

Data Protection Authorities

2010 Global Benchmarking Survey

Executive Summary and Findings

International Association of Privacy Professionals

Data Protection Authorities: 2010 Global Benchmarking Survey

Executive Summary and Findings

International Association of Privacy Professionals



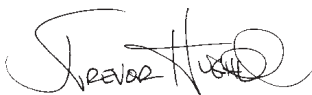
Dear Data Protection Professional,

It is my great pleasure to share with you this second edition of the IAPP's annual analysis of the state of the practice of data protection authorities (DPAs) around the world.

The Data Protection Authorities 2010 Global Benchmarking Survey offers you informative and revealing insights into how data protection regulators do their work within a rapidly evolving marketplace and across a variety of issues and concerns. You will gain a better understanding of how today's regulators are funded, structured, staffed and deployed. This year, we have expanded our study to provide perspective on how enforcement approaches are changing, how public education and advocacy efforts are being integrated and how DPAs are meeting the increasingly technical nature of data protection challenges today.

Whether you serve in government or work in industry, I trust you will find the report an invaluable tool in helping to benchmark your own data protection and information access programs and practices. You are encouraged to learn from these findings and participate in our future research efforts as we continue to examine global data protection regulation in the years to come.

Sincerely,



J. Trevor Hughes, CIPP
Executive Director
International Association of Privacy Professionals



Table of Contents

I. Introduction	5
II. Executive Summary	6
III. Survey Findings	
1. Responsibilities and focus areas	8
2. Authority and enforcement	12
3. The DPA office: staff, size and allocation	16
4. Transborder issues	32
IV. Survey Methodology	35
V. Appendices	
APPENDIX A: Global data protection authorities audited survey results	36
APPENDIX B: Data protection offices and officials	40
APPENDIX C: Appointing bodies	42
APPENDIX D: Concerted efforts	43

I. Introduction

The 2010 IAPP Global Data Protection Authority Benchmarking Survey, conducted by the International Association of Privacy Professionals (IAPP), examines federal-level privacy offices and data protection authorities (DPAs) in 38 countries and territories. This is the second edition of this annual survey.

The IAPP designed this study to examine the scope, authority and resources of DPAs; to investigate the present state of data protection, privacy, and information sharing; and to provide a reliable and useful platform for exploring these issues, and their evolution, on an ongoing basis each year.

Most of all, we sought to answer the following questions:

- **Scope:** What are DPAs' primary focus areas and responsibilities?
- **Resources:** How are DPAs staffed and budgeted, and how are their budgets allocated across different areas of responsibility?
- **Authority:** What are DPAs' present enforcement powers and how are these powers evolving?

The goal of this study is to benchmark current practices—how different authorities approach, construct, manage, perceive and staff their data protection programs—and to create a baseline for future surveys so we may examine how these practices evolve to meet future privacy challenges.

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

Australia	Isle of Man
Austria	Israel
Bulgaria	Italy
Canada	Latvia
Colombia	Liechtenstein
Cyprus	Lithuania
Czech Republic	Macao
Estonia	Macedonia
European Union	Malta
Faroe Islands	Mauritius
Finland	Netherlands
France	New Zealand
Gibraltar	Norway
Greece	Poland
Guernsey	Serbia
Hong Kong	Slovakia
Hungary	Slovenia
Iceland	Sweden
Ireland	United Kingdom

II. Executive Summary

The 2010 DPA survey revealed some intriguing trends across the global privacy regulatory community that, in part, build on themes introduced in our inaugural report of 2009.

Among this study's key findings:

- **The DPA mandate has expanded from data protection to also include public education and privacy advocacy**

While most DPAs' primary responsibility is to manage data protection matters in both the public and private sectors (only one DPA handles solely public-sector data protection matters), the vast majority also focus on public education and the advocacy of individual privacy rights. In addition, 19 percent of respondents also have information-access responsibilities.

92 percent of DPAs report educating the public and 84 percent report advocating privacy rights as primary responsibilities.

DPAs describe research, policy work and arbitration as additional focus areas.

- **The DPA enforcement regime now includes fines and, in growing instances, criminal sanctions**

More than two-thirds of DPAs (68%, or 26 out of 38) have the authority to issue cease-and-desist orders for data protection infractions. More than half (53%) of DPAs can issue fines.

Only seven DPAs said they have the authority to impose criminal sanctions for data protection violations. However, this represents a nine percent increase (from 9% in 2009 to 18% in 2010) from our 2009 results. Additionally, several DPAs noted that breaches of enforcement orders or remedy directives would qualify as criminal offenses.

Some authorities also have the power to bring cases to civil court or privacy tribunal, issue enforcement notices or order remedies. Others can issue recommendations, have the power of entry and search or can order penalty payments.

Eleven DPAs are actively involved in the enforcement of regulations relating to security breach notifications.

- **More DPAs are going outside of their offices to meet growing technical challenges in data protection**

Some DPAs choose to hire external consultants over internal staff to address growing in-house technical data protection concerns.

As data protection issues become increasingly more technical in nature and private sector innovations continue to push the "privacy envelope," DPAs appear to be outsourcing this function rather than having dedicated technical experts on staff. This represents a significant change—a decrease of 28 percent—in the number of DPAs who reported having internal staff to fulfill technical expertise functions in 2009.

- **A "professionalization divide" has emerged between privacy regulators and privacy practitioners**

At most, approximately one third of responding DPAs (11 out of 30) surveyed in 2010 have staff members who hold professional certifications in privacy/data protection, information security, information audit or related fields. The most common credential among staff members of responding DPAs is in information security (11 out of 30). By comparison, 3,200 of the IAPP's 7,000 private-sector members currently hold one or more privacy certifications (47%) and 1,056 (30%) hold a security or audit certification in addition to privacy.

However, 28 out of 33 DPAs employ staff members who do hold an advanced degree in a legal or compliance-related specialty. Business administration and computer science degrees are also common among DPA staff members.

Lastly, few DPAs have a formal liaison to the privacy profession. The vast majority (34 of 38, or 89%) indicated that they do not have a formal liaison to the privacy profession at large.

- **A relatively limited number of resources have been allocated by DPAs to transborder data protection**

Only five DPAs dedicate more than 10 percent of the investigative and enforcement work of their office to transborder issues, with the European Union leading the way at 50 percent, albeit having no enforcement powers. Notably, the majority of DPAs commit 10 percent or less of their investigative and enforcement work to such issues. This stands in stark contrast to a considerable investment of time and budget on the part of private-sector organizations in compliance programs that seek to ensure transborder data protection.

The majority of DPAs are enforcing laws that protect citizens from the misuse of their data by organizations located within their country as well as organizations transferring data outside of the country. Fourteen out of 29 responding DPAs enforce laws that protect citizens from the misuse of their data by organizations in other countries, while only seven DPAs guard against the misuse of data by organizations regardless of location.

- **Limited cooperation or coordination among global DPAs and U.S.-based regulatory entities**

Only four of the 38 reporting DPAs have cooperated with the FTC or another U.S. regulatory agency to bring an enforcement action against a U.S.-based organization.

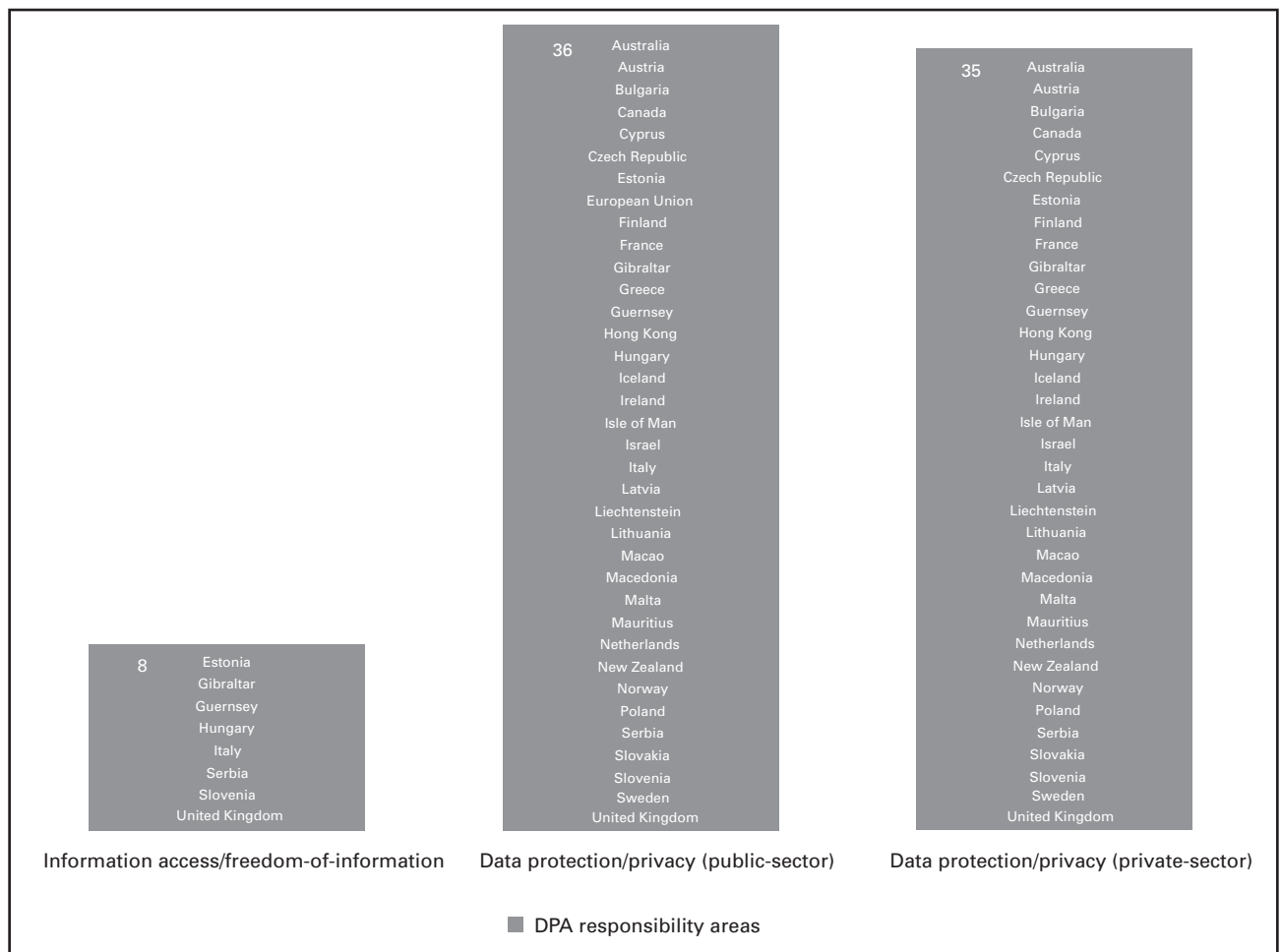
III. Survey Findings

I. Responsibilities and focus areas

We asked DPAs to share their focus areas and primary activities. In terms of focus, we found that 36 authorities handle public-sector data protection, 35 of which also handle private-sector data protection. Eight DPAs—all European—indicated that in addition to their data protection duties, they also have responsibilities relating to information access and freedom of information.

Figure 1 shows how responsibilities differ by country.

Figure 1: Areas of focus



The following DPAs indicated that their purview includes information access:

- Estonia
- Gibraltar
- Guernsey
- Hungary
- Italy
- Serbia
- Slovenia
- United Kingdom

While information access and freedom of information seem to be areas of focus for only a small number of European DPAs, Australia noted that as of November 1, 2010, the Office of the Information Commissioner will replace the Office of the Privacy Commissioner, extending the scope of its authority to include such responsibilities.

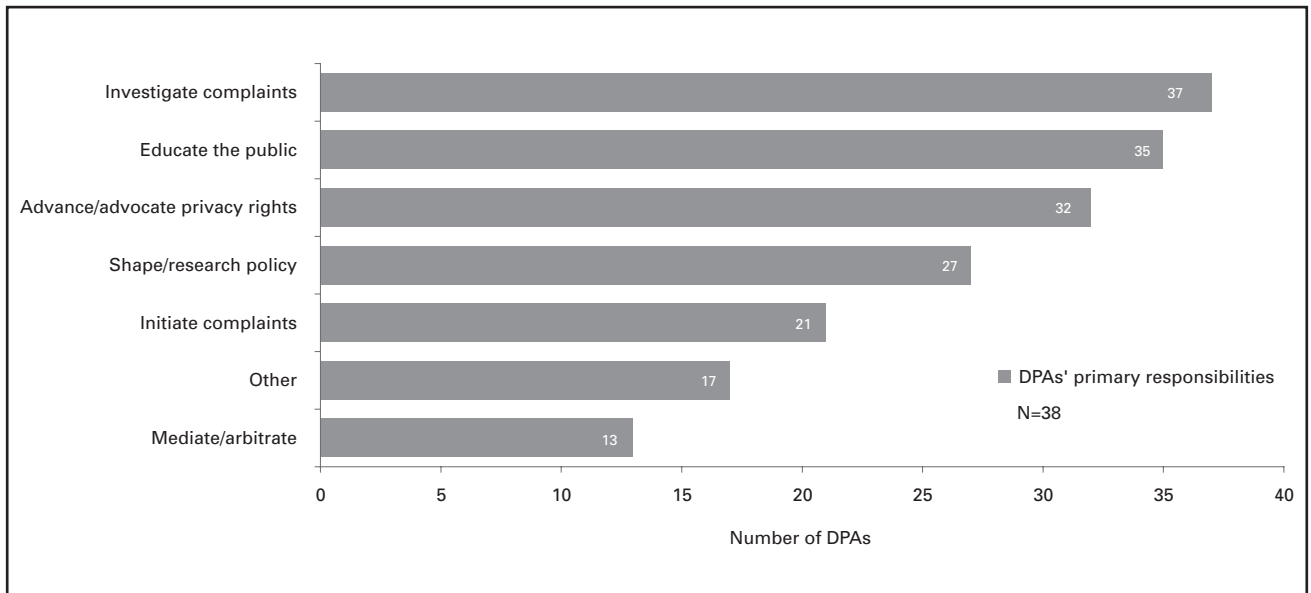
Figure 2: DPAs with freedom-of-information responsibilities



The office of the European Data Protection Supervisor (EDPS), whose mission is to manage governmental privacy issues, was the only DPA that said it works solely with data protection within the sphere of the public sector.

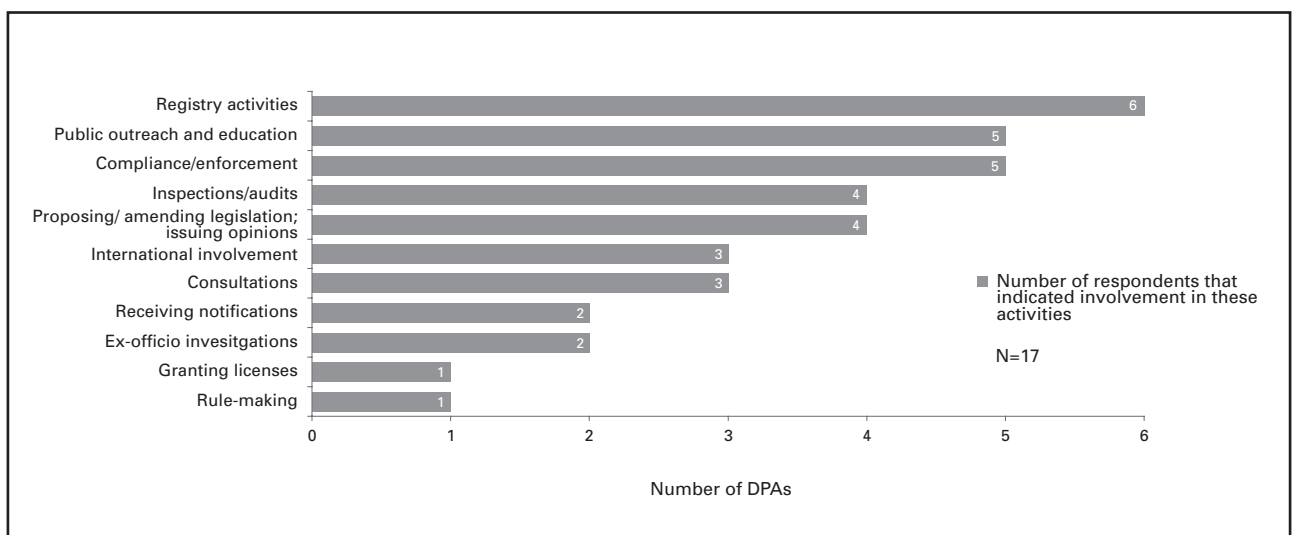
In terms of primary activities, the survey found that all but one DPA focuses on responsibilities related to the investigation of complaints. Additionally, the vast majority of DPAs—92 percent and 84 percent, respectively—focus on educating the public and advancing and advocating privacy rights. More than two-thirds of responding DPAs noted having responsibilities dedicated to shaping and researching policy, and more than half are initiating complaints. These results are very similar to those found in our 2009 survey, suggesting that the relative importance that DPAs place on their primary activities has not changed.

Figure 3: DPAs' primary responsibilities



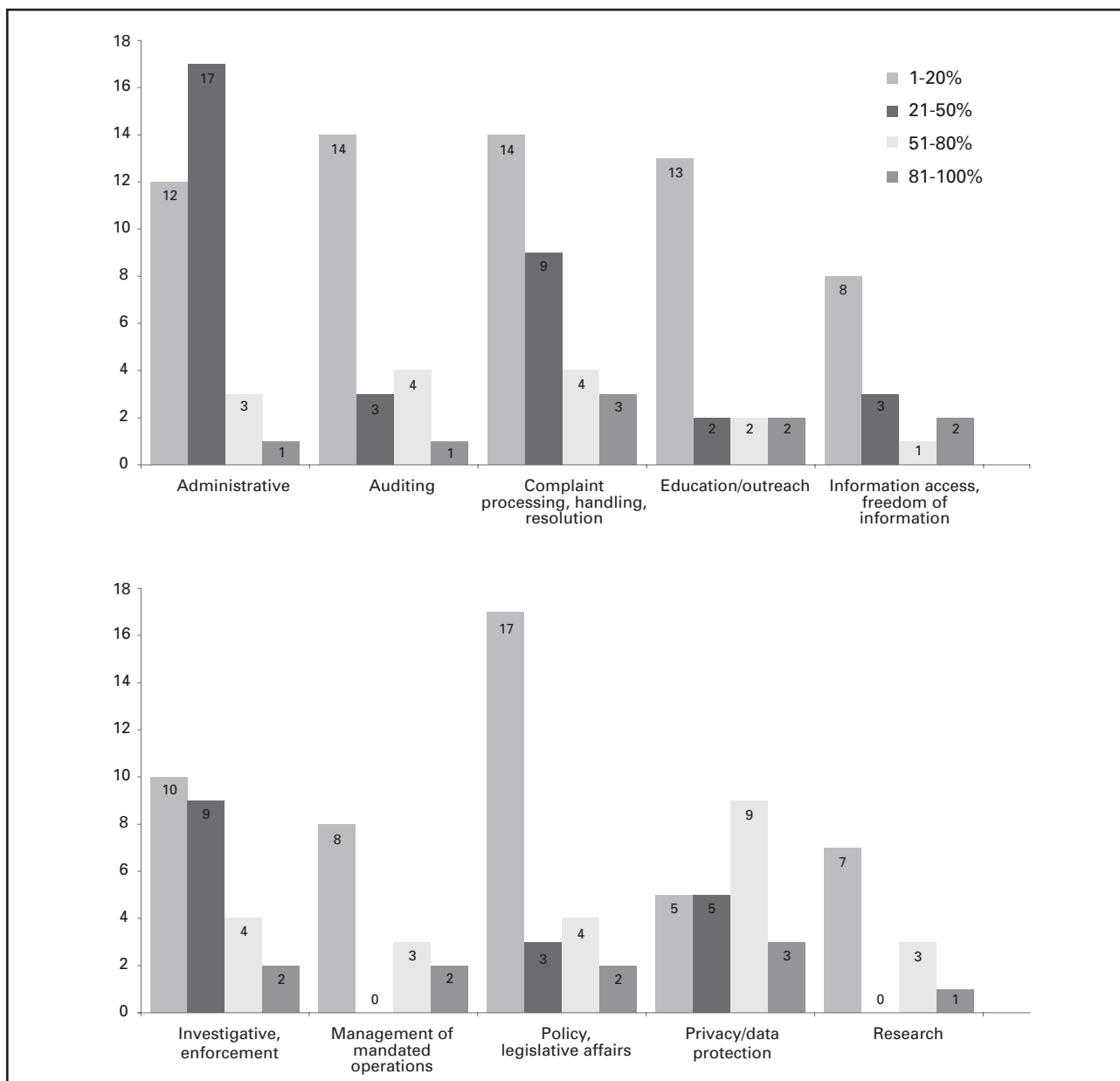
Seventeen out of 34 responding DPAs remarked that they have “other” responsibilities not specified in the answer options. In this category, responsibilities included data controller registry activities, audits and inspections and rule-making. The variety of the “other” responses is detailed in figure 4 below.

Figure 4: Other responsibilities



DPA's were asked to specify the number of full-time employees (FTEs) currently working in different activity areas. Figure 5 illustrates where DPA's are focusing their human resources. Three respondents, for example, indicated that between 81-100 percent of FTEs work on privacy/data protection, while nine DPA's said that between 21-50 percent of FTEs work on complaint-related issues.

Figure 5: FTEs dedicated to activity areas

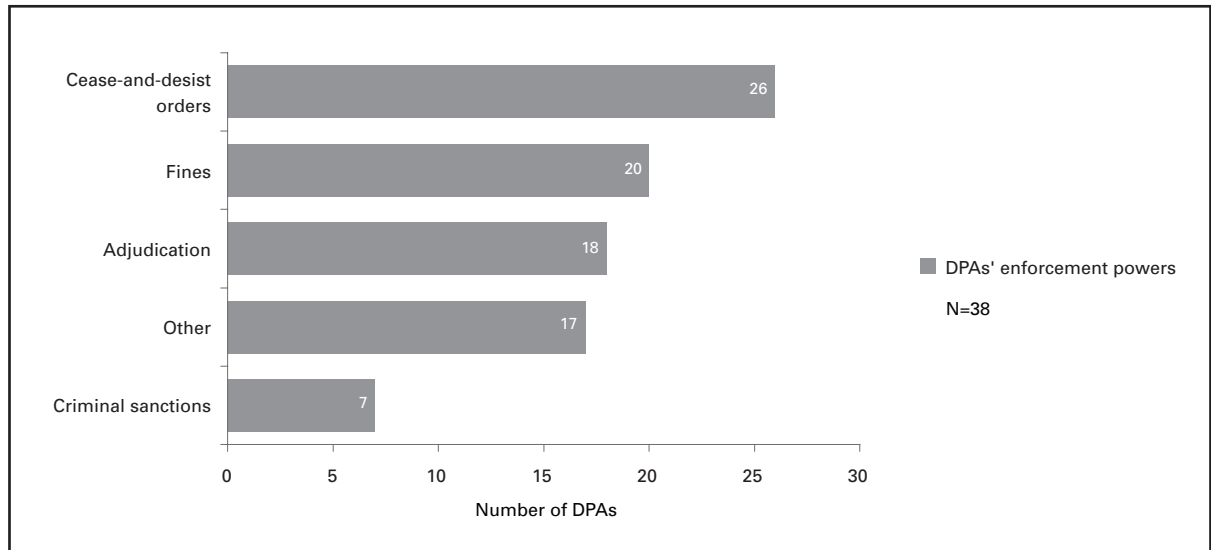


In terms of geographic distribution of staff, nearly all DPA's operate from a central office. However, the United Kingdom's Information Commissioner's Office (ICO) operates a central office in London as well as regional offices in Scotland, Wales and Northern Ireland. New Zealand's Office of the Privacy Commissioner operates two offices in different cities, but describes neither as "central" nor "regional." The central office of Australia's Office of the Privacy Commissioner encompasses two sites: one in Canberra and one in Sydney. And, in addition to its Ottawa headquarters, the Office of the Privacy Commissioner of Canada has a regional office in Toronto.

2. Authority and enforcement

More than two-thirds of respondents—68 percent—have the power to issue cease-and-desist orders, 59 percent can issue fines and approximately half of responding DPAs said adjudication is within their authority. Interestingly, seven DPAs indicated that they can impart criminal sanctions for data protection violations—representing a nine percent increase from our 2009 results.

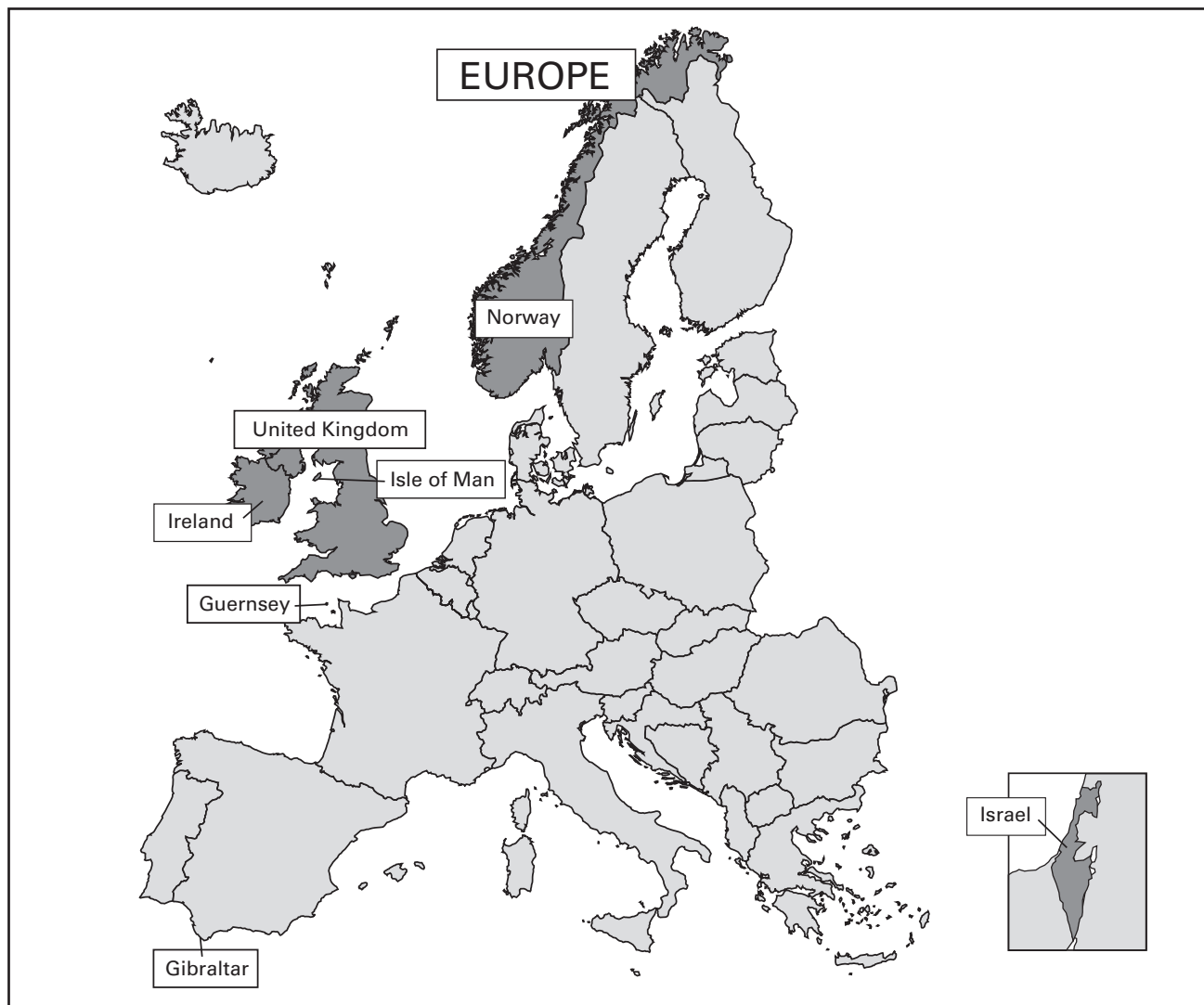
Figure 6: Means of enforcement



The following DPAs reported that the enforcement powers of their office include criminal sanctions:

- Gibraltar
- Guernsey
- Ireland
- Isle of Man
- Israel
- Norway
- United Kingdom

Figure 7: DPAs with authority to impart criminal sanctions

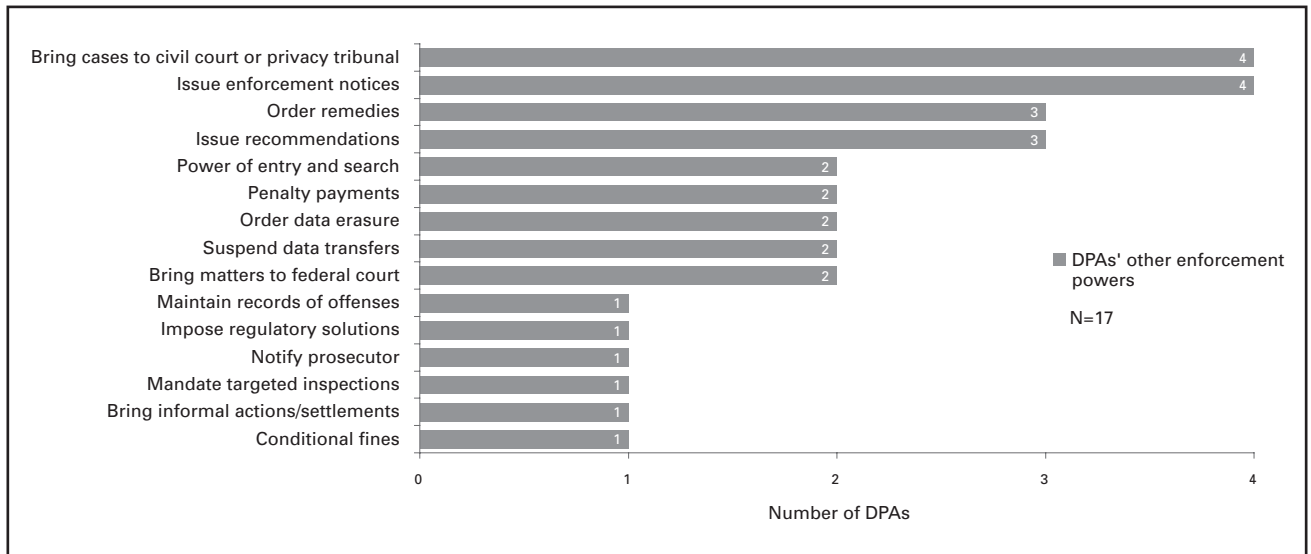


In future surveys, we will explore whether such enforcement powers apply to individuals, organizations, or both. We are also aware of other DPAs that have the authority to impart criminal sanctions but did not indicate this in their response.

In addition to the growth in the number of authorities who have the power to impart criminal sanctions, several DPAs remarked that they have the authority to issue enforcement notices requiring organizations to take certain steps. The United Kingdom is among those DPAs with the power to issue enforcement notices, the breach of which results in a criminal offense. Additionally, the Information Commissioner's Office (ICO) of the United Kingdom has the power to audit government departments without consent by means of an Assessment Notice and to issue civil monetary penalties up to a maximum of £500,000 for serious breaches of data protection principles. The ICO notes that such powers are not always utilized, as many complaints are settled through informal action (i.e., coming to an agreement with both parties).

Seventeen of the responding DPAs reported that they have enforcement powers that were not specified in our survey. Some of these other enforcement actions include issuing recommendations or enforcement notices, suspending foreign data transfer activities and initiating criminal investigations. Figure 8 collects these “other” responses.

Figure 8: Other means of enforcement



Privacy as a Crime

In 2009, after an extensive investigation and on-site inspection, the UK Information Commissioner's Office (ICO) prosecuted a Droitwich consultant on data protection charges. The ICO found that Ian Kerr, on behalf of the Consulting Association, had maintained and sold for profit the details of more than 3,000 construction workers over the course of three decades.

"Trading people's personal details in this way is unlawful and we are determined to stamp out this type of activity," said Deputy Information Commissioner David Smith at the time of sentencing.

Kerr was fined £5,000 for failing to register with the ICO as a data controller, and the organizations that purchased the data were also reprimanded. However, although Kerr's activities breached the UK's data protection principles, the ICO could not prosecute on those violations due to a lack of sanction powers.

The ICO has since received strengthened fining powers, but the Kerr incident and others have prompted UK officials to repeat calls for custodial sentences for those who violate UK privacy laws.

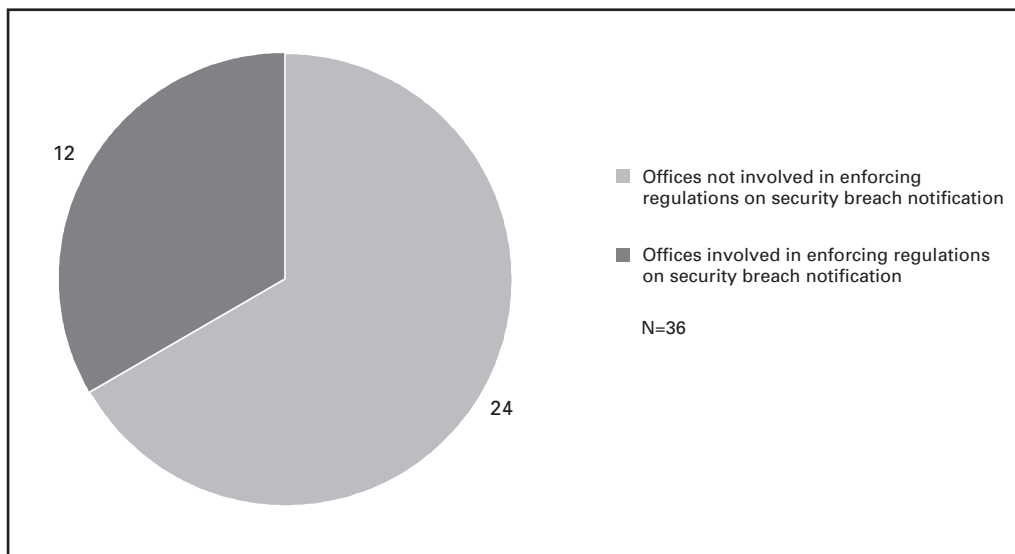
In the U.S., officials have increasingly imposed custodial sentences for those who have violated patient privacy. In April 2010, a former medical researcher became one of the first in the U.S. to be sentenced to prison for violating the federal Health Insurance Portability and Accountability Act (HIPAA). Huping Zhou received a four-month sentence for illegally viewing the medical files of celebrities and others during his employment at the UCLA School of Medicine. The following month, another former hospital worker was sentenced to two years behind bars for stealing patients' identities.

As the numbers of privacy breaches continue to mount, calls for tougher enforcement will likely grow louder.

Notice of security breach

When asked about security breach notifications, we found that only 12 DPA offices are actively involved in the enforcement of regulations in this area. Figure 9 illustrates authorities involved in enforcing regulations on security breach notification.

Figure 9: DPAs involved in enforcement of regulations on security breach notification



3. The DPA office: staff, size and allocation

The staff sizes of various DPAs range from very small to very large. For example, while the Data Protection Office of the Bailiwick of Guernsey and the Office of the Data Protection Supervisor of the Isle of Man each have just two full-time employees (FTEs), the Information Commissioner's Office (ICO) of the United Kingdom tops out at 319 FTEs.

The median staff size of the DPAs surveyed is 33 FTEs. Due to the wide range of sizes represented in the sample, we can further distinguish the organizations by breaking them into four groups: large, intermediate, medium, and small. This year's sample comprises several additional authorities whose sizes can be characterized as medium or small, explaining the decrease from last year's median staff size of 55 FTEs.

Figure 10 illustrates a breakdown of this year's sample by organizational size, noting the number of FTEs for each authority.

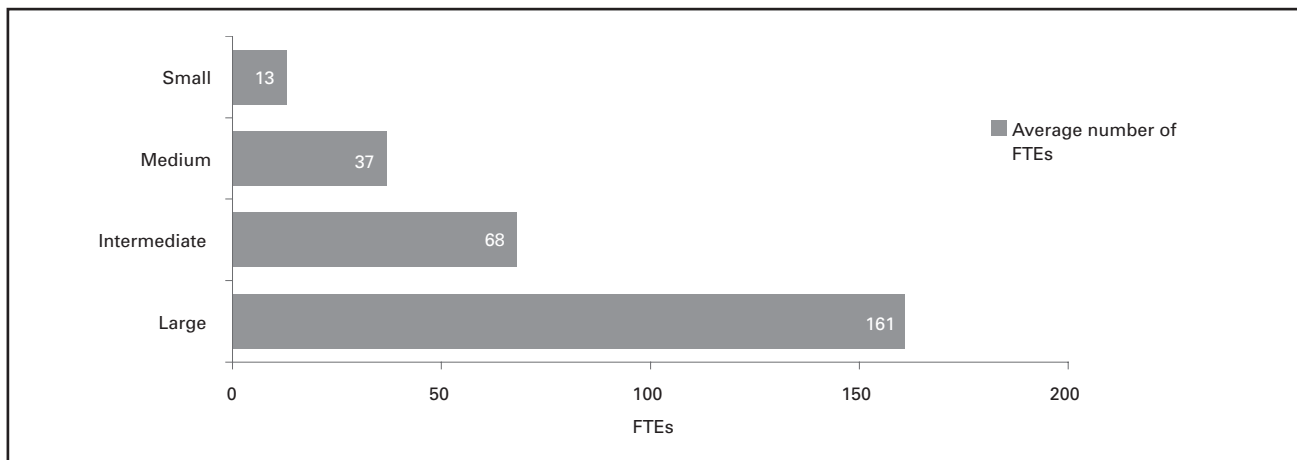
Figure 10: Number of FTEs by organization size

Large organizations (more than 100 FTEs)		Small organizations (1-24 FTEs)	
United Kingdom*	319	Macedonia	22
Canada**	173	Israel	21
France	132	Austria	20
Poland	121	Ireland	20
Italy	120	Latvia	19
Czech Republic	102	Estonia*	18
		Gibraltar*	18
Intermediate organizations (50-99 FTEs)		Cyprus	17
Netherlands	82	Macao	17
Colombia	73	Finland	16
Bulgaria	67	Malta	7
Hong Kong	62	Mauritius	7
Australia	58	Iceland	5
Medium organizations (25-49 FTEs)		Liechtenstein	4
Sweden	43	Faroe Islands	3
European Union	40	Guernsey*	2
Greece	40	Isle of Man	2
Hungary*	40		
Serbia*	38		
Norway	37		
Slovakia	35		
Lithuania	33		
Slovenia*	32		
New Zealand	31		

*These DPAs also have information access responsibilities. The staff numbers listed here may include employees who work on information access.

**FTE estimate includes employees on maternity leave.

Figure 11: Average number of FTEs by organization size



To better understand the degree of focus placed on data protection by each DPA, the study calculated the ratio of FTEs in a given regulators' office to the national population within its jurisdiction and then ranked the DPAs by the resulting proportions.

Gibraltar ranks first with about one FTE per 1,600 citizens, while Colombia ranks last among federal DPAs, with a proportion of roughly one FTE per 598,000 citizens. The European Data Protection Supervisor has the lowest concentration of FTEs to population (one FTE to approximately 12.3 million EU residents). Figure 12 contains the rankings.

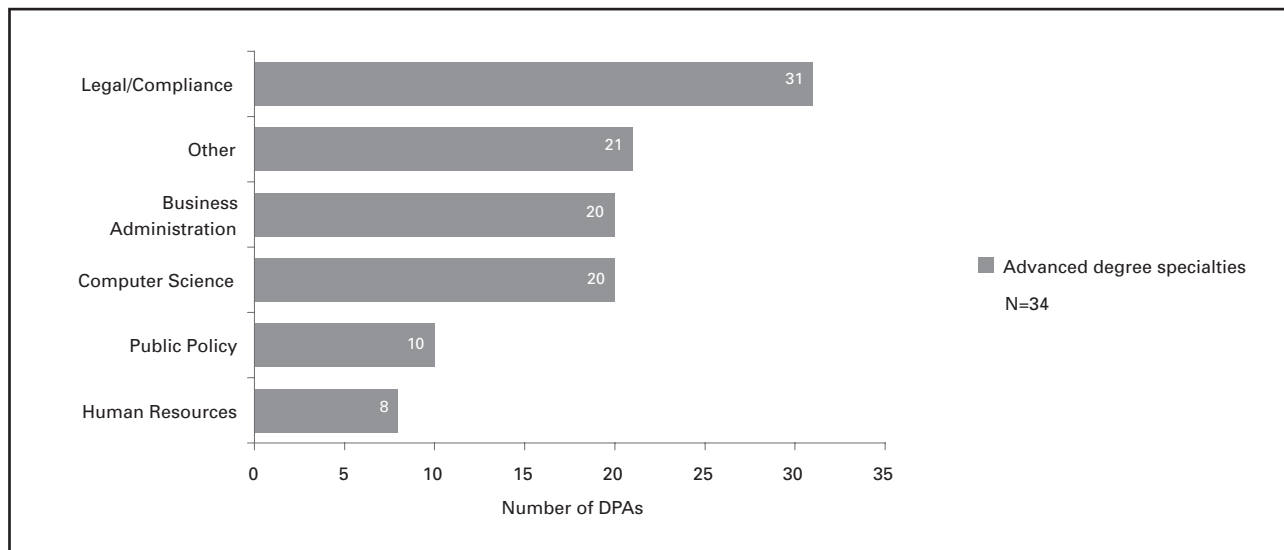
Figure 12: FTEs: Population

Jurisdiction	1 FTE per # Citizens	Rank (1 = most FTEs to citizens)
Gibraltar	1,600	1
Liechtenstein	8,690	2
Faroe Islands	16,265	3
Guernsey	32,742	4
Macao	32,932	5
Isle of Man	38,256	6
Malta	57,881	7
Iceland	61,339	8
Cyprus	63,809	9
Slovenia	62,678	10
Estonia	72,187	11
Macedonia	93,942	12
Czech Republic	100,117	13
Bulgaria	107,533	14
Lithuania	107,733	15
Hong Kong	113,791	16
Latvia	117,448	17
Norway	125,961	18
New Zealand	135,917	19
Slovakia	156,087	20
Mauritius	183,466	21
United Kingdom	191,577	22
Canada	193,568	23
Serbia	194,193	24
Netherlands	203,854	25
Ireland	210,160	26
Sweden	210,690	27
Hungary	247,640	28
Greece	268,436	29
Poland	318,041	30
Finland	328,142	31
Israel	344,462	32
Australia	366,597	33
Austria	410,514	34
Italy	484,385	35
France	488,031	36
Colombia	598,320	37
European Union (EDPS)	12,309,684	38

Education and professionalization of DPA staff

We also inquired into the backgrounds of staff that data protection authorities are hiring. We found that the vast majority of respondents currently employ staff holding advanced university degrees in legal or compliance-related specialties. Additionally, more than half of responding DPAs reported that they have staff with advanced university degrees in business administration and computer science.

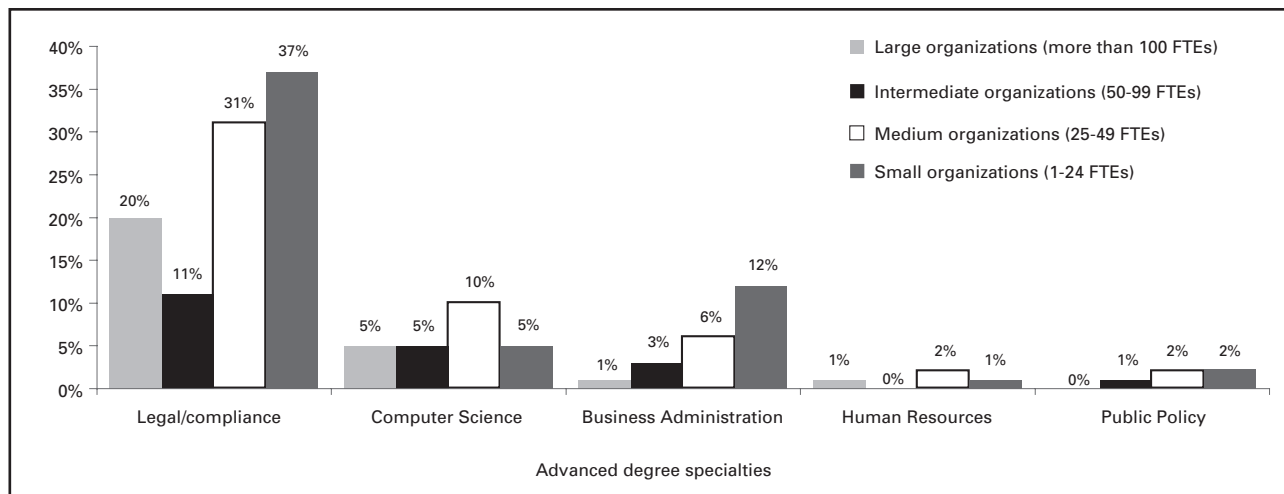
Figure 13: DPAs with staff holding advanced university degrees



Twenty-one authorities also indicated that they have staff members who hold advanced university degrees in specialties that were not specified in our survey, specifically, banking/finance, history, education, communications, social work and engineering.

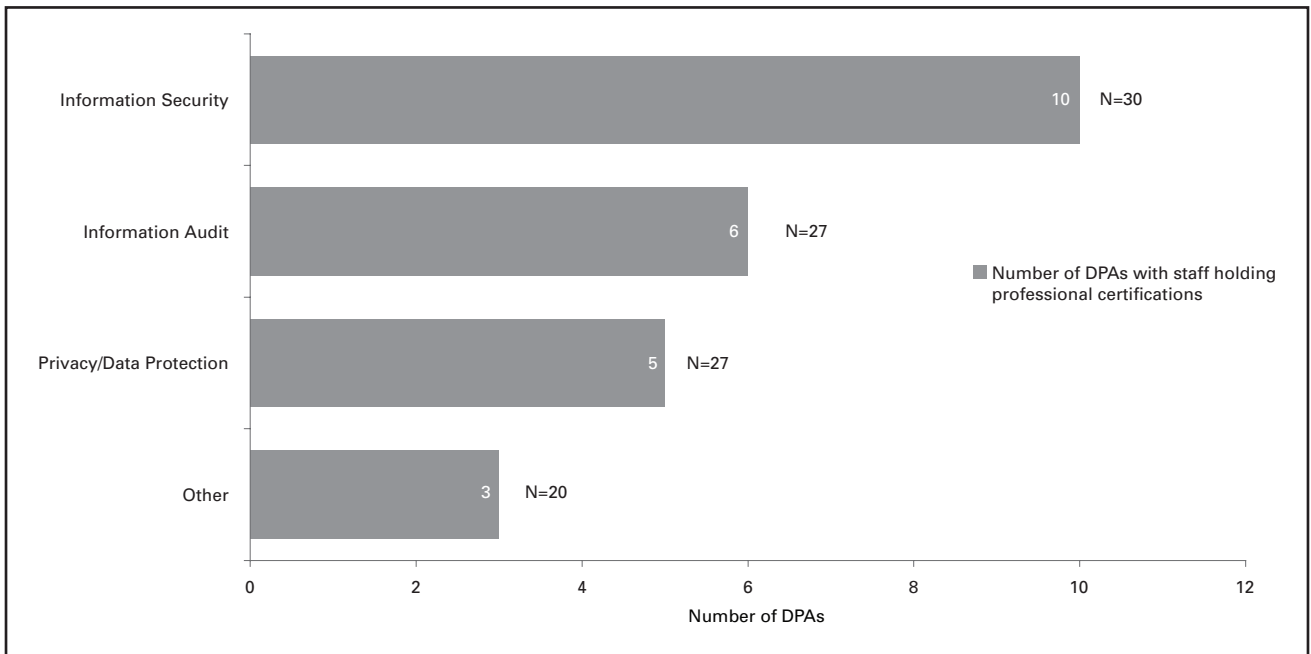
Taking the analysis one step further, we calculated the percentage of FTEs holding advanced university degrees in the identified specialties, expressing this as an average depending upon organizational size. For example, 37 percent of FTEs at small DPAs have advanced university degrees in legal or compliance-related specialties. Figure 14 illustrates these percentages.

Figure 14: Average percentage of FTEs with advanced degrees by organization size



When queried about whether staff members hold professional certifications, the majority of DPAs responded that staff do not. Of those authorities who responded affirmatively, the most common professional certifications held by staff members are in the field of information security. Figure 15 displays DPAs with staff holding professional certifications.

Figure 15: DPAs with staff holding professional certifications



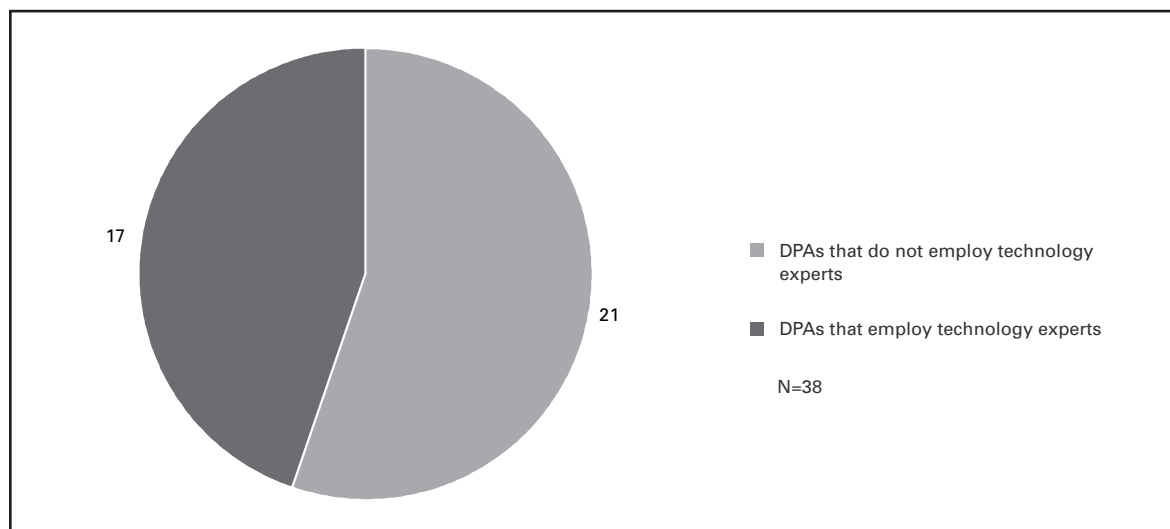
Three authorities have staff that hold professional certifications other than those identified in our survey. DPAs in Israel and Gibraltar specified that they employ staff holding legal certifications, while the Information Commissioner's Office of the United Kingdom noted that staff hold Data Protection Information Systems Examinations Board (ISEB) awards, and that staff in their audit department are working towards certification in internal audit and business risk.

Compared to the membership of the IAPP which represents the largest single association of practicing privacy professionals in both the public and private sector, there appears to be significantly less credentialed DPA staff worldwide. In 2010, approximately 43 percent of IAPP members held one or more privacy certifications. Our findings indicate that at most approximately one third (10 out of 30) responding DPAs reported that their staff hold professional certifications in privacy/data protection, information security, information audit or any other field. Of those DPAs whose staff hold professional certifications, the most common certification is in information security (10 out of 30 respondents), followed by information audit (seven out of 27 respondents) and privacy/data protection (five out of 26 respondents).

Technical expertise of DPA staff

Although data protection concerns continue to become increasingly technical in nature, only 17 DPAs said they have dedicated technical experts on staff to help execute investigations and complaint resolutions. This represents a 28 percent decrease from the 2009 results. However, we found that many offices now report that they hire or consult with external experts to deal with complex technical matters.

Figure 16: DPAs that employ technical experts for investigations and complaints



Buy it or build it?

Data protection matters continue to become increasingly technical in nature, a fact that is not necessarily reflected in DPAs' staffing compositions. Rather, in this year's study, we noticed a significant decrease in the number of staff members dedicated to the technical aspects of DPAs' investigative efforts.

Between 2009 and 2010, there was a 28 percent decrease in the number of DPAs who employ technical experts on staff. The numbers seem to reflect a growing trend among DPAs—a move toward the outsourcing of data forensics.

Some respondents to the 2010 study indicated that instead of having technical experts on staff, they hire outside consultants to

handle technically complex matters. These DPAs pointed to resource limitations and a dearth of qualified candidates as reasons for moving to an outsourcing model. Others noted that they derive greater value by contracting outside experts.

"In practice, [consulting with outside experts] has proven to be beneficial to the DPA's supervision operations since it is possible to hire the expert with the most expertise in the field being supervised at a given time," said Thordur Sveinsson, legal counsel for the Icelandic Data Protection Authority.

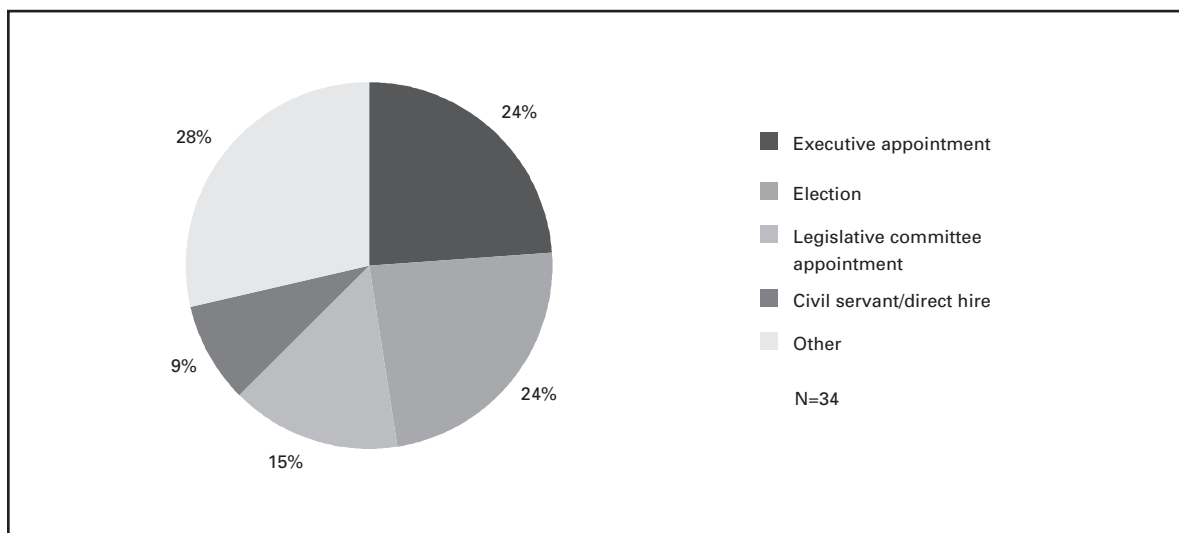
DPA appointment and term of office

Thirty-five of 38 DPAs surveyed said that there is at least one dedicated official in charge of their data protection and privacy efforts. The study found that approximately 24% of responding DPAs have data protection commissioners that are appointed by executive and 15 percent by legislative processes. Twenty-four percent of authorities said that an election is the primary appointment method. Three DPAs reported that their officials are civil servants or direct hires.

Interestingly, the Austrian Data Protection Commission is headed by more than one official. Austria remarked that its commission is organized like a court; there is not a single commissioner but a commission headed by a chairman.

See Appendix B for a complete list of data protection commissioners.

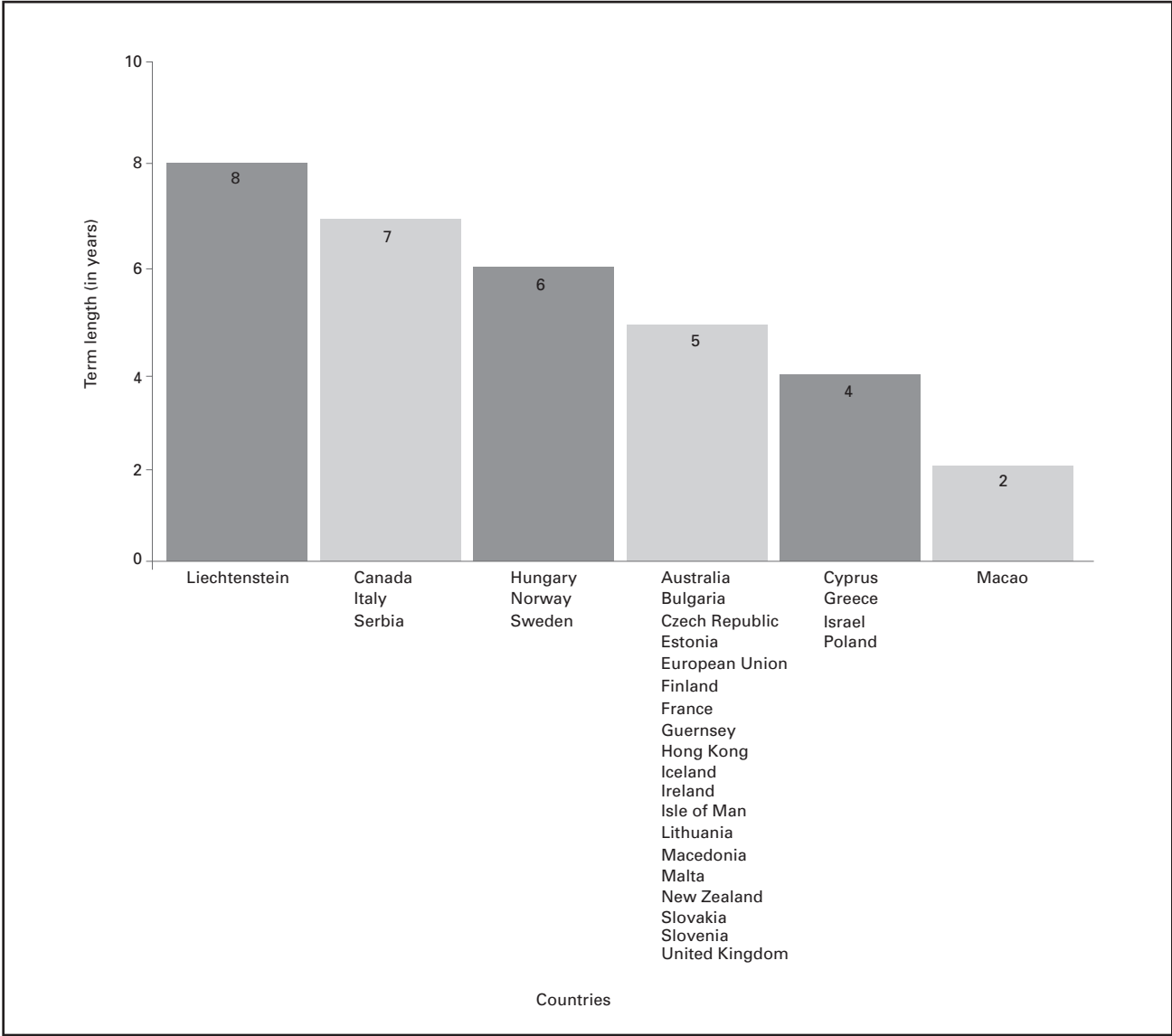
Figure 17: DPA appointment processes



Twenty-eight percent of responding DPAs indicated that the individual who heads their organization is appointed by a method other than one specified in our survey. For example, the head of the European Data Protection Supervisor (EDPS) is selected by joint decision of Council and European Parliament. Similarly, Hungary's commissioner is appointed by the president, and the parliament elects him or her by a two-thirds majority. Other responses include appointment after recommendations of search committees or responsible ministers or leaders. See Appendix C for a list of appointing bodies by jurisdiction.

Specified term lengths for data protection commissioners vary from two years in the Office for Personal Data Protection of Macao to eight years for the Data Protection Office of Liechtenstein. Interestingly, DPAs in three countries—Faroe Islands, Gibraltar, and Mauritius—reported that their term lengths are indefinite or permanent postings. The most common term length reported is five years.

Figure 18: Commissioners’ term lengths



When asked whether or not they have a formal liaison to the privacy profession, 89 percent of responding authorities indicated that they do not. DPAs in Australia, Canada, France and Mauritius were the only authorities to report having such a liaison.

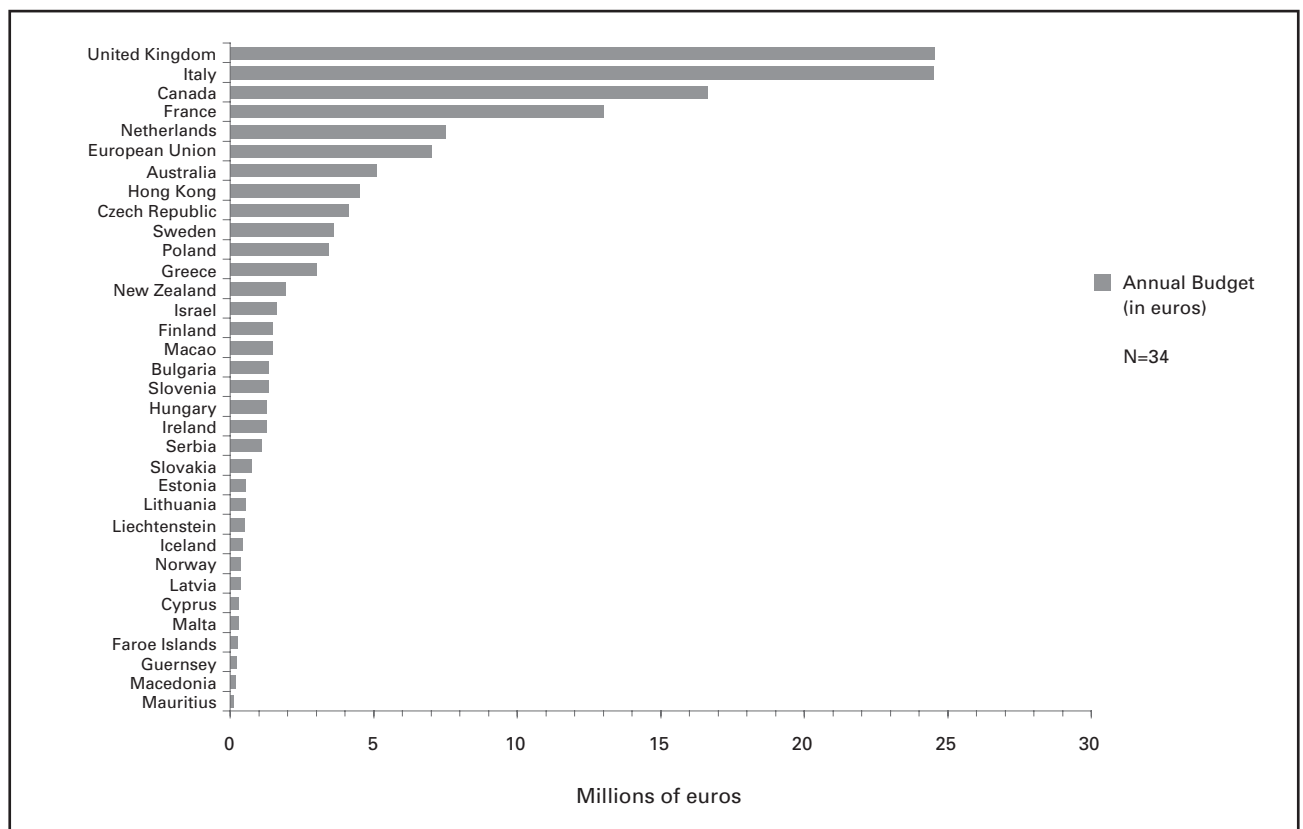
Australia's Office of the Privacy Commissioner remarked that it coordinates a network of Privacy Contact Officers (PCOs), which holds meetings four times per year to discuss current privacy issues. Additionally, Australia's office maintains a network of professionals in corporate and not-for-profit sectors, which provides a forum for the exchange of ideas relating to good privacy practice, promotes awareness of privacy developments and enhances interaction with the Office of the Privacy Commissioner.

Canada's Office of the Privacy Commissioner (OPC) noted that it has an Access to Information and Privacy (ATIP) Office, and DPAs in Canada, France and Mauritius reported holding the further authority to liaise with the international privacy community.

The DPA office: budget size and allocation

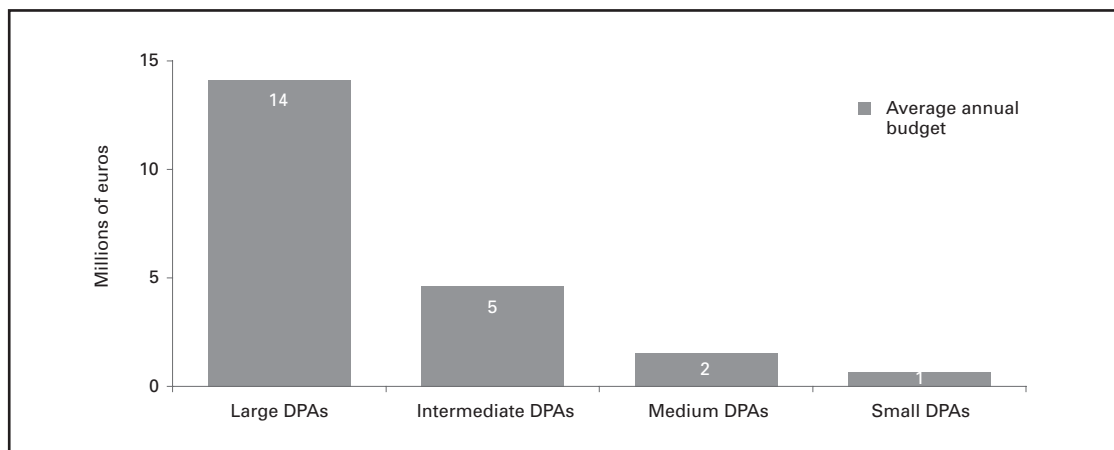
DPAs' annual budgets range from relatively large to relatively small. The average annual budget of respondents is 3,969,470 euros. Furthermore, our study revealed a strong correlation between organizations' staff sizes and annual budgets.

Figure 19: DPAs' annual budgets in euros*



*Austria, Colombia, Gibraltar and the Isle of Man did not submit budget data.

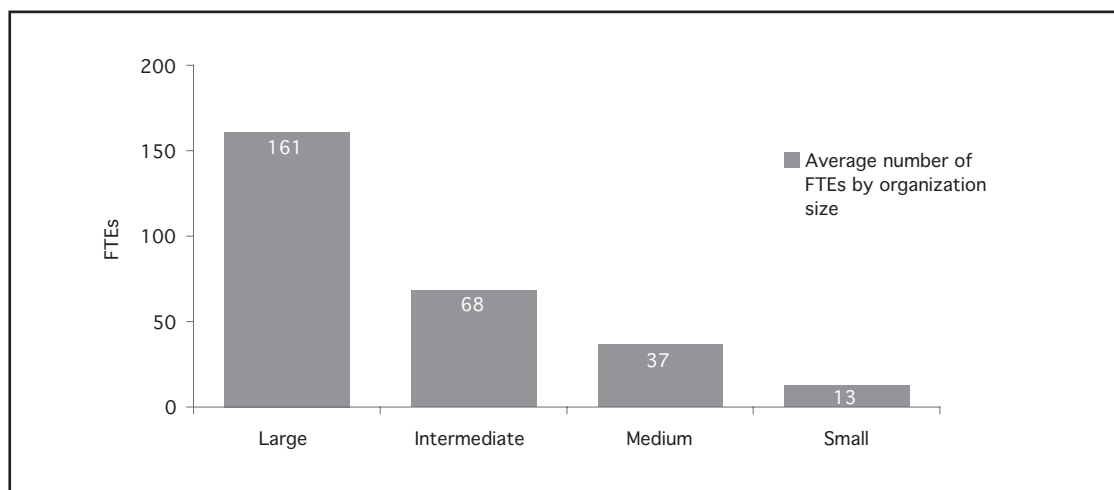
Figure 20: Average annual budget (in euros) by DPA size * **



*Currencies were converted into euros between August 13 – 27, 2010.

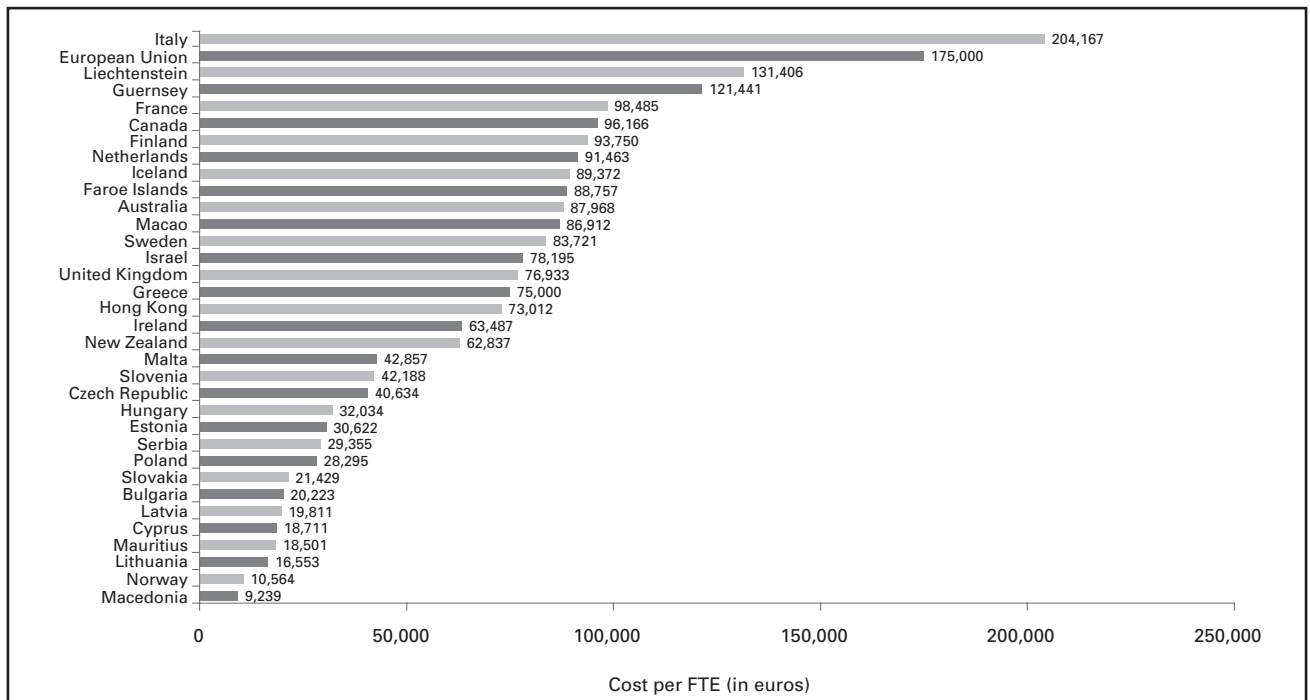
** Does not include European Data Protection Supervisor (EDPS) budget data.

Figure 21: Average number of FTEs by organization size



Taking the budget numbers a step further, we determined that the average cost per FTE at an authority is 64,545 euros. However, the European Data Protection Supervisor (EDPS) somewhat skews the average. Removing the EDPS from the calculation results in an average annual FTE cost of 61,297 euros. Figure 22 shows the cost per FTE at each DPA.

Figure 22: Cost per FTE* **

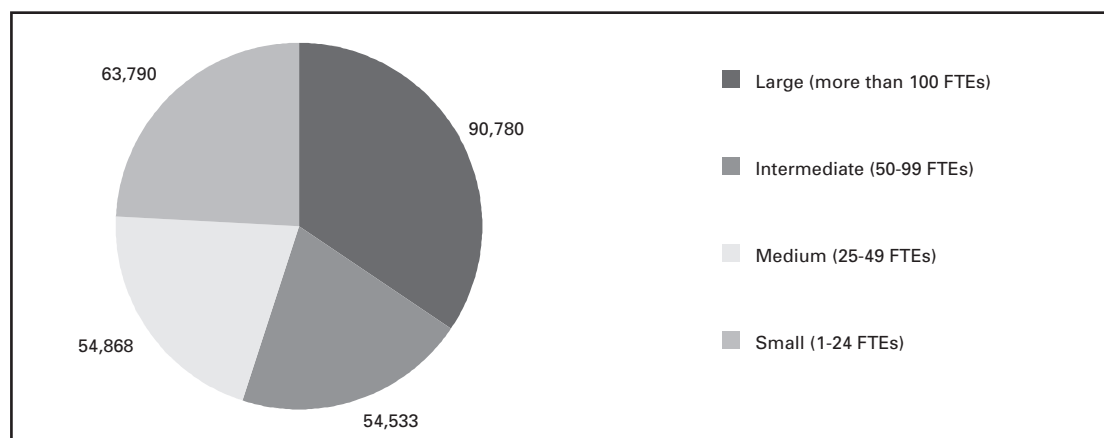


* Currencies were converted to euros between August 13—27, 2010.

** Austria, Colombia, Gibraltar and Isle of Man did not submit budget data.

Figure 23 illustrates the average cost per FTE by organization size.

Figure 23: Average cost per FTE (in euros) by organization size* **



* Currencies were converted to euros between August 13—27, 2010.

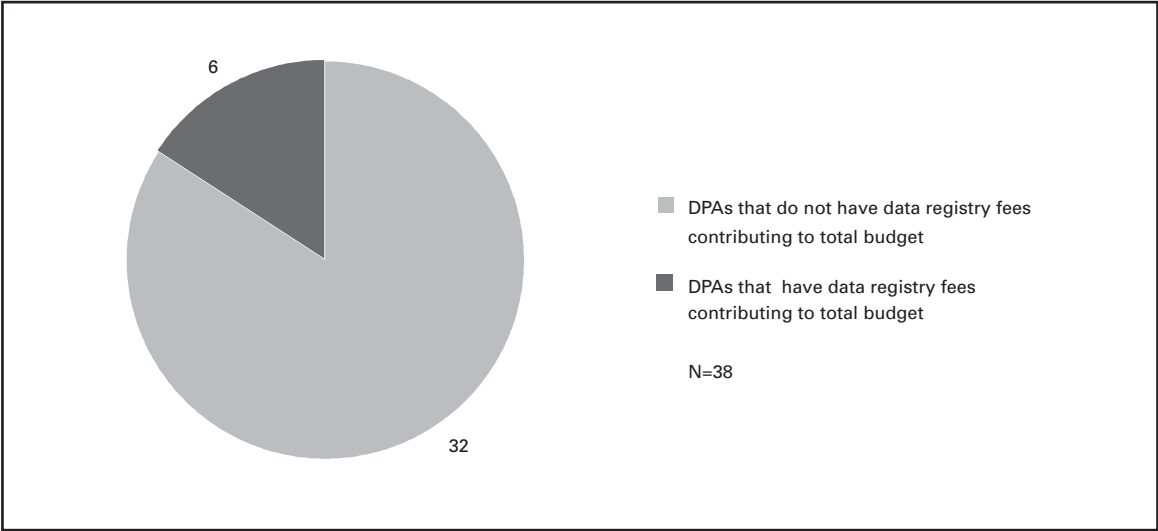
** Austria, Colombia, Gibraltar and Isle of Man did not submit budget data.

The 2009 DPA Global Benchmarking Survey sought to determine whether or not DPAs’ enforcement capabilities corresponded to the size of their annual budgets. Specifically, it examined whether the organizations that have the authority to levy fines (i.e. greater enforcement powers) had larger annual budgets as a result. From our analysis, it seemed unlikely that there was any meaningful correlation.

In this year’s survey, DPAs were asked whether enforcement fines contribute to their annual budgets and discovered that while 20 DPAs reported having the authority to issue fines, only three DPAs—Italy, Malta and Macedonia—said enforcement fines contribute to their annual budgets.

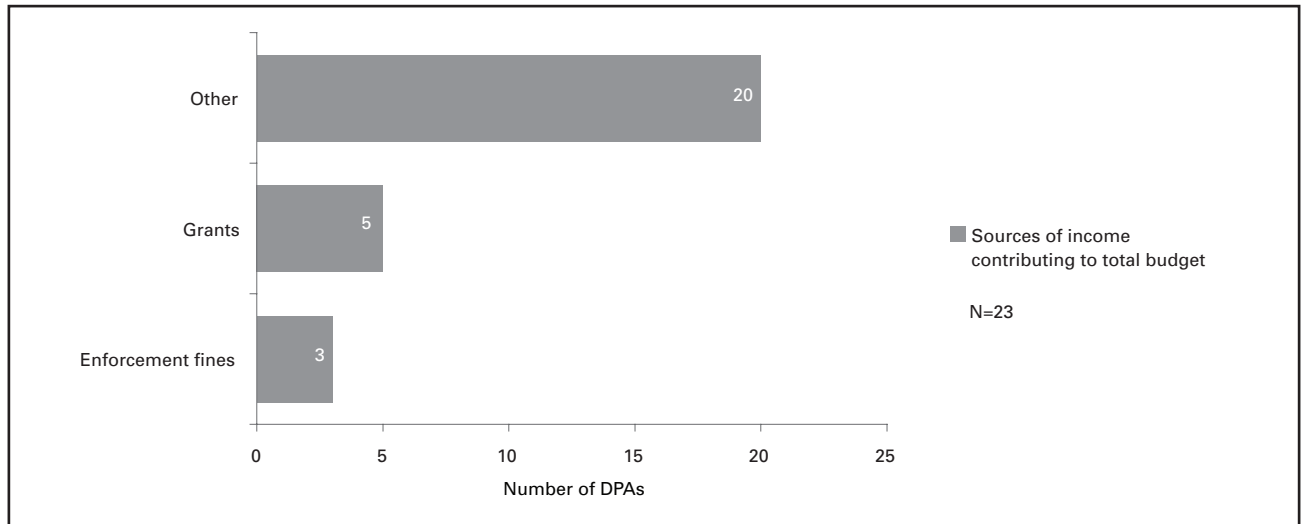
We also noted in last year’s report that it would be interesting to determine the impact, if any, of data controller registry fees on annual budgets. This year we sought to answer this question, finding that only six DPAs responded affirmatively. Figure 24 displays these results.

Figure 24: DPAs with data registry fees contributing to budget



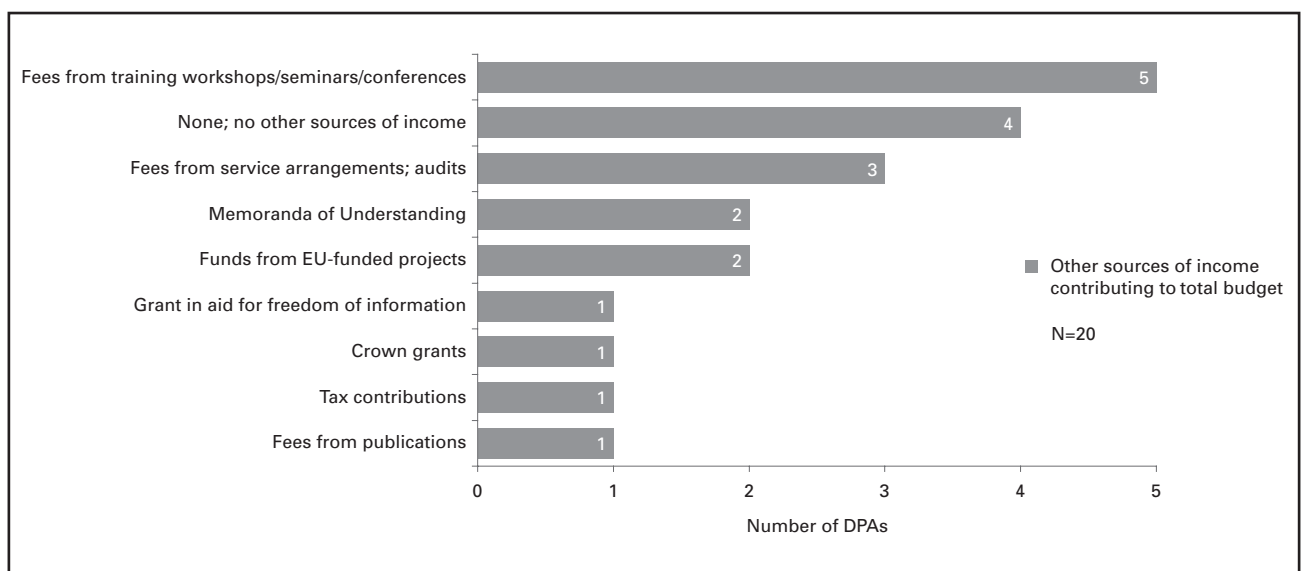
Additionally, we sought to determine what other sources of income contribute to the total budgets of DPAs. The Italian DPA (*Il Garante per la Protezione dei Dati Personali of Italy*), the Directorate for Personal Data Protection of Macedonia, and the Office of the Data Protection Commissioner of Malta reported that enforcement fines add to the overall budgets of their offices, while five DPAs in other countries—the Czech Republic, Hong Kong, Hungary, Poland, and Serbia—reported that grants contribute to their overall budgets. Figure 25 illustrates the sources of income contributing to DPAs’ total budgets.

Figure 25: Sources of income contributing to DPAs’ budgets



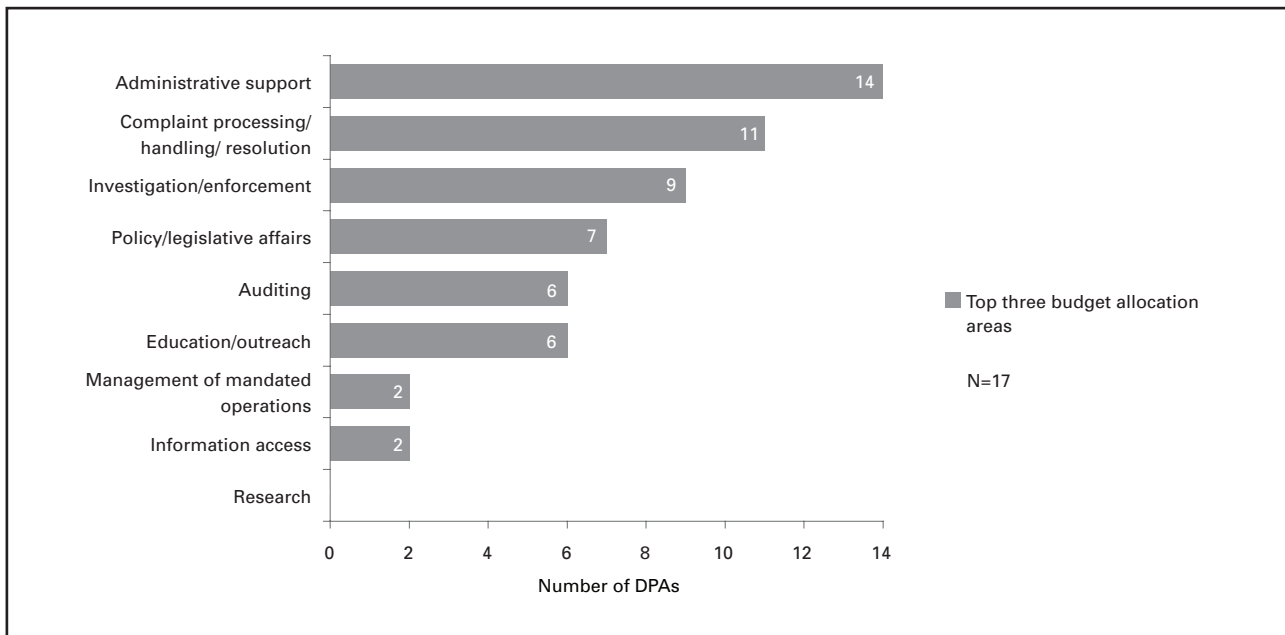
Importantly, 20 DPAs reported that they have “other” sources of income that contribute to their offices’ total budgets, besides those specified in our survey. Other sources of income include funds from European Union (EU)-funded projects, tax contributions, fees from publications, training workshops/seminars and audits. Figure 26 collects all of these “other” sources of income.

Figure 26: Other sources of income contributing to DPAs’ budgets



We analyzed DPAs’ top-three budget allocation areas to create Figure 27, which shows where DPA spending is most concentrated. For example, 13 of 16 respondents indicated that “administrative support” was among their top-three spending areas, while no respondents reported that “research” was a top-three spending area.

Figure 27: Top budget allocation areas*



*In certain instances, more than three areas qualified as being within a DPA’s top-three spending areas. For example, the European Union’s top-three spending areas are policy/legislative affairs (25 percent), followed by investigation/enforcement (20 percent) and then administrative support and complaint processing/handling/resolution—each at 15 percent.

We looked at DPAs' annual budgets alongside the annual government expenditures of each jurisdiction, finding that data protection spending as a percentage of total government spending is greatest in the governments of Serbia and Iceland, as illustrated in Figure 28.

Figure 28: Percent of annual government expenditures directed to data protection* **

MORE THAN 1%		LESS THAN .0050%	
DPA	% of Annual Gov't Expenditures	DPA	% of Annual Gov't Expenditures
Serbia	1.0200%	Czech Republic	0.0046%
Iceland	1.0189%	Canada	0.0038%
		Cyprus	0.0029%
		Latvia	0.0024%
		Italy	0.0023%
		Slovakia	0.0021%
		Australia	0.0021%
		Greece	0.0019%
		Netherlands	0.0018%
		Norway	0.0018%
		United Kingdom	0.0018%
		Ireland	0.0018%
		Finland	0.0011%
		France	0.0009%
BETWEEN 1% AND .1%			
DPA	% of Annual Gov't Expenditures		
Hungary	0.6122%		
Macao	0.4199%		
Macedonia	0.3966%		
Mauritius	0.2275%		
Faroe Islands	0.1741%		
Hong Kong	0.1033%		
BETWEEN .1% AND .0050%			
DPA	% of Annual Gov't Expenditures		
Estonia	0.0994%		
Liechtenstein	0.0839%		
Guernsey	0.0376%		
Sweden	0.0153%		
Bulgaria	0.0146%		
Poland	0.0142%		
Israel	0.0137%		
Lithuania	0.0117%		
Malta	0.0080%		
New Zealand	0.0065%		
Slovenia	0.0059%		

*Austria, Colombia, Gibraltar and Isle of Man did not submit budget data.

**No estimate available for the European Union.

Next, we looked at DPAs' annual budgets alongside gross domestic product, as shown in Figure 29.

Figure 29: Data protection spending as a percentage of GDP*

BETWEEN 1% AND .1%

DPA	% of GDP
Iceland	0.5609%
Hungary	0.2810%
Serbia	0.2677%
Macedonia	0.1354%

BETWEEN .1% AND .0050%

DPA	% of GDP
Faroe Islands	0.0809%
Macao	0.0681%
Mauritius	0.0581%
Estonia	0.0451%
Hong Kong	0.0214%
Liechtenstein	0.0149%
Guernsey	0.0072%
Bulgaria	0.0056%
Lithuania	0.0051%

LESS THAN .0050%

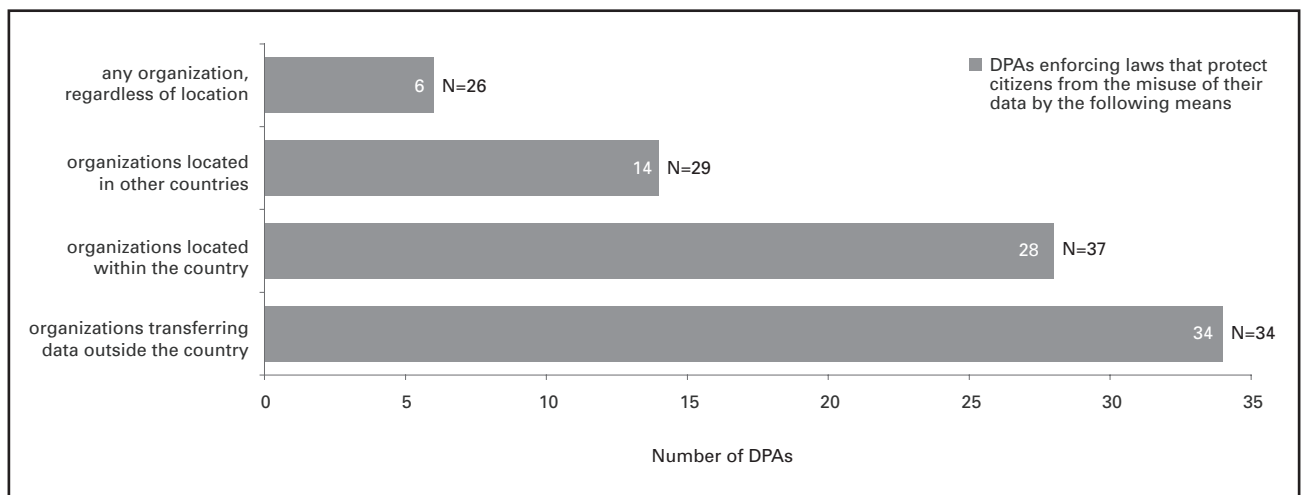
DPA	% of GDP
Israel	0.0041%
Malta	0.0038%
Poland	0.0032%
New Zealand	0.0030%
Slovenia	0.0027%
Czech Republic	0.0021%
Canada	0.0017%
Cyprus	0.0013%
Italy	0.0012%
Latvia	0.0010%
Netherlands	0.0009%
United Kingdom	0.0009%
Greece	0.0009%
Sweden	0.0009%
Slovakia	0.0009%
Norway	0.0008%
Australia	0.0007%
Ireland	0.0006%
Finland	0.0006%
France	0.0005%
European Union	0.0004%

*Austria, Colombia, Gibraltar and Isle of Man did not submit budget data.

4. Transborder issues

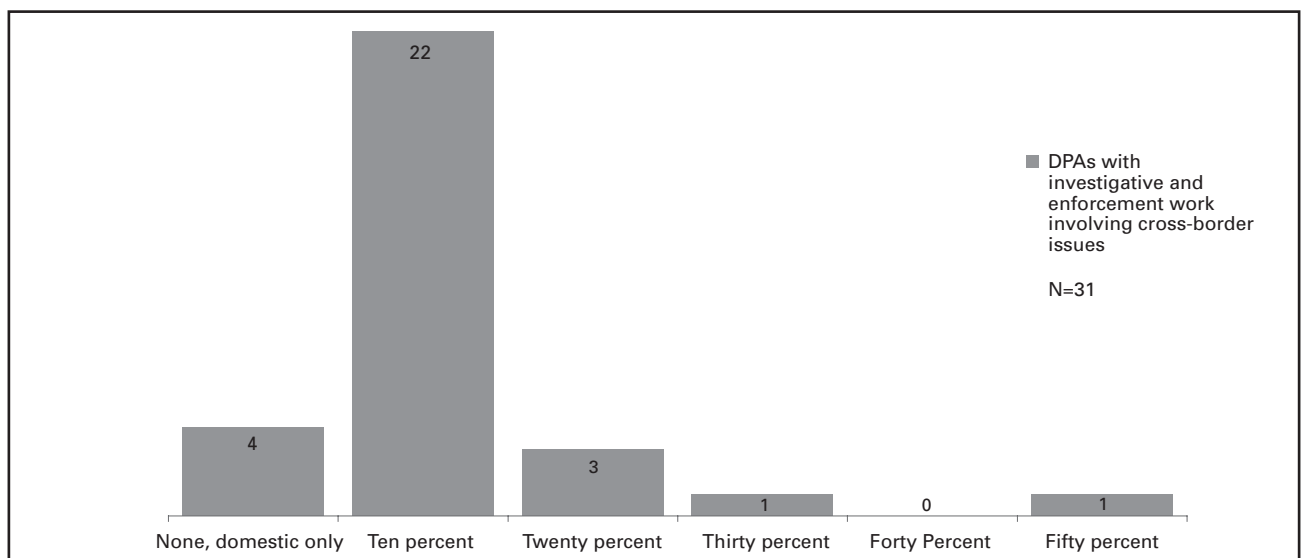
We sought to gauge the level of protection that citizens are given under the laws that guide their country's data protection authority. We found that the majority of responding DPAs are enforcing laws that protect citizens from the misuse of their data by organizations located within their country as well as organizations transferring data outside of their country. A smaller number of DPAs—14 out of 29 respondents—indicated that the laws they enforce protect citizens from the misuse of their data by organizations located in other countries, while only six DPAs—Bulgaria, Canada, France, Israel, Italy and the Netherlands—stated that under their countries' laws, citizens receive protection from the misuse of their data by any organization, regardless of location. Figure 30 illustrates the level of protection citizens are given under the laws enforced by their jurisdiction's DPA.

Figure 30: Protection from misuse of data under laws guiding DPAs



The vast majority of responding DPAs reported that 10 percent or less of the investigative and enforcement work of their office involves transborder issues, with four DPAs stating that their investigative and enforcement work is domestic oriented only. Figure 31 illustrates the percentage of transborder investigative and enforcement work done by DPAs.

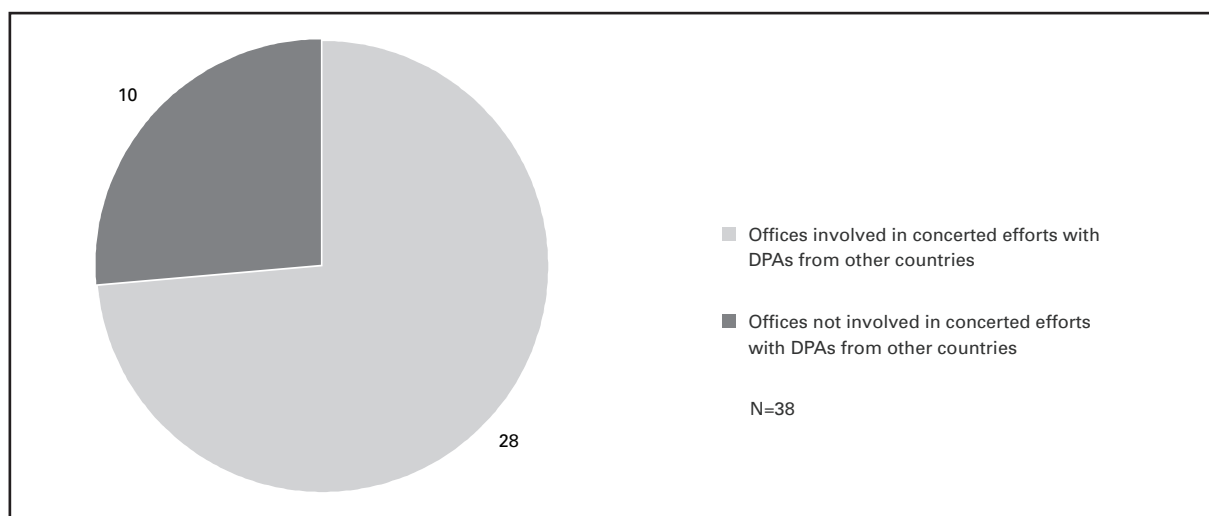
Figure 31: Percent of transborder investigative and enforcement work



Multi-regulator coordination and cooperation

Nearly three-quarters of those surveyed—74 percent—stated that their office is involved in some sort of concerted effort with DPAs from other countries. (See Appendix D for a full list of all responses.) Many European DPAs reported that they are involved in international concerted efforts within the framework of the Article 29 Working Party. DPAs in Australia and New Zealand revealed that they are involved with the Asia Pacific Privacy Authorities (APPA) as well as APEC’s Transborder Privacy Enforcement Arrangement (CPEA). APPA is the principal forum for privacy authorities in the Asia Pacific region to form partnerships and exchange ideas about privacy regulation, new technologies and the management of privacy enquiries and complaints, while the CPEA provides a framework for privacy regulators to cooperate and to seek information and advice on transborder enforcement matters.

Figure 32: Offices involved in concerted efforts with other DPAs



Other examples of cooperation among DPAs include participation in the Global Privacy Enforcement Network (GPEN) and involvement in specific issues such as data retention in the electronic communications sector and Google Street View services.

Canada, Cyprus, Italy and the Netherlands were the only DPAs to indicate that their office has cooperated with the FTC or any other U.S. regulatory agency to bring an enforcement action against a U.S.-based organization.

IV. Survey Methodology

Survey Methods

The IAPP identified 64 federal-level data protection/privacy offices on five continents to receive the benchmarking survey. In mid-July 2010, the IAPP sent individual e-mails to pre-identified contacts at each DPA to invite them to participate in the survey. The survey link was included as well as a note from the IAPP executive director about the objectives and intended use of the findings. Additionally, contact information for each DPA was listed and recipients were asked to respond to confirm the accuracy of such information. The IAPP informed recipients that they would be provided with a copy of the published report when it became available in the fall. In the meantime, recipients were invited to access the results of last year's report (the 2009 Data Protection Authorities Global Benchmarking Survey) by visiting the IAPP Web site.

Two weeks after the initial fielding, the IAPP sent a reminder e-mail to those who had not yet completed the survey. The IAPP collected responses through mid-September.

Survey Considerations

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. The IAPP sent 64 surveys and received responses from 38 DPAs for a response rate of 59 percent. Based on the breadth of respondents, the data offered here provides insight on a range of federal DPAs—large and small, centralized and regional. However, it is possible that substantial differences exist among the 26 DPAs who chose not to participate, and this fact must be taken into account when considering the findings.

In addition, the IAPP selected DPAs to target for survey participation using published resources and other publicly available references online and in print. This resulted in a highly qualified sample of relatively mature DPAs in mostly first-world nations across five continents (Asia, Australia, Europe, North America and South America). Even so, it is possible that newly established DPAs would have had a significant impact on the findings had they been asked to complete the survey.

Timing

We began conducting our survey at the beginning of the northern hemisphere's summer holiday season, which may have affected the response rate.

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 level data protection authorities, we included data pertaining to the European Union's DPA (the European Data Protection Supervisor). We did this because the EDPS is devoted to promulgating best practices for protecting personal data and privacy in all EU institutions and bodies, and itself serves as a model for DPAs in the EU, and possibly beyond.

Benchmarking

This is the second survey of this issue. 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 may vary as issues evolve and change over time. This year's survey contains the addition of several new questions, which should be taken into account when analyzing the results for comparative purposes.

V. Appendices

APPENDIX A: Global data protection authorities audited survey results

DPA Responses

Q1.	Country (contextual response)
Q2.	Name of your office or organization (contextual response)
Q3.	Please enter the number of full-time staff in your office (numerical response)
Q4.	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) specialties: legal/compliance, computer science, business administration, human resources, public policy, other
Q5.	If any staff members in your office hold advanced university degrees in specialties other than those identified above, please specify: (contextual response)
Q6.	Do any of your staff hold professional certifications (i.e., CIPP, CPA, CISSP, CISA) in:
Pct %	
	Yes No
Information security (N=30)	33% 67%
Information audit (N=27)	22% 78%
Privacy/data protection (N=27)	19% 81%
Other (N=20)	15% 85%
Q7.	Please enter the number of full-time staff members that work in the following areas: (numerical response) (areas: administrative (HR, tech support, operations, etc.), auditing, complaint processing/handling/resolution, education/outreach, information access/freedom of information, investigative/enforcement, management of mandated operations, policy/legislative affairs, privacy/data protection, research, other)
Q8.	If any of your full-time staff members work in areas other than those identified above, please specify: (contextual response)
Q9.	Does your office employ staff who provide technological expertise (i.e., data forensics) for investigations/complaint resolution? (if yes, contextual response)
N=38	Pct %
Yes	35%
No	65%
Q10.	Please enter the number of full-time staff who work in: (numerical response) (central office, regional offices, other)

Q11. If any of your full-time staff work somewhere other than a central or regional office, please specify: (contextual response)

Q12. Does your office have a data protection commissioner or other similar official? (if yes, contextual response)

N=38	Pct %
Yes	92%
No	8%

Q13. If your office has a data protection commissioner, what is the appointment process?

N=34	Pct %
Executive appointment	24%
Legislative committee appointment	15%
Election	24%
Civil servant/direct hire	9%
Other	29%

Q14. If your office has a data protection commissioner, how long is this person's term? (contextual response)

Q15. Does your office have a formal liaison to the privacy profession? (if yes, contextual response)

N=38	Pct %
Yes	11%
No	89%

Q16. What is the overall annual budget of your office? (please specify currency) (contextual response)

Q17. Do data registry fees contribute to your office's total budget?

N=38	Pct %
Yes	16%
No	84%

Q18. What other sources of income contribute to your office's total budget? (multiple responses allowed)

N=24	Pct %
Enforcement fines	13%
Grants	21%
Other	83%

Q19. What percentage of your total budget is allocated to each of the following areas? (Please include payroll/staff in each area's allocation; estimates are fine; total budget should add up to 100%)

N=17	None	1-10%	11-20%	21-30%	31-40%	41-50%	51-60%	61-70%	71-80%	81-90%	91-100%
Administrative (HR, tech support, operations, etc.)	0%	35%	41%	6%	0%	12%	0%	0%	0%	0%	6%
Auditing	24%	47%	29%	0%	0%	0%	0%	0%	0%	0%	0%
Complaint processing/handling/resolution	24%	12%	35%	12%	18%	0%	0%	0%	0%	0%	0%
Education/outreach	18%	47%	35%	0%	0%	0%	0%	0%	0%	0%	0%
Information access	59%	29%	0%	12%	0%	0%	0%	0%	0%	0%	0%
Investigation/enforcement	29%	24%	35%	12%	0%	0%	0%	0%	0%	0%	0%
Management of mandated operations (i.e., data processor filings)	47%	53%	0%	0%	0%	0%	0%	0%	0%	0%	0%
Policy/legislative affairs	29%	35%	18%	12%	6%	0%	0%	0%	0%	0%	0%
Research	53%	41%	6%	0%	0%	0%	0%	0%	0%	0%	0%
Other areas	68%	12%	0%	6%	0%	12%	6%	0%	0%	0%	0%

Q20. If a percentage of your total budget is allocated to areas other than those identified above, please specify: (contextual response)

Q21. What is the scope of authority of your office? (multiple responses allowed)

N=37	Total %
Information access/freedom of information	19%
Data protection, public sector (managing governmental privacy issues)	95%
Data protection, private sector	92%
Data protection, specific private-sector industries (i.e., healthcare only)	27%
Other	22%

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

	Pct%	
	Yes	No
Organizations located within the country only? (N=36)	78%	22%
Organizations transferring data outside of the country? (N=34)	100%	0%
Organizations located in other countries? (N=29)	48%	52%
Any organization, regardless of location? (N=26)	23%	77%

Q23. What are the primary responsibilities of your office? (multiple responses allowed)

N=38	Total %
Advance/advocate privacy rights	84%
Investigate complaints	97%
Initiate complaints	55%
Mediate/arbitrate	34%
Shape/research policy	71%
Educate the public	92%
Other	45%

Q24. What enforcement powers does your office have? (multiple responses allowed)

N=38	Total %
Adjudication	47%
Fines	53%
Cease-and-desist orders	68%
Criminal sanctions	18%
Other	42%

Q25. Approximately what percentage of the investigative and enforcement work of your office involves transborder issues?

N=31	Total %
None, domestic only	13%
Ten percent	71%
Twenty percent	10%
Thirty percent	3%
Forty percent	0%
Fifty percent	3%
Sixty percent	0%
Seventy percent	0%
Eighty percent	0%
Ninety percent	0%
One hundred percent	0%

Q26. Is your office involved in enforcing regulations on security breach notification?

N=36	Pct %
Yes	33%
No	67%

Q27. Has your office cooperated with the FTC or any other U.S. regulatory agency to bring an enforcement action against a U.S.-based organization?

N=37	Pct %
Yes	11%
No	89%

Q28. Is your office involved in any concerted efforts with DPAs from other countries? (if yes, contextual response)

N=38	Pct %
Yes	74%
No	26%

APPENDIX B: Data protection offices and officials

Australia	Office of the Privacy Commissioner	Timothy Pilgrim
Austria	Austrian Data Protection Commission (Datenschutzkommission)	Commission headed by Chairman
Bulgaria	Commission for Personal Data Protection	The Commission for Personal Data Protection is collective body. It consists of President and four members, as follows: Veneta Shopova- President of the CPDP, Krassimir Dimitrov, Valentin Enev, Mariya Mateva and Veselin Tselkov.
Canada	Office of the Privacy Commissioner of Canada	Jennifer Stoddart
Colombia	Regulatory Communications Commission	
Cyprus	Office of the Commissioner for Personal Data Protection	Panayiota Polychronidou
Czech Republic	Office for Personal Data Protection	Igor Němec
Estonia	Data Protection Inspectorate	Viljar Peep
European Union	European Data Protection Supervisor	Peter Hustinx
Faroe Islands	Dátueftirlitið	Ingunn Eiríksdóttir
Finland	Office of Data Protection Ombudsman	Reijo Aarnio
France	La Commission Nationale de l'Informatique et des Libertés (CNIL)	Alex Türk
Gibraltar	Gibraltar Regulatory Authority	Paul Canessa
Greece	Hellenic Data Protection Authority	Christos Yerasis
Guernsey	Bailiwick of Guernsey Data Protection Office	Peter Harris
Hong Kong	Office of the Privacy Commissioner for Personal Data	Allan Chiang
Hungary	Parliamentary Commissioner for Data Protection and Freedom of Information	András Jóri
Iceland	Data Protection Authority (Persónuvernd)	Sigrún Jóhannesdóttir
Ireland	Office of the Data Protection Commissioner	Billy Hawkes
Isle of Man	Office of the Data Protection Supervisor	
Israel	The Israeli Law Information and Technology Authority	Yoram Hacohen
Italy	Garante per la Protezione dei Dati Personali	Francesco Pizzetti
Latvia	Data State Inspectorate	
Liechtenstein	Data Protection Office	Philipp Mittelberger
Lithuania	State Data Protection Inspectorate	Algirdas Kuncinas
Macao	Office for Personal Data Protection	Sonia Chan
Macedonia	Directorate for Personal Data Protection	Jovica Strasevski
Malta	Office of the Data Protection Commissioner	Joseph Ebejer
Mauritius	Data Protection Office	Drudeisha Madhub
Netherlands	Dutch Data Protection Authority – College Bescherming Persoonsgegevens	Jacob Kohnstamm
New Zealand	Office of the Privacy Commissioner	Marie Shroff
Norway	Datatilsynet	Bjorn-Erik Thon

Poland	Inspector General for Personal Data Protection	Rafał Wiewiórowski
Serbia	Commissioner for Information of Public Importance and Personal Data Protection	Rodoljub Sabic
Slovakia	The Office for Personal Data Protection of the Slovak Republic	Gyula Veszelei
Slovenia	Information Commissioner	Nataša Pirc Musar
Sweden	Datainspektionen (Data Inspection Board)	Göran Gräslund
United Kingdom	The Information Commissioner's Office	Christopher Graham

APPENDIX C: Appointing bodies

Australia	Governor General in Council (on advice from Federal Executive Council)
Bulgaria	Election
Canada	Order of Governor in Council
Cyprus	Executive appointment
Estonia	Executive appointment
European Union	Council and European Parliament (joint decision)
Finland	Civil servant/direct hire
Faroe Islands	Executive appointment
France	Election
Gibraltar	Executive appointment
Greece	Legislative committee appointment
Guernsey	Government
Hong Kong	Executive appointment
Hungary	President suggests; Parliament elects
Iceland	Executive appointment
Ireland	Executive appointment
Isle of Man	Legislative committee appointment
Israel	Government (on recommendation of search committee)
Italy	Election by Parliament
Liechtenstein	Election
Macao	Executive appointment
Macedonia	Election
Malta	Prime Minister (after consultation with the Leader of the Opposition)
Mauritius	Civil servant/direct hire
New Zealand	Governor-General (on recommendation of responsible Minister)
Norway	Civil servant/direct hire
Poland	Election
Serbia	Legislative committee appointment
Slovakia	Election
Slovenia	Legislative committee appointment
Sweden	Government
United Kingdom	Legislative committee appointment

APPENDIX D: DPA concerted efforts

Australia	Asia Pacific Privacy Authorities (APPA): The principal forum for privacy authorities in the Asia Pacific Region to form partnerships and exchange ideas about privacy regulation, new technologies and the management of privacy enquiries and complaints. APEC Transborder Privacy Enforcement Arrangement (CPEA): Provides a framework for privacy regulators to cooperate, and to seek information and advice from each other on transborder enforcement matters. OECD Working Party on Information Security and Privacy (WPISP): Develops policy options to sustain trust in the Internet Economy.
Austria	Cooperation with other DPAs via the Article 29 Working Group of the EU
Canada	Joint letter to Google Buzz with nine other DPAs; Global Privacy Enforcement Network; London Initiative
Cyprus	Coordinated audits/inspections of filing systems within the framework of JSA and JSB
Czech Republic	International Polish-Czech-Hungarian project funded from the EU Leonardo grant and focused on privacy at work
European Union	Close cooperation and coordination with national DPAs
Faroe Islands	Participation in annual meetings (by turn) in Iceland, Norway, Sweden, Finland and Denmark.
Finland	Nordic Inspection cooperation
France	Article 29 Working Party; GPEN; International Conference of Privacy Commissioners
Greece	Cooperation related to issues such as data retention in the electronic communications sector and Street View Services within the framework of the Article 29 Working Party DATA RETENTION IN ELECTRONIC COMMUNICATIONS SECTOR
Guernsey	Cooperative efforts with the United Kingdom, Jersey and the Isle of Man
Hong Kong	Asia Pacific Privacy Authorities Forum (held twice annually) and the International Conference of Privacy Commissioners
Hungary	Enforcement action at European level regarding data retention, cooperation with the Czech and Polish DPAs preparing a joint publication in the field of employment
Iceland	Audits of Schengen processing conducted by European DPAs
Ireland	Joint enforcement activities within the framework of the Article 29 Working Party and joint efforts on specific cases (either giving or asking for cooperating with other DPAs)
Italy	Involvement in enforcement actions concerning spamming and/or unsolicited mail, coordinated enforcement initiatives in Brussels regarding processing of personal data (at EU level) by private insurance companies, compliance with data retention obligations set forth in directive 2006/24 Reference should also be made to the coordinated enforcement initiatives launched and managed by the WP29 in Brussels to address processing of personal data at EU level by private insurance companies and – more recently, compliance with the data retention obligations laid down in directive 2006/24 and enforcement actions concerning Google Street View.
Latvia	Joint enforcement activities carried out within the framework of the Article 29 Working party
Liechtenstein	Cooperative efforts within the framework of the Article 29 Working Party
Netherlands	Enforcement actions (in Europe) coordinated via the Article 29 Working
New Zealand	Policy, educative and communications initiatives (e.g. Asia Pacific Privacy Awareness Week), co-signed public letter with 10 DPAs expressing concern at Google Buzz. Member of several networks e.g. APPA Forum, ICDPPC, GPEN, CPEA.
Poland	Coordinated efforts within framework of the Article 29 Working Party (e.g. European data retention directive 2006/24/EC, or cooperation in the case of Google Street View).
Slovakia	All joint actions within the framework of the Article 29 Working Party

Slovenia	Joint enforcement actions within the framework of the Article 29 Working Party
Sweden	Joint enforcement actions within the framework of the Article 29 Working Party



About the IAPP

The International Association of Privacy Professionals (IAPP) is the world's largest organization of privacy professionals, representing more than 7,000 members from businesses, governments and academic institutions across 52 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 by Caitlin Fullerton for the IAPP. Additional content and editing was contributed by Dave Cohen, Tracey Bentley and Peter Kosmala of the IAPP.

The IAPP wishes to express our sincere thanks to the offices of the data protection authorities (DPAs) who 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.



For more information, please contact us at:

IAPP

Global Headquarters

170 Cider Hill Road, York, Maine 03909 USA

+1 207.351.1500

www.privacyassociation.org