jurisdictions**

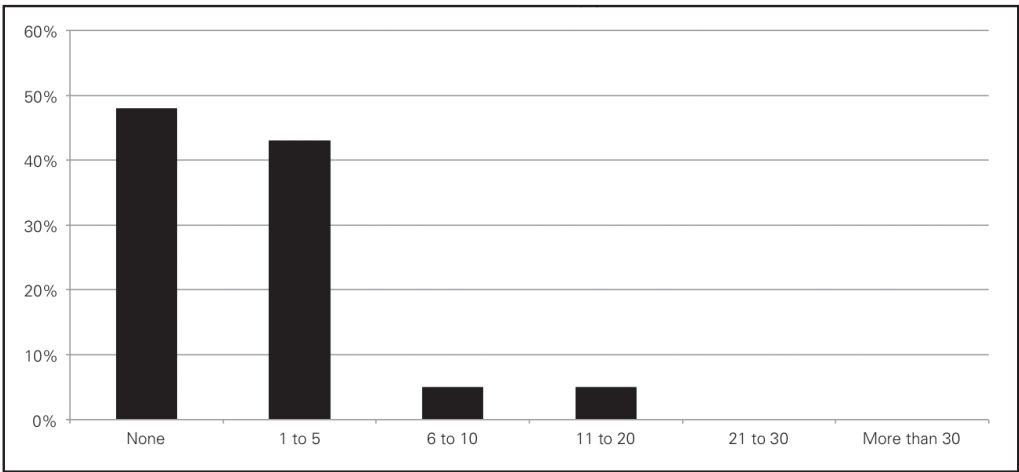


Responses varied significantly between 2010 and 2011, with the largest shift coming in the category of jurisdiction organizations that transfer data outside of a given DPA's country.

A. Binding Corporate Rules

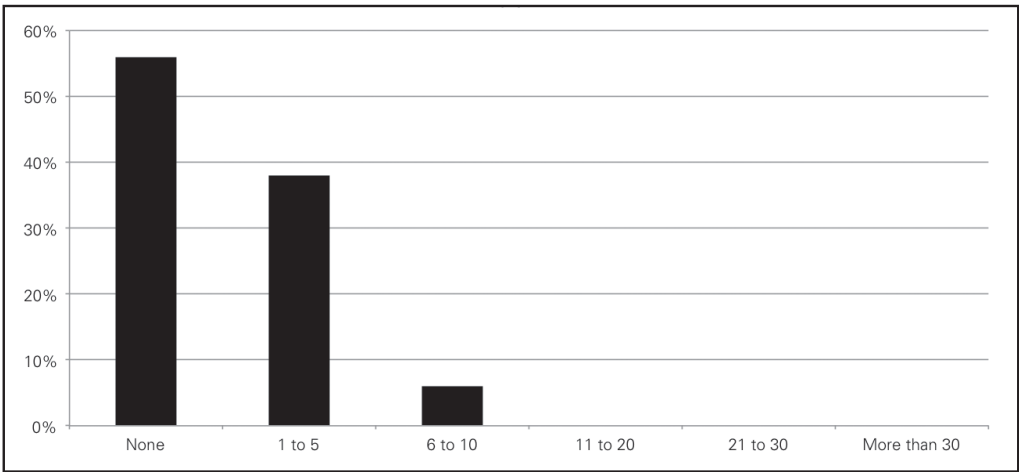
Binding Corporate Rules (BCRs) may have received a significant amount of media attention in the past year, but DPAs reported handling relatively few applications in 2011. While the vast majority of European respondents reported they handled five or fewer applications, Lithuania and Italy handled the most, between six and 20 applications.

Figure 26: Prevalence of BCR applications



The percentages of approved BCR applications track closely with the number of overall applications, though it is important to note that no DPA reported approving more than 10 applications in 2011.

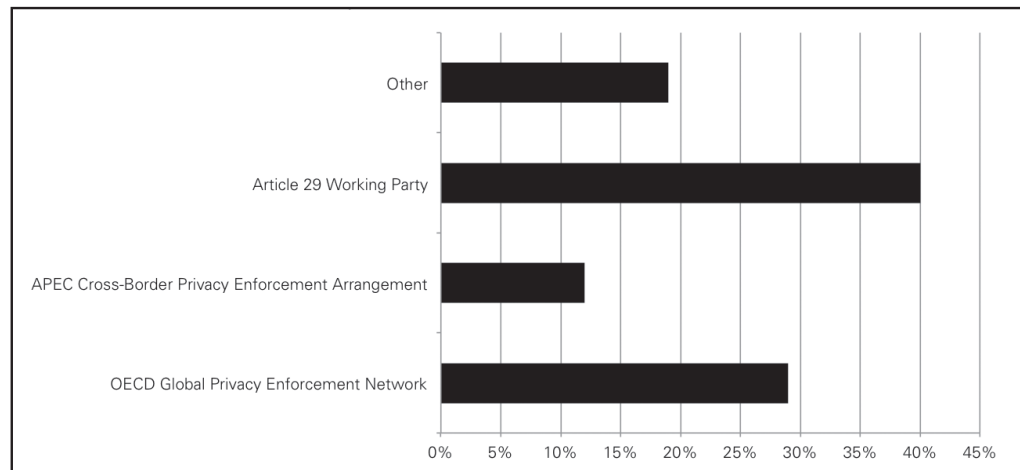
Figure 27: BCR approvals



## B. DPA Coordination

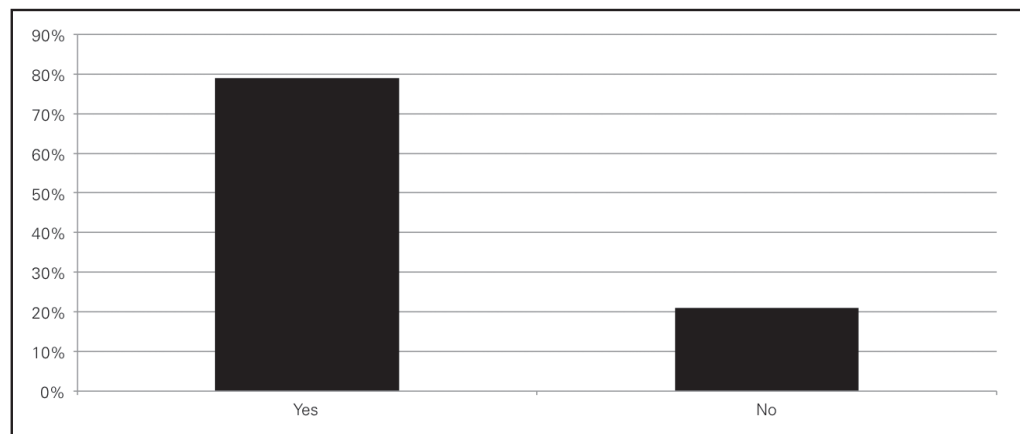
DPA participation in enforcement networks mirrored the responses from specific geographical regions. Given the large proportion of EU respondents, it is not surprising that the EU's Article 29 Working Party was the most popular enforcement network in 2011.

**Figure 28: Participation in enforcement networks**



Other enforcement networks cited included Eurodac; Europol; Schengen and Customs Joint Supervisory Bodies; Nordic Cooperation; Central and East European Data Protection Authorities; International Berlin Cooperation Work Group for Data Protection in Telecommunications, and the Contact Network of Spam Enforcement Authorities.

**Figure 29: DPA cross-border coordination**



Participation in such multilateral networks may be facilitating bilateral coordination among DPAs as well, based on respondents' answer to the question of whether their officers are involved in any concerted efforts with DPAs from other countries or U.S. regulators related to cross-border issues. More than three-quarters reported involvement in such cooperative efforts.

### C. Privacy Awareness Initiatives

International Data Privacy and Protection Day on January 28 is the most popular privacy awareness initiative in which DPAs participated, followed by Asia-Pacific Privacy Awareness Week, which is held each May.

**Figure 30: Awareness**

Is your office involved in cross-border privacy awareness education initiatives? If so, which one(s)?

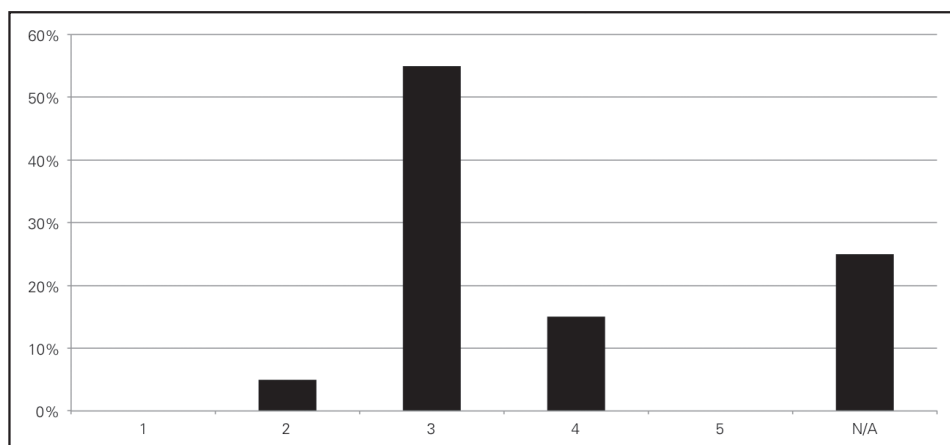
	Respondents	Percentage
Asia-Pacific Privacy Awareness Week	5	16%
Data Privacy and Protection Day	23	72%
Other*	4	13%
	32	

\*Other initiatives cited by DPAs include Safer Internet Day, Data Protection Day of the European Union, Leonardo da Vinci, Fundamental Rights and Citizenship and other programs financed by the European Union.

### D. EU-U.S. Safe Harbor Framework

European respondents were asked to rate, on a scale of 1 to 5 with 1 denoting a strongly negative opinion and 5 meaning strongly positive, their overall opinion of the EU-U.S. Safe Harbor framework. In spite of periodic criticism highlighted in the media, no European DPA reported a strongly negative view of the EU-U.S. Safe Harbor framework.

**Figure 31: EU-U.S. Safe Harbor opinions**



The majority of respondents reported neither a favorable nor unfavorable view of the agreement, suggesting that while there may not be a push for a wholesale change of the framework, there may well be receptivity for improving the agreement.

## Profiles in Privacy: Mexico's Federal Data Protection Law and the IFAI



In this question-and-answer feature prior to Mexico's hosting of the 33rd International Conference of Data Protection and Privacy Commissioners (ICDPPC 2011), the Federal Institute for Access to Information and Data Protection (IFAI) shares insights into the enactment of the nation's Federal Data

Protection Law after its first year in place.

### **What changes have the enactment of Mexico's Federal Data Protection Law meant for the IFAI?**

Since 2003, the Federal Institute for Access to Information and Data Protection (IFAI) as authority has been taking several actions to guarantee data protection held by both private and public entities. Ever since then, this institute has promoted a culture of protection and data security; has developed and applied normative instruments such as the Data Protection Guidelines; has also solved several controversies related to the rights of access and rectification, as well as supervised the compliance through the issuance of verifications, general guidelines and recommendations.

The issue of the Federal Data Protection Law of July 2010 has strengthened the IFAI's authority as the guarantee on data protection, now extended to the private sector with the possibility to impose sanctions to those whom infringe the law. This means that the institute is compelled to ensure the due observance of a fundamental right that empowers individuals to decide upon their information and that is held by both federal sector as well as private parties, whether being enterprises, organisations or natural person. The abovementioned recognises that this right has to coexist harmoniously with other rights and freedoms such as the access to public information and the free flow of goods, people and data.

**Have you seen changes in the past year in the way the Federal Institute of Access to Information and Data Protection monitors the collection, processing and disclosure of personal data held by the private sector, as regulated by the new law?**

Even though there are several resemblances on data treatment by the federal government and by private parties as they are governed by similar principles, each sector represents diverse challenges. As data protection authority to the public sector, IFAI has aimed for a balance between the right to personal data protection and the access to public information as it is of the utmost importance to the transparency of the governmental activity. As authority to the private sector, IFAI, on the other hand, seeks to reach a balance between the right to personal data protection and the national and international free flow of goods, merchandise, capital, people and data.

In such a difficult task, IFAI has adopted a more proactive approach to enhance the compliance to current legislation by third parties. In this sense, since July 2010, IFAI has met with the regulated sectors to promote the principles, duties and obligations that rule the legitimate treatment of data in the private sector and has developed strong widespread media coverage.

Furthermore, IFAI has worked along with the Ministry of Economy to draw the Secondary Regulation of the Law and has designed a self-regulated scheme adequate to the Mexican context. Both authorities have presented two guidelines for privacy notices to be elaborated by data controllers and to appoint a department or person responsible for the information. In this process, IFAI has a preventive approach as to encourage an accurate data treatment.

Moreover, and taking into account the international implications of the new law especially in relation with international transfers and the use of new technology that allows the ubiquity of personal data, IFAI has approached several authorities of other countries—as well as firms and international organisations—to encourage the exchange of perspectives, needs and current challenges in the globalised world and to avoid unnecessary barriers to the flow of goods, people and data. In this framework, this institute will host the International Conference of Data Protection and Privacy Commissioners in November.

**Has your staffing size and workload expanded along with the increase in oversight powers to cover the private sector as well as government entities?**

When IFAI became the data protection authority for the private sector in 2010, the number of regulated subjects increased from approximately 240 government entities

to more than 5,140,000 taking solely into consideration those economic entities registered in the 2009 national census elaborated by the National Institute of Statistics and Geography (INEGI). In addition, the law established new attributions to the institute, including legal and advisory powers so as to oversee the procedures of rights protection, verification and sanction imposition as well as to cooperate domestically and internationally with the data treatment due by private parties.

The increase on the oversight powers to be covered by IFAI implicated that the Mexican Congress appoint a higher budget for these new duties so as to expand and restructure the organisational chart of the institute. Up to this date, the institute is undergoing a restructuring to comply with the new tasks, and this workload has meant the increase of staffing.

**In an early analysis piece, we learned that the law included provisions for existing authorities to issue sectoral regulations along with those issued by the institute, with issues initially addressed by existing regulatory authorities in such sectors as economy, health and telecomms. Has this process begun in the first year of the law being enacted, where the institute and authorities are coordinating on regulations?**

The law oversees basic dispositions and creates a general regulatory framework that covers the minimum bases necessary to guarantee proper personal treatment on the part of private parties in all its phases. In addition, it states that such dispositions should be complemented by a secondary regulation that is being developed jointly with other regulatory authorities as required. To begin with, IFAI—along with the Ministry of Economy—have requested the opinion of several sectoral authorities such as the Ministry of the Interior, Treasury, Telecommunications and Transports, Public Education, Tourism, Health and Labour and Social Security with the aim to consider their feedback needed to reach a Secondary Regulation compatible with sectoral regulations in this matter and as to underline needs for each sector. This effort is the beginning of a permanent link between IFAI and several governmental entities, as the data protection involves a great diversity of fields such as the health, financial, trade, telecomm and labour, among many others.

The issuance of the Secondary Regulation is under process, and it will soon be published as a basic regulatory

framework. The IFAI looks forward to the issue of such rules as to ensure a suitable level of protection as a consolidated democracy providing legal certainty.

**Could you share details with us about the setup of the new office in terms of staffing structure and organization?**

Since the restructuring of the organisational chart, the IFAI has now a new Data Protection Secretariat with several General Directions under its leadership aim to meet the attributions stated in law. Each area will have under its supervision a group of the most expert civil servants on data protection that will cover topics such as Studies and Research, Self-regulation, Procedures and Verifications.

Moreover, as mentioned above, the congress designated new budget to IFAI as shown in the Federal Budget 2011. Currently, this institute is working on the amendments to its Internal Regulation and developing the required changes so as to in 2012 start answering the submitted requests of data protection of behalf of private parties as provided by law.

## E. DPAs Offering Secondment Opportunities

For the first time, we asked respondents whether their offices offer or encourage secondments. Well over half of this year's respondents do offer such opportunities, with 18 DPAs reporting secondments, including opportunities for staff to take courses and work with government departments as well as placements within their organizations for college students or other DPA colleagues.

Those survey responses follow.

- **Australia:** We have seconded staff to the NZ Privacy Commissioner's Office and to our policy department within government.
- **Bulgaria:** We have proposed candidates from CPDP for national experts in the data protection sphere.
- **Canada:** We have done so with several countries and welcome the opportunity to continue.
- **European Union:** We offer secondments from national data protection authorities. Those who apply for a position usually stay at the EDPS from one to two years.
- **Finland:** We offer possibilities for trainee periods for students of foreign universities and colleagues from other EU countries.
- **Greece:** Given its limited human resources, the HDPA offered in 2010 one outward secondment, that is a Seconded National Expert in Data Protection at the European Commission.
- **Hungary:** Yes, in the program for seconded national experts by the Eurojust and EDPS.
- **Ireland:** We have engaged in such in the past and, where appropriate, would do so again.
- **Italy:** Yes, to the European Data Protection Supervisor (EDPS); to the Council of Europe (CoE).
- **Lithuania:** One civil servant worked for European Council as national expert for two years.
- **Mauritius:** The DPO is sending two investigators to attend a course on network security to Bangalore, India, and would be glad to join other privacy organizations for cooperation on this level.
- **Mexico:** IFAI has just started promoting secondments. It has received training sessions at headquarters from the Federal Trade Commission of the U.S. and from the private firm Hewlett Packard. IFAI is also looking forward to encourage secondments along with countries like Spain.
- **New Zealand:** We support the APPA Forum Secondment Framework. This year, we had an outward secondment of a staffer part-time for several months to a government department.
- **Poland:** Nonpaid internships for students, participation in the Leonardo da Vinci exchange program with other data protection authorities and other such programs.
- **Slovenia:** We don't have any extra budget for secondments but accept candidates who agree not to be additionally funded by us.
- **Spain:** We cooperate with the Spanish Association of Privacy Professionals (APEP), and we have international agreements and cooperation.
- **Sweden:** They work within the EU, for instance, within the Article 29 Working Party.
- **United Kingdom:** We have two members of staff on secondment at European Commission institutions.



# Appendices

## Appendix A: Global DPA Audited Survey Results

<b>Q1.</b>	<b>Country (contextual response)</b>		
<b>Q2.</b>	<b>Name of your office or organization (contextual response)</b>		
<b>Q3.</b>	<b>Please enter the number of full-time staff in your office (numerical response)</b>		
<b>Q4.</b>	<b>Please enter the number of staff members in your office that hold advanced university degrees (i.e., Masters, PhD, LLM) in the following specialties: (numerical response)</b>  <b>specialties: computer science/engineering, business administration, banking/financial, human resources, public policy, marketing/communications, education, other</b>		
<b>Q5.</b>	<b>Do any of your staff members hold professional certifications (i.e., CIPP, CISSP, CISA, CPA) in:</b>	<b>2010</b>	<b>2011</b>
	Information security	29%	31%
	Auditing	26%	34%
	Privacy/data protection	26%	19%
	Other (Please Specify)	19%	16%
<b>Q6.</b>	<b>How many full-time equivalent staff members work in the following areas: Administrative/executive (management, HR, support, operations, etc.), auditing, complaint processing/handling resolution, education/outreach, information access/freedom of information, investigative/enforcement, management of mandated operations (i.e. data processor filings), policy/legislative affairs, privacy/data protection, research)? (numerical response)</b>		
<b>Q7.</b>	<b>Does your office offer or encourage secondments within the data protection and privacy realm, such as inward/outward, domestic/cross-border, with privacy authority/data controller/government department or international organization? (If so, please describe.) (contextual response)</b>		
<b>Q8.</b>	<b>How does your office manage its technological needs (i.e., data forensics) for investigations/complaint resolutions?</b>	<b>2011</b>	
	Multiple full-time staff	42%	
	One full-time staff member	23%	
	Part-time staff	3%	
	Outside experts/contracted firms	16%	
	Other	16%	
<b>Q9.</b>	<b>Please enter the number of full-time staff equivalents who work in your central office: (numerical response)</b>		

**Q10. Please enter the number of full-time staff equivalents who work in regional offices: (numerical response)**

**Q11. Is your office involved with enforcement-oriented networks? If so, which one(s):**

	2011 %
Yes	79%
No	21%
	100%

**Q12. Does your office have a data protection commissioner/supervisor or other similar official?**

	2011	2010
Yes	100%	92%
No	0%	8%

**Q13. If your office has a data protection commissioner/supervisor, what is this person's name? If not, who holds the leadership role in your office? (contextual response)**

**Q14. If your office has a data protection commissioner, what is the appointment process?**

	2010	2011
Executive appointment	24%	35%
Legislative committee appointment	15%	13%
Election	24%	6%
Civil servant/direct hire	9%	6%
Other (please specify)	29%	39%

**Q15. If your office has a data protection commissioner, how long is this person's term? (contextual response)**

**Q16. Are there state or provincial-level data protection authorities in your country? If so, what involvement do you have with them, if any? (contextual response)**

**Q17. What is the annual budget of your office? (Please specify currency.) (contextual response)**

**Q18. What other sources of income contribute to your office's total budget? (Select all that apply.)**

	2010	2011
Data registry fees	0%	21%
Enforcement fines	100%	17%
Grants	0%	3%
Government allocations	0%	41%
Other	0%	17%

**Q19. Please list the estimated percent of your budget allotted to each of the following:**

	Zero	1 to 10	11 to 20	21 to 30	31 to 40	41 to 50	51 to 60	61 to 70	71 to 80	81 to 90	91 to 100
Administrative (HR, tech support, operations, etc.)	0	3	9	2	0	2	2	0	1	0	2
Auditing	3	7	3	0	0	0	0	0	0	0	0
Complaint processing/handling/resolution	1	3	3	6	2	0	1	1	0	0	0
Education/outreach	3	8	3	1	0	0	0	0	0	0	0
Information access	3	6	2	1	0	0	0	0	0	0	0
Investigation/enforcement	1	7	3	5	1	0	0	0	0	0	0
Management of mandated operations (such as data processor filings)	5	5	1	1	0	0	0	0	0	0	0
Policy/legislative affairs	2	4	8	2	0	0	0	0	0	0	0
Research	6	6	1	0	0	0	0	0	0	0	0
Other areas	4	2	2	0	0	0	0	0	0	0	0
	28	51	35	18	3	2	3	1	1	0	2

**Q20. What is the scope of authority of your office? (Select all that apply.)**

	2010	2011
Data protection, specific private-sector industries	10%	10%
Specific private-sector industries and/or other	9%	10%
Information access/freedom of information	9%	13%
Data protection, private sector	35%	31%
Data protection, public sector	37%	36%

**Q21. Is your office involved in cross-border privacy awareness education initiatives? If so, which one(s)?**

Yes	79%
No	21%

**Q22. Does the law(s) that your office enforces protect citizens from the misuse of their data by:**

	2011	2010
Organizations located within the country only?	53%	74%
Any organization, regardless of location?	25%	16%
Organizations transferring data outside of the country?	19%	89%
Organizations located in other countries?	9%	37%

**Q23. What are the primary responsibilities of your office? (Select all that apply.)**

	2011	2010
Other	25%	45%
Mediate/ arbitrate	34%	34%
Shape/research policy	56%	71%
Initiate complaints	66%	55%
Registry activities	72%	0%
Auditing/ inspections	75%	0%
Public outreach/ education	75%	92%
Advance/ advocate privacy rights/ legislation	78%	84%
Compliance/ investigations/ enforcement	91%	97%

**Q24. Is your office involved in any concerted efforts with DPAs from other countries/U.S. regulators related to cross-border issues?**

	Respondents	Percentage
Asia-Pacific Privacy Awareness Week	5	16%
Data Privacy and Protection Day	23	72%
Other	4	13%

**Q25. What enforcement powers does your office have? (Select all that apply.)**

	2010	2011
Adjudication	20%	23%
Fines/penalty payments	23%	22%
Cease-and-desist orders/data removal/suspension of data transfers	30%	33%
Criminal sanctions/prosecutions	8%	7%
Other	19%	15%

**Q26. Do your enforcement powers apply to (Select all that apply.)**

	2011	2011
Individuals	26	81%
Private-sector organizations	27	84%
Public-sector organizations	29	91%

**Q27. Is your office involved in enforcing regulations on security breach notifications?**

	2011	2010
Yes	43%	33%
No	57%	67%

**Q28. How many privacy investigations has your office initiated in the past year? (numerical response)**

<b>Q29.</b>	<b>Of those investigations, how many resulted in enforcement actions? (numerical response)</b>	
<b>Q30.</b>	<b>Of those enforcement actions, what was the total amount of all monetary fines levied? (Specify currency.) (contextual response)</b>	
<b>Q31.</b>	<b>What was the primary cause of those enforcement actions?</b>	
	Inadequate data security	19%
	Inappropriate data collection	16%
	Inappropriate data sharing or disclosure	22%
	Inappropriate data uses	16%
	Not sufficiently obtaining or respecting privacy choices or consents	14%
	Not sufficiently responding to data access requests	8%
	Other	6%
<b>Q32.</b>	<b>What is the estimated number of data security breaches that your office was notified of in the past year?</b>	
	None; our country does not require or recommend security-breach notification	29%
	None, although our country does require or recommend security-breach notification	4%
	1-10	25%
	11-25	14%
	26-50	11%
	51-100	4%
	More than 100	14%
<b>Q33.</b>	<b>What were the primary causes of any data security breaches reported to your office in the past year? (Select all that apply.)</b>	
	Lost or stolen computers or media	14%
	Network and database hacking	16%
	Deficient web application development and testing	12%
	Insufficient oversight of data processors	23%
	Employee error	28%
	Employee fraud	7%
<b>Q34.</b>	<b>Approximately how many organizations have submitted database registrations to your office in the past year?</b>	
	None	39%
	1 to 10 percent	52%
	11 to 25 percent	4%
	26 to 50 percent	0%
	51 to 75 percent	0%
	76 to 100 percent	4%

**Q35. If you have received database registration submissions, approximately what percentage came from organizations not based in your country?**

	2010	2011
Organizations located within the country only?	34%	27%
Organizations transferring data outside of the country?	41%	10%
Organizations located in other countries?	17%	3%
Any organization, regardless of location?	7%	23%
Other	0%	37%

**Q36. For European respondents, how many Binding Corporate Rules (BCR) applications have you fielded in the past year? (numerical response)**

**Q37. If you did field BCR applications, how many did you approve? (numerical response)**

**Q38. For European respondents, on a scale of 1 to 5, where 1 means strongly negative and 5 is strongly positive, what is your overall opinion of the EU-U.S. Safe Harbor framework? (numerical response)**

## Appendix B: Data Protection Offices and Officials

Argentina	Dirección Nacional de Protección de Datos Personales	Juan Antonio Travieso
Australia	Office of the Australian Information Commissioner	John McMillan is the Australian Information Commissioner and CEO. Timothy Pilgrim is the Privacy Commissioner. James Popple is the FOI Commissioner. All have privacy/data protection functions, but Timothy Pilgrim takes the lead on privacy/data protection matters.
Bulgaria	Commission for Personal Data Protection	The Commission for Personal Data Protection is a collective body consisting of Veneta Shopova, president, and Krassimir Dimitrov, Valentin Enev, Mariya Mateva and Veselin Tselkov.
Canada	Office of the Privacy Commissioner of Canada	Jennifer Stoddart
Cyprus	Office of the Commissioner for Personal Data Protection	Panayiota Polychronidou
Estoni	Estonian Data Protection Inspectorate	Viljar Peep
European Union	European Data Protection Supervisor	Peter Hustinx
Faroe Islands	Dátueftirlitið	Ingunn Eiríksdóttir
Finland	Office of the Data Protection Ombudsman	Reijo Aarnio
Germany	Federal Commissioner for Data Protection and Freedom of Information	Peter Schaar
Gibraltar	Data Protection Commissioner — Gibraltar Regulatory Authority	
Greece	Hellenic Data Protection Authority	Christos Paliokostas
Guernsey	Bailiwick of Guernsey Data Protection Office	Peter Harris
Hong Kong	Office of the Privacy Commissioner for Personal Data	Allen Chiang
Hungary	Parliamentary Commissioner for Data Protection and Freedom of Information	András Jóri
Ireland	Office of the Data Protection Commissioner	Billy Hawkes
Italy	Garante per la Protezione dei Dati Personali	Francesco Pizzetti
Latvia	Data State Inspectorate	Signe Plimiņa
Lithuania	State Data Protection Inspectorate	Algirdas Kuncinas
Macao	Office for Personal Data Protection	Sonia Chan
Malta	Office of the Information and Data Protection Commissioner	Joseph Ebejer
Mauritius	Data Protection Office (Prime Minister's Office)	Drudeisha Madhub

Mexico	Federal Institute For Access To Information And Data Protection	IFAI is composed of five commissioners all dedicated to access to information and data protection: President Commissioner Jacqueline Peschard, Commissioners Angel Trinidad, Maria Marvan, Sigrid Arzt and Maria Elena Perez-Jaen.
New Zealand	Office of the Privacy Commissioner	Marie Shroff
Norway	Data Protection Authority	Bjørn Erik Thon
Republic of Poland	Inspector General for Personal Data Protection	Wojciech R. Wiewiórowski
Serbia	Commissioner for Information of Public Importance and Personal Data Protection	Rodoljub Sabic
Slovak Republic	Office for the Protection of Personal Data	
Slovenia	Information Commissioner	Nataša Pirc Musar
Spain	Spanish Data Protection Agency	Artemi Rallo
Sweden	Datainspektionen (Data Inspection Board)	Göran Gräslund
United Kingdom	Information Commissioner's Office	Christopher Graham



## APPENDIX C: Appointing Bodies

Argentina	Executive appointment
Australia	Governor-General on the advice of the government; however, the incumbent cannot be removed by the government
Bulgaria	Election
Canada	Officer of Parliament Order in Council appointment
Cyprus	Executive appointment
Estoni	Executive appointment
European Union	Legislative committee appointment
Faroe Islands	Executive appointment
Finland	Civil servant/direct hire
Germany	Election
Gibraltar	Legislative committee appointment
Greece	Appointed by presidential decree issued upon proposal of the cabinet following a report by the minister of justice
Guernsey	Appointment by parliament
Hong Kong	Executive appointment
Hungary	President appoints; Parliament elects by two-thirds majority
Ireland	Executive appointment
Italy	Elected by parliament
Latvia	Executive appointment
Lithuania	Executive appointment
Macao	Executive appointment
Malta	Appointed by the Prime Minister after consultation with the Leader of the Opposition
Mauritius	Civil servant/direct hire
Mexico	Executive appointment
New Zealand	Appointed by Governor-General on recommendation of responsible minister
Norway	Executive appointment
Poland	Appointed and dismissed by the Diet of the Republic of Poland with the consent of the senate
Serbia	Legislative committee appointment
Slovak Republic	Elected by parliament
Slovenia	President's proposal, confirmed by parliament
Spain	Selection by consultative council, election by parliament
Sweden	Government appointment
United Kingdom	Legislative committee appointment

## APPENDIX D: DPA Concerted Efforts

Australia	APEC and APPA processes
Bulgaria	We cooperate with other DPA's under the rules of the Directive 95/46/EC and in specific privacy and data protection groups.
Canada	We are a member of GPEN and APEC CBPEA. As well, we interact with other DPAs on specific issues.
Estoni	Supervisory cooperation with other EU member states
European Union	We generally participate in selective issues that have a global dimension mostly as part of the Article 29 Working Party. We cooperate with international organisations on data protection such as OECD, Council of Europe, etc.
Finland	European Union
Germany	Article 29 Working Party
Gibraltar	European Union
Greece	Binding Corporate Rules (BCR) Subgroup of Article 29, Financial Matters Subgroup of Article 29, PNR Subgroup of Article 29
Hong Kong	APEC Privacy Subgroup
Ireland	Joint enforcement with other EU member states
Italy	Case Handling Network set up by the EU data protection authorities; coordinated enforcement initiatives launched and managed by the Article 29 Working Party; cooperation among DPAs pursuant to the Directive 95/46/EC.
Mauritius	Mauritius is also a member of the AFAPDP such that if any such issue would crop up, it can initiate some action for cooperation.
New Zealand	Ongoing work through GPEN, APEC CPEA, APEC DPS, OECD WPISP Volunteer Group. During the year, we cosigned a public letter by 10 DPAs expressing concern at Google Buzz incident.
Norway	Apple's data location storage
Poland	Cooperation with other data protection authorities within the Article 29 Working Party, amongst other initiatives
Serbia	CoE 108 Convention, obligation to cooperate; through CEEDPA; bilateral agreements of cooperation (usually include the issue of data transfer)
Slovenia	The issues covered by the Article 29 Working Party, Europol, Eurodac, customs, schengen...
Spain	Memorandum of understanding with the FTC
United Kingdom	Through Article 29 in Europe and GPEN



## About the IAPP

The International Association of Privacy Professionals (IAPP) is the world's largest organization of privacy professionals, representing more than 8,000 members from businesses, governments and academic institutions across 70 countries.

The IAPP was founded in 2000 with a mission to define, support and improve the privacy profession through networking, education and certification. We are committed to providing a forum for privacy professionals to share best practices, track trends, advance privacy management issues, standardize the designations for privacy professionals and provide education and guidance on opportunities in the field of information privacy.

The IAPP is responsible for developing and launching the first broad-based credentialing program in information privacy, the Certified Information Privacy Professional (CIPP). The CIPP remains the leading privacy certification for thousands of professionals around the world who serve the data protection, information auditing, information security, legal compliance and/or risk management needs of their organizations.

In addition, the IAPP offers a full suite of educational and professional development services and holds annual conferences that are recognized internationally as the leading forums for the discussion and debate of issues related to privacy policy and practice.

**This study was executed with the assistance of Jay Cline, CIPP, and Minnesota Privacy Consultants.**

Additional content was contributed by IAPP Publications Manager Jennifer Saunders, CIPP, and Staff Writers Jedidiah Bracy, CIPP, and Angelique Carson, CIPP.

We at the IAPP wish to express our sincere thanks to the data protection authorities that participated in this study and so generously provided their time and insights.

To participate in future IAPP research efforts please contact us at [research@privacyassociation.org](mailto:research@privacyassociation.org).



**For more information, please contact us at:**

IAPP

Pease International Tradeport

75 Rochester Ave., Suite 4, Portsmouth, NH 03801 USA

+1 603.427.9200

[www.privacyassociation.org](http://www.privacyassociation.org)