

Data Protection Authorities

2009 Global Benchmarking Survey

Executive Summary and Findings

International Association of Privacy Professionals



iapp

international association of privacy professionals

Data Protection Authorities: 2009 Global Benchmark Survey

Executive Summary and Findings

International Association of Privacy Professionals



Welcome

Dear Data Protection Professionals,

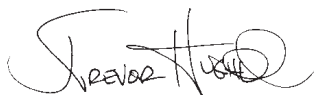
We are pleased to present you with these insights into the workings of data protection authorities (DPAs) worldwide.

This report presents the key findings of our first benchmarking study of global DPAs. We examined the characteristics—size, scope, responsibilities, and enforcement powers—of regulators to gain a better understanding of how governmental authorities approach data protection, information access, and other leading privacy issues.

The results offer valuable perspectives into the principle challenges faced by data protection authorities, as well as their structures. In addition, these DPAs' detailed responses to our survey questions provide *all* privacy professionals with a baseline for later explorations into data protection's evolution.

We plan to revisit these questions on a regular basis through future surveys, to create an ongoing benchmark of governmental approaches to data protection. I invite all to participate.

Sincerely,



J. Trevor Hughes, CIPP
Executive Director
IAPP



Table of Contents

I. Executive Summary	4
II. Survey Findings	
1. Responsibilities and focus areas	6
2. Authority and enforcement	10
3. Resources:	
<i>Staff</i>	11
<i>Budget</i>	15
4. Privacy perceptions	21
III. Appendices	
APPENDIX A: Survey Methodology	23
APPENDIX B: Considerations	23
APPENDIX C: Instrument and Results	24
APPENDIX D: Data Protection Offices and Officials	27
APPENDIX E: Appointing Bodies	28

I. Executive Summary

This 2009 Global Benchmarking Survey of Data Protection Authorities, conducted by the International Association of Privacy Professionals (IAPP), examines privacy offices and data protection authorities (DPAs) in 24 countries and territories. This is the first survey of this issue.

We designed this study to examine the scope, authority, and resources of DPAs; to interrogate the present state of data protection, privacy, and information sharing; and to provide a platform for exploring these issues, and their evolution, again in the future.

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

- **Scope:** What are DPAs' 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' enforcement powers?

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 authorities in the following jurisdictions.

DPAs that responded

Andorra	Hungary
Australia	Ireland
Austria	Isle of Man
Bahamas	Macao
Belgium	Macedonia
Canada	New Zealand
Cyprus	Poland
Czech Republic	Slovakia
Estonia	Slovenia
European Union	Sweden
Finland	United Kingdom
France	
Guernsey	

Key Findings

Among the study's key findings:

1. Data protection is DPAs' primary responsibility

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.) In addition, 22 percent of respondents also have information-access responsibilities.

Key Finding 1: Complaint handling, education, and advancing the state of privacy rights are among respondents' main responsibilities.

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

2. Primary enforcement powers are cease-and-desist orders and fines

A majority of DPAs (77%, or 17 of 22) have the authority to issue cease-and-desist orders for data protection infractions. More than half (55%) of DPAs can issue fines.

Key Finding 2: Only two DPAs said they have the authority to impose criminal sanctions for data protection violations, though several noted that a violator's failure to comply with enforcement orders or remedy directives would qualify as a criminal offense.

Some authorities also have the power to suspend foreign data transfers, initiate criminal investigations, or undertake civil actions. Others can take matters to federal court or issue enforcement notices, which specify the steps a data controller must take to comply with relevant regulations.

3. Data protection challenges require tech-savvy employees, while budgets and fining powers do not correlate

Staffing:

DPA staff sizes vary widely—from quite small to relatively large—with a mean of 55 full-time employees (FTEs). The Isle of Man (a British crown possession with home rule) had the highest ratio of FTEs to citizens (1 : 19,128). Among federal DPAs, Cyprus had the highest ratio of FTEs to citizens (1: 49,796), while France had the lowest (1 : 485,286).

Key Finding 3: As data protection concerns become increasingly technical in nature, DPAs appear to be employing greater numbers of technologists for consultations and investigations. In fact, nearly three-quarters of respondents indicated that they employ technology experts for these purposes.

All DPAs surveyed said that a dedicated official(s) (commissioner, inspector general) leads their data protection and privacy efforts. The average term length for a commissioner is five years and the vast majority of commissioners are government appointees.

The majority of DPAs (15 of 22, or 68%) indicated that they do not have a formal liaison to the privacy profession at large.

Budgets:

DPAs' annual budgets vary widely. The median budget of respondents is 4,028,855 euros. The average annual cost per FTE is 62,620 euros. There is a strong correlation between authorities' annual budgets and their staff size.

Key Finding 4: There appears to be no meaningful correlation between DPAs' ability to issue fines, and their annual budgets. In other words, it appears that DPAs that have the authority to levy fines for data protection violations do not have higher annual budgets than those that lack the power to fine.

Across all surveyed jurisdictions, data protection spending as a percentage of total government expenditures ranges from .0013% to .0720%.

4. DPAs' privacy perceptions correlate strongly with those of privacy professionals

We queried DPAs' perceptions of privacy via three questions relating to the importance, complexity, and anticipated data privacy regulatory environment in the future, and then compared their answers to those of privacy professionals polled in an IAPP survey conducted in mid-2009. Interestingly, a strong correlation exists between the responses of both groups. In particular:

- **Privacy is more important now than in the past**, according to 70% of DPAs and 76% of privacy professionals at large.
- **Privacy compliance issues are becoming more complex and difficult to manage**, according to a majority of respondents (almost 80% of DPAs and 88% of general privacy professionals)
- **Expect more (not fewer) privacy-related issues as well as regulations in the future**, predict both DPAs (78%) and general privacy professionals (90%)

5. Next steps

The IAPP is dedicated to bringing new knowledge into the privacy realm. We plan to continually refine and build upon this research to provide more comprehensive DPA benchmarks in the future. The IAPP will also explore other research opportunities based on information gleaned from these findings.

II. Survey Findings

I. Responsibilities and focus areas

This section describes the focus areas and activities of responding DPAs. In terms of focus, 100 percent of the responding authorities indicated they handle public-sector data protection, while 22 said they also handle private-sector data protection. Five DPAs—all European—noted that in addition to their data protection duties, they also have responsibilities relating to information access—that is, providing the public with access to information held by public authorities, or setting the policies and procedures for such access.

Figure 1 shows how responsibilities differ by country.

Figure 1: Areas of responsibility



The following DPAs indicated that their purview includes information access:

- Andorra
- Estonia
- Hungary
- Slovenia
- United Kingdom

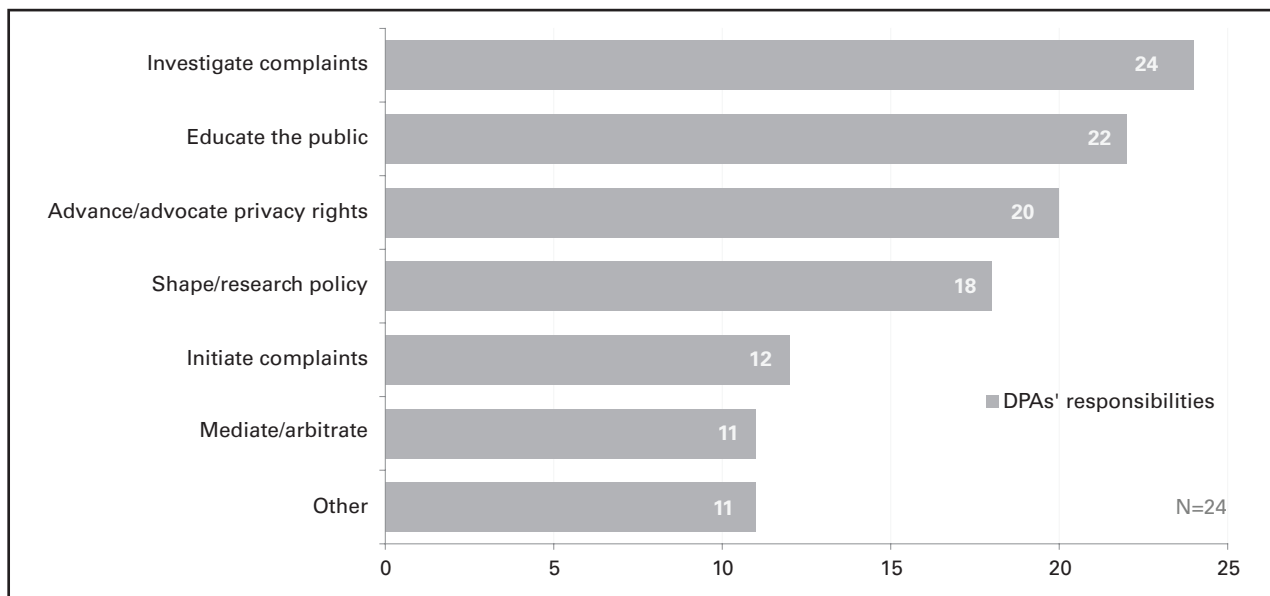
Figure 2: DPAs with freedom-of-information responsibilities



Only one DPA said that it works exclusively on public-sector (not private-sector) data protection. Perhaps unsurprisingly, this was the European Data Protection Supervisor (EDPS), whose remit is to manage governmental privacy issues—and not freedom-of-information or information access.

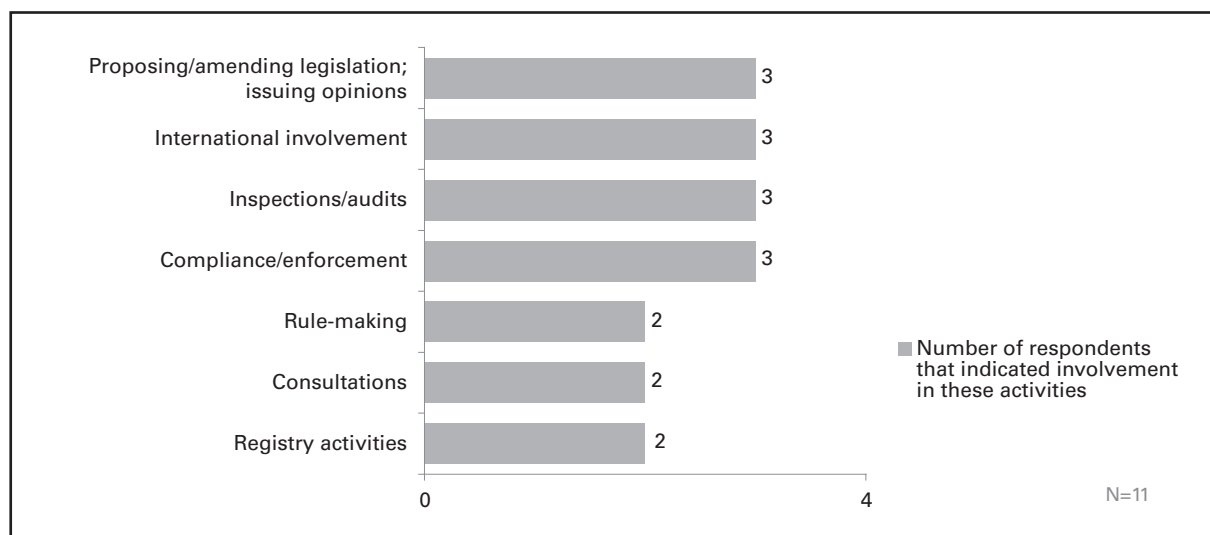
When queried about organizational activities, every respondent reported that one of their primary areas of focus is investigating complaints. In addition, a large majority (all but two authorities) noted that one of their main objectives is education. Another major focus—for 83 percent of those surveyed—is the advancement and advocacy of privacy rights. Figure 3 illustrates these and other responsibility areas.

Figure 3: DPAs' responsibilities



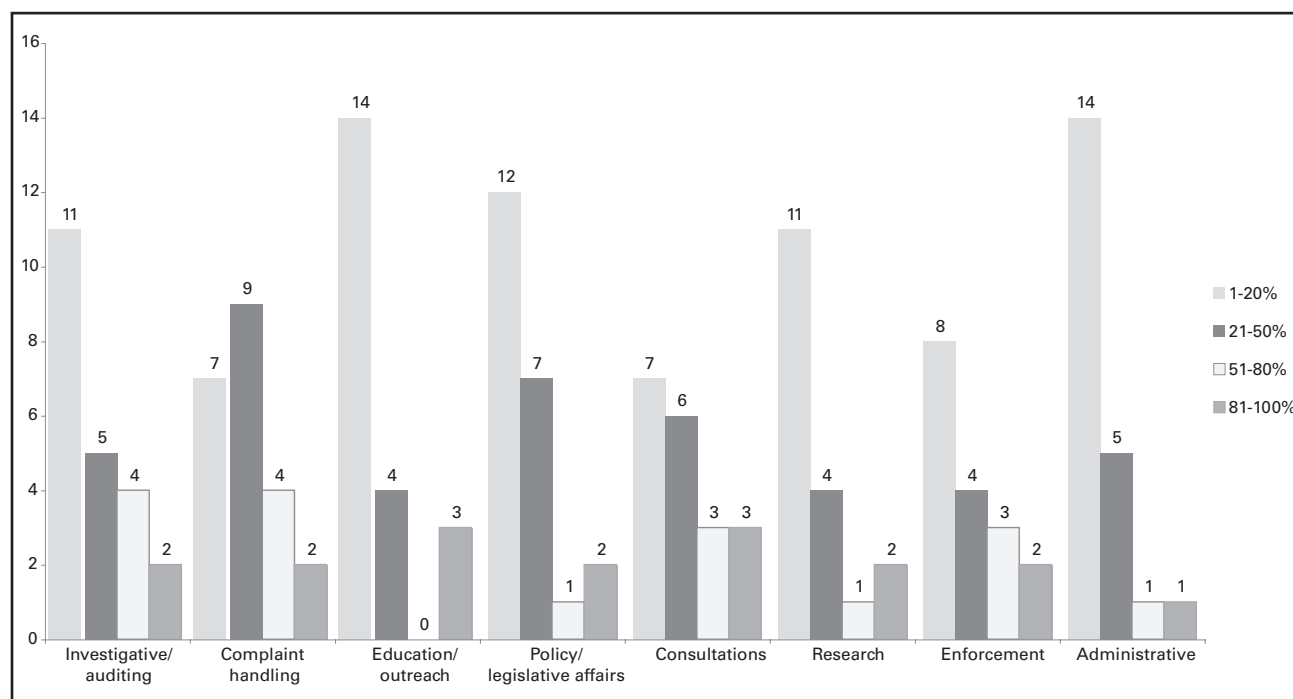
Eleven out of 24 respondents indicated that they also have “other” responsibilities not specified in the answer options. In this category, areas of focus included: data controller registry activities, audits and inspections, and rule-making. Figure 4 shows the “other” focus areas.

Figure 4: Other responsibilities



DPA's estimated what percentage of full-time employees (FTEs) work in various activity areas. For example, three respondents indicated that between 81–100% of FTEs work on education and outreach, while nine DPAs said that between 21–50% of FTEs work on complaint-related issues. The following figure illustrates where authorities are focusing their human resources.

Figure 5: FTEs dedicated to activity areas



In terms of geographic distribution of staff, nearly all DPAs operate from a central office. However, the United Kingdom's 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 (Auckland and Wellington), but describes neither as "central" nor "regional." And Australia's Office of the Privacy Commissioner encompasses two sites: one in Canberra and one in Sydney.

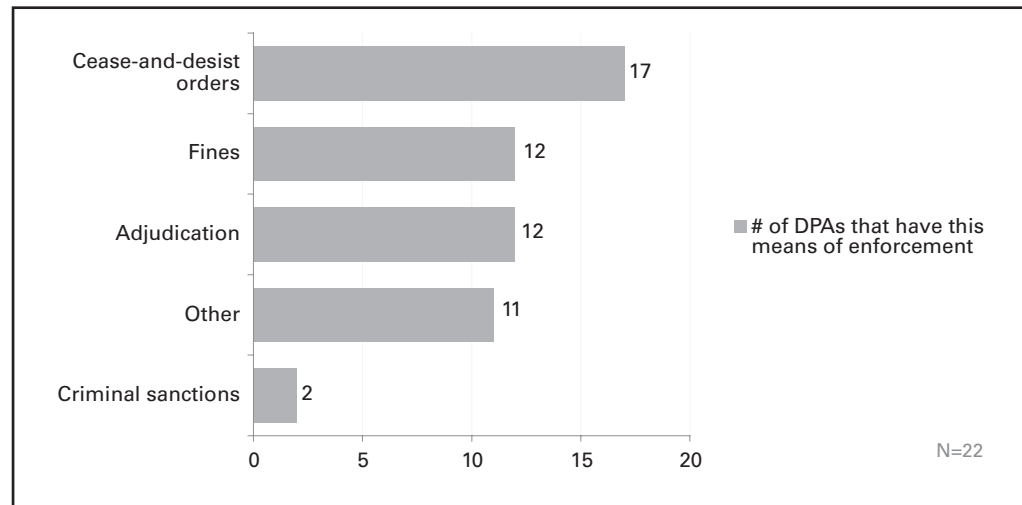
Figure 6: UK Information Commissioner's regional offices



2. Authority and enforcement

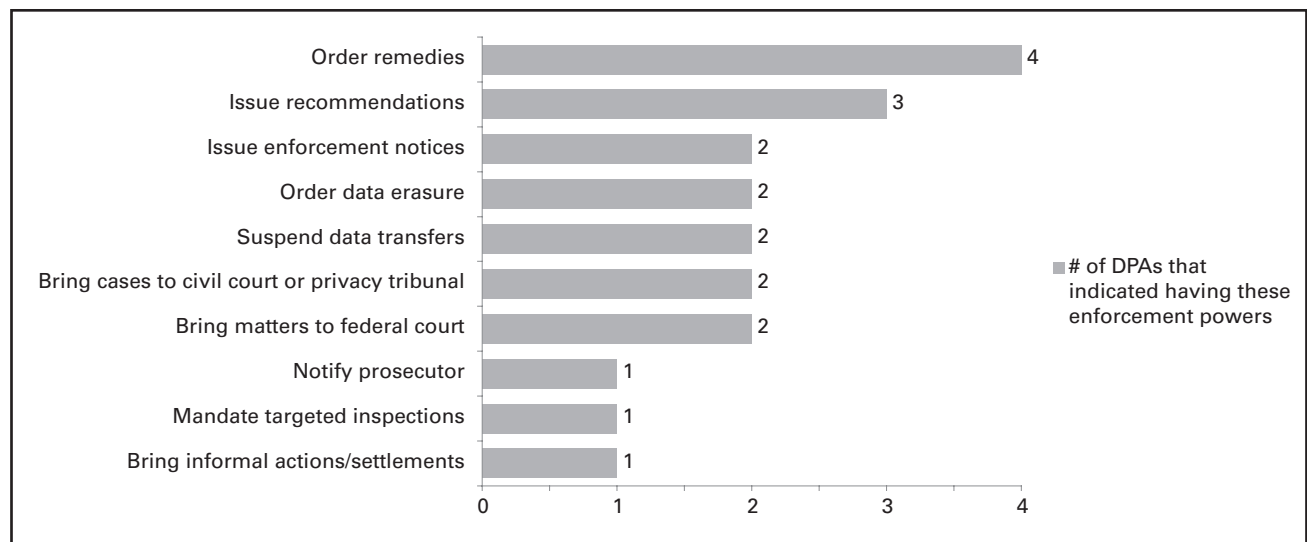
We asked DPAs to describe their authority and enforcement powers, and found that while only two out of 22 authorities can impart criminal sanctions for data protection violations, more than three-quarters (17) have the power to issue cease-and-desist orders. In addition, more than half of the DPAs noted that adjudication and issuing fines are within their authority.

Figure 7: Means of enforcement



More than half of the 22 respondents to this question indicated that their enforcement powers include actions not specified in our survey. Some of these other enforcement actions include issuing recommendations or enforcement notices, suspending foreign data transfer activities, and initiating civil actions. Figure 8 collects these “other” responses.

Figure 8: Other means of enforcement



While only the Bailiwick of Guernsey and Australia indicated that criminal sanctions were part of its enforcement authority, Finland's DPA may initiate criminal investigations, and several DPAs noted that a violator's failure to comply with enforcement orders or remedy directives is a criminal offense.

3. Resources: staff and budget

A. Staff

The staff sizes of the various DPAs range from very small to very large. For example, the Office of the Data Protection Commissioner of the Bahamas has just two full-time employees (FTEs), while the Information Commissioner's Office (ICO) of the United Kingdom tops out at 323 FTEs (although 100 of them work on information access exclusively).

The median staff size of the DPAs surveyed is 55 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. As shown in Figure 9, this provides us with a better understanding of the correlation between the size of a data protection authority and the number people it employs.

Figure 9: Number of FTEs by organization size

Large organizations (more than 100 FTEs)

United Kingdom*	323
Canada	160
France	132
Poland	120

Intermediate organizations (50–99 FTEs)

Czech Republic	95
Australia	64
Belgium	54

Medium organizations (25–49 FTEs)

Hungary*	49
Sweden	43
EDPS	35
New Zealand	34
Slovakia	34
Slovenia*	31
Macedonia	25

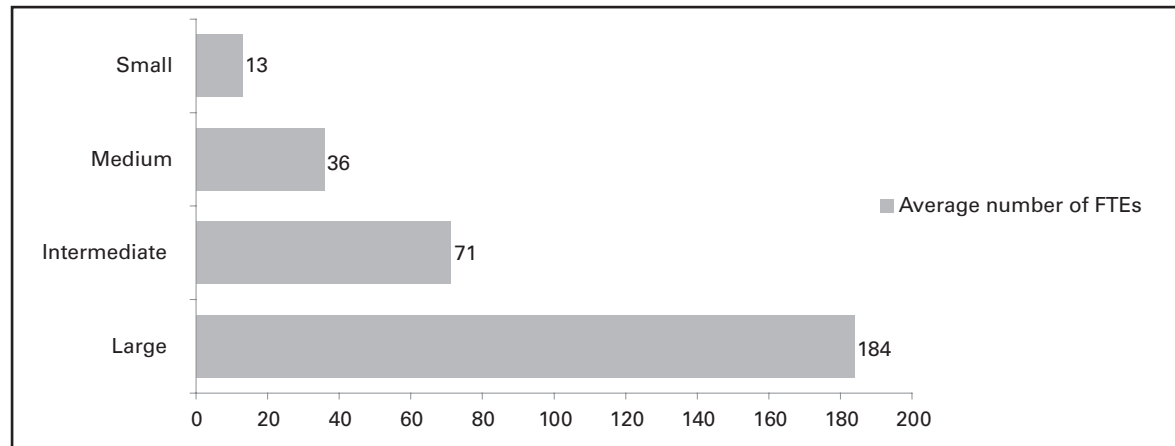
Small organizations (1–24 FTEs)

Estonia*	23
Ireland	21
Austria	20
Finland	20
Cyprus	16
Macao	15
Isle of Man	4
Andorra*	4
Guernsey	3
The Bahamas	2

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

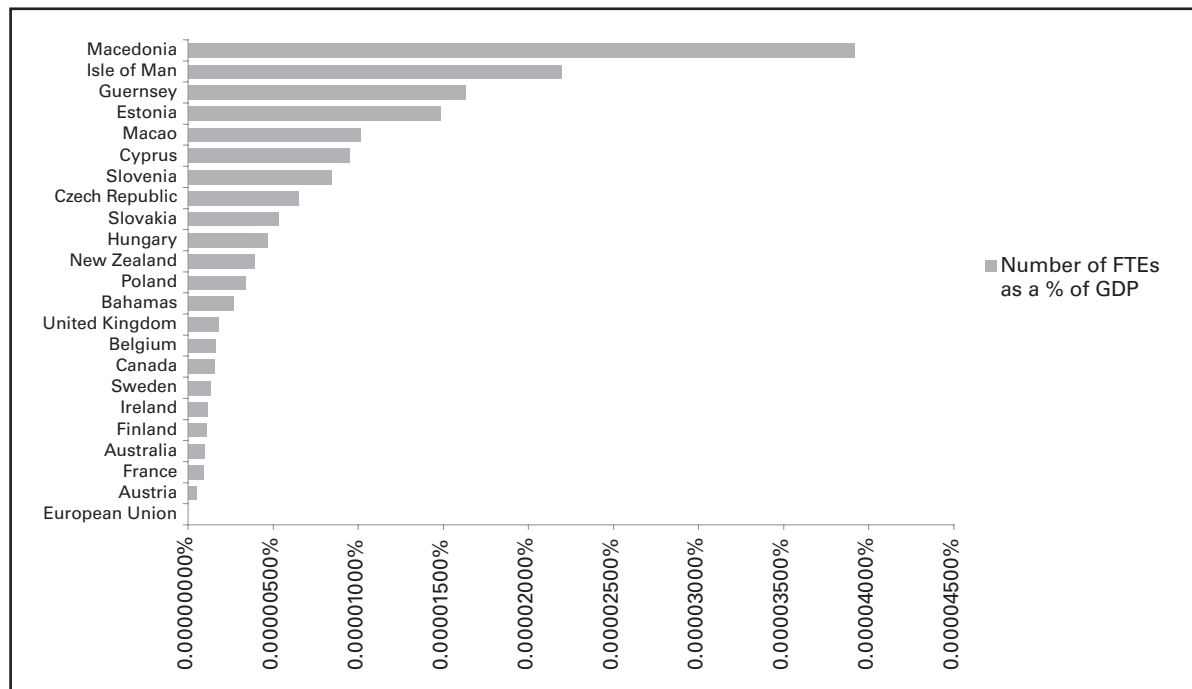
Figure 10 shows the average number of FTEs in each of the four DPA size categories.

Figure 10: Average number of FTEs by organization size



Next, we looked at authorities' staff sizes against their respective gross domestic product (GDP), as illustrated in Figure 11, below.

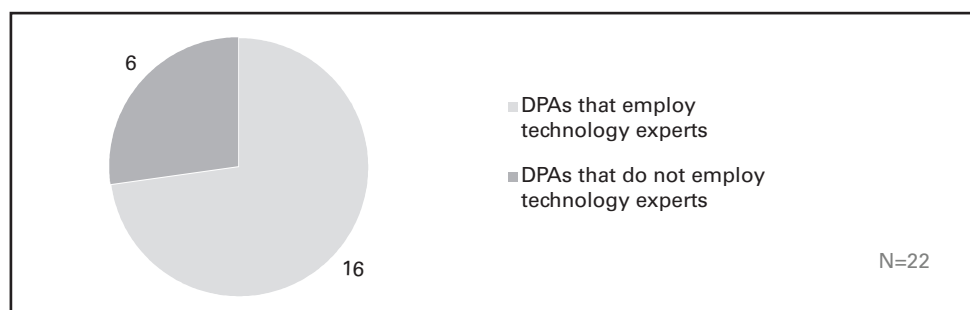
Figure 11: Number of employees as a percentage of GDP*



*No GDP data for Andorra

As data protection concerns become increasingly technical in nature, DPAs seem to be employing a greater number of tech-savvy individuals to help execute investigations. In fact, almost three-quarters of the 22 DPAs that responded to this question reported that they have dedicated technical experts on staff, as illustrated in Figure 12.

Figure 12: DPAs that employ technical experts for investigations and complaints



To understand more about each jurisdiction's focus on data protection, we calculated the ratio of FTEs in a data protection agency to population, and then ranked the DPAs by the resulting proportions. The Isle of Man ranks first with about one FTE per 19,000 citizens. Although the European Data Protection Supervisor has the lowest concentration of FTEs to population (one FTE to approximately 14 million EU residents), among federal DPAs, Cyprus ranked first, with one FTE per roughly 50,000 citizens, while France ranked last, with a proportion of roughly one FTE per 485,000 citizens. Figure 13 contains the rankings.

Figure 13: FTE : Population

Jurisdiction	1 FTE per # Citizens	Rank (1 = most FTEs to citizens)
Isle of Man	19,128	1
Andorra	20,972	2
Guernsey	21,956	3
Macao	37,323	4
Cyprus	49,796	5
Estonia	56,494	6
Slovenia	64,699	7
Macedonia	82,668	8
Czech Republic	107,493	9
New Zealand	123,924	10
The Bahamas	154,578	11
Slovakia	160,677	12
United Kingdom	189,204	13
Belgium	192,858	14
Ireland	200,152	15
Hungary	202,155	16
Canada	209,295	17
Sweden	210,689	18
Finland	262,513	19
Poland	320,690	20
Australia	332,228	21
Austria	410,515	22
France	485,286	23
European Union (EDPS)	14,045,224	24

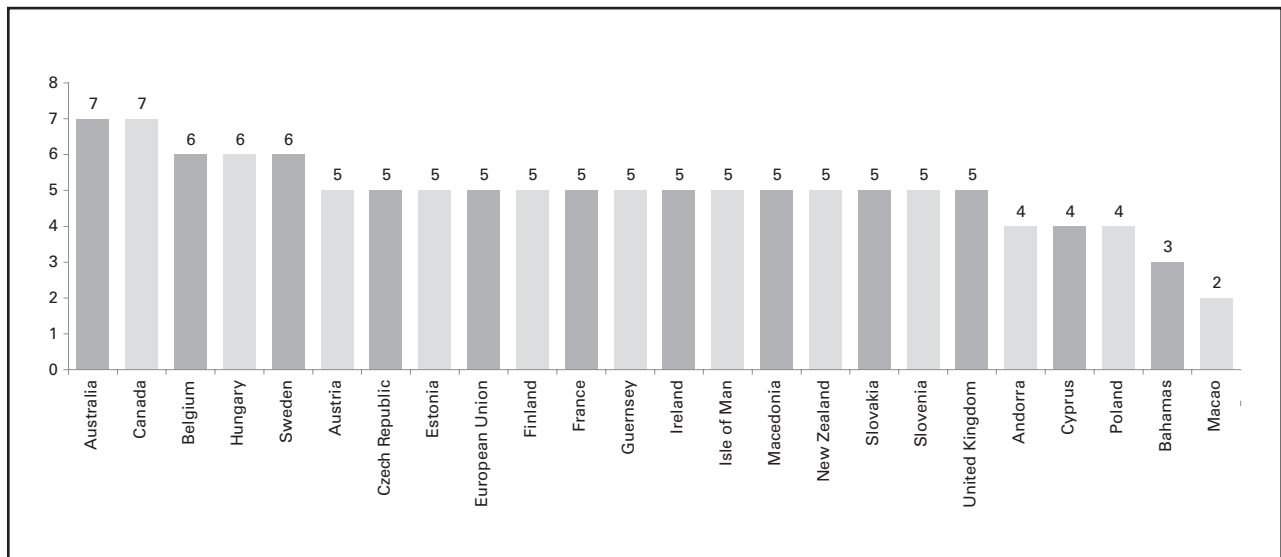
All DPAs surveyed indicated having at least one dedicated official in charge of data protection and privacy efforts. (See Appendix D for a complete list of data protection commissioners.)

Interestingly, two DPAs are headed by more than one official. In Austria, a six-person commission handles data protection. In Belgium, the Commission for the Protection of Privacy comprises 16 members—six permanent members, eight substitute members, and a president and vice president. The president and vice president are the only members occupying full-time positions in the commission.

All but one of the surveyed authorities reported that the data protection commissioner is appointed. (See Appendix E for a list of appointing bodies by jurisdiction.) The United Kingdom stands in contrast. It is the only jurisdiction surveyed which requires Her Royal Majesty's approval in the hiring of a data protection commissioner. All told, the British Information Commissioner must secure parliamentary, prime ministerial, as well as monarchical approval. Candidates for the position are recruited through an executive search agency and interviewed by public- and private-sectors representatives.

Term lengths for data protection commissioners vary from two years in the Office of Personal Data Protection of Macao to seven years for the privacy commissioners of Australia and Canada. The average term length is five years.

Figure 14: Commissioners' term lengths

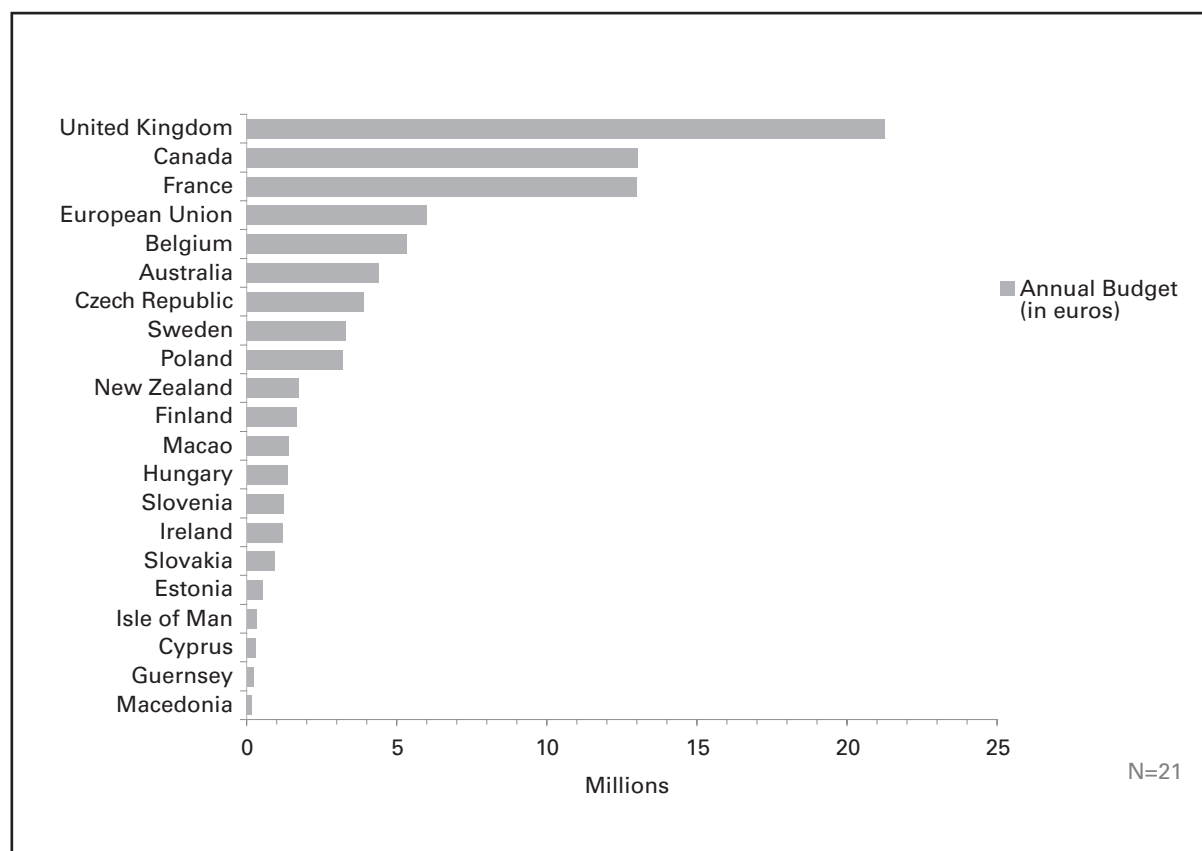


We asked DPAs if they had a formal liaison with privacy professionals at large—whether in the public or private sector—and found that the majority do not. Among the almost one-third of respondents who indicated having such connections, two authorities (Australia and Guernsey) indicated that their commissioners serve this role. Most others involve members of academia or networks of privacy professionals.

B. Budget

As expected given the sample, DPAs' annual budgets range from relatively large to relatively small. The average annual budget of respondents is 4,028,855 euros.

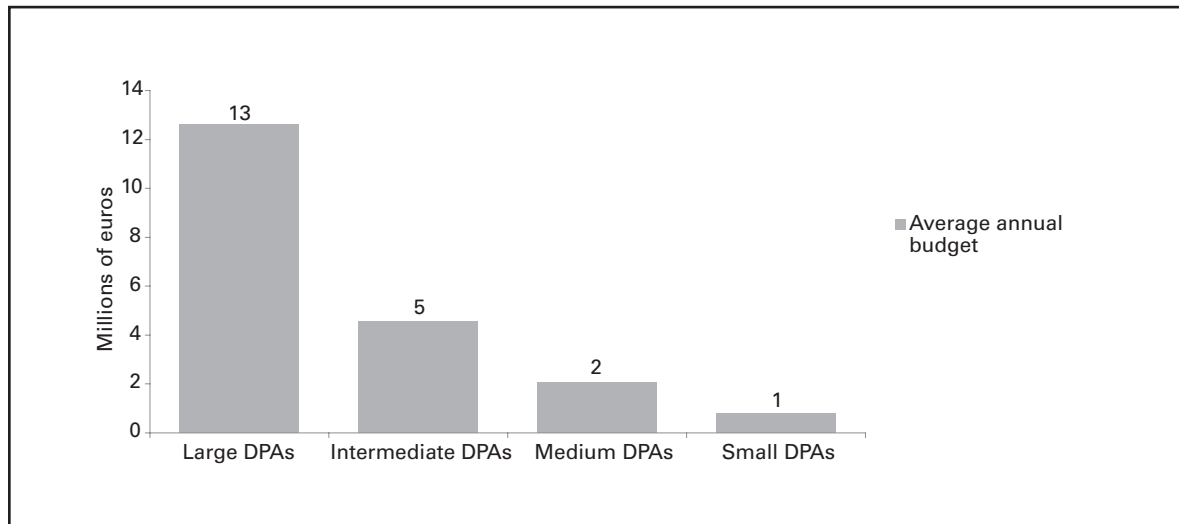
Figure 15: DPAs' annual budgets in euros*



*Andorra, Austria, and the Bahamas did not submit budget data.

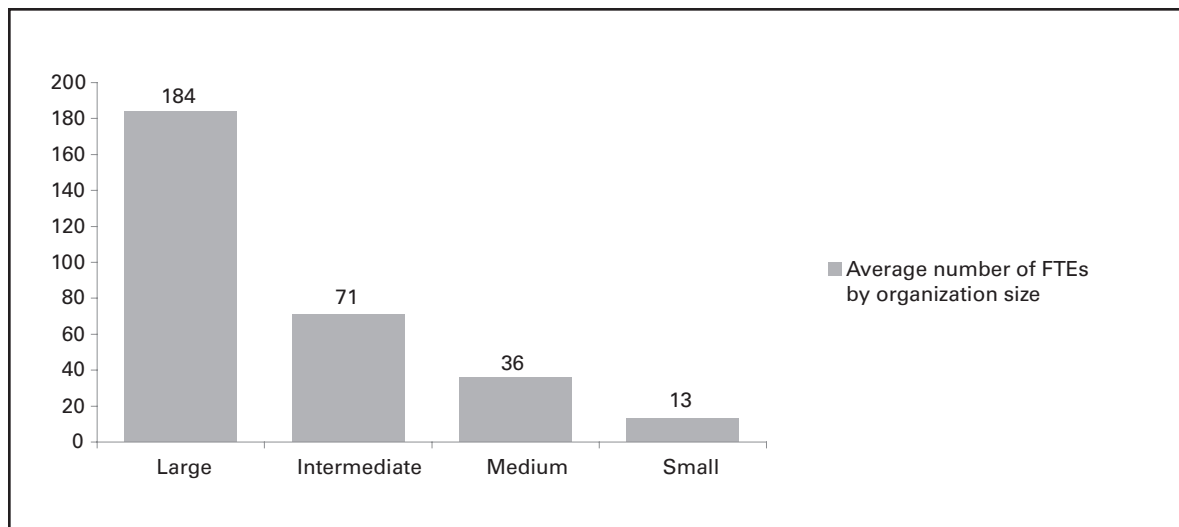
There is a strong correlation between organizations' staff sizes and annual budgets.

Figure 16: Average annual budget (in euros) by DPA size*



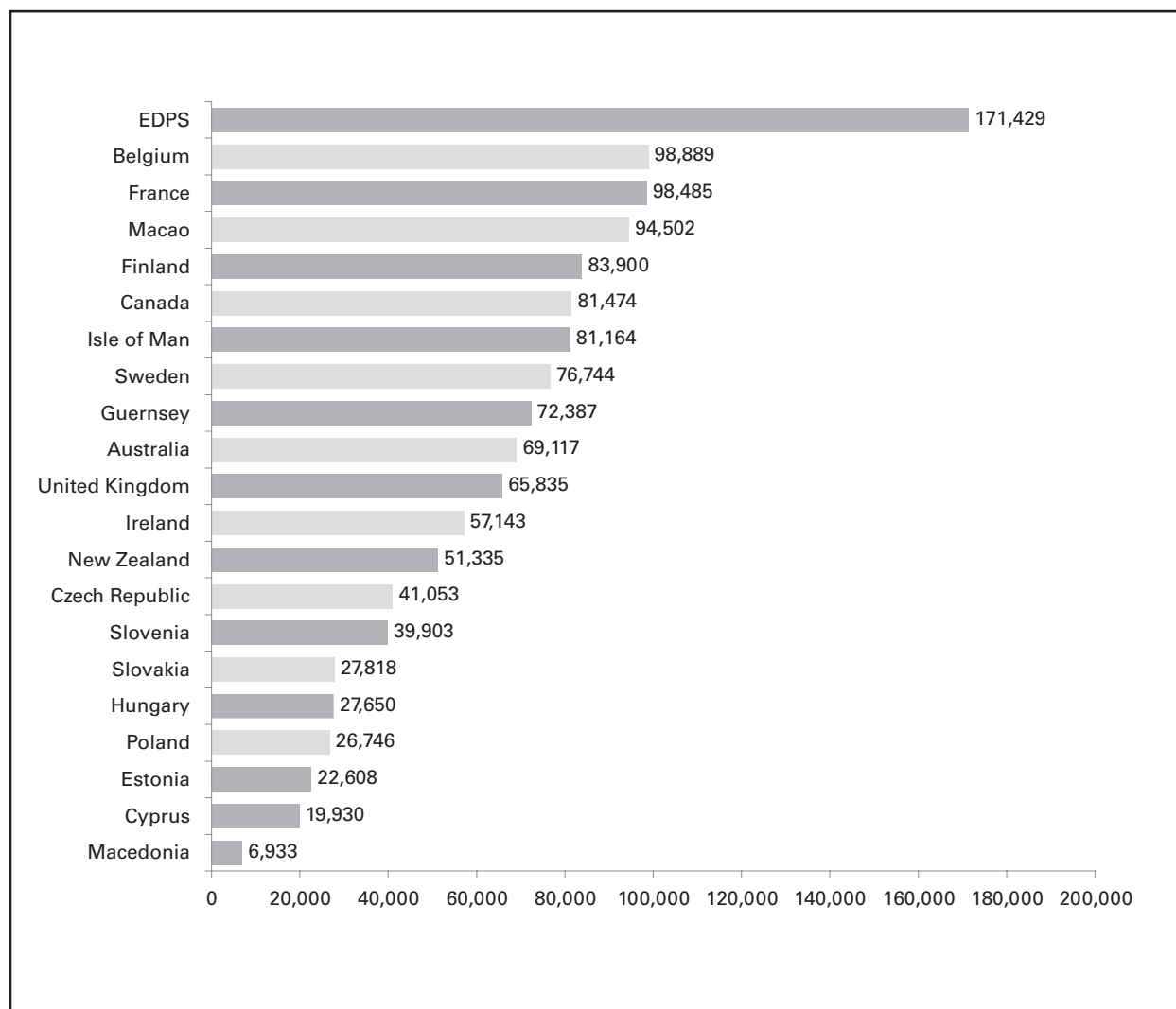
*Currencies were converted into euros between October 1–16, 2009.

Figure 17: 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 62,620 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 57,180 euros. Figure 18 shows the cost per FTE at each DPA.

Figure 18: Cost per FTE (in euros)* **

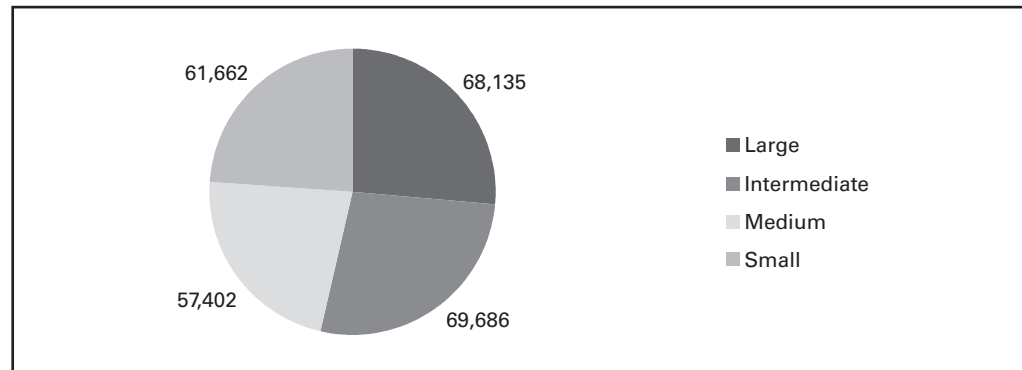


*Currencies were converted into euros between October 1–16, 2009.

**Andorra, Austria, and the Bahamas did not submit budget data.

Figure 19 illustrates the average cost per FTE by organization size.

Figure 19: Average cost per FTE (in euros) by organization size



We wanted to determine whether DPAs' enforcement capabilities correspond to the size of their annual budgets. Specifically, we sought to discover whether the organizations that have the authority to levy fines have larger annual budgets as a result. In Figure 20, below, the euro symbols denote DPAs that have the authority to issue fines. As shown, it seems unlikely that there is any meaningful correlation between DPAs' fining powers and their annual budgets, although ideally we would examine other factors to confirm this.

Figure 20: Effect of fining powers on annual budget (in euros)* **

LARGE		SMALL	
DPA	Annual budget	DPA	Annual budget
United Kingdom	21,264,546	€ Finland	1,678,000
Canada	13,035,853	€ Macao	1,417,526
€ France	13,000,000	Ireland	1,200,000
Poland	3,209,471	€ Estonia	520,000
		Isle of Man	324,657
		€ Cyprus	318,887
		Guernsey	217,162
INTERMEDIATE			
DPA	Annual budget		
Belgium	5,340,000		
Australia	4,423,467		
€ Czech Republic	3,900,000		
MEDIUM			
DPA	Annual budget		
EDPS	6,000,000		
€ Sweden	3,300,000		
New Zealand	1,745,375		
Hungary	1,354,829		
€ Slovenia	1,237,000		
€ Slovakia	945,828		
€ Macedonia	173,345		

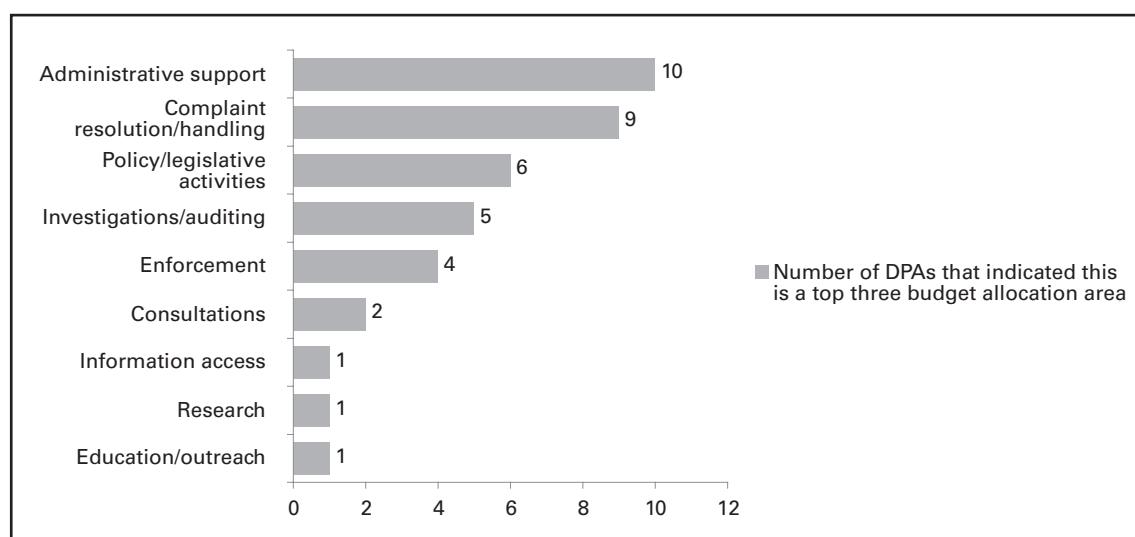
*Andorra and the Bahamas also have fining authority, but did not submit budget figures and are therefore not included in this table. Austria does not have fining authority, but is also not included in this figure due to a lack of budget data.

**Currencies were converted into euros between October 1–16, 2009.

It would be interesting to determine the impact, if any, of data controller registry fees on annual budgets. For example, according to the UK Information Commissioner's Office, its data protection activities are "funded through collection and retention of the notification fee paid by data controllers." Although this was not one of the questions in this benchmark, we plan to explore this area in the future.

We analyzed DPAs' top-three budget allocation areas to create Figure 21, which shows where spending is most concentrated. For example, 10 of 14 respondents indicated that "administrative support" is a top-three spending area, while only one reported that "research" is a top-three spending area.

Figure 21: Top budget allocation areas



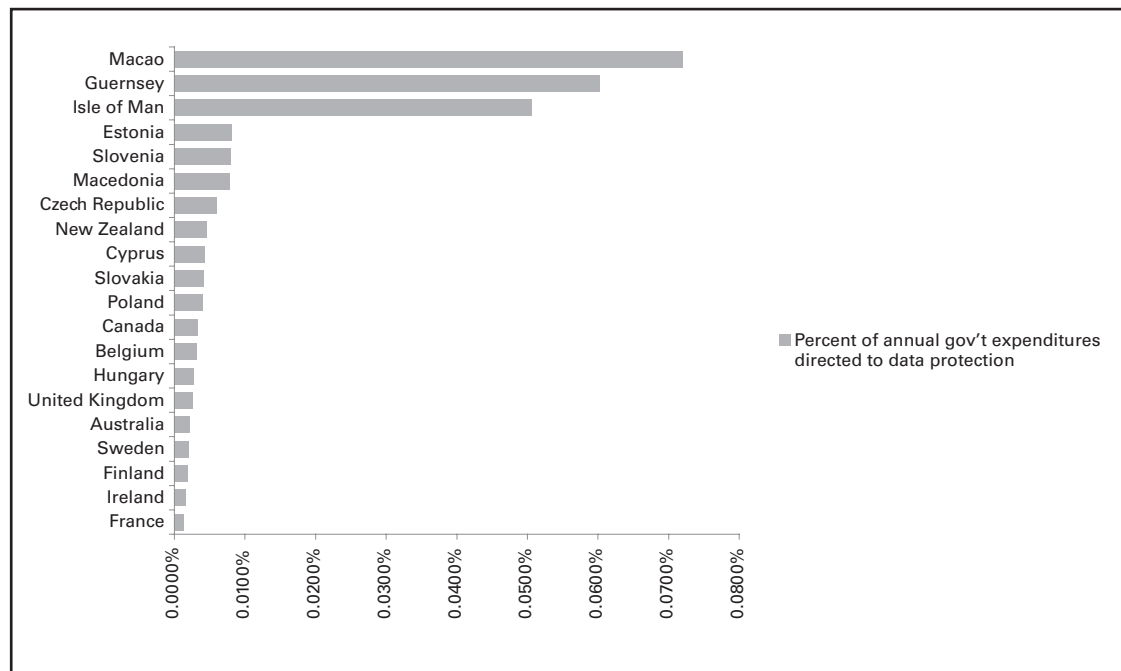
Governmental officials are responsible for approving the budgets of almost all of those surveyed. Figure 22 details the approval bodies for responding jurisdictions.

Figure 22: DPA budget approval

Andorra	Legislative committee	Hungary	Legislature
Australia	Executive approval	Ireland	Legislature
Austria	Federal Chancellery	Isle of Man	Legislature
Bahamas	Ministry of Finance	Macao	Legislature
Belgium	Federal Chamber of Representatives	Macedonia	Assembly
Canada	Parliament	New Zealand	Parliament
Cyprus	Ministry of Finance and House of Representatives	Poland	Parliament
Czech Republic	Parliament	Slovakia	National Council
Estonia	Executive approval - Ministry of Justice	Slovenia	Parliament
European Union	Council and European Parliament approval	Sweden	Parliament
Finland	Parliament	United Kingdom	Parliament
France	Legislature		

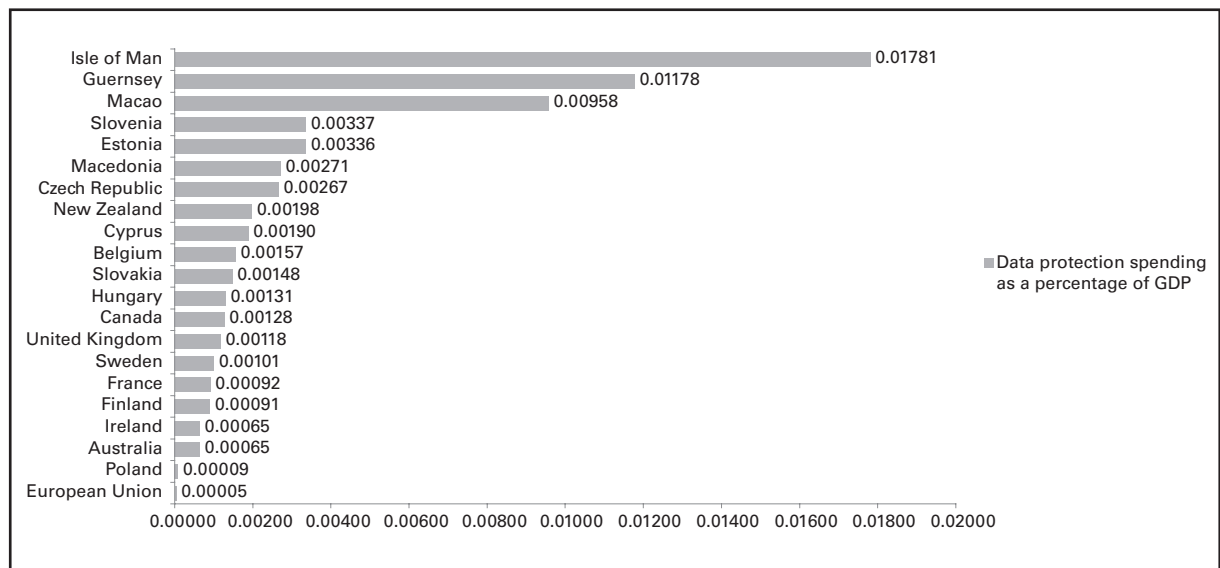
We looked at DPAs' annual budgets alongside the annual government expenditures of each jurisdiction, finding that data protection spending as a percentage of total government spending is greatest in the governments of Macao, Guernsey, and Isle of Man, as illustrated in Figure 23.

Figure 23: Percent of annual government expenditures directed to data protection



Next, we looked at DPAs' annual budgets alongside gross domestic product, as shown in Figure 24.

Figure 24: Data protection spending as a percentage of GDP

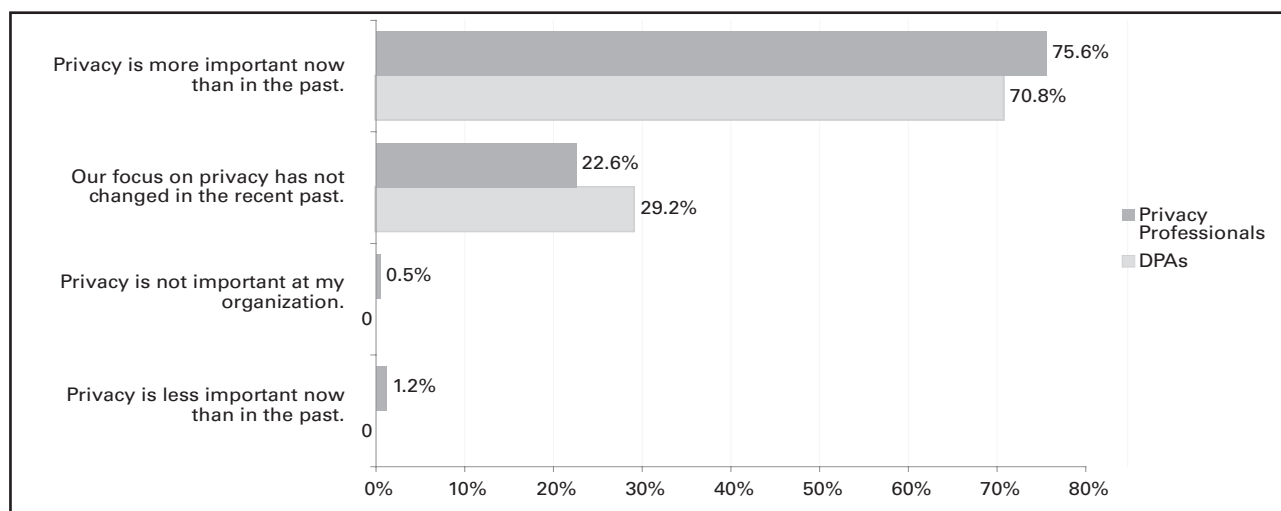


4. Privacy perceptions

In mid-2009 the IAPP polled its 6,000 members—all data protection and privacy practitioners—to gauge their perceptions of the industry and where it is headed. We posed the same three questions to DPAs in this survey, and found a strong similarity between the views of these regulators and privacy professionals at large.

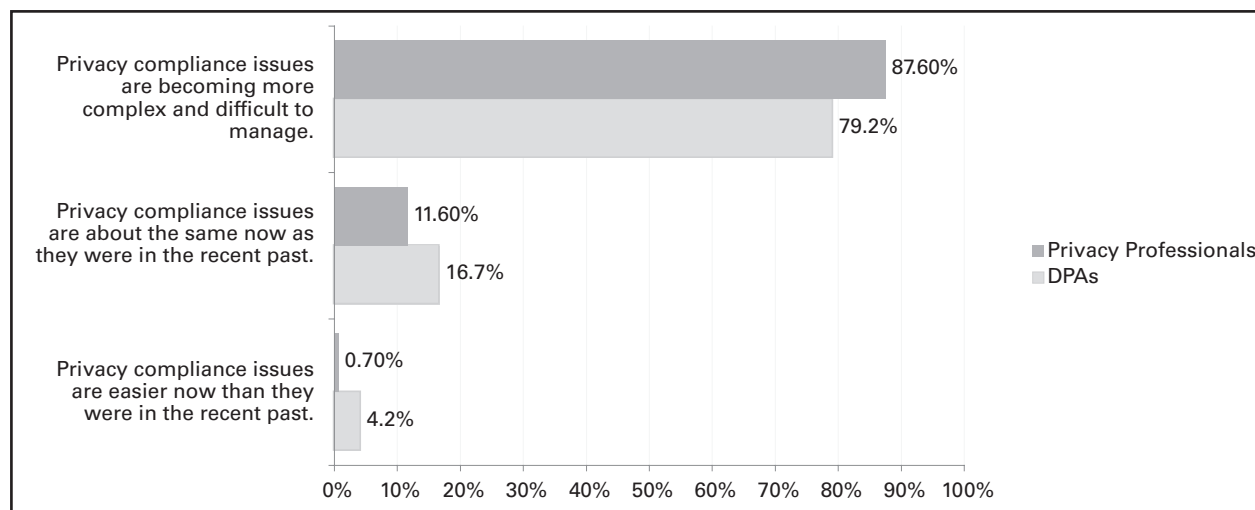
When asked to describe their organization's focus on privacy and the protection of personal data, more than two-thirds of DPAs surveyed said that privacy is more important now than in the past. None of the respondents said that their focus on privacy has become less important.

Figure 25: DPAs and privacy professionals describe importance of privacy



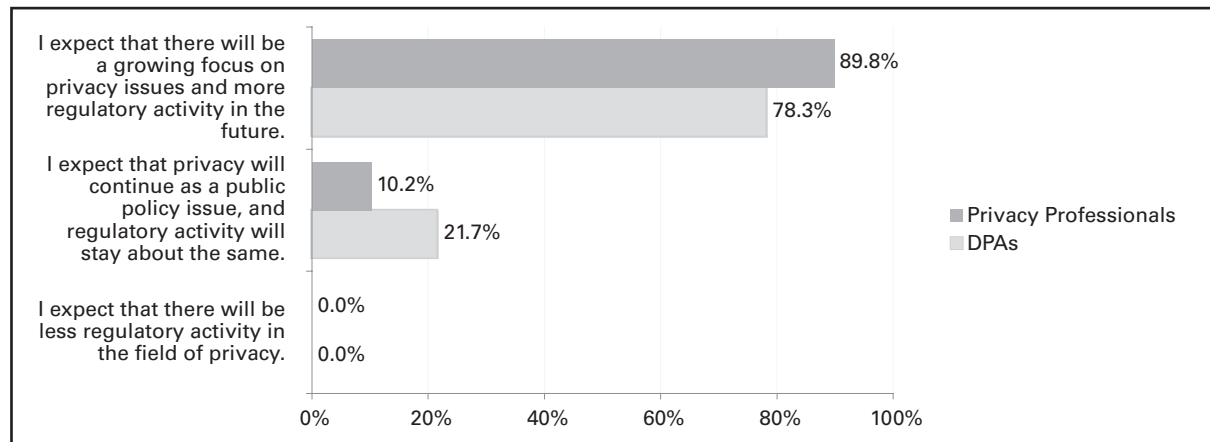
When asked to describe the complexity of complying with privacy and data protection standards today, only four percent of responding DPAs said that compliance issues are easier today than in the recent past. The vast majority (79%) agreed that privacy compliance issues are becoming more complex and difficult to manage, as illustrated in Figure 26.

Figure 26: DPAs and privacy professionals describe compliance complexity



When asked to describe their expectations with regard to future privacy regulation, most responding DPAs (78%) said they anticipate a growing focus on privacy issues and more regulatory activity in the future. None of the respondents predicted less regulatory activity in the field.

Figure 27: DPAs and privacy professionals describe future regulatory environment



III. Appendices

APPENDIX A: Survey Methodology

The IAPP identified 47 data protection/privacy authorities on five continents to receive the benchmarking survey. One week before sending the actual survey, the IAPP sent individual e-mails to pre-identified contacts at each DPA to notify them of the impending survey and to preview its objectives. In the e-mail, the IAPP also asked recipients to respond with the name of the person who should receive the survey, if not them. The IAPP updated the list of targets based on responses.

In mid-July 2009, the IAPP e-mailed the survey link to recipients. The e-mail included a note from the IAPP executive director about the objectives and intended use of the findings. Recipients were notified that the results would be presented at the 2009 IAPP Data Protection and Privacy Workshop in Madrid. Two weeks after that, the IAPP sent a reminder to those who had not yet completed the survey. The IAPP collected responses through early October.

APPENDIX B: 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 47 surveys and received responses from 24 DPAs. Based on the breadth of respondents, the data offered here provides insight on a range of DPAs—large and small, centralized and regional. However, it is possible that substantial differences exist among the 23 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 qualified sample of relatively mature DPAs in mostly first-world nations across five continents (Asia, Australia, Europe, North America, South America). Even so, it is possible that more newly established DPAs would have had a significant impact on the findings, had they been asked to complete the survey.

Timing

We began conducting this 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 have also included data pertaining to the European Union's DPA (the European Data Protection Supervisor, or EDPS). We included 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.

APPENDIX C: Instrument and Results

DPA Responses

Q1.	Please enter the name of your country here. (Contextual response)	
Q2.	Please enter the name of your office or organization here. (Contextual response)	
Q3.	What is the scope of authority of your office? (multiple responses allowed)	
	Data protection/privacy (all industries, all sectors)	87%
	Data protection, public sector (managing governmental privacy issues)	48%
	Data protection, private sector	44%
	Information access/freedom of information	22%
	Data protection, specific private-sector industries (please list industries:)	9%
Q4.	What are the primary responsibilities of your office? (multiple responses allowed)	
	Investigate complaints	100%
	Educate the public	92%
	Advance/advocate privacy rights	83%
	Shape/research policy	75%
	Initiate complaints	50%
	Mediate/arbitrate	46%
	Other	46%
Q5.	What enforcement powers does your office have? (multiple responses allowed)	
	Cease-and-desist orders	77%
	Adjudication	55%
	Fines	55%
	Criminal sanctions	9%
	Other	50%
Q6.	Does your office have a data protection commissioner/official? If yes, what is that person's name? (Contextual response)	
	Yes	96%
	No	4%
Q7.	If your office has a data protection commissioner, what is the appointment process (i.e. executive appointment, legislative committee appointment, election, civil servant/direct hire, etc.)? (contextual response)	

Q8. If your office has a data protection commissioner, how long is this person's term?
(contextual response)

Q9. What is the total number of staff in your office? (contextual response)

Q10. How many full-time staff members work on privacy/data protection? (contextual response)

Q11. How many full-time staff members work on information access/freedom of information?
(contextual response)

Q12. What percentage of full-time staff members work in the following areas?

	None	1–10%	11–20%	21–30%	31–40%	41–50%	51–60%	61–70%	71–80%	81–90%	91–100%
Investigation/auditing	0	22.7	27.3	9.1	9.1	4.5	4.5	9.1	4.5	0	9.1
Complaint processing/ handling/resolution	0	13.6	18.2	18.2	18.2	4.5	0	9.1	9.1	0	9.1
Education/outreach	0	42.9	23.8	9.5	9.5	0	0	0	0	0	14.3
Policy/ legislative affairs	0	36.4	18.2	18.2	4.5	9.1	0	0	4.5	0	9.1
Consultations	5.0	30.0	5.0	15.0	5.0	10.0	5.0	5.0	5.0	0	15.0
Research	10.0	50.0	5.0	15.0	0	5.0	0	0	5.0	0	10.0
Enforcement	10.5	31.6	10.5	5.3	10.5	5.3	5.3	5.3	5.3	0	10.5
Administrative (HR, tech support, operations, etc...)	0	14.3	52.4	19.0	0	4.8	0	4.8	0	0	4.8
Information access	53.3	20.0	13.3	6.7	0	0	0	6.7	0	0	0
Other areas	33.3	66.7	0	0	0	0	0	0	0	0	0

Q13. Please describe the geographic distribution of your staff.

Central office (only)	79%
Regional offices (only)	0%
Central and regional offices	8%
Other	13%

Q14. Does your office employ staff members who provide technological expertise for investigations/complaint resolution?

Yes	73%
No	27%

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

No	68%
Yes	32%

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

Q17. What percent of your overall budget is allocated to each of the following areas? (Please include payroll/staff in each area's allocation.)

	None	1–10%	11–20%	21–30%	31–40%	41–50%	51–60%	61–70%	71–80%	81–90%	91–100%
Investigation/auditing	0	63.6	9.1	9.1	9.1	0	0	0	9.1	0	0
Complaint processing/ handling/resolution	0	33.3	8.3	41.7	8.3	0	0	0	8.3	0	0
Education/outreach	8.3	83.3	0	8.3	0	0	0	0	0	0	0
Policy/ legislative affairs	8.3	50.0	16.7	16.7	8.3	0	0	0	0	0	0
Consultations	30.0	60.0	0	10.0	0	0	0	0	0	0	0
Research	20.0	80.0	0	0	0	0	0	0	0	0	0
Enforcement	0	70.0	0	10.0	10.0	0	0	0	10.0	0	0
Administrative (HR, tech support, operations, etc...)	8.3	8.3	50.0	8.3	8.3	0	16.7	0	0	0	0
Information access	57.1	28.6	14.3	0	0	0	0	0	0	0	0
Other areas	0	100.0	0	0	0	0	0	0	0	0	0

Q18. Please describe the budget approval process for your office—i.e., legislative committee approval, legislative approval, executive approval, etc. (contextual response)

Q19. How would you describe your organization's focus on privacy and the protection of personal data?

Privacy is more important now than in the past.	71%
Our focus on privacy has not changed in the recent past.	29%
Privacy is less important now than in the recent past.	0%
Privacy is not important at my organization.	0%

Q20. How would you describe the complexity of compliance with privacy and data protection standards today?

Privacy compliance issues are becoming more complex and difficult to manage.	79%
Privacy compliance issues are about the same now as they were in the recent past.	17%
Privacy compliance issues are easier now than in the recent past.	4%

Q21. What is your expectation with regard to future privacy regulation?

I expect that there will be a growing focus on privacy issues and more regulatory activity in the future.	78%
I expect that privacy will continue as a public policy issue, and regulatory activity will stay about the same.	22%
I expect that there will be less regulatory activity in the field of privacy.	0%

APPENDIX D: Data Protection Offices and Officials

Andorra	Andorra Data Protection Agency	Joan Crespo Piedra
Australia	Office of the Privacy Commissioner	Karen Curtis
Austria	Austrian Data Protection Commission	Six-member commission
Bahamas	Office of the Data Protection Commissioner	George E. Rodgers
Belgium	Commission for the Protection of Privacy	Willem Debeuckelaere & Stefaan Verschuere
Canada	Office of the Privacy Commissioner of Canada	Jennifer Stoddart
Cyprus	Office of the Commissioner for Personal Data Protection	Goulla Frangou
Czech Republic	Office for Personal Data Protection	Igor Němec
European Union	European Data Protection Supervisor	Peter Hustinx
Estonia	Estonian Data Protection Inspectorate	Viljar Peep
Finland	Office of the Data Protection Ombudsman	Reijo Aarnio
France	La Commission Nationale de l'Informatique et des Libertés	Alex Türk
Guernsey	Data Protection Office	Peter Harris
Hungary	Parliamentary Commission for Data Protection and Freedom of Information	András Jóri
Ireland	Office of the Data Protection Commissioner	Billy Hawkes
Isle of Man	Office of the Data Protection Supervisor	Iain McDonald
Macao	Office for Personal Data Protection	Sonia Chan
Macedonia	Directorate for Personal Data Protection	Marijana Marusic
New Zealand	Office of the Privacy Commissioner	Marie Shroff
Poland	Inspector General for Personal Data Protection	Michał Serzycki
Slovakia	Office for Personal Data Protection	Gyula Veszelei
Slovenia	Information Commissioner	Nataša Pirc Musar
Sweden	Data Inspection Board	Göran Gräslund
United Kingdom	Information Commissioner's Office	Christopher Graham

APPENDIX E: Appointing bodies

Andorra	Legislative committee
Australia	Governor General In Council (on advice from Federal Executive Council)
Austria	President of the republic
Bahamas	Governor General (on advice of Prime Minister after consultation with the Leader Of The Opposition)
Belgium	Federal Chamber of Representatives
Canada	Governor In Council (after consultation with the leader of every recognized party in the Senate and House Of Commons and approval of the appointment by resolution of the Senate and House Of Commons)
Cyprus	Executive appointment
Czech Republic	President of the republic (on the proposal of the Parliament)
Estonia	Government of the republic (at the proposal of Minister of Justice after hearing the opinion of the Constitutional Committee of the Parliament)
European Union	Council and European Parliament (joint decision)
Finland	Council of State
France	Elected by peers
Guernsey	Government
Hungary	President suggests; Parliament elects
Ireland	Government
Isle of Man	Legislative committee
Macao	Executive appointment
Macedonia	Assembly elects
New Zealand	Governor-General (on recommendation of the Cabinet)
Poland	Diet of the republic (with the consent of the Senate)
Slovakia	National Council elects (upon Government proposal)
Slovenia	Parliament (upon proposal of the president of the republic)
Sweden	Government
United Kingdom	Hired after parliamentary and monarchial approval



About the IAPP

The International Association of Privacy Professionals (IAPP) is the world's largest organization for those working in the field of data protection and privacy, with more than 6,000 members in 49 countries.

Since 2000, the IAPP has worked to define, nurture, and improve the privacy profession globally. The association provides data protection professionals with the forums and tools to learn and network, develop professionally, and help advance privacy management issues.

In addition, the IAPP offers a broad-based credentialing program in information privacy—the Certified Information Privacy Professional (CIPP). The CIPP is the leading certification for many thousands of privacy and information professionals around the world.

This study was executed by Jonathan McPhee for the IAPP.

Special thanks to the aforementioned data protection authorities for generously sharing their time and insights.

To complete this survey, please contact
research@privacyassociation.org.



For more information, please contact us at:

IAPP

Global Headquarters, 170 Cider Hill Road, York, Maine USA

+1 207.351.1500

www.privacyassociation.org