

Navigating
the global data
privacy landscape

THE 2023 GPA
CENSUS

MESSAGE FROM THE CHAIR

(FOREWORD)

Dear Colleagues,

Every three years we take stock of the work of the Global Privacy Assembly (GPA) membership through the GPA Census. 2020 is one such year, so it is with pleasure that I present to you the results of the GPA Census 2020.

The regular census is an important stock-taking exercise. It gives a comprehensive insight on how the privacy landscape is evolving – from the way data protection and privacy authorities are structured, to the powers they have and how they deliver their work.

The 2020 Census builds upon the work of the first Census in 2017, providing points of comparison and new insight into how the approach of member authorities supports the GPA's 2019–2021 strategic priorities. By measuring the work of the GPA, we can further our vision towards a global regulatory environment with clear and consistent high standards of data protection. Most importantly, it highlights the collaborative efforts of our membership when sharing experiences, strategies and best practices from around the world, including developing cooperation tools.

The 2020 Census provides considerable measures of growth and change, and we expect

further in-depth analysis of these initial results from our Working Groups and committees.

That being said, we have more work to do to improve the global interoperability of data protection and privacy laws as well as cross-sectoral regulation, so we can increase our cooperation and respond to the challenges arising from our increasingly digital world. The GPA is committed to addressing this through its current Policy Strategy and this work will be further developed through a new strategic plan for 2021–23. The Census 2023 will be developed in time to reflect that new work and sentiment, whilst also providing important

points of comparison with the 2017 and 2020 documents in order to track trends.

I give my sincere thanks to the GPA Working Groups that provided their expertise to the

census questionnaire, the large number of GPA members that participated in the

Table of contents

4

Executive Summary

8

Introduction

9

Methodology

10

Authority Profile

15

Data protection law,
jurisdiction and
exemptions

20

Authority's funding and
resources

25

Authority's enforcement
powers, case handling
and reporting

34

Cross-border data
flows, enforcement and
cooperation

44

Breach notification

48

Other matters

50

Appendix

Executive Summary

The Global Privacy Assembly (GPA) aims to exercise international leadership in data protection and privacy. It connects the efforts of more than 130 data protection and privacy authorities around the world.

This Census - based on data from 2023 - gathered information from 78 GPA members to provide a timely picture of the policies and delivery approaches that currently guide and regulate data protection and privacy around the world.

In an interconnected and globalized world, where the fluidity of information transcends geographical barriers, this report is a valuable reference tool for those involved in cross-border activities and whose data are in different jurisdictions. In addition, it is a fundamental source of knowledge for national policy makers looking to explore new approaches. It also promotes collaboration and the exchange of experiences between GPA authorities, by providing a detailed analysis of practices adopted in other regions, thus providing opportunities for learning and continuous improvement.

This report has some similarities with the picture presented in the 2020 census, both these and the most relevant differences are explicit throughout the different sections presented. One of the most notable differences is the adoption of social networks for information purposes, as well as extending the jurisdiction in terms of data protection and privacy to newly created technologies.

Section A: Authority Profiles

This section focuses on geographically locating the different authorities participating in the Census and that are part of the GPA and specifying their respective regions, the online presence they have, their leadership, the legal system that governs them, and relevant data of the most recent annual report in terms of the preparation of their staff. It defines the people surveyed and identifies any patterns or trends that will affect other areas in the Census.

On the other hand, this section shows findings such as the continuity of the appointment of the head of authority by the executive branch compared to 2020, and recognizes that most of the respondents have a staff that is constantly updated.

Section B: Data protection law, jurisdiction and exemptions

This section identifies the sectors that the authorities supervise and the powers granted to them by the respective law, including the ability to take actions, whether administrative, civil or criminal.

In turn, it shows the most relevant regulatory provisions for the issue of personal data protection, whose findings show that 74.3% of the authorities surveyed have laws to regulate cross-border data flows. In addition to the above, these data are supervised by each authority, and the distribution of them is in the hands of the public and private sector.

Section C: Authority's funding and resources

This section details the budget that the authorities allocate (or are allocated) for data protection, which is mostly less than one million dollars. There are authorities that are the exception, receiving even more than 10 million dollars, however, that budget may not be exclusive to the activities or authorities in charge of data protection and privacy

It should be noted that the budget allocated to data protection has increased in most authorities, compared to 2022. This budget comes, in at least 96.1% of the authorities surveyed, from each corresponding government; other relevant sources are: bank interests and public financing plans.

Overall, as with the budget, the staff of most authorities has grown consistently compared to 2020.

Section D: Authority's enforcement powers, case handling and reporting

This section sets out the volume of cases accepted for investigation/action and the types of coercive measures and powers that may be applied, including the powers of authorities to investigate and punish civil or administrative offences, as well as the jurisdiction they have in individual cases.

This section also covers notification of cases and fines or penalties imposed in case of violation of the law. The roles, as well as the pattern of responsibilities and activities, are similar to those reported in the 2020 Census. The number of cases reviewed varies significantly between authorities, reflecting the size of the authorities and the time they have been in place. Many authorities can make binding decisions, although almost all are subject to appeal. Most authorities impose fines and penalties for breaches of data protection or privacy legislation.

Compared to the 2020 responses, the prevalence of different faculties in individual cases is similar, as is public information on the cases they handle, and the volume of authorities imposing fines or penalties for breaking the law has also remained the same.

Section E: Cross-border data flows, enforcement and cooperation

This section discusses the involvement of authorities in international law enforcement cooperation and joint investigations. The authorities were asked about their requirements for the treatment of evidence in coordinated or joint investigations, and any restrictions on the cross-border transfer of information.

The responses showed that provisions on cooperation and cross-border law enforcement increased compared to 2020. Participation in international cooperation figures remain similar to those of 2020. Most of the authorities are somehow involved in international law enforcement cooperation initiatives, and many have participated in joint investigations or cooperated in the handling of international complaints.

There is a high level of involvement of all authorities in a number of networks or cooperation agreements in terms of law enforcement. Although the number of authorities participating in secondment has remained almost the same, indicating that in these 3 years the attention to cooperation has not increased much, as opposed to growth with respect to the 2017 census.

Section F: Breach notification

This section asks about the authorities' guidelines for voluntary and mandatory notifications.

Most authorities reported that they have mandatory breach notification requirements in their jurisdiction and many (though not most) also have voluntary breach notification guidelines in place. Most authorities publish information about notifications of violations they receive.

Section G: Other matters

This section focuses on authorities' engagement with the public and shows that, as in 2017 and 2020, most authorities do not have a formal civil society engagement process in place. In proportion, fewer authorities conducted a public opinion survey in 2022 compared to 2020. And just over half of the authorities publish their regulatory priorities.

Introduction

The GPA 2023 Census supports the goals of the Resolution on the Conference Census, which took place at the 40th Conference in October 2018. This is the third census the GPA has conducted, the first dating back to 2017, followed by the second, 2020. For this report, comparisons to the 2020 census have been made in limited circumstances where relevant.

GPA Vision

An environment in which privacy and data protection authorities around the world can act effectively to fulfil their mandates, both individually and jointly, through the dissemination of knowledge and supportive connections.

Mission of the GPA

The World Privacy Assembly aims to:

- Be a leading global forum for privacy and data protection authorities.
- Disseminate knowledge and provide practical assistance to aid the authorities in carrying out their mandates more effectively.
- Provide international leadership in data protection and privacy.

Connect and support national and regional efforts, and in other international forums, so that authorities can better protect and promote privacy and data protection.

The GPA aims to achieve its vision through cooperation, collaboration and training to develop policy positions, as well as guidance, tools and implementation approaches, with the aim of delivering consistency and predictability of the supervisory system, as data flows.

This Census provides a combined dataset to inform stakeholders about the policies and enforcement approaches used by authorities guiding/regulating data protection and privacy in 78 jurisdictions from different nations, whose authorities completed the survey.

Methodology

The survey questions were developed in collaboration with the working groups of the “GPA”, largely the Data Metrics Working Group, the International Compliance Working Group and the Strategic Direction Subcommittee of the Executive Committee.

The survey questionnaire was also consulted with the Secretariat of the “GPA” (Presidential Authority).

78 of the 137 members from all regions of the world represented in the “GPA” responded to the survey, of which 1 was a supranational member. This represents 57% of responses (counting 137 member authorities in total.) Compared to the 70 authorities out of 130 that responded to the previous Census in 2020, 2 of these respondents were supranational authorities. A regional breakdown of 2020 and 2023 responses can be found in Section A: “Authority Profiles”. Different authorities responded to this census compared to 2020, which may have an effect on the results.

The survey was completed by each authority with a deadline of April 21, 2023. Authorities were asked to report on 2022 figures. An “off-line” version was made available to authorities who were unable to access the online survey platform and contributed to the overall results (full version available in Appendix 1).

The survey data were analyzed at the level of the total sample. The report was written by X-DATA DDO.

SECTION A

Authority profiles

OVERVIEW

- **78 authorities around the world** participated in the GPA's 2023 Census. Most were authorities from Europe, however, all continents participated.
- **All the authorities surveyed** have an online presence, through websites as well as social networks, with Twitter being the most used among those surveyed.
- **Compared to 2020**, the appointment of the head authority by the executive branch prevails in most of the authorities surveyed.

Authority Profile

Region

78 authorities around the world participated in the GPA's 2023 Census. The participating regions were Europe, North America, Africa and Middle East, South and Central America, Asia, Oceania and Other Regions (the Caribbean).

In 2022, The Global Privacy Assembly were integrated by 137 members, 7 more than its total of 130 members in 2020, year when 70 members answered the survey, participating the regions below:

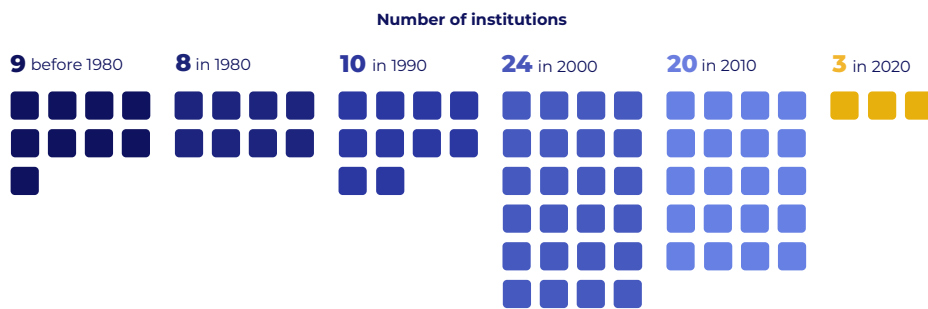
Region	2023's Members	2020's Members
Europe	42	40
North America	11	8
Africa and Middle East	9	7
South and Central America	7	5
Asia	4	2
Oceania	4	3
Other regions	1	5
Total	78	70



Decade of Establishment

Some authorities have existed for several decades, however, since the beginning of the 21st century there has been a notable increase in the creation of organizations interested in data protection, with the 2000s and 2010s being the decades in which the greatest number of organizations have been established

Year of Establishment – Decades

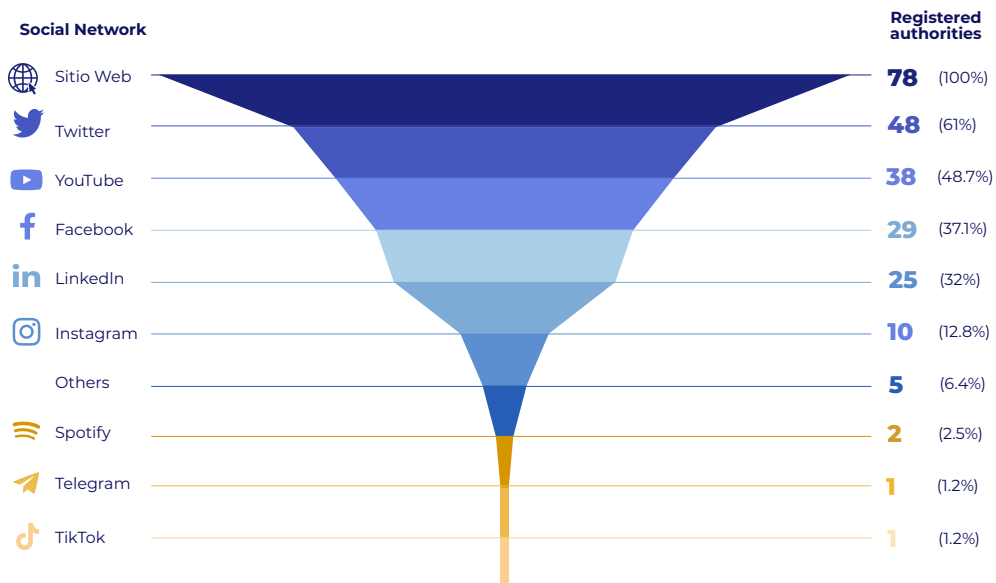


Base: Total responses Census 2023, n=78 authorities

Online Presence

The total of authorities surveyed have an online presence, all 78 having a website (a list of links can be found in Appendix 2), some even being part of the most relevant social networks, as shown below.

Distribution of online presence



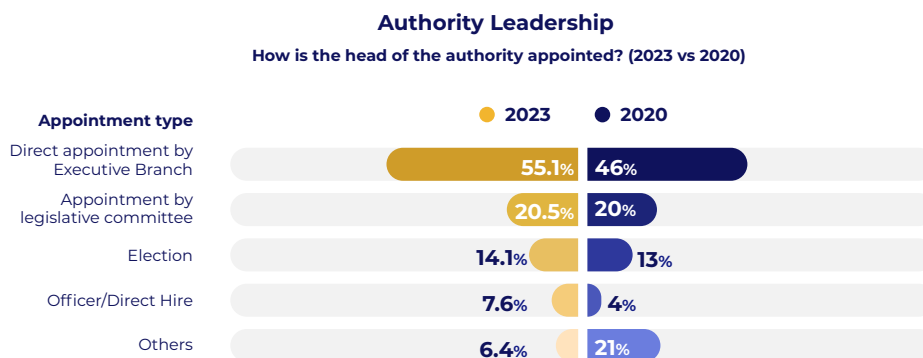
Base: Total responses Census 2023, n=78 authorities

Annual Reports

Almost all of the authorities, 77 out of 78, publish annual reports, of which 70 are published as accountability to some governmental body and 71 of them are available online.

Authority leadership

The most common way to appoint the head authority is by executive appointment (55.1%), i.e., the Government or Head of State appoints someone to the position; followed by appointment by a legislative commission (20.5%) and other methods expressed below, compared to the 2020 report.

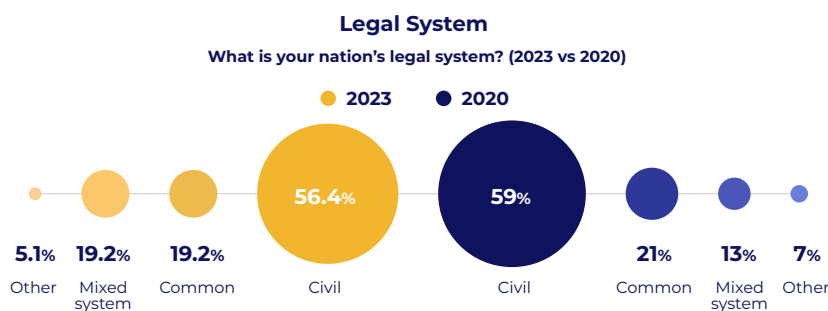


Base: Total responses Census 2023, n=78 authorities; Total responses Census 2020, n=70 authorities Source: THE 2020 GPA CENSUS

This shows a constant in the way the authorities assign their leaders, except for the “Others” section where we can observe an interesting decrease in the selection of ways to assign their leader.

Legal System

Most authorities have a civil law system (56.4%), followed by a common law system (19.2%), mixed systems (19.2%) and others (5.1%). Compared to the 2020 Census, we can see that the mixed system has increased in participation, however, the similarity in the rest of the legal systems remains.



Base: Total responses Census 2023, n=78 authorities; Total responses Census 2020, n=70 authorities Source: THE 2020 GPA CENSUS

Education programs

As technology advances, the need to stay up-to-date on data issues, such as its digital protection, becomes more latent. That is why in the 2023 Census it was requested to mention the participating authorities if their staff is constantly updated. The results were as follows:

53 of the members offer internal training programs, while 25 do not. Considering members whose staff receives training, it behaves as follows.



Base: Total responses Census 2023, n=78 authorities

In addition to staff training, 35 of the 78 members offer professional qualifications. This figure is distributed as follows: 11 institutions have more than 75% of their staff with these qualifications; 9 have 51-75% of their staff with professional qualifications; 6 have between 26-50% of their staff with these qualifications; and 9 have between 1-25% of their staff with professional qualifications.

SECTION B

Data protection law, jurisdiction and exemptions

OVERVIEW

- **Most authorities** aim to regulate the cross-border flow of data.

- **The authorities monitor** those who handle the data, a finding being that both individuals and authorities share the management of all data.

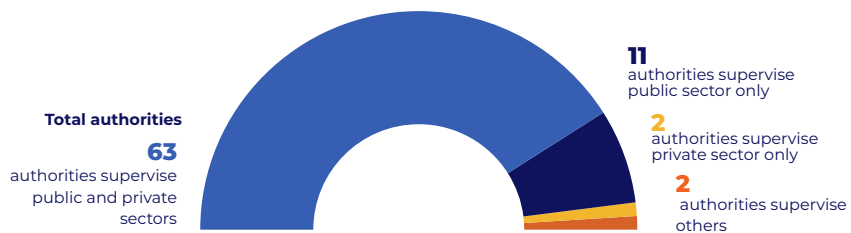
- **The laws give the authorities** various powers in the field of data protection, not only in specialized laws, but in an additional set of laws. In addition, it grants the necessary powers to initiate or process civil, administrative or criminal actions for the misuse of data.

Data protection law, jurisdiction and exemptions

Supervision by sectors

The 78 authorities participants supervise privacy protection practices, distributed as it follows:

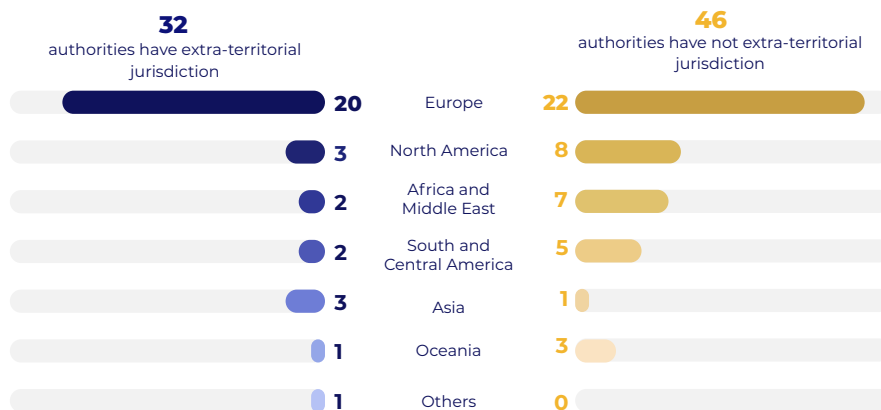
Does the authority oversee privacy protection practices?



Base: Total responses Census 2023, n=78 authorities

58.97% of the participants (46 authorities) do not have extraterritorial jurisdiction, while 41.02% of them (32 authorities) report having extraterritorial jurisdiction. This extraterritorial jurisdiction is shown in the authorities established in the following regions:

Does the authority have extra-territorial jurisdiction?



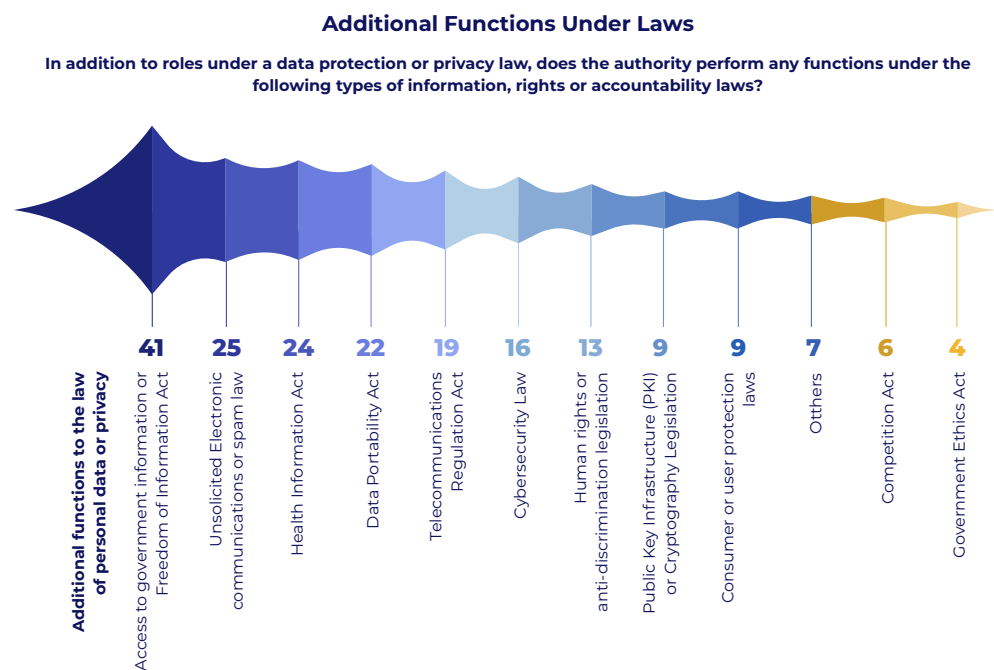
Base: Total responses Census 2023, n=78 authorities

Availability of laws online

77 of the authorities participating in the census (98.7%) have their data protection or privacy legislation available online. In addition, 84.6% (66 of the authorities) provide references to the protection of personal data or privacy in their Constitution.

Functions additional to the law

Some institutions perform functions under different types of information laws, rights and responsibilities, going beyond only the functions covered by the law of protection of personal data or privacy. More than one of these additional functions can be carried out at the same time by an authority, and their distribution is as follows:



Base: Total responses Census 2023, n=78 authorities

Exemptions

57 of the authorities responding to the Census claim to have certain exemptions within their data protection or privacy law: 45 of the authorities (57.6%) provide partial exemption to state intelligence and security agencies within their data protection or privacy laws, while 12 authorities (15.3%) provide full exemption to state intelligence and security agencies within the same laws. Only 21 of the authorities (26.9%) do not submit the previous exemptions.

Provisions on administrative and criminal offences

91% of members

(71) have provisions on **civil and/or administrative infringements** within their data protection or privacy laws.

8.9%

(7) do not have these provisions.

58.9% of members

(46) have provisions on **criminal offences** within their data protection or privacy laws.

41%

(32) do not have these provisions.

These figures have not changed significantly compared to the results of the 2020 Census, where 89% of the authorities (62 out of 70) had these provisions on civil and/or administrative infractions, and 57% of the authorities (40 out of 70) had provisions on criminal infractions.

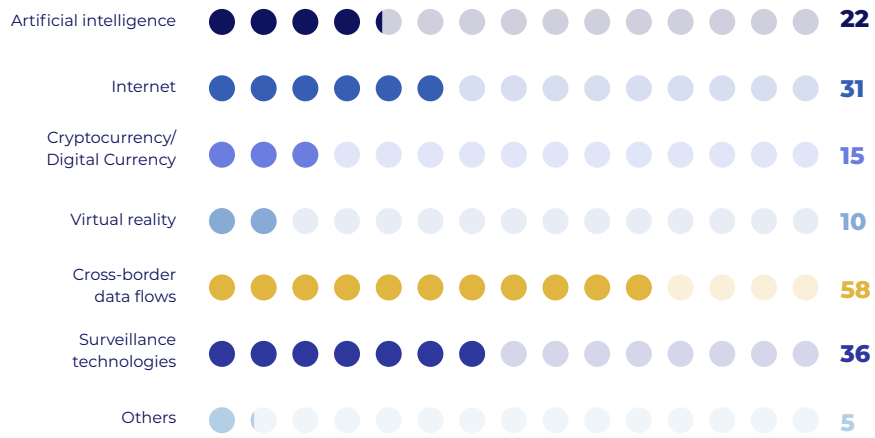
Legislative reforms

46.1% of the authorities are constantly updating their legislation on data protection or privacy, having amended or modified it at least once in the last 3 years. On the other hand, 53.8% of the members surveyed have not made changes to their data protection or privacy legislation in at least the last 3 years. In other words, only 36 out of 78 authorities surveyed have updated their legislation on data protection or privacy since 2020, the same year that, according to the corresponding Census, had 52 out of 70 authorities with updates in their legislation in the last 3 years (2017-2020)

Legislation in the field of technology

As technology advances, so must legislation. Below are some technological aspects where legislation of the authorities surveyed provides for its regulation:

Technological fields with regulation at the legislative level



Base: Total responses Census 2023, n=78 authorities

SECTION C

Authority's funding and resources

OVERVIEW

•**The budget that the authorities** allocate to data protection and privacy is mostly less than one million dollars.

•**The funding, in at least 96.1%** of the authorities surveyed, comes from their respective government. Other relevant sources of financing are: bank interests and public financing plans.

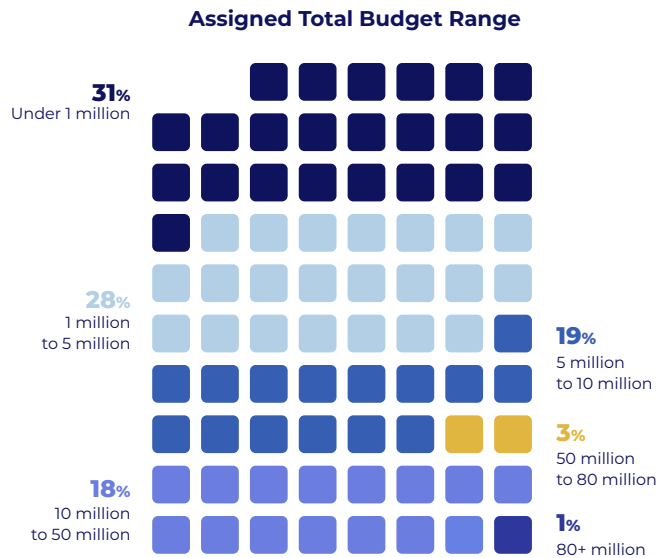
•**The staff of each authority** has grown steadily, compared to the 2020 Census.

Authority's funding and resources

Total revenue

The GPA Census collected detailed information on the authorities' total revenue in their local currency, this information was converted to USD for ease of comparison.*

Authorities reported a wide range of budgets, from <\$1,000 to over \$300,000,000 USD. This figure is more than 4 times higher than the second-highest budget (\$79,000,000). Omitting the atypical figure, the average range ranges from <\$1,000 to ~\$79,000,000. It should be noted that some authorities may receive budgets for other implementation mandates in addition to those in the area of data protection and privacy, which may explain some of the higher reported budgets.



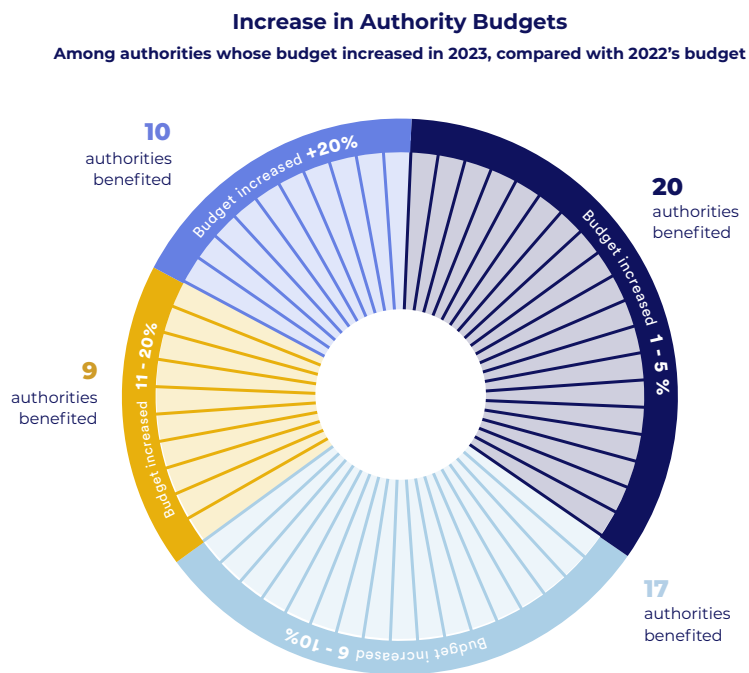
Base: Total responses Census 2023, n=78 authorities

Changes in total budget

Authorities were asked how their budget had changed compared to the previous year (2022).

71.7% received an increase in their budget (56 authorities); 15.3% maintained the same budget (12 authorities); and 12.8% suffered a decrease in their budget (10 authorities).

Among the authorities whose budget increased in 2022, the following range of budget increase is appreciated:



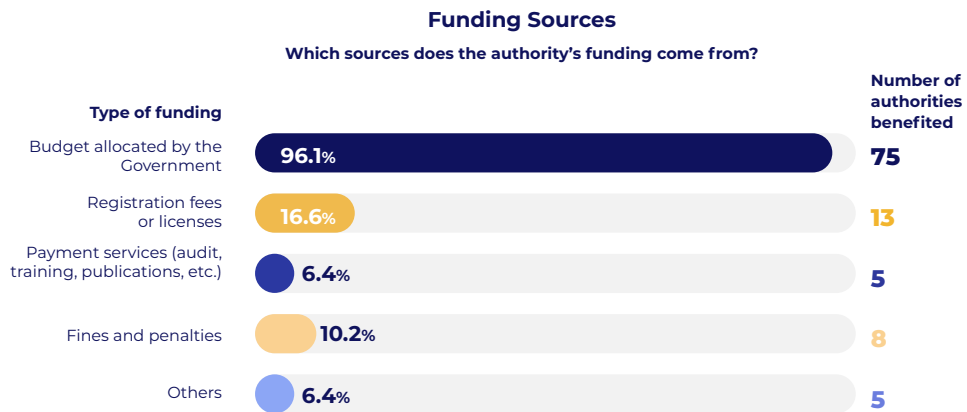
Base: Total authorities whose budget increased in 2022, n=56 authorities

Comparing the above with the 2020 data, it is observed that budgets maintain a constant growth. In the 2020 Census, whose data is based on the 2019 budget, 71% of the authorities that responded to the survey reported an increase in budgets, that is, 50 of the 70 authorities surveyed. Although, in 2022 it can also be observed that 71% of the authorities (56 of 78) received an increase, this number may have greater relevance to be considered an increase and not a constant figure, considering the health emergency due to SARS-CoV-19 that began in 2020 and until the end of 2022 the economy could be considered to have returned to more favorable conditions

Sources of income/funds

75 of the 78 authorities (96.1%) stated that their funding comes from the budget allocated by their respective governments. Other sources of income are: bank interest, public financing schemes, EU funding through participation in European programs, EU budget, regulatory fees.

Below are the different types of funding available to the authorities surveyed (some of them have more than one source of funding).



Base: Total responses Census 2023, n=78 authorities

Staff numbers

In the census GPA requested precise information on the number of employees that each authority has, and measured in full-time equivalent employees (FTEs).

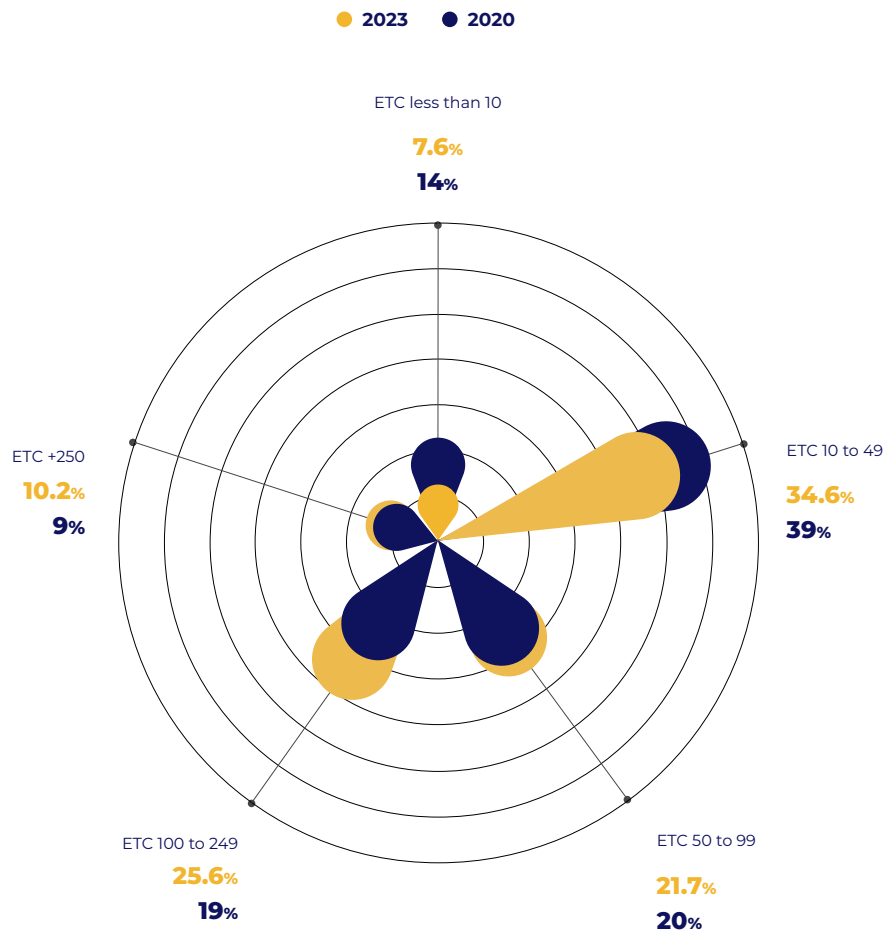
The size of the authorities varies considerably, with a total FTE workforce ranging from 2 to more than 1,000 employees.

The average workforce is 124 people.

49 of the authorities (62.8%) reported having increased their staff compared to the previous year, while 8 (10.2%) indicated a reduction and 21 authorities (26.9%) indicated that FTE remained with the same number of members. Of the total authorities that increased their permanent staff, only 2 out of 49 did not plan this increase; on the other hand, of the total authorities that suffered a decrease in their FTEs, 6 out of 8 were unplanned. In other words, 85.9% of reported changes were planned in advance.

Compared to 2020, these figures suggest that authorities continue to grow quickly. However, it is important to consider that the total number of authorities that responded to the Census in 2023 is slightly higher than in 2020.

Full-time staff 2023 vs 2020



Base: Total responses Census 2023, n=78 authorities;
 Total responses Census 2020, n=70 authorities
 Source: THE 2020 GPA CENSUS

SECTION D

Authority's enforcement powers, case handling and reporting

OVERVIEW

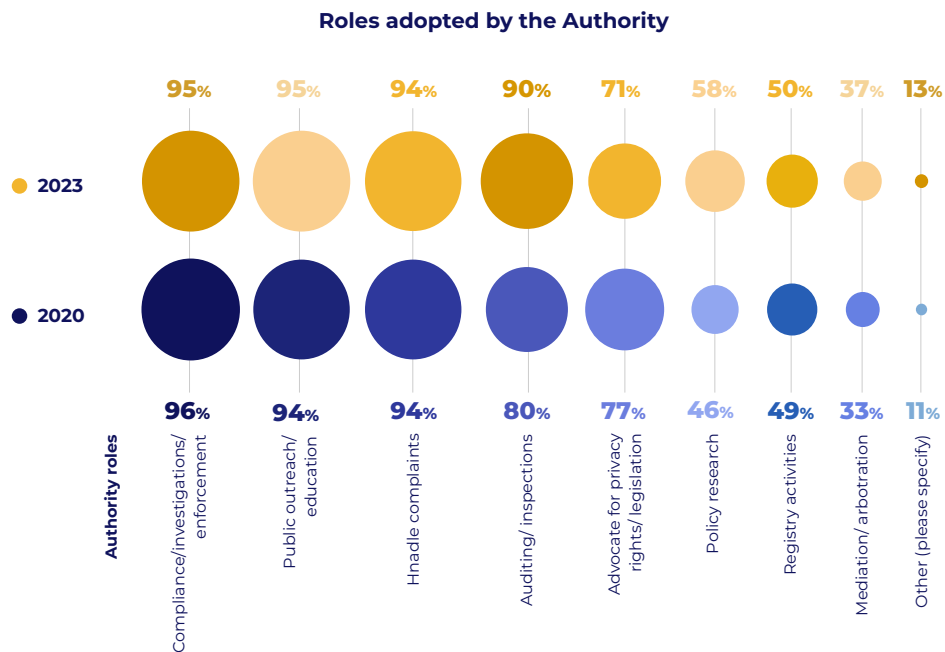
- **Almost all authorities** fulfill roles of complaint handling, public outreach/education and compliance/investigation/law enforcement.
- **The number of cases reviewed** varies significantly, reflecting the size of the authorities and the longevity of some of them.
- **Most authorities impose** fines or penalties for breaches of data protection law. But only very few receive a portion of that fine

Authority’s enforcement powers, case handling and reporting

Roles of the authority

Similar to the 2017 and 2020 census, the roles most authorities surveyed respond to are “complaint handling” (94%), “public outreach/education” (95%), and “compliance / research / enforcement” (95%).

The roles that saw slight growth over the 2020 census were “policy research” (58%) and “audit inspections” (90%). Which in 2020 were reported at 46% and 80% respectively.



Total responses: **78**

Base: Total responses Census 2023, n=78 authorities;
 Total responses Census 2020, n=70 authorities
 Source: THE 2020 GPA CENSUS

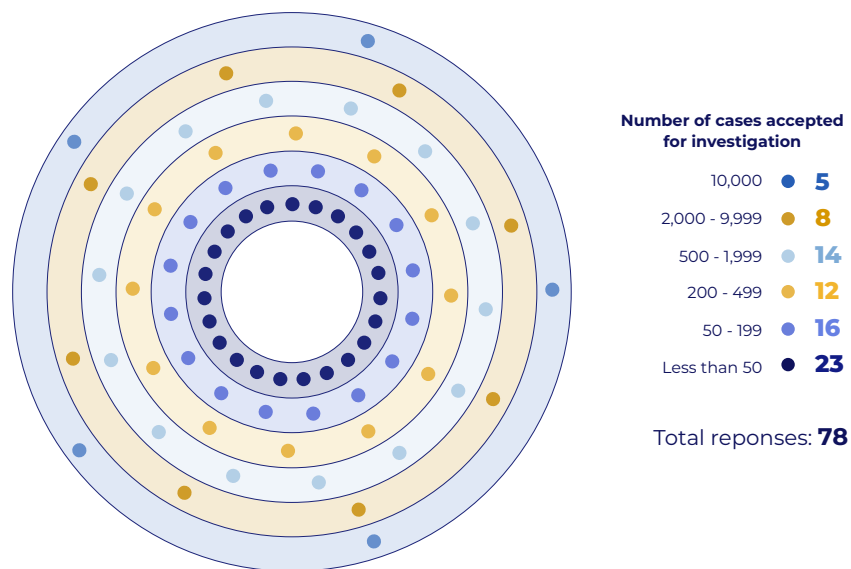
For the rest of the roles, a pattern similar to that reported in the 2020 census is observed. Almost all roles increased by a small percentage with the exception of the “privacy rights/ legislation advocate” role, which decreased by 6%.

Cases accepted for investigation

A wide range of cases accepted for investigation was recorded among the authorities surveyed, said range was from 0 to more than 30,000. The maximum figure was lower than that recorded in 2020, which was greater than 50,000.

By 2023, cases accepted for research were distributed very similarly to the 2020 census.

Accepted cases for investigation



Base: Total responses Census 2023, n=78 authorities;
 Total responses Census 2020, n=70 authorities
 Source: THE 2020 GPA CENSUS

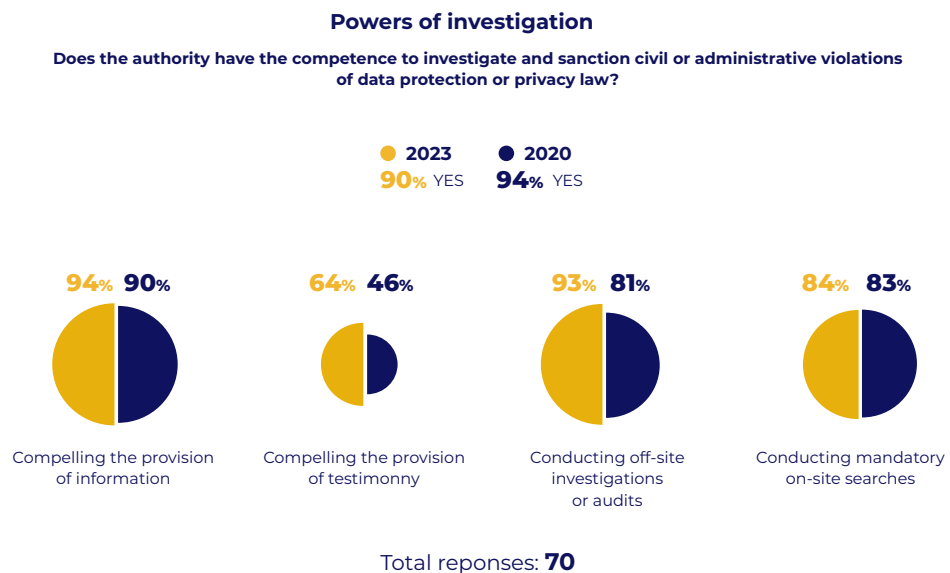
Most authorities accept fewer than 50 cases for investigation. Referring to the 2020 census report, it is suggested that the wide range of values in these responses is due to the fact that the authorities interpret the term “investigate” differently and it is proposed that the number of cases accepted for investigation is directly proportional to the size of the authority in terms of staff.

Investigation and sanctioning powers

Powers of investigation

70 of the 78 authorities surveyed (90%) have the power to investigate and sanction civil/administrative breaches of their privacy or data protection law. This percentage did not change much compared to 2020 (94%).

Similarly, investigative powers followed a trend similar to that of the previous census. By 2023, 94% of authorities have the power to compel the provision of information, 64% can compel the provision of testimony, 93% conduct off-site audits or investigations, and 84% conduct mandatory on-site searches.

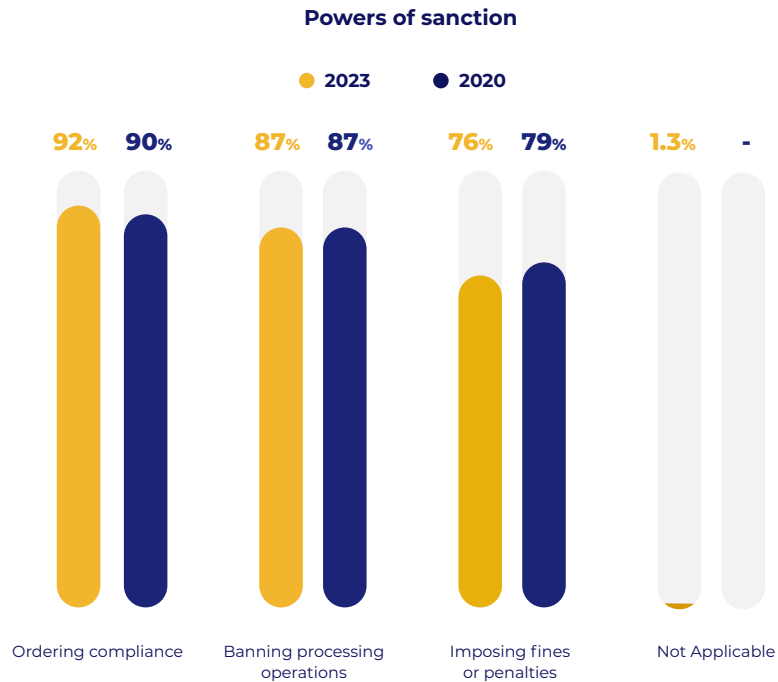


*Base: Total responses Census 2023, n=78 authorities;
Total responses Census 2020, n=70 authorities
Source: THE 2020 GPA CENSUS*

Compelling testimony and conducting off-site audits or investigations were the research powers with significant growth for this 2023 census. In 2020 the values were 46% and 81% respectively.

Powers of sanction

Without significant changes from 3 years ago, the vast majority of authorities declared having the following 3 sanctioning powers:



Total reponses: **78**

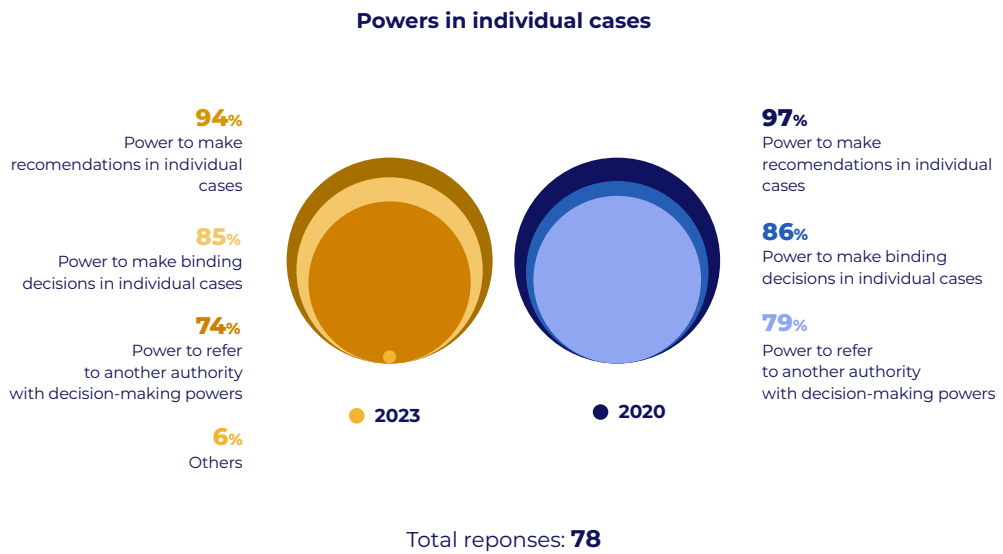
*Base: Total de respuestas Censo 2023, n=78 autoridades;
Total de respuestas Censo 2020, n=70 autoridades
Fuente: THE 2020 GPA CENSUS*

66 out of 78 authorities (85%) responded that they had no power to investigate or sanction criminal violations of their respective privacy law or data protection law. Of the 12 authorities that do possess this power, some detailed that part of these powers of sanction are: Making accusations, imposing fines, criminal prosecution and investigation.

On the other hand, a majority (62%) of the authorities answered yes to having the power to present violations of the privacy or data protection law before the court.

Powers in individual cases

Most authorities have all 3 powers with respect to individual cases raised in the survey, with the power to make recommendations in individual cases being the most adopted (94%). Likewise, only 5 authorities (6%) responded to have other powers in addition to those mentioned in the survey.



*Base: Total responses Census 2023, n=78 authorities;
Total responses Census 2020, n=70 authorities
Source: THE 2020 GPA CENSUS*

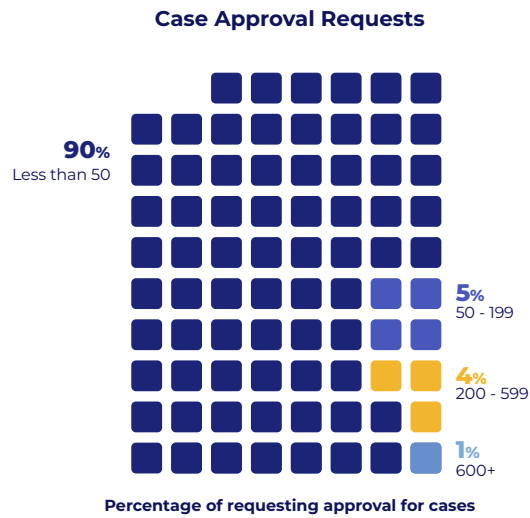
These results were similar to those obtained in the 2020 census.

Appeals

90% of the authorities surveyed do resort to some other entity for decision-making or recommendations. In 2020 this figure was 96%.

Case reporting

The authorities surveyed reported requesting approval for cases in a range from 0 to 99,998, this being a very atypical value, since the vast majority of the authorities (90%) requested approval for cases in an amount less than 50.



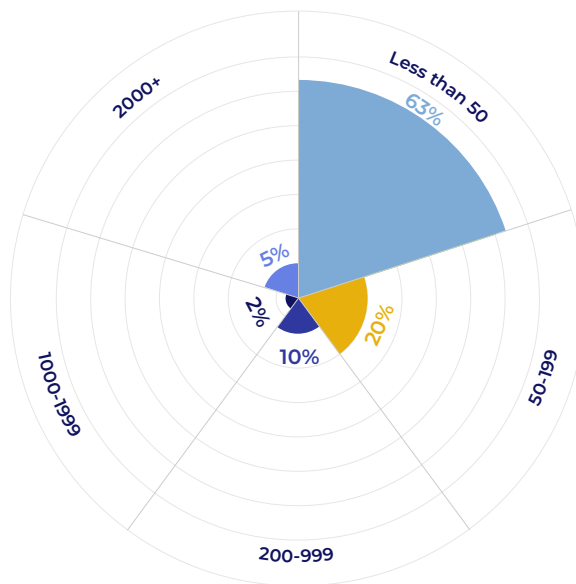
Total reponses: **78**

Base: Total de respuestas Censo 2023, n=78 autoridades.

Of the 78 authorities surveyed, 59 (76%) publish their processed documents and/or resolutions. In proportion this percentage is exactly the same as that obtained in the 2020 census.

Of this 76% that publish documents/resolutions, the majority (63%) published fewer than 50 in 2022. And the other authorities responded in a range ranging from 50 to more than 2,000 documents and/or resolutions published that same year.

Documents and/or processed resolutions published in the last year



Documents and applications applied per authority

Total responses: **59**

Base: Total responses Census 2023, n=78 authorities.

In addition, of the 59 institutions that publish, more than half (61%) do not have a central repository. This represents a slight increase compared to 2020, with a percentage of 57% .

Fines and Penalties

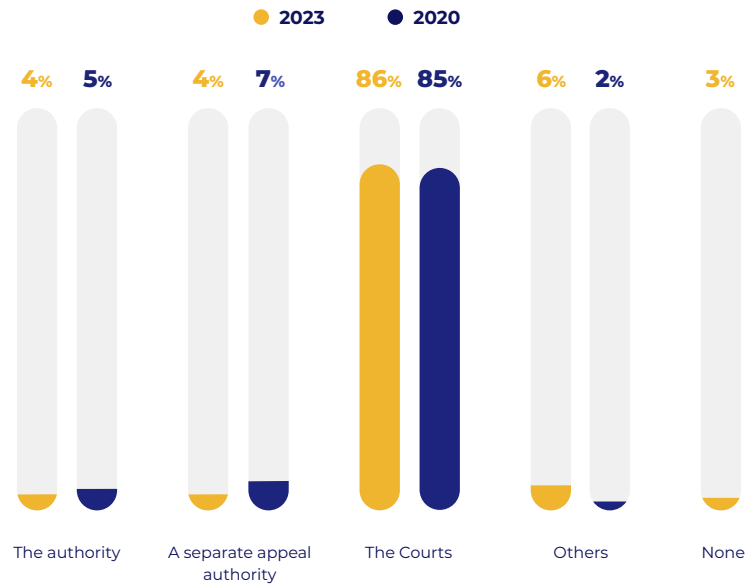
Like the last census, the majority of authorities (74%) impose fines or penalties for non-compliance and/or violation of data protection or privacy laws.

Of the 58 authorities that impose fines and/or penalties, 49 (84%) receive no portion of the fine and only 9 authorities receive a portion. This aspect likewise did not change much with respect to 2020.

Just over half of the authorities surveyed responded that they obtain compensation for non-compliance with legislation (55%).

Regarding which authority is granting this compensation, the pattern was similar to that of 2020, where most authorities reported that the court is the one granting compensation. Only a very small part of the authorities reported granting it themselves or obtaining it from a separate authority.

Authorities granting compensation



Authorities that granting compensation

Total reponses: **71**

*Base: Total responses Census 2023, n=78 authorities;
Total responses Census 2020, n=70 authorities
Source: THE 2020 GPA CENSUS*

Size of fines and number of organizations named

Of the 78 authorities surveyed, 61 (78%) publicly name organizations that violated privacy and data protection laws.

Among all the authorities that participated in the survey, a total of 615 organizations were publicly named for non-compliance with the law. This number increased compared to 2020 where 563 organizations in total were publicly named.

SECTION E

Cross-border data flows, enforcement and cooperation

OVERVIEW

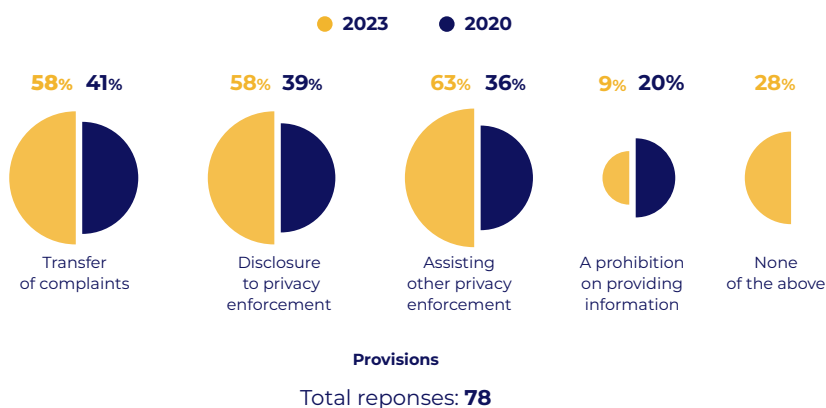
- **There is an increase in provisions** on cross-border law enforcement and cooperation.
- **Most authorities are able to participate** in some form in international law enforcement cooperation initiatives and many have participated in joint investigations or cooperated in international complaints.
- **The authorities have a high level of participation** in different networks or cooperation agreements.

Cross-border data flows, enforcement and cooperation

Provisions within the privacy or data protection law

The authorities reported that their privacy and data protection laws include express provision in almost equal parts between “Transfer of complaints to privacy enforcement authorities in other jurisdictions” (58%), “Disclosure of privacy enforcement authorities in other jurisdictions of information obtained in investigations” (58%) and “Assisting other privacy enforcement authorities in cross-border investigations” (63%). These 3 in proportion did not change much compared to 2020 (57%, 59% and 74% respectively). 22 of the authorities surveyed (28%) stated that they did not provide any of the options.

Express provisions included in the laws



Base: Total responses Census 2023, n=78 authorities;
Total responses Census 2020, n=70 authorities
Source: THE 2020 GPA CENSUS

Disclosure of confidential information

Similar to the 2020 response where 51% of authorities stated that their data protection laws did determine how and when to share sensitive information. In 2023 the response was equally divided. 46% declared “No” and the remaining 54% declared “Yes.”

Legal/practical requirements to deal with evidence in coordinated/joint investigations

62% of authorities have no practical/legal requirements for the collection and handling of evidence in coordinated/joint investigations. Of the 30 authorities that do have these requirements, 38% refer to constitutional articles and different types of agreements/treaties.

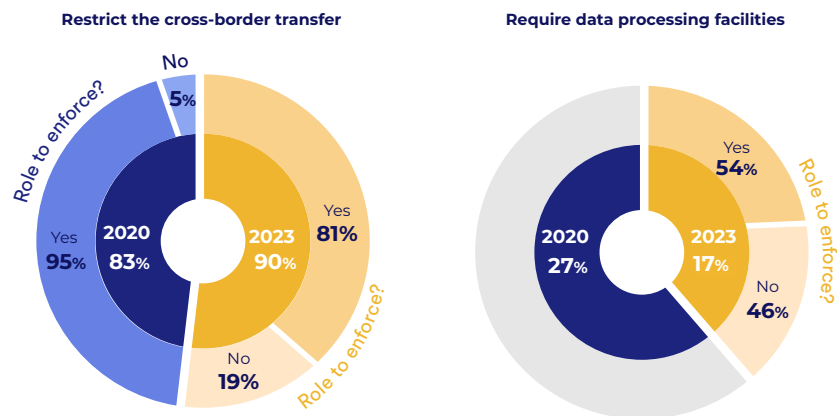
Legal provisions of the jurisdiction on data localisation and restricting cross-border transfers

Most of the authorities surveyed (90%) have laws restricting transfers of personal information across borders. This figure increased slightly compared to 2020 (83%). Of these authorities, 81% have the role of applying these laws.

On the other hand, only a minority of authorities (17%) reported requiring facilities in the jurisdiction for data processing. This figure was lower than that reported in 2020 (27%).

Legal provisions of jurisdiction

● 2020 ● 2023



Total responses: 78

Base: Total responses Census 2023, n=78 authorities;
Total responses Census 2020, n=70 authorities
Source: THE 2020 GPA CENSUS

Process for formally recognising other jurisdictions

Similar to 2020, most authorities (60%) responded that their data protection or privacy law establishes a process to formally recognize other jurisdictions that have laws that establish comparable data protection standards.

However, the majority of authorities (58%) play no role in this recognition process. Different from what was reported in the 2020 census, where 74% of the authorities responded that they did have a role in this process.

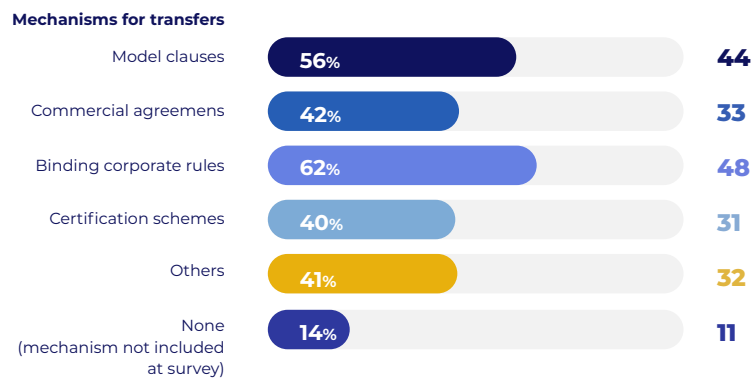
Mechanisms for cross-border transfers

The authorities were asked in the survey what mechanisms exist in their legislation for cross-border transfers of personal data. Most authorities adopt mechanisms such as modeling clauses (56%) and binding corporate rules (62%).

To a lesser extent, the authorities carry out commercial agreements (42%) and certification schemes (40%).

11 of the 78 authorities surveyed (14%) responded that they do not adopt any of the mechanisms mentioned in the survey..

Mechanisms for cross-border transfers



Total responses: **78**

Base: Total responses Census 2023, n=78 authorities.

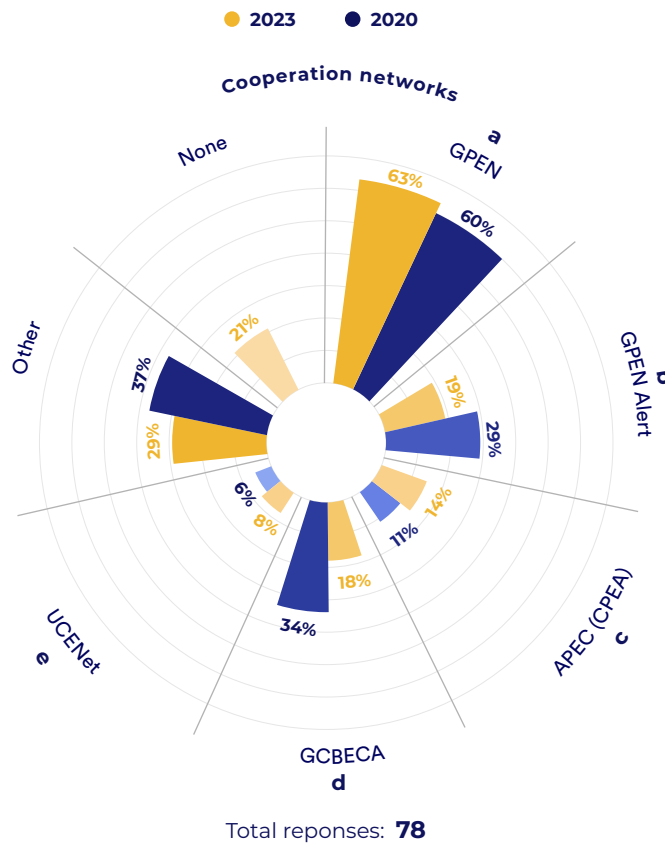
Secondments

Despite the growth of authorities participating in a secondment with another privacy protection authority between the 2017 and 2020 censuses (from 12% to 21%), in 2022 the percentage of authorities participating in a secondment remained the same in proportion (22%).

Participation in enforcement cooperation networks or arrangements

Regarding the participation of the authorities surveyed in networks or cooperation agreements for law enforcement, a pattern similar to the participations reported in the 2020 census is reported. With a notable decrease in participation in GPEN alert, where 19% of the authorities participated, against 29% reported in 2020; and in Global Cross Border Enforcement Cooperation Arrangement GCBECA where 18% participated compared to 34% who participated in 2020.

Participation in cooperation networks



Base: Total responses Census 2023, n=78 authorities;
Total responses Census 2020, n=70 authorities
Source: THE 2020 GPA CENSUS

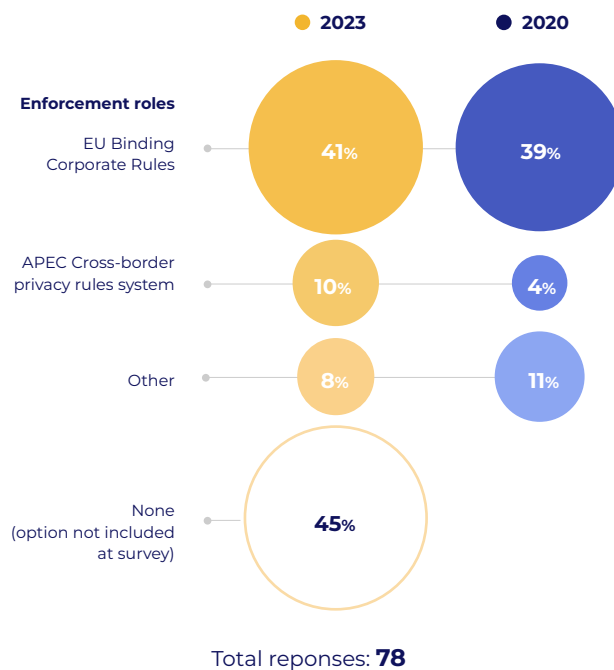
- a. Global Privacy Enforcement Network (GPEN)
- b. GPEN Alert
- c. APEC Cross-border Privacy Enforcement Arrangement (CPEA)
- d. Global Cross Border Enforcement Arrangement GCBECA (Global Cross Border Enforcement Cooperation Arrangement)
- e. Unsolicited Communications Enforcement Network

Enforcement roles in supra-national arrangements

Law enforcement roles in authorities' supranational agreements were reported in a pattern similar to that reported in 2020. With a slight increase in the role of "APEC Cross Border Privacy Rules (CBPR) system" that was 10% in contrast to the 2020 report where the figure was 4%.

Almost half of the authorities surveyed (45%) reported not exercising any of the roles mentioned in this part of the survey.

Law enforcement roles in supra-national agreements



Base: Total responses Census 2023, n=78 authorities;
 Total responses Census 2020, n=70 authorities
 Source: THE 2020 GPA CENSUS

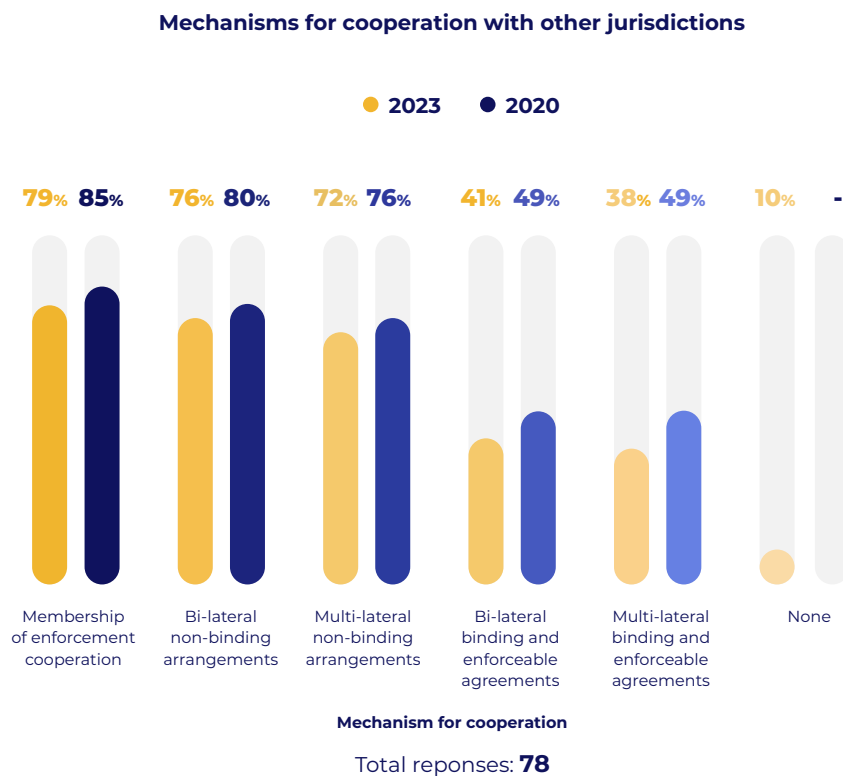
Bilateral arrangements with DPAs in other countries

31 of the 78 authorities surveyed (40%) have some bilateral agreement with the privacy protection authorities of other countries to cooperate in the enforcement of privacy protection laws. Similar to the 34% who reported having this type of agreement in 2020.

Mechanisms for cooperating with other regulatory authorities

Most authorities (63%) have some mechanism for cooperation with other regulatory authorities.

Regarding the mechanisms that can be used by the authority to cooperate with the authorities of other jurisdictions are distributed as follows:



*Base: Total responses Census 2023, n=78 authorities;
Total responses Census 2020, n=70 authorities
Source: THE 2020 GPA CENSUS*

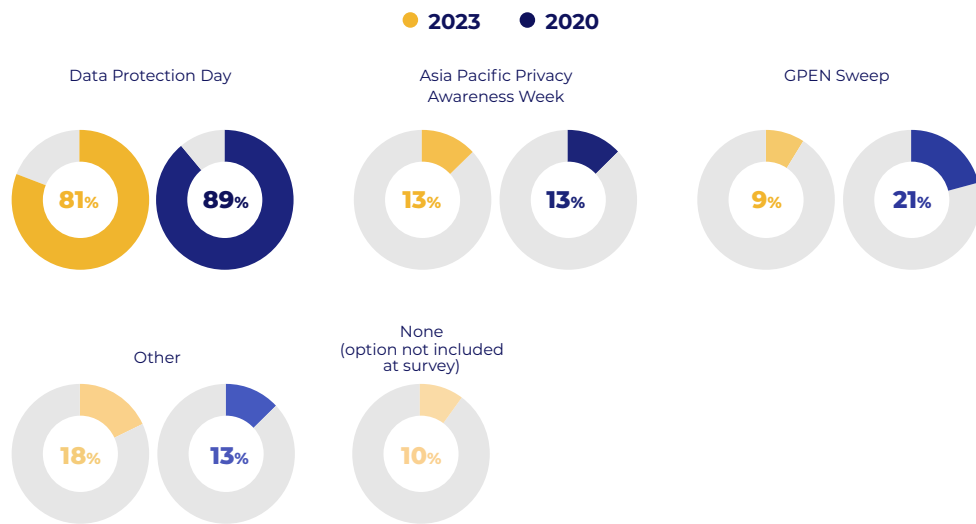
Of the 8 authorities that do not use any of these mechanisms, 4 responded that the legal and/or practical obstacles that their authority faces for each mechanism are given because the legal framework does not require it.

Involvement in efforts to raise awareness of privacy and data protection

The involvement of authorities in coordinated efforts to raise awareness about privacy and data protection in 2022 followed a similar trend to the results reported in 2020. The event with the highest participation (81% of the authorities surveyed) was “Data Protection Day”. There was also a notable decrease in participation in “GPEN Sweep”, where only 7 authorities participated (9%) compared to the 21% participation reported in 2020.

8 authorities (10%) did not participate in any of the coordinated efforts.

Coordinated Awareness Efforts



Total responses: **78**

Base: Total responses Census 2023, n=78 authorities;
Total responses Census 2020, n=70 authorities
Source: THE 2020 GPA CENSUS

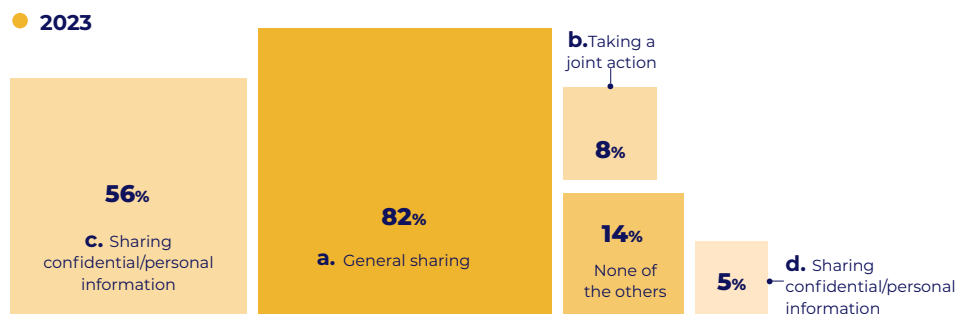
International enforcement cooperation

Participants were asked what forms of international law enforcement cooperation the authority could participate in. Most authorities (82%) conduct general exchange of non-confidential/non-personal information. Most also share confidential/personal information for separate but coordinated investigations by each authority (56%).

To a lesser extent, authorities take joint action not including the exchange of confidential/personal information (8%), and they exchange confidential/personal information for joint investigations of all authorities (5%).

11 authorities (14%) do not participate in any of these forms of international cooperation.

Forms of international law enforcement cooperation



Total responses: 78

Base: Total responses Census 2023, n=78 authorities.

- a. General sharing of non-confidential/non-personal information (e.g. sharing policy/enforcement approaches)
- b. Taking a joint action (e.g. joint letter) with another authority(s), not including the sharing of confidential/personal information.
- c. Sharing confidential/ personal information for separate but coordinated investigations by each authority(s).
- d. Sharing confidential/personal information for joint investigations by both/all authority (s)

Recent participation in joint investigations or cooperating in international complaints

Authorities were asked if they had been involved in any of the typical incidents of cross-border cooperation in terms of law enforcement in 2022. As reported in 2020, many authorities have transferred a complaint to a privacy authority of another country or have received the transfer of a complaint from a privacy authority of another country.

To a lesser extent, compared to 2020, they have assisted an investigation undertaken by a privacy protection authority of another country (18% of the authorities in 2022 vs. 39% in 2019).

A considerable number of authorities (37%) stated that they had not participated in any of the incidents described.



Base: Total responses Census 2023, n=78 authorities;
 Total responses Census 2020, n=70 authorities
 Source: THE 2020 GPA CENSUS

Furthermore, with regard to the authority's disposition of a contact point/contact person for international law enforcement cooperation, exactly half (39 authorities) reported having such a contact point or person while the other half did not have it.

SECTION F

Breach notification

OVERVIEW

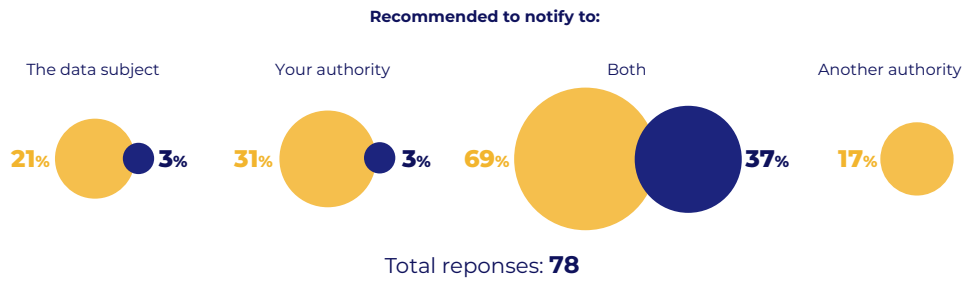
- **Most authorities have mandatory** notification of infringements in their jurisdiction, and less than half have guidelines for voluntary notifications of infringements.
- **Most authorities publish** information about notifications of violations they receive.

Guidelines for voluntary notifications

49% of the authorities surveyed responded that there are voluntary reporting guidelines for infringements issued in their jurisdiction. This percentage grew slightly compared to that reported in 2020 (43%).

Most authorities (69%) recommend that both the subject concerned and the authority be notified.

Voluntary notification recommendation



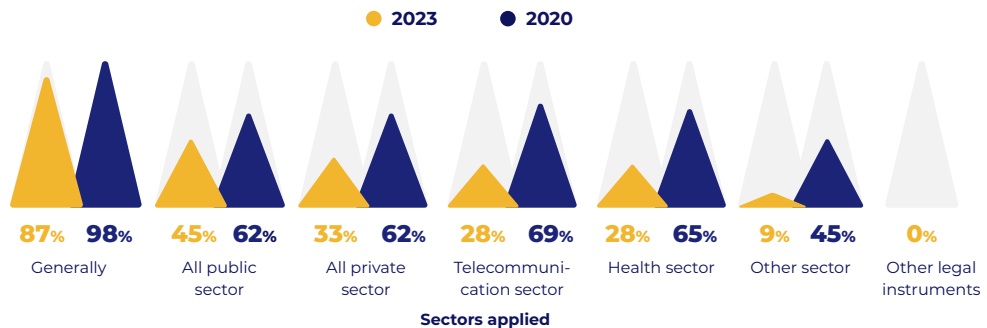
Base: Total responses Census 2023, n=78 authorities;
Total responses Census 2020, n=70 authorities
Source: THE 2020 GPA CENSUS

Requirements for mandatory notifications

67 of 78 authorities surveyed responded that there are mandatory infringement notification requirements in their jurisdiction.

With regard to the implementation of mandatory infringement reporting requirements, the authorities responded as follows:

Mandatory infringement reporting requirements

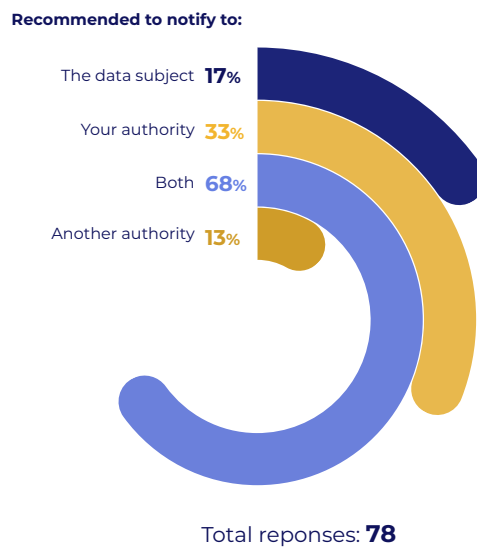


Base: Total responses Census 2023, n=78 authorities;
Total responses Census 2020, n=70 authorities
Source: THE 2020 GPA CENSUS

There was a significant change in the pattern of implementation of mandatory requirements, as there was a decline in the telecommunications and health sectors.

Similar to voluntary notifications, most authorities (68%) recommend that both the data subject and the authority be notified.

Mandatory notification recommendation



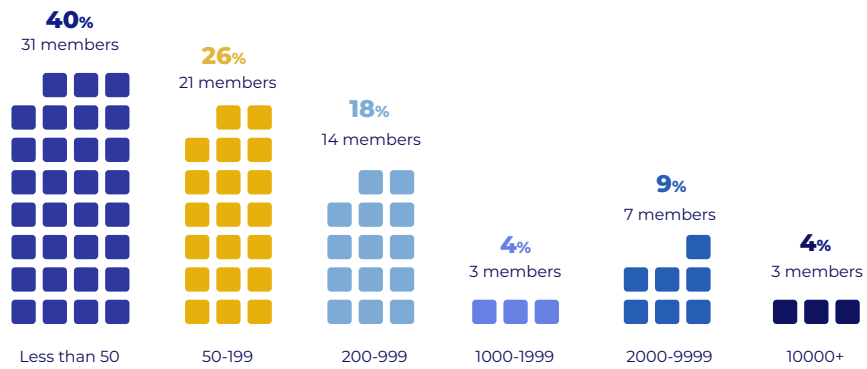
Base: Total responses Census 2023, n=78 authorities.

Most authorities also responded that the requirements do not provide any explicit guidance on notification to persons living in other jurisdictions (83%).

Breach notifications received in 2022

The authorities received notifications of infringement, under voluntary and mandatory agreements, in a range of less than 50 to more than 10,000.

Infringement notifications received



Total infringements received

Total reponses: **78**

Base: Total responses Census 2023, n=78 authorities

Publication of breach notifications

Most authorities (68%) publish some information on the notifications of infringement they receive, for example, the total number of notifications received, the breakdown by sector or the details of which give rise to formal action.

SECTION **G**

Other matters

Engagement with civil society

Only 35% of authorities have a formal process in place to engage with civil society. This represents a slight increase compared to the 30% of the authorities that reported having this process in 2020.

Public opinion surveys

Only 14 authorities (18%) conducted a public opinion survey in 2022. Similar to the 23% reported in the 2020 census.

Publication of regulatory priorities

41 of 78 authorities publish their regulatory priorities.

Appendix 1

GPA Census 2023

All GPA member authorities are requested to complete this survey which will provide a comprehensive snapshot of Data Protection and Privacy Authorities in 2023.

The Census supports the objectives of the Resolution on the Conference Census adopted at the 40th Conference in October 2018

Instructions:

Please complete the survey by 21 April 2023.

Only one response per member authority.

Please complete the census in English for a better statistical analysis of the answers. If the authority is a unit within a much larger public body, please answer these questions only in relation to your unit (particularly Part C questions on funding and resources).

A few questions ask for information relating to 2022, as the most recent complete year. Please answer such questions with information relating either to the calendar year 2022 or, where more convenient, the most recently completed financial year for which you have figures.

Please note that the information will be saved until you finish the survey and click the submit button. Therefore, the Secretariat recommend that you pre-fill the survey in word and then upload your answers to the platform.

Further information about publication and release of information gathered in this census is available here:

<https://globalprivacyassembly.org/the-assembly-and-executive-committee/gpa-census/>

GPA Secretariat

TABLE OF CONTENTS

The census has 7 Parts as follows:

- A. Authority profile
- B. Data protection law, jurisdiction and exemptions
- C. Authority's funding and resources
- D. Authority's enforcement powers, case handling and reporting
- E. Cross-border data flows, enforcement and cooperation
- F. Breach notification
- G. Other matters

A. Authority profile

1. Please provide the following details regarding your data protection or privacy authority:

- a) Name of Authority:
- b) Regulations, agreement, decree, document in which the creation of the agency is stated.
- c) Country/economy:
- d) Please indicate the region in which the authority is located:
 - d.1 Africa and Middle East
 - d.2 Asia
 - d.3 Europe
 - d.4 Oceania
 - d.5 North America
 - d.6 South or Central America
 - d.7 Other
- e) Year of establishment:
- f) What is (are) the primary language(s) of your authority?
- g) If applicable, what is (are) the secondary language(s) of your authority?

2. Does the authority have an official digital presence? Yes/No

If your answer is affirmative, please put the URL to the website:

2 (a) As relevant, please provide the details for the following social media:

- i. Website link or username: ...
- ii. Twitter account: @...
- iii. Facebook link or username: ...
- iv. YouTube channel link ...
- v. Any other social media account address?

3. Does the authority publish an annual report? Yes/No

3 (a) Is the issuance of the annual report considered an action of accountability presented to any governmental instance, power, authority, or similar?

3 (b) Is the annual report available online? Yes/No

If yes, please provide the link:

4. How is the Head of the authority appointed?

- a. Appointment by the executive branch (e.g., Government/Head of State)
- b. Legislative committee appointment
- c. Election
- d. Civil servant/direct hire
- e. Other

5. What is your nation's legal system?

- a. Civil
- b. Common
- c. Mixed systems, please specify.
- d. Other, please specify.

6. Does your authority offer internal training programs? Yes/No

- a. If your answer is positive, what is the percentage of staff that are trained?
 - i. 1-25%
 - ii. 26-50%
 - iii. 51-75%
 - iv. More than 75%
- b. Does your authority offer professional career qualifications for its staff? Yes/No
If your answer is positive, what is the percentage?
 - i. 1-25%
 - ii. 26-50%
 - iii. 51-75%
 - iv. More than 75%

B. Data protection law, jurisdiction and exemptions

1. Does the authority oversee privacy protection practices by:

- a. The public sector only
- b. The private sector only
- c. Both public and private sectors
- d. Other. Please Specify.

2. Does the authority have extra-territorial jurisdiction? If yes, please provide brief detail.

3. Are your data protection or privacy law available online? Yes/No

If yes, please provide a link.

4. If relevant, in addition to a data protection or privacy law, does the Constitution of your country include a reference to personal data or privacy protection? Yes/No

4(a) If yes, please provide the specific reference to the Constitution.

5. In addition to the functions covered by the personal data protection or privacy law, does the authority perform any functions under the following types of information, rights, or accountability laws?

- a. Government information access or Freedom of Information law
- b. Unsolicited electronic communications or spam law
- c. Human rights or anti-discrimination law
- d. Public key infrastructure (PKI) or cryptography law
- e. Cyber-security law
- f. Data portability law
- g. Government ethics law
- h. Competition law
- i. Telecommunications regulation law
- j. Health information law
- k. Consumer or user protection laws
- l. Others, please specify.

6. Does your data protection or privacy law contain:

- a. A partial exemption for State intelligence and security agencies?
- b. A complete exemption for State intelligence and security agencies?
- c. N/A

7. Does your data protection or privacy law contain:

- a. Provisions on civil / administrative infringements? Yes/No
If yes, provide specific reference to or brief detail on these provisions.
- b. Provisions on criminal infringements? Yes/No
If yes, provide specific reference to or brief detail on these provisions.

8. Have your data protection or privacy law been reviewed (amended or modified) in the last 3 years?

Yes/No

9. Do your laws provide for regulation on:

- a) Artificial intelligence. Yes/No.
- b) Internet. Yes/No. c) Cryptocurrency/Digital currency Yes/No.
- d) Virtual Reality Yes/No.
- e) Cross Border Data Flows Yes/No.

- f) Surveillance technologies. Yes/No.
- g) Others.

C. Authority's funding and resources

1. What was your total budget/ income for 2022 in your national currency? (no decimals, please do not put commas or dots to differentiate thousands)

	Income	Currency
2022		

2. How does the authority's total budget compare to the previous year?

- a. The budget increased.
- b. The budget remained the same
- c. The budget decreased.

2(a) If the authority's budget increased from the previous year, by what percentage did it increase?

- i. 1-5%
- ii. 6-10%
- iii. 11-20%
- iv. more than 20%

2 (b) Were these changes pre-planned or did recent external factors have a bearing on the increase/decrease?

- i. pre-planned
- ii. unplanned

2(c) If unplanned and due to recent external factors please specify reasons.

3. Which sources does the authority's funding come from (select all that apply):

- a. Budget allocated from the Government Yes/No
- b. Registration or licensing fees Yes/No
- c. Chargeable services (e.g.auditing, training, publications) Yes/No
- d. Fines and penalties Yes/No
- e. Other Yes/No (please specify):

4. How many staff are employed by the authority (full time equivalent employees)?

5. How does the authority's total number of staff compare to the previous year?

- a. The number of staff has increased
- b. The number of staff has remained the same

c. The number of staff has decreased

6. If the number has increased/decreased, was it pre-planned or was it unplanned and are there external factors have a bearing on this?

- a. Pre-planned
- b. Unplanned.

6(a) If you have checked the option “Not planned” and due to external factors, please explain briefly the reasons why.

D. Authority’s enforcement powers, case handling and reporting

1. What are the principal roles performed by the authority under the privacy or data protection law (indicate as many as apply):

- a. Mediation / arbitration
- b. Policy research
- c. Handle complaints
- d. Registry activities
- e. Auditing/ inspections
- f. Public outreach/ education
- g. Advocate for privacy rights/ legislation
- h. Compliance/ investigations/ enforcement
- i. Other (please specify)

2. How many cases did the authority investigated in 2022?

3. Does the authority have powers to investigate and sanction civil / administrative infringements of your data protection or privacy law? Yes/No

If yes, does the authority have any of the following investigatory powers:

- a. Compelling the provision of information? Yes/No
- b. Compelling the provision of testimony? Yes/No
- c. Conducting off-site investigations or audits? Yes/No
- d. Conducting mandatory on-site searches? Yes/No

4. Does the authority have any of the following sanctioning powers?

- a. Ordering compliance? Yes/No
- b. Banning processing operations? Yes/No
- c. Imposing fines or penalties? Yes/No

5. Does the authority have powers to investigate and sanction criminal infringements of your data protection or privacy law? Yes/No

If Yes, provide brief detail on these powers.

6. Does the authority have the power to bring infringements of your data protection or privacy law to court? Yes/No

7. Does the authority:

- a. Have the power to make binding decisions in individual cases? Yes/No
- b. Have the power to make recommendations in individual cases? Yes/No
- c. Have the power to refer to another authority with decision-making powers? Yes/No
- d. Others

8. Are the decisions or recommendations of the authority subject to appeal to another body (agency, court or tribunal)? Yes/No

11 (a) How many cases were taken on appeal in 2022?

9. Does the authority publish the files and/or resolutions it has processed? YES/NO

If YES:

9.a How many dossiers and /or decisions were published in the last year?	Yes/No
9.b In the case reports are posted on the authority's website, please provide the URL	
9.c Are the case reports uploaded to a central repository (such as an online legal information institute)?	

Note: Please respond to Q. 10b and Q13 in your country's national currency

10. Does the authority impose fines or penalties for a data breach and/or violation of the data protection or privacy law? Yes/No

10 (a) If yes, does the authority keep:

- c. a portion of the fine
- d. none of the fine.

10. (b) Please provide the amount of the largest fine or penalty imposed by the authority (or an appeal authority, court or tribunal) for a breach and/or violation of the data protection

11. Do your data protection or privacy law provide for the award of compensation caused by breach of the legislation.

Yes/No

12. Which authority has the power to award such compensation:

- a. The authority
- b. A separate appeal authority
- c. The Courts
- d. Other. Please specify.

13. What was the largest amount of compensation awarded by the authority (or an appeal authority, court or tribunal) for harm caused by a breach of the privacy or data protection law in the last year?

14. Does the authority ever publicly name organisations that have breached the privacy or data protection law? Yes/No

14 (a) How many organisations were publicly named in 2022 as having breached the law?

E. Cross-border data flows, enforcement, and cooperation

1. Does the privacy or data protection law include express provision for any of the following:

- a. Transfer of complaints to privacy enforcement authorities in other jurisdictions? Yes/No
- b. Disclosure to privacy enforcement authorities in other jurisdictions of information obtained in investigations. Yes/No
- c. Assisting other privacy enforcement authorities in cross-border investigations? Yes/No
- d. A prohibition on providing
- e. None of the above

2. Does your privacy or data protection law contain provisions that determine when and how confidential information held by a privacy or data protection authority can be disclosed or shared? Yes/No

If yes, please provide a link to, or the wording of, the relevant provisions.

3. Does your authority have specific legal and / or practical requirements for the gathering and handling of evidence in coordinated or joint investigations? Yes/No

If yes, provide brief detail on these requirements.

4. Does the jurisdiction have legal provisions (whether in the privacy or data protection law or otherwise) that:

- a. Restrict the cross-border transfer of personal information? Yes/No
If yes, does the authority have a role to enforce this law? Yes/No
- b. Require data processing facilities to be located within the jurisdiction? Yes/No

If yes, does the authority have a role to enforce this law? Yes/No

5. Does the data protection or privacy law establish a process for formally recognising other jurisdictions that have laws establishing comparable data protection standards? Yes/No

5 (a) Does the authority perform any role in that recognition process? Yes/No

6. What mechanisms exist in your legislation for cross-border transfers of personal data?

- a. Model clauses
- b. Commercial agreements with provisions on cross-border data transfers
- c. Binding corporate rules
- d. Certification schemes.
- 5. Other (please specify)

7. In 2022, has the authority participated in a secondment with another privacy enforcement authority?

Yes/No

8. Which of these enforcement cooperation networks or arrangements does the authority participate in (select all that apply):

- a. Global Privacy Enforcement Network (GPEN) Yes/No
- b. GPEN Alert Yes/No
- c. APEC Cross-border Privacy Enforcement Arrangement (CPEA) Yes/No
- d. Global Cross Border Enforcement Cooperation Arrangement GCBECA (Global Cross Border Enforcement Cooperation Arrangement) Yes/No
- e. Unsolicited Communications Enforcement Network (UCENet) Yes/No
- f. Other (please specify)

9. Does the authority perform an enforcement role under any of these supra-national arrangements (select all that apply):

- a. EU Binding Corporate Rules Yes/No
- b. APEC Cross-border Privacy Rules system (CBPRs) Yes/No
- c. Other (please specify)

10. Does the authority have any bilateral arrangements with the privacy enforcement authorities of other countries to co-operate in the enforcement of privacy laws? YES/NO

11. Does the authority have any mechanism for cooperating with other regulatory authorities (e.g. consumer protection authorities)?

Yes/No/Not applicable

12. Which of the following mechanisms can the authority use to cooperate with authorities in other jurisdictions?

- a. Membership of enforcement cooperation networks. Yes/No
- b. Bi-lateral non-binding arrangements. Yes/No
- c. Multi-lateral non-binding arrangements. Yes/No
- d. Bi-lateral binding and enforceable agreements. Yes/No
- e. Multi-lateral binding and enforceable agreements. Yes/No

If you answered NO for any of the above, provide brief detail on the legal and / or practical barriers that your authority faces for each mechanism.

- a. Legal framework does not allow it
- b. Legal framework does not require it
- c. Other

13. In 2022, was your authority involved in any of the following coordinated efforts, involving authorities from other countries, to raise awareness on privacy and data protection:

- a. Data Protection Day
- b. Asia Pacific Privacy Awareness Week
- c. GPEN Sweep
- d. Other

14. Which of the following forms of international enforcement cooperation can the authority take part in:

- a. General sharing of non-confidential / non-personal information (e.g. sharing policy/enforcement approaches). Yes/No
- b. Taking a joint action (e.g. joint letter) with another authority(s), not including the sharing of confidential / personal information. Yes/No
- c. Sharing confidential / personal information for separate but coordinated investigations by each authority(s). Yes/No
- d. Sharing confidential / personal information for joint investigations by both/all authority(s). Yes/No

15 (a) If YES at previous question, provide brief detail on the legal and /or practical requirements and limitations for each form of cooperation (max 100 words)

15 (b) If NO at previous question, provide brief detail on the legal and / or practical barriers that your authority faces for each form of cooperation (max 100 words)

15. In 2022, has the authority (select all that apply):

a. Undertake a joint investigation with any other enforcement authority or regulator within the same country?	
b. Undertake a joint investigation with a privacy enforcement authority from another country?	
c. Provide assistance to an investigation being undertaken by a privacy enforcement authority from another country?	
d. Transfer a complaint to a privacy enforcement authority in another country?	
e. Receive the transfer of a complaint from a privacy enforcement authority in another country?	
f. Other, please specify	

16. Does the authority have a contact point/person for international enforcement cooperation? Yes/No

If Yes, provide a brief summary of the initial information they require to assess a request for enforcement cooperation from another authority (max 100 words)

F. Breach notification

1. Are there any voluntary breach notification guidelines issued by the authority in your jurisdiction? Yes/No

1 (a) Do they recommend notification to:

- i. the data subject
- ii. your authority
- iii. both the data subject and your authority
- iv. another authority

2. Are there any mandatory breach notification requirements in your jurisdiction? Yes/No

2 (a) Do the mandatory breach notification requirements apply generally or to particular sectors?

i. Generally	Yes/No
ii. All public sector	Yes/No
iii. All private sector	Yes/No
iv. Telecommunications sector	Yes/No
v. Health sector	Yes/No
vi. Other sector (please specify):	Yes/No
vii. Other legal instruments	Yes/No

- 2 (b) Do mandatory breach notification requirements recommend notification to:
- i. the data subject
 - ii. your authority
 - iii. both the data subject and your authority
 - iv. Another authority
- 2 (c) Do the requirements provide any explicit direction on notification to individuals living in other jurisdictions?
- 2.c.i If Yes, please briefly describe:

3. How many breach notifications (under voluntary or mandatory arrangements) did the authority receive in 2022?

4. Does the authority publish any information on the breach notifications it receives, for example total number of notifications received, sectoral breakdown, details of those that result in formal action? Yes/No

- 4 (a) If yes, where is this information published? Select as appropriate and/or provide other examples.

G. Other matters

1. Does the authority have a formal process for engaging with civil society (e.g. regular scheduled meetings)? Yes/No

- 1 (a) If yes, please specify:

2. Did the Authority conduct a public opinion survey in 2022?

- 2 (a) If the survey report is available publicly, please provide URL:

**3. Does your authority publish its regulatory priorities? Yes/No
If yes, please provide a link.**

Appendix 2

Authorities' names, country and website.

Federal Data Protection and Information Commissioner (Préposé fédéral à la protection des données et à la transparence)	Switzerland	www.edoeb.admin.ch/edoeb/en/home.html
Data Protection Inspectorate (Andmekaitse Inspektsioon)	Estonia	www.aki.ee
Office of the Privacy Commissioner of Bermuda	Bermuda	www.privacy.bm
Quebec: Information Access Commission (Commission d'accès à l'information)	Canada	https://www.cai.gouv.qc.ca
Cayman Islands Ombudsman	Cayman Islands	https://ombudsman.ky/
National Data Protection Commission (Commission nationale pour la protection des données)	Luxembourg	www.cnpd.lu
Ukrainian Parliament Commissioner for Human Rights	Ukraine	https://www.ombudsman.gov.ua/
Data Protection Office of Mauritius	Mauritius	http://dataprotection.govmu.org
Commissioner for Information of Public Importance and Personal Data Protection (Повереник за информације од јавног значаја и заштиту података о личности)	Serbia	https://www.poverenik.rs/sr/
Personal Data Protection Authority (Kişisel Verileri Koruma Kurumu)	Turkiye	https://www.kvkk.gov.tr/
Data Inspectorate (Datatilsynet)	Norway	https://www.datatilsynet.no/
Agency for the Protection of Personal Data of Inhabitants	Costa Rica	www.prodhab.go.cr
Queensland: Office of the Information Commissioner	Australia	https://www.oic.qld.gov.au/
Superintendence of Industry and Commerce of Colombia (Superintendencia de Industria y Comercio)	Colombia	https://sic.gov.co/historia
Data Protection Commission (now known as Autoriteit Persoonsgegevens)	Netherlands	https://autoriteitpersoonsgegevens.nl/
Information Regulator	South Africa	https://www.datatilsynet.no/
Nova Scotia: (Office of the Information and Privacy Commissioner for Nova Scotia)	Canada	https://oipc.novascotia.ca/
New South Wales: Privacy Commissioner	Australia	http://www.ipc.gov.au

Data Protection Authority	Liechtenstein	https://www.datenschutzstelle.li
Autorità Garante per la protezione dei dati personali	San Marino	https://www.garanteprivacy.sm/publ/garante/en/
Data Protection Agency (Agencija za zaštitu osobnih Podataka)	Croatia	https://azop.hr/
Parliamentary Commissioner for Data Protection and Freedom of Information (Nemzeti Adatvédelmi és Információszabadság Hatóság) (now known as National Authority for Data Protection and Freedom of Information)	Hungary	www.naih.hu
Privacy Commissioner for Personal Data	Hong Kong	https://www.pcpd.org.hk/
Data Protection Agency (Datatilsynet)	Denmark	https://www.datatilsynet.dk
Catalonia: Catalan Data Protection Agency (Agència Catalana de Protecció de Dades)	Spain	www.apdcat.cat
Information and Data Protection Commissioner of Albania)	Albania	www.idp.al
Office of the Data Protection Authority (Bailiwick of Guernsey)	Guernsey	https://www.odpa.gg/
Hellenic Data Protection Authority (ΑΡΧΗ ΠΡΟΣΤΑΣΙΑΣ ΔΕΔΟΜΕΝΩΝ ΠΡΟΣΩΠΙΚΟΥ ΧΑΡΑΚΤΗΡΑ)	Greece	https://www.dpa.gr
Personal Data Protection Service of Georgia	Georgia	https://personaldata.ge/
Office for Personal Data Protection of the Slovak Republic (Úrad na ochranu osobných údajov Slovenskej republiky)	Slovakia	https://dataprotection.gov.sk/uouu/sk
National Privacy Commission	Philippines	www.privacy.gov.ph
Commission for Personal Data Protection (Комисия за защита на личните данни)	Bulgaria	https://www.cdpd.bg/index.php
Personal Data Protection Agency in Bosnia and Herzegovina (Agencija za zaštitu ličnih podataka u Bosni i Hercegovini)	Bosnia and Herzegovina	www.azlp.ba
Personal Data Protection Commissioner (Επίτροπος Προστασίας Δεδομένων Προσωπικού Χαρακτήρα)	Cyprus	www.dataprotection.gov.cy
Office for Personal Data Protection (Úrad Pro Ochranu Osobnich Udaju)	Czech Republic	https://www.uouu.cz
Ombudsman's office of the City of Buenos Aires	Argentina	https://defensoria.org.ar/derechos/democracia-y-digitalidad/derechos-digitales-y-proteccion-de-datos-personales/
Victoria: Office of the Victorian Information Commissioner (OIVC)	Australia	www.ovic.vic.gov.au
Personal Information Protection Commission (개인정보보호위원회)	Republic of Korea	https://www.pipc.go.kr/

Lower Saxony: Data Protection Commissioner (Die Landesbeauftragte fuer den Datenschutz)	Germany	https://fd.niedersachsen.de/startseite/
Data Protection Commissioner	Gibraltar	https://www.gra.gi/data-protection
Information Commissioner of the Republic of Slovenia (Informacijski pooblaščenec)	Slovenia	https://www.ip-rs.si/
Jersey Office of the Information Commissioner	Jersey	www.jerseyoic.org
North Rhine: Westphalia: Data Protection and Information Commissioner	Germany	https://www.ldi.nrw.de/
Newfoundland and Labrador: Office of the Information and Privacy Commissioner for Newfoundland and Labrador	Canada	www.oipc.nl.ca
National Agency for the Protection of Personal Data (Agência Nacional de Protecção de Dados Pessoais)	São Tomé and Príncipe	www.anpdp.st
Information Commissioner's	United Kingdom	https://www.ico.org.uk
State of Mexico Transparency, Public Information Access and Personal Data Protection Institute of Estado de México and municipalities, INFOEM (Instituto de Transparencia, Acceso a la Información Pública y Protección de Datos Personales del Estado de México y Municipios, INFOEM)	Mexico	https://www.infoem.org.mx/
Institute for Access to Public Information of the Federal District (Instituto de Acceso a la Informacion Publica del Distrito Federal) (2010)	Mexico	https://www.infocdmx.org.mx/
Federal Data Protection Commissioner (Bundesbeauftragten für den Datenschutz)	Germany	https://www.bfdi.bund.de/DE/Home/home_node.html
European Data Protection Supervisor (Contrôleur européen de la protection des données)	European Union	https://edps.europa.eu/en
Data Protection Commissioner (An Coimisinéir Cosanta Sonraí)	Ireland	https://www.dataprotection.ie
Ontario: Information and Privacy Commissioner (Commissionaire à l'information et à la protection de la vie privée)	Canada	https://www.ipc.on.ca
State Data Inspectorate (Datu Valsts Inspekcija)	Latvia	https://www.dvi.gov.lv/lv
National Authority for Data Protection (Autoridad Nacional de Protección de Datos Personales)	Peru	https://www.gob.pe/anpd https://www.gob.pe/antaip
Personal Information Protection Commission (個人情報保護委員会)	Japan	https://www.ppc.go.jp/en/index.html
National Commission for the Protection of Personal Data (Commission Nationale pour la Protection des Données à Caractère Personnel)	Gabon	www.cnpdcp.ga

Privacy Commissioner of Canada (Commissariat à la protection de la vie privée du Canada)	Canada	www.priv.gc.ca
National Data Protection Commission (Comissão Nacional de Protecção de Dados)	Portugal	https://www.cnpd.pt/
National Institute for Transparency, Access to Information and Personal Data Protection (Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales INAI)	Mexico	https://home.inai.org.mx/
Agencia de Acceso a la Información Pública	Argentina	https://www.argentina.gob.ar/aaip
Berlin: Data Protection and Freedom of Information Commissioner (Beauftragter für Datenschutz und Informationsfreiheit)	Germany	https://www.datenschutz-berlin.de/
Institute for Transparency, Access to Information and Data Protection of Michoacán (Instituto Michoacano de Transparencia, Acceso a la Información y Protección de Datos Personales)	Mexico	http://imaip.org.mx
Personal Data Protection Authority (Autorité de Protection de Données à Caractère Personnel)	Mali	https://apdp.ml/
Federal Trade Commission	United States of America	https://www.ftc.gov/
Telecommunications/ICT Regulatory Body (L'Autorité de Régulation des Télécommunications de Côte d'Ivoire – ARTCI)	Côte d'Ivoire	www.autoritedeprotection.ci
Office of the Australian Information Commissioner	Australia	https://www.oaic.gov.au/
Israeli Privacy Protection Authority (תוֹיִטְרָפָה תְּגוּלָּה תוֹשֵׁרָה)	Israel	https://www.gov.il/en/departments/the_privacy_protection_authority/govil-landing-page
National Commission for Informatics and Liberties (Commission Nationale de l'Informatique et des Libertés)	Burkina Faso	www.cil.bf
Office of Data Protection	Abu Dhabi Global Market	https://www.adgm.com/operating-in-adgm/office-of-data-protection/overview
Personal Data Protection Office (Urząd Ochrony Danych Osobowych)	Poland	https://uodo.gov.pl/
Data Protection Agency (Agència Andorrana de Protecció de Dades)	Andorra	https://www.apda.ad/
Isle of Man Information Commissioner (Oik Recortysser Codey Fysseree Ellan Vannin)	Isle of Man	www.inforights.im
Chilean Transparency Council (Consejo para la Transparencia)	Chile	https://www.consejotransparencia.cl/

National Commission for Informatics and Liberties (Commission Nationale de l'Informatique et des Libertés)- France	France	https://www.cnil.fr
State Institute for Transparency, Access to Information and Personal Data Protection (Instituto Estatal de Transparencia, Acceso a la Información y Protección de Datos PersonalesPersonales) (INFO NL)	Mexico	https://infonl.mx/
Data Inspection Board (now known as Swedish Authority for Privacy Protection) (Integritetsskyddsmyndigheten) (2002)	Sweden	https://www.imy.se/
Data Protection Authority (Persónuvernd)	Iceland	https://www.personuvernd.is/
Data Protection Commissioner (Agencia Española de Protección de Datos)	Spain	https://sedeagpd.gob.es/sede-electronica-web/

Este documento se terminó de realizar
el día 19 de julio del 2023, en Ciudad de México, México.
Su ejecución estuvo a cargo
del equipo de X-DATA

*