NAVIGATING THE GLOBAL DATA PRIVACY LANDSCAPE:

THE 2020 GPA CENSUS

GPA
Global Privacy Assembly

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 census and the Secretariat. I commend the results of the Census to you.

Elizabeth Denham

Chair of the Global Privacy Assembly
UK Information Commissioner

Contents

EXECUTIVE SUMMARY

The Global Privacy Assembly (GPA) (Global Privacy Assembly) **seeks to provide leadership at international level in data protection and privacy. It does this by connecting the efforts of more than 130 data protection and privacy members and observers from across the globe.**

This census – based on 2019 data – collected information from 70 GPA members to provide a point in time picture of the policies and delivery approaches that currently guide and regulate data protection and privacy globally.

In a globalised economy where data has no boundaries it provides a useful reference tool for those whose business and data crosses jurisdictions, and to national policy makers considering new legislative approaches. It also supports member authorities' capacity building and collaboration through dissemination of "how it's done" in other jurisdictions. Finally, the data in this Census informs the GPA's Working Groups which are charged with delivering activity in support of the GPA 2019–2021 Conference Strategic direction[1] and its successor document (currently under development and to be agreed at the GPA Conference in Oct 2021).

This report bears many similarities to the picture reported in the 2017 census, but there are some noteworthy differences in 2020. Most notably, the growth in size of data protection authorities around the world in terms of budgets and personnel indicates the increasing importance of ensuring that citizens' personal data and privacy are protected, and seen to be protected, via the oversight of an independent regulator. This census also includes a new authority, established since the previous 2017 Census.

SECTION A: AUTHORITY PROFILES

This section focuses on the authorities' respective regions, their leadership, legal systems and most recent annual reporting on their operation and delivery. This section defines the Census respondents and identifies any patterns and trends which go on to affect other areas of the Census.

Further findings in this section show the increase in online presence since the first Census in 2017 and changes to appointment processes for the head of the authority: a majority now report this as being appointment by the executive, whereas in 2017 it was by election and 'other' methods.

1 Resolution on the Conference Strategic Direction 2019 - 2021 FINAL (globalprivacyassembly.org)

SECTION B: DATA PROTECTION LAW, JURISDICTION AND EXEMPTIONS

This section identifies the sectors which authorities oversee and the powers the relevant law provides, including their ability to take administrative, civil or criminal actions. It also shows where revisions to relevant governing legislation have been made within the last three years, an indicator of a continued global focus on ensuring that data protection and privacy legislation and its oversight remain fit for purpose in the modern data economy. Key findings include that a large majority (83%) of authorities continue to oversee privacy protection in both the public and private sectors, with a minority of authorities (17%) primarily overseeing privacy protection practices solely in the public sector, maintaining the trend of the 2017 Census. Many also have additional roles beyond those mandated in data privacy or protection law, the most common being additional oversight of some form of Freedom of Information or Transparency law. Most authorities also have provisions in law for civil or administrative infringements, but far fewer have the same for criminal infringements. These additional functions are largely similar to those reported in 2017.

SECTION C: AUTHORITIES' FUNDING AND RESOURCES

This section focuses on the authorities' income and staff numbers. Member authorities are continuing to grow in terms of budget and personnel, with most of their changes pre-planned. When taken together with the 2017 data, this shows that overall budgets committed globally to data protection and privacy continue to grow, and the relative increases reported by members in this Census are also greater overall than in 2017. Currently, authorities' funding remains relatively centralised, with most allocated from central government. Increases in staff numbers also demonstrate that authorities are not just continuing to grow but are growing at an expanded rate.

SECTION D: AUTHORITIES' ENFORCEMENT POWERS, CASE HANDLING AND REPORTING

The section sets out the volumes of cases accepted for investigation/action and types of enforcement action and powers that can be applied, including authorities' powers to investigate and sanction civil or administrative infringements, as well as the powers they have in individual cases.

This section also covers case reporting and the fines or penalties imposed in cases of a breach of the law. The roles, as well as the pattern of responsibilities and activities, are similar to that reported in the 2017 Census. The numbers of cases reviewed vary significantly across authorities, reflecting the size of authorities and how long they have been established. Many authorities can make binding decisions, although nearly all (96%) are subject to appeals. Most authorities impose fines and penalties for a breach of data protection or privacy law. Compared to responses from 2017, the prevalence of the different powers in individual cases is similar, but public reporting on cases they handle has increased and more authorities now impose fines or penalties for breaching the law.

SECTION E: CROSS-BORDER DATA FLOWS, ENFORCEMENT AND COOPERATION

This section explores the authorities' participation in international enforcement cooperation and joint investigations. Authorities were asked about their requirements for dealing with evidence in coordinated or joint investigations, and any restrictions on cross-border transfer of information.

The responses showed that provision for cooperation and cross-border enforcement continues to be widespread among the authorities, with provisions in law and practical involvement in international cooperation remaining in similar numbers as in 2017. Most authorities take part in some way in international enforcement cooperation initiatives, and many have participated in joint investigations or cooperated in handling international complaints. There is a high participation across authorities in a range of enforcement cooperation networks or arrangements. Whilst the number of authorities participating in secondments has increased, also signalling an increasing focus on cooperation, it should be noted that this data reflects 2019 figures and the ongoing pandemic will likely impact that trend from 2020 onwards.

SECTION F: BREACH NOTIFICATION

This section asks about authorities' guidelines for voluntary and mandatory notifications. Most authorities reported that they have mandatory breach notification requirements in their jurisdiction, and many also have voluntary breach notification guidelines in place. While most of the authorities publish information on the breach notifications they receive, only one authority publishes this on their website.

SECTION G: OTHER MATTERS

This section focuses on authorities' engagement with the public and showed that, similarly to 2017, most authorities do not have a formal process for engagement with civil society, only a few authorities conducted a public opinion survey in 2019 (an increase from 2017) and half of the authorities publish their regulatory priorities.

INTRODUCTION

The GPA 2020 Census was created based on the 2019–2021 GPA strategic plan[2] which informs the vision and mission of the GPA as set out below. This is the second GPA census that has been conducted, the first dates from 2017 under a previous strategic plan. Comparisons have been made with the 2017 census in limited circumstances where relevant.

VISION OF GPA

An environment in which privacy and data protection authorities around the world are able effectively to act to fulfil their mandates, both individually and in concert, through diffusion of knowledge and supportive connections.

MISSION OF GPA

The Global Privacy Assembly seeks:

- To be an outstanding global forum for privacy and data protection authorities.
- To disseminate knowledge, and provide practical assistance, to help authorities more effectively to perform their mandates.
- To provide leadership at international level in data protection and privacy.
- To connect and support efforts at domestic and regional level, and in other international forums, to enable authorities better to protect and promote privacy and data protection.

The GPA seeks to achieve its Vision through cooperation, collaboration and capacity building to develop policy positions, guidance, tools and enforcement approaches aiming to provide consistency and predictability in the system of oversight as data continues to flow. This census provides a set of combined data to inform stakeholders about the policies and delivery approaches already in place in the authorities that guide/regulate data protection and privacy across 70 national jurisdictions whose authorities completed the survey.

2 http://globalprivacyassembly.org/wp-content/uploads/2019/11/GPA-Strategic-Plan-2019–2021.pdf

METHODOLOGY

The survey questions were developed in liaison with the GPA Working Groups, largely the Data Metrics Working Group, the International Enforcement Working Group and the Executive Committee's Strategic Direction Sub-Committee. The survey questionnaire was also consulted on with the GPA Secretariat (Chair Authority).

70 out of 130 members from all global regions represented in the GPA completed the survey, 2 respondents being supranational members. This represents a 54% return (counting 130 member authorities in total with. This compares to 87 member authorities of 114 who responded to the previous Census in 2017, 2 of these respondents were also supranational authorities. Analysis in the 2017 Census also considered using the figure of 85 members, depending on the applicability of the question to supranational members.

A regional breakdown of 2017 and 2020 responses can be found in Section A: Authority profiles. Different authorities responded to this census compared to 2017, which may have an effect on the results.

The survey was completed by each authority between 16 December 2020 and 12 February 2021. Authorities were asked to report on 2019 figures. Offline versions were made available to authorities who could not access the online survey platform and contributed to the overall results (full version available in Appendix 1).

Survey data was analysed initially at the total sample level, with responses among sub-groups explored where relevant. The report was drafted by Revealing Reality with input from the ICO GPA team, particularly on more technical aspects of the survey.

Authority profiles

Overview:

- 70 authorities from around the world participated in the Census. The majority are from Europe, but all continents are represented.
- Since the last Census in 2017, all authorities responding on this occasion have some presence online and all publish their annual reports.
- The most notable difference between 2017 and this Census is that the most common means of appointing the head of an authority is now appointment by executive, where in 2017 it was by election and ‘other’ methods.

REGION

70 authorities from all over the world answered the survey, covering the following regions:

- **40 from Europe**
- **7 from Africa and Middle East**
- **8 from North America**
- **5 from South or Central America**
- **3 from Oceania**
- **2 from Asia**
- **5 from other regions**

This indicated some differences from the responses obtained in the 2017 Census – where 85 authorities responded, 15 more than on this occasion. In 2017 the numbers from each region were as follows:

- **54 from Europe**
- **9 from Africa and Middle East**
- **12 from North America**
- **3 from South or Central America**
- **3 from Oceania**
- **3 from Asia**
- **1 from Other regions**

Please note that differences between 2017 and this latest Census, therefore, could be due to differences in the participants.

The Global Privacy Assembly has grown to 130 members and observers, many of which are data protection and privacy authorities, and more are joining each year. This increase in size reflects an expansion in data protection laws around the world. However, membership is not evenly spread across all regions as can be seen from the Conference's membership list. The census survey was only shared with GPA member authorities. The total return that could have been expected was therefore 130. However, the ongoing global pandemic is expected to have had some impact on reducing the rate of return for this second census.

Europe: including 25[3] from the European Union (EU) where the provisions of the General Data Protection Regulation (GDPR) apply[4]

Other regions: which include the Caribbean, British overseas territory and international organisations

3 Including at both federal and sub-national level

4 It should be noted that the 25 responses from EU countries, where the overarching GDPR applies, represents some 36% of overall responses to this survey. This may impact some of the data presented here.

DECADE OF ESTABLISHMENT

Most authorities have been established for many years, but the 2020 Census did include several recently established authorities.

YEAR OF ESTABLISHMENT – DECADES

Base: Total Census 2020 responses, n=70 authorities

PRESENCE ONLINE

All authorities have an online presence. A previous GPA Secretariat has built a 'Members Online' directory listing all websites and social media accounts given in census returns. This was the first major deliverable from the previous census. The GPA should consider revising this directory with the fresh census data.

ANNUAL REPORTS

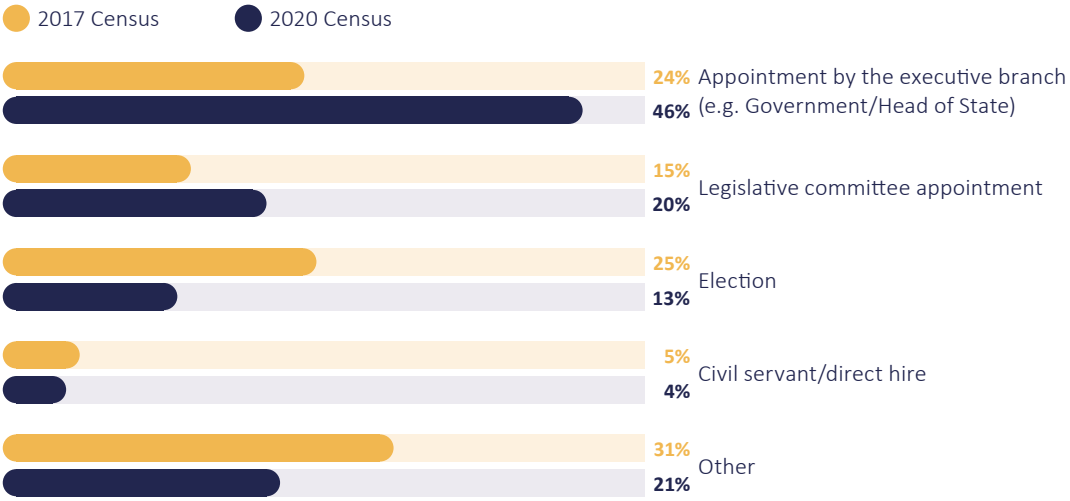
All authorities publish an annual report and most of them (80%) share this online (a list of links can be found in Appendix 4).

AUTHORITY LEADERSHIP

The most common way of appointing the head of the authority is by executive appointment (46%) (i.e. the current government/head of state appoints someone to the position), followed by appointment by legislative committee and 'other' approaches. The range of ways authorities appoint their head of authority is shown below:

AUTHORITY LEADERSHIP

How is the head of the authority appointed? (2017 to 2020)



Base: Total Census 2020 responses, n=70; Total Census 2017 responses, n=87.
Source: ICDPPC – Census Report 2017

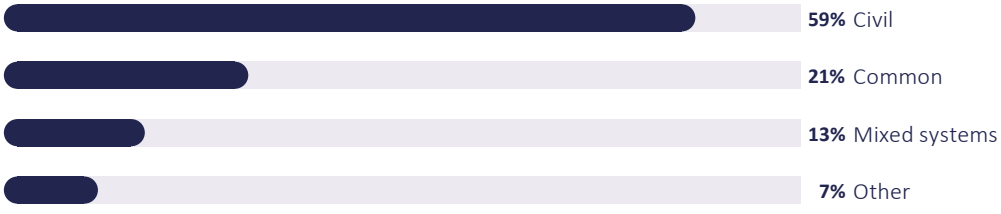
This shows a difference in how authority heads are appointed from the last census in 2017. Previously, the most common ways reported were 'other' and election, followed by executive appointment.

LEGAL SYSTEM

Most authorities have a civil legal system (59%), followed by a common legal system (21%), mixed systems (13%) or other (7%).

LEGAL SYSTEM

What is your nation's legal system?



Base: Total Census 2020 responses, n=70 authorities

Data protection law, jurisdiction & exemptions

Overview:

- On the whole, authorities continue to oversee privacy protection in the public and private sectors.
- Many have additional roles beyond those mandated in data privacy or protection law.
- Most authorities have provisions in law for civil/administrative infringements, but far fewer have the same for criminal infringements.

SECTOR OVERSIGHT

Most authorities oversee privacy protection practices in both the public and private sectors (83%). This is consistent with what was reported in the 2017 census. The remaining 17% primarily oversee privacy protection practices in the public sector, similar to 2017.

Authorities showing scope of activity only in the public sector are most likely to be sub-national authorities in countries with a federal state structure, where private sector regulation usually takes place at the national (federal) level.

A comfortable majority of authorities report that they don't have extra-territorial jurisdictional powers (59%).

Does the authority have extra–territorial jurisdiction?

	Yes (Y)	Yes (%)	No (N)	No (%)
Overall	**29**	**42**	**40**	**58**
Africa and Middle East	4	57	3	43
Asia	1	50	1	50
Europe	15	38	24	62
Europe (EU members)	13	52	12	48
Oceania	2	67	1	33
North America	4	50	4	50
South or Central America	1	20	4	80
Other	2	40	3	60

Please note that not all EU authorities consider themselves to have extra-territorial 'jurisdiction'. As one response noted: "It is unclear among Member States whether extra-territorial jurisdiction arises from the extra-territorial scope of the GDPR under Article 3 GDPR."

On the whole however, respondents indicated that they interpret provisions in GDPR to mean that all EU member state-based authorities have extra-territorial jurisdiction.

AVAILABILITY OF LAWS ONLINE

All authorities report that their data protection or privacy law is available online (list of links in Appendix 5). It is worth noting that it is not necessarily the DPA that makes this available, and often can be a parliamentary repository or similar.

Therefore, this question does not seem relevant for future censuses, as all laws are now online. However, it would be useful to ask instead whether the law is available in official translation in other languages than the local language (e.g. in EN, FR, ESP).

CONSTITUTIONAL REFERENCES

Most of the authorities (72%) said that there is a reference about data protection or privacy law in their country's constitution (detailed list in Appendix 3).

ADDITIONAL FUNCTIONS UNDER LAWS

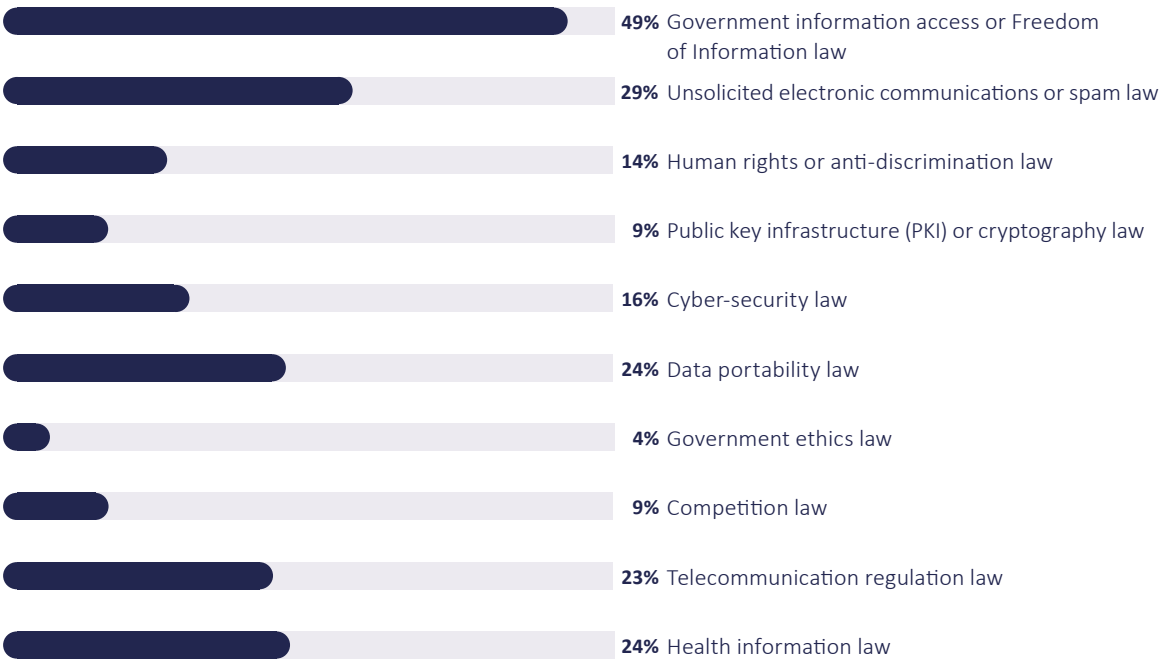
The most common 'extra role' undertaken by GPA members is managing government information access or Freedom of Information law (34 authorities).

This is followed by unsolicited electronic communications or spam law (20); supervising/ regulating data portability law (17); and health information law (17).

These additional functions are largely similar to those reported in 2017.

ADDITIONAL FUNCTIONS UNDER LAWS

In addition to roles under a data protection or privacy law, does the authority perform any functions under the following types of information, rights or accountability laws?



Base: Total Census 2020 responses, n=70 authorities

57 of the 70 authorities (81%) report having at least one of these extra roles.

EXEMPTIONS

Among the 57 authorities answering this question, three quarters (75%) report that their countries have a partial exemption in their applicable data protection/privacy law for State intelligence and security agencies, the other quarter (25%) have a complete exemption. These rates are the same as in 2017, even though the sample of authorities responding on this occasion is slightly different to 2017.

PROVISIONS ON CIVIL, ADMINISTRATIVE AND CRIMINAL INFRINGEMENTS

89%
Of authorities have provisions on civil/ administrative infringements (62 of 70).

37%
Of which only have these provisions (26 of 62).

57%
Fewer authorities have provisions on criminal infringements (40 of 70).

4
Authorities only have these provisions (i.e. none for civil/ administrative infringements).

4
Authorities do not have provisions in their data protection/privacy law for civil or criminal infringements.

Having these provisions in place does not necessarily mean authorities have the power to investigate.

LAW REFORM

The majority of authorities had revised their data protection or privacy law in the last 3 years (75%). This includes 93% of authorities who completed the census who are current EU members and are likely to be referring to changes in their law as a result of the GDPR (not all EU members have yet finalised their changes). Please note that the UK was still an EU member at the time of the census and as such has been included in data analysis.

Has your data protection or privacy law been revised in the last 3 years?

	Yes (N)	Yes (%)	No (N)	No (%)
Overall	**52**	**75**	**18**	**25**
Africa and Middle East	4	57	3	43
Asia	0	0	2	100
Europe	35	88	5	12
Europe (EU members)	23	92	2	8
Oceania	1	33	2	67
North America	4	50	4	50
South or Central America	5	100	0	0
Other	3	60	2	40

In 2017, 37% of authorities reported that their data protection or privacy law had been revised in the last 3 years, and 80% that the laws were currently being revised. Given that revisions reported in 2020 appear to be occurring in all regions—i.e. not confined only to EU members—this suggests that data protection and privacy laws are, on the whole, being updated and amended relatively regularly.

Authorities' funding & resources

Overview:

- On the whole, authorities are continuing to grow in terms of budget and personnel.
- Most of this change is pre-planned.
- Funding remains relatively centralised, with most allocated from central government.

TOTAL INCOME

The GPA Census gathered detailed information about authorities' total income in local currency. We have converted to USD for comparison[5].

Authorities reported a wide range of budgets, from <$40,000 to over $300,000,000. Please note this highest figure is more than three times the size of the second largest budget, removing this as an outlier results in a range of <$40,000 to ~$85,000,000, with a median budget for 2019 of $2.39 million USD. It should be noted here that a few authorities may receive budget for other enforcement mandates than those in the data protection and privacy domain alone, which may explain some of the higher budgets reported.

Budget range (USD)	(N)	(%)
Under 1 million	22	31
1 to 5 million	21	30
5 to 10 million	12	17
10 to 50 million	12	17
50+ million	2	3

CHANGE IN TOTAL BUDGET

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

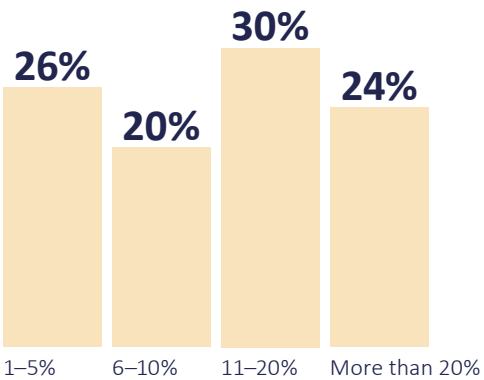
71%
50 authorities reported that their budget had increased.

10%
7 authorities reported a decrease.

19%
13 authorities reported no change.

INCREASE IN AUTHORITY BUDGETS

Among authorities whose budget increased in 2019



Base: Those authorities who reported their 2019 budget had increased, n=50

5 Conversions calculated based on rates from national currency to USD on 10 March 2021.

When compared with the 2017 data this shows that budgets continue to grow—in 2017 60% of authorities who responded to the survey reported increasing budgets.

The relative increases reported by authorities in this Census are also greater overall than in 2017.

year **2017**

Only **31%** of authorities with budget increases reported increases that were greater than **10%.**

year **2020**

In this census this was 54% (11–20% and more than 20% in the chart above).

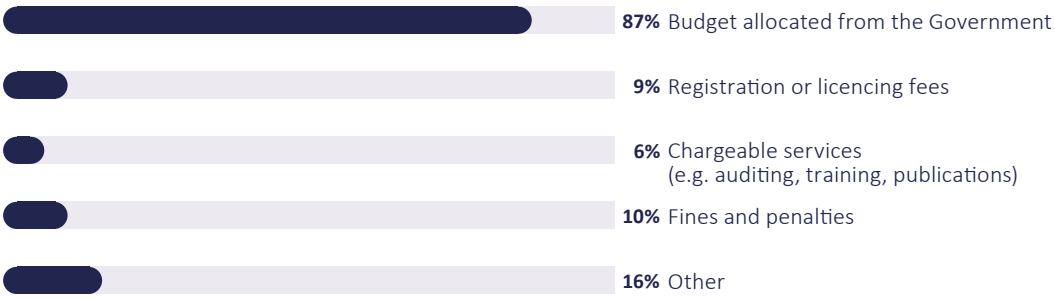
81% of those authorities experiencing an increase or decrease in their budget reported that these were pre-planned.

SOURCE OF INCOME/FUNDS

61 of the 70 authorities (87%) reported their funding comes from budget allocated from their respective governments. Additional income sources include registration or licensing fees, chargeable services, fines and penalties and 'other' sources.

FUNDING SOURCES

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



Base: Total Census 2020 responses, n=70 authorities

Most other sources of income were reported by authorities who also receive budget allocated from Government. 'Other' sources include income such as bank interest and funding from international organisations.

STAFF NUMBERS

The GPA census asked for precise information about the number of staff that each authority has, and it was measured in full time equivalent (FTE) employees.

Authorities range significantly in size, with total FTE staff ranging from 2 to over 1,000. The median number of staff was 46.

46 of the authorities (66%) reported having increased the number of staff they have, while 3 (4%) reported reducing the number. As with budgetary changes, the vast majority of the authorities who had changed staff numbers reported that the changes were pre-planned (90%).

Compared to 2017, these numbers suggest that authorities are not just continuing to grow but grow at an expanded rate (in 2017, just 42% had increased their number of staff). Although please note that the sample of authorities responding to this census is slightly different to 2017.

Full-time staff (ranges)	(N)	(%)
Less than 10	10	14
10 to 49	27	39
50 to 99	14	20
100 to 249	13	19
250+	6	9

Authorities' enforcement powers, case handling and reporting

Overview:

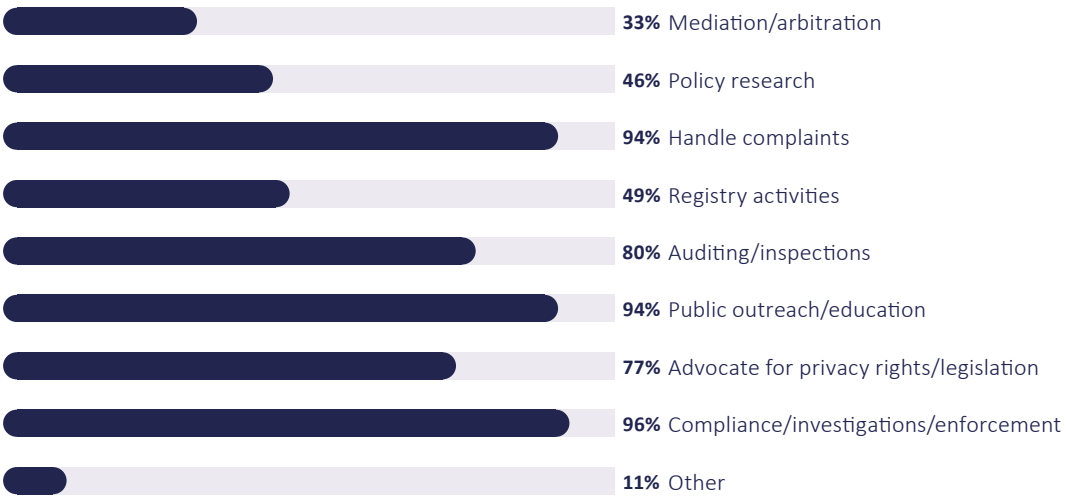
- The vast majority of authorities are able to make binding decisions, although they are subject to appeals where appropriate.
- Numbers of cases reviewed vary significantly, reflecting the size of authorities and how long some of them have been established for.
- A majority of authorities impose fines and penalties for a breach of data protection or privacy law.

ROLES OF THE AUTHORITY

In line with the 2017 Census, nearly all authorities responding to this census have the role of 'compliance/investigation/enforcement' (96%), 'handling complaints' (94%) and 'public outreach/education' (94%).

AUTHORITY ROLES

What are the principal roles performed by the authority under the privacy or data protection law



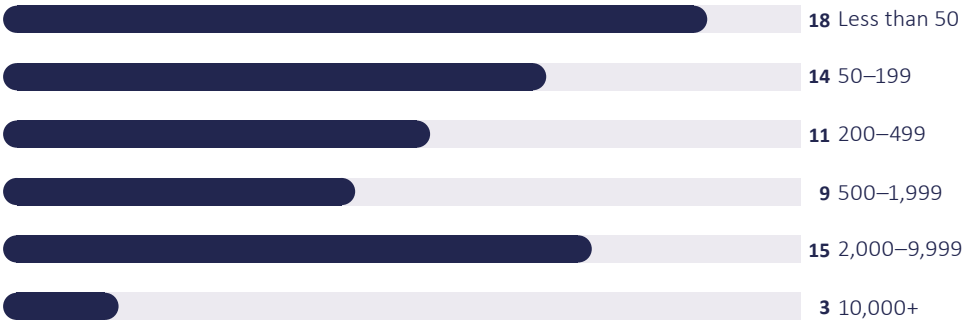
Base: Total Census 2020 responses, n=70 authorities

This pattern of responsibilities and activities is similar to what was reported in the 2017 Census, suggesting authorities have not, on the whole, dramatically changed or increased the scope of their work over the past few years.

CASES ACCEPTED FOR INVESTIGATION

Authorities were asked how many cases they accepted for investigation in 2019. The results suggest that authorities had interpreted the question differently compared with the 2017 Census, but cases investigated range from 0 to over 50,000.

NUMBER OF CASES ACCEPTED FOR INVESTIGATION



Base: Total Census 2020 responses, n=70 authorities

It is worth noting that the term 'investigate' could be interpreted slightly differently in different authorities. Larger authorities tend to deal with more cases, but a notable variation among each size band (based on number of staff) suggests it may be helpful to provide more categorisation of the term 'investigate' in a future Census.

Number of cases accepted for investigation	Number of staff (range)					
	Less than 10	**10–49**	**50–99**	**100–249**	**250+**	**Grand Total**
Less than 50	7	5	2	2	2	18
50–199	1	8	3	2	-	14
200–499	2	6	1	1	1	11
500–1,999	-	6	1	2	-	9
2,000–9,999	-	2	6	5	2	15
10,000+	-	-	1	1	1	3
Grand Total	10	27	14	13	6	70

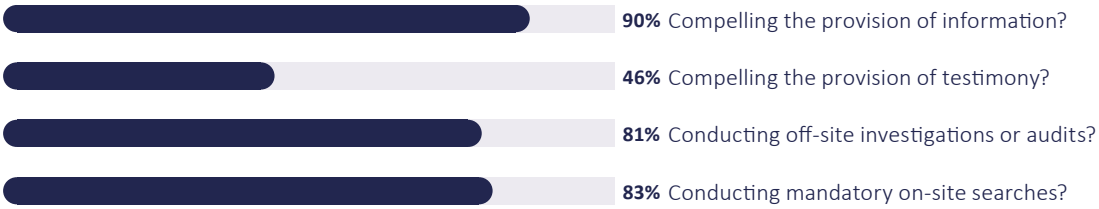
INVESTIGATION AND SANCTIONING POWERS

66 of the 70 authorities (92%) have the power to investigate and sanction civil/administrative infringements of their data protection or privacy law.

The vast majority of authorities (90%) also have the investigatory power to compel provision of information, 83% of authorities have the power of conducting mandatory on-site searches and 81% of conducting off-site investigations. 46% have the power to compel testimony.

INVESTIGATORY POWERS

Does the authority have any of these…

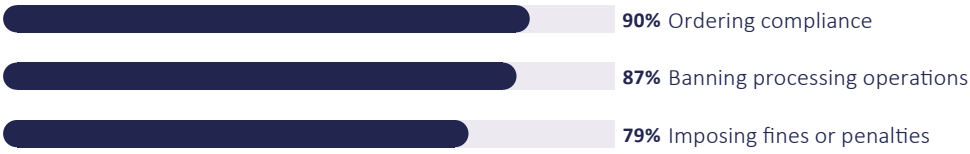


Base: Total Census 2020 responses, n=70 authorities

Most of the authorities responding to the survey have a range of sanctioning powers available to them: ordering compliance, banning processing operations and imposing fines or penalties.

SANCTIONING POWERS

Does the authority have any of these…



Base: Total Census 2020 responses, n=70 authorities

Over half the authorities responding to the census have the power to bring infringements of their data protection or privacy law to court (59%). However, most of the authorities (79%) report that they do not have the powers to investigate and sanction criminal infringement of their data protection or privacy law.

It is worth noting that this could be interpreted in a number of ways by authorities – potentially highlighting a distinction between civil/administrative infringements and criminal infringements, or where an authority can take court action but it is the responsibility of a different body to progress cases.

POWERS IN INDIVIDUAL CASES

The vast majority of authorities responding to the census have the power to make binding decisions in individual cases (86%), make recommendations (97%) and to refer to another authority with decision-making powers (79%).

The prevalence of these different powers is similar to that reported in 2017.

APPEALS

96% of the authorities surveyed confirmed that their decisions or recommendations are subject to appeal to another body. This is very similar to what was reported in the 2017 census (92%).

CASE REPORTING

53 authorities (76% of those surveyed) report publicly on cases they handle, although only 22 (43%) upload their case reports to a central repository such as an online legal information institute. This is an increase from 2017, when 65% of authorities indicated that they report publicly on cases they handle. At the time it was suggested that there was room for improvement in this regard and the 2020 data suggests authorities are taking this on board, although it should be noted the sample of authorities responding on this occasion is slightly different to 2017.

Most authorities publicly name organisations that have breached the privacy or data protection law (77%), however, almost a quarter (23%) still do not have these powers.

FINES AND PENALTIES

A majority of authorities (76% of those surveyed) impose fines or penalties for a breach of the law. This is another increase from 2017, where only 56% of authorities reported having this power.

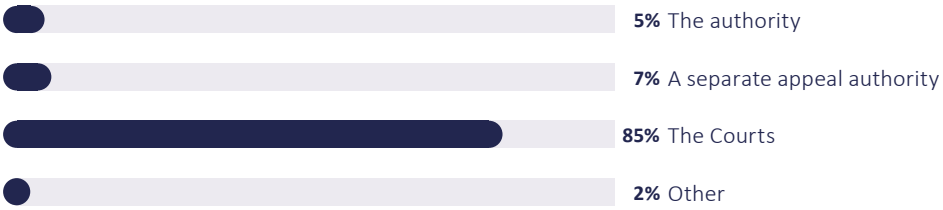
Of those who do impose fines or penalties, only a small number keep all (6%) or part of (9%) the fine. 85% do not keep any of the fine. In the 2017 census, 56% of the authorities reported that they imposed fines or penalties, and 71% of these did not keep any of the fine, suggesting this has become less common.

59% of the authorities reported that their data protection or privacy law provides for the award of compensation caused by breach of the legislation.

When it comes to awarding this compensation, in the majority of cases this falls to the courts in the relevant regulated jurisdiction. In a small number of cases the authority itself or a separate appeal authority award the compensation.

WHICH BODY HAS THE POWER TO AWARD COMPENSATION?

Among those whose data protection or privacy law provides for the award of compensation caused by a breach of the legislation



Base: Those whose data protection or privacy law provides for the award of compensation caused by a breach of legislation, n=41 authorities

SIZE OF FINES AND NUMBER OF ORGANISATIONS NAMED

The Census also asked for the largest size of fines imposed and the numbers of organisations named for breaching laws.

The largest fines that authorities imposed ranged from US$1 to US$5,000,000,000.

In total, authorities reported that they had publicly named 563 organisations for breaching data protection or privacy law.

Cross-border data flows, enforcement & cooperation

Overview:

- Provision for cooperation and cross-border enforcement is widespread among the authorities who responded to this Census.
- Most authorities can take part in some way in international enforcement cooperation initiatives, and many have participated in joint investigations or cooperated in international complaints.
- There is a high level of participation across authorities in a range of enforcement cooperation networks or arrangements.

Cooperation is now an important aspect of managing data privacy and protection activities for many countries. The census explored this topic with authorities in terms of their experience of, and provisions for, participating in cross-national enforcement activities.

Provisions for, or engagement in, activities around enforcement and cooperation remain the same or have increased since the last Census. This trend suggests that cross-border cooperation is increasingly important for authorities and there is a high level of willingness to engage with other authorities in achieving shared data protection and privacy goals.

Please note, in this section of the report answers from global organisations have been discounted.

PARTICIPATION IN INTERNATIONAL ENFORCEMENT COOPERATION

In terms of international enforcement cooperation initiatives that authorities can take part in, almost all (96%) authorities can share non-confidential/non personal data.

90% of authorities responding to the survey can take a joint action with another authority (not including the sharing of confidential/personal information).

74% of the authorities can also share confidential/personal information for separate but coordinated investigations by each authority.

76% can share confidential/personal information for joint investigations by both/all authorities.

Of the 18 authorities who report they are not able to share confidential/personal information, 11 provided some more information. There was no specific answer that was consistent across all or many of these authorities. Examples provided include:

- There being no explicit authority in legislation with which the authority can share information
- The agency not having powers for that exchange of data
- Sub-national bodies may not be able to collaborate directly with other national bodies (as such collaboration is reserved for the remit of the federal authority)
- Competencies and powers of the authorities regulated by 'special regulations'
- Privacy statutes not containing explicit provisions allowing the sharing of confidential or personal information with other authorities
- Confidentiality provisions not explicitly authorizing such disclosures

For those who can share confidential/personal information in these circumstances, GDPR law is often cited by EU members as providing the appropriate legal basis for authorities to share information. Others refer to:

- The importance of a valid legal basis
- Bilateral and multilateral agreements
- Practical barriers such as time and budget
- Procedures for determining sharing confidential/personal information still to be established (e.g. for new authorities)
- The authority having the power to define forms of exchange of confidential information

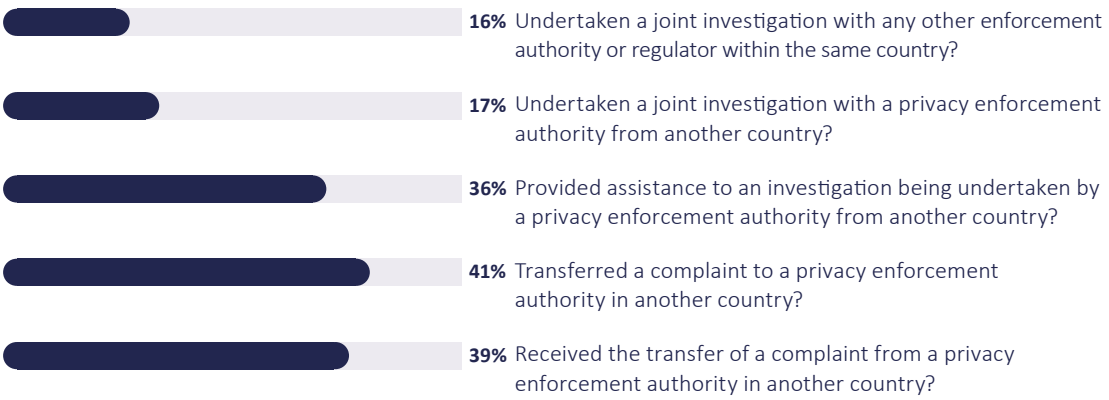
RECENT PARTICIPATION IN JOINT INVESTIGATIONS OR COOPERATING IN INTERNATIONAL COMPLAINTS

The Census asked whether authorities had been involved in any of the typical incidents of cross-border enforcement cooperation in 2019. Many have transferred a complaint to a privacy enforcement authority in another country, received the transfer of a complaint from a privacy enforcement authority in another country or provided assistance to an investigation being undertaken by a privacy enforcement authority from another country. This pattern of participation is similar to 2017.

The chart below shows the numbers for each:

PARTICIPATION IN JOINT INVESTIGATIONS AND INTERNATIONAL COMPLAINTS

Has the authority...



Base: Total Census 2020 responses, n=70 authorities

PROVISIONS WITHIN THE PRIVACY OR DATA PROTECTION LAW

74% of the authorities responding to the census have provisions in their privacy or data protection law for assisting other privacy enforcement authorities in cross-border investigations.

20% of the authorities have a prohibition on providing information to other enforcement authorities. Interestingly, this number has increased from 2017, when 11% of authorities had this prohibition.

57% of respondents reported that their privacy or data protection law includes express provision for transfer of complaints to privacy enforcement authorities in other jurisdictions. This has increased from 32% of authorities who reported this in 2017. Please note that this is higher than the number who report they have transferred a complaint (see previous chart). This may be because the provision exists in law, but has not been implemented. Please note, the sample of authorities responding to this Census was slightly different to 2017.

59% of the authorities responding to the census reported that their privacy or data protection law allows for disclosure of information obtained in investigations to privacy enforcement authorities in other jurisdictions. This represents an increase from 2017, when only 29% of respondents' laws allowed this type of disclosure.

DISCLOSURE OF CONFIDENTIAL INFORMATION

51% of authorities responded that their laws contain provisions that determine when and how confidential information held by a privacy or data protection authority can be disclosed or shared.

LEGAL/PRACTICAL REQUIREMENTS TO DEAL WITH EVIDENCE IN COORDINATED/JOINT INVESTIGATIONS

61% of respondents don't have specific legal and/or practical requirements for the gathering and handling of evidence in coordinated or joint investigations.

LEGAL PROVISIONS OF THE JURISDICTION ON DATA LOCALISATION AND RESTRICTING CROSS-BORDER TRANSFERS

Most of the authorities who responded to the census (83%) have laws in place that restrict private sector organisations or public sector entities from making cross-border transfers of personal information. In almost all cases (95%), the authority has the role of enforcing such laws.

Although the laws of most jurisdictions (73%) do not require data processing facilities to be located within the same jurisdiction.

PROCESS FOR FORMALLY RECOGNISING OTHER JURISDICTIONS

For most of the authorities (61%), their data protection or privacy law established a process for formally recognising other jurisdictions that have laws establishing comparable data protection standards. This has increased from the 49% of authorities who had such a process in 2017.

Most authorities perform at least some role in that recognition process (74%), similar to the 80% of authorities who did in 2017.

SECONDMENTS

Most authorities (79%) reported they did not participate in any secondment with another privacy enforcement authority in 2019. However, the 21% of authorities who are participating in secondments is higher than the 12% who reported this in the 2017 census. Please note that the list of authorities responding to this census is different to 2017.

This shows that participation in secondments could become an increasing trend and should continue to be monitored with this census in years to come.

PARTICIPATION IN ENFORCEMENT COOPERATION NETWORKS OR ARRANGEMENTS

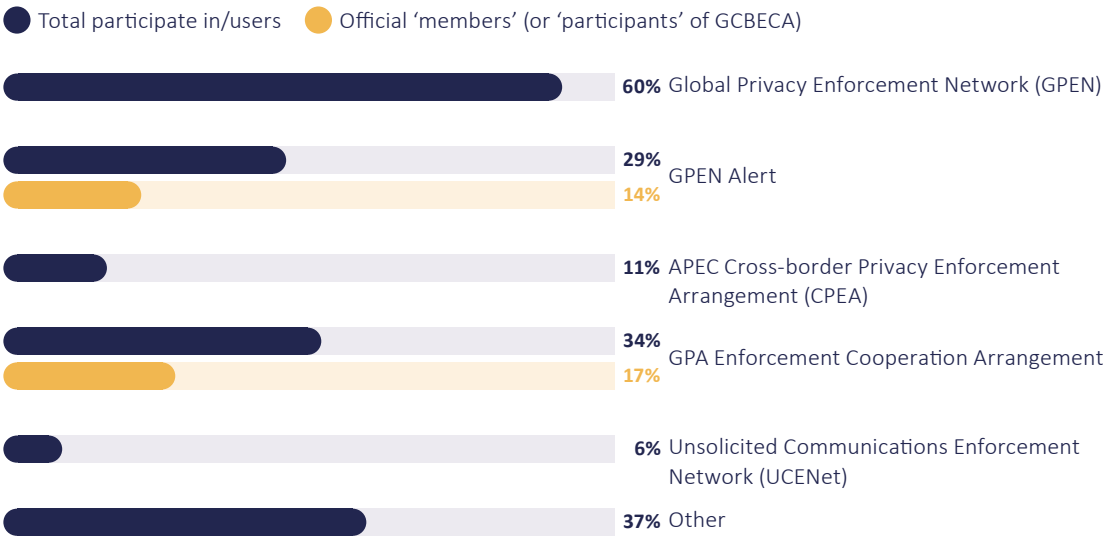
Authorities were asked if they participated in any of five named enforcement cooperation networks or arrangements. 42 authorities participated in the Global Privacy Enforcement Network. 12 authorities who are official participants of the GPA's own enforcement cooperation arrangement known as the GCBECA responded to the census. A further 12 authorities indicated they had also participated in this group, possibly referring to the GPA's International Enforcement Cooperation Working Group. The level of involvement from authorities demonstrates the GPA has a very active enforcement cooperation community, and is supported in several ways to engage with each other through different tools and mechanisms.

20 authorities reported that they participate in the GPEN Alert, including 10 of the 12 official current members. This suggests that beyond the official current members, authorities may be engaging with GPEN and possibly using GPEN's discussion forum for cooperation purposes. This may suggest there is appetite for further participation and joining the GPEN Alert tool could prove beneficial for authorities wanting to further their enforcement cooperation capabilities. Fewer authorities reported that they participated in the APEC Cross border Privacy Enforcement Arrangement (CPEA) and the unsolicited communications enforcement network (UCENet).

The pattern of participation shows the same trend as the 2017 Census, and, like 2017, this indicates that these additional fora provide useful networks for authorities to progress their interests and develop relationships with each other.

PARTICIPATION IN ENFORCEMENT COOPERATION NETWORKS OR ARRANGEMENTS

Which of these does the authority participate in?



Base: Total Census 2020 responses, n=70 authorities

'Other' networks and arrangements that were mentioned include: Association Francophone des Autorités de protection des Données Personnelles (AFAPDP), European Data Protection Board, Common Thread Network. A full list of the networks that were mentioned can be found in Appendix 6.

ENFORCEMENT ROLES IN SUPRA-NATIONAL ARRANGEMENTS

As was seen in the 2017 Census, authorities sometimes perform an enforcement role under supra-national arrangements, such as the following:

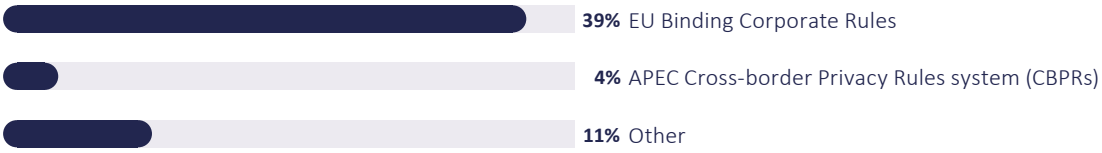
- EU Binding Corporate Rules
- APEC Cross Border Privacy Rules (CBPR) system
- Other[6]

The supra-national arrangements that were presented differ from the 2017 Census, but a detailed list of the authorities' responses can be found in the footnote.

6 'Other' enforcement roles that the authorities performed were under these arrangements: Council of Europe's Convention 108, the Gibraltar Binding Corporate Rules, the State Data Protection Inspectorate of Lithuania issues authorisations for personal data transfer to third countries in their GDPR, and the Information and Data Protection Commissioner of the Republic of Albania under decision No.8 and Instruction No.41.

ENFORCEMENT ROLES IN SUPRA-NATIONAL ARRANGEMENTS

Does the authority perform an enforcement role under any of these supra-national arrangements?



Base: Total Census 2020 responses, n=70 authorities

BILATERAL ARRANGEMENTS WITH DPAs IN OTHER COUNTRIES

Authorities were asked about bilateral arrangements that they have negotiated themselves, and 34% have such arrangements in place, similar to the 32% of authorities which had these in 2017.

MECHANISMS FOR COOPERATING WITH OTHER REGULATORY AUTHORITIES

Authorities were asked what cooperation mechanisms they can make use of. 61% of authorities can make use of a mechanism for cooperating with other regulatory authorities.

Most authorities can cooperate through:

- Membership of enforcement cooperation networks (85%);
- Bi-lateral non-binding arrangements (80%);
- Multi-lateral non-binding arrangements (76%).

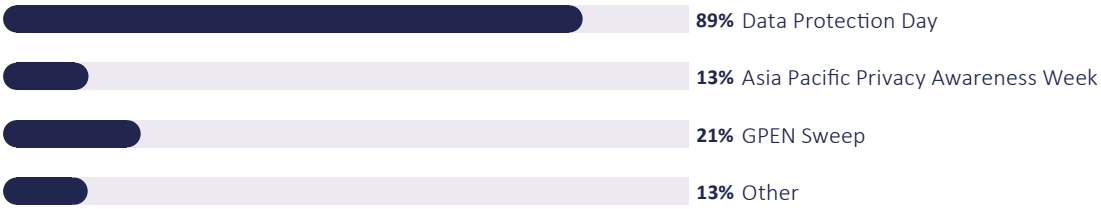
On the other hand, multi-lateral binding and enforceable agreements, and bi-lateral binding and enforceable agreements were less common (49% each).

INVOLVEMENT IN EFFORTS TO RAISE AWARENESS OF PRIVACY AND DATA PROTECTION

62 authorities have been involved with the International Data Protection Day (28 January) as part of coordinated efforts between countries to raise awareness of privacy and data protection. 15 authorities took part in the GPEN Sweep, 9 authorities took part in Asia Pacific Privacy Awareness week and 9 authorities participated in other awareness raising initiatives. Participation in these initiatives shows the same trend as results from the 2017 census.

INVOLVEMENT IN EFFORTS TO RAISE AWARENESS OF PRIVACY AND DATA PROTECTION

Has your authority been involved with the following coordinated efforts to raise awareness of privacy and data protection?



Total Census 2020 responses, n=70 authorities

22 (31%) participated in more than one awareness-raising effort, and only 4 (6%) authorities responding to the census didn't participate in any such efforts.

Breach notification

Overview:

- Most authorities have mandatory breach notification requirements in their jurisdiction, and many also have voluntary breach notification guidelines in place.
- Although most of the authorities publish information on the breach notifications they receive, only 1 authority does this in their website.

GUIDELINES FOR VOLUNTARY NOTIFICATIONS

30 of the 70 authorities responding (43%) reported that there are voluntary breach notification guidelines issued in their jurisdiction, a slight increase from 2017 (36%).

The vast majority (26) of authorities who issue guidelines for voluntary breach notifications recommend that both the data subject and the authority are notified; 2 authorities recommend notifying only the data subject and the other 2 authorities to only notify the authority. This shows the same trend as 2017, although the sample is slightly different for this Census.

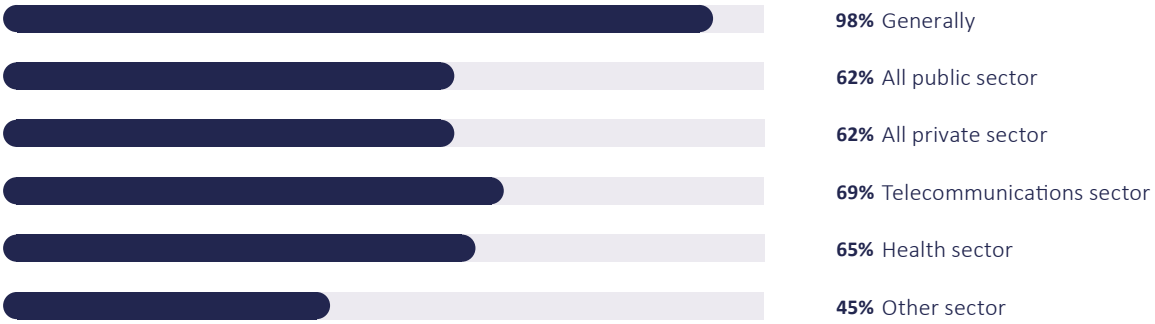
REQUIREMENTS FOR MANDATORY NOTIFICATIONS

79% authorities have mandatory breach notifications requirements in their jurisdiction, but 21% still do not. The latter number is reducing from 2017.

On the whole, mandatory breach notifications requirements apply to all sectors, but there is some variation:

REQUIREMENTS FOR MANDATORY NOTIFICATIONS

Where do the mandatory breach notification requirements apply?



Base: Those authorities who have mandatory breach notifications requirements, n=55 authorities

The pattern of where mandatory breach notification requirements apply have changed slightly from 2017, where it was more predominant in the telecommunications sector, followed by generally, all public sector, the health sector and all private sector.

As with voluntary breach notifications and in line with the 2017 census, the vast majority of authorities who require mandatory breach notifications (87%) recommend that both the data subject and the authority themselves are notified.

PUBLICATION OF BREACH NOTIFICATIONS

Most of the authorities publish information on the breach notifications they receive (74%), but only one authority, the USA's Federal Trade Commission, reported that it publishes it on its website. The publication of the breach notifications has increased since 2017, when 48% reported they published this.

Other matters

ENGAGEMENT WITH CIVIL SOCIETY

Similarly to 2017, 49 authorities (70%) do not have a formal process for engagement with civil society.

PUBLIC OPINION SURVEYS

Only 16 (23%) of the 70 authorities conducted a public opinion survey in 2019, which has increased slightly from 2017.

PUBLICATION OF REGULATORY PRIORITIES

Half of the authorities (35 out of 70) reported that they publish their regulatory priorities.

Appendix

Appendix 1 – Census questions (French and Spanish versions were also used)

GPA
Global Privacy Assembly

GPA Census 2020

All GPA member authorities are requested to complete this survey which will provide a comprehensive snapshot of Data Protection and Privacy Authorities in 2020.

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 12 February 2020.
- Only one response per member authority.
- 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 2019, as the most recent complete year. Please answer such questions with information relating either to the calendar year 2019 or, where more convenient, the most recently completed financial year for which you have figures.
- Please attempt to complete all questions. However, if you are not able to answer a question please move on to the following questions and submit the incomplete response.

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 55 questions in 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) Country/economy:
c) Please indicate the region in which the authority is located:
   a. Africa and Middle East
   b. Asia
   c. Europe
   d. Oceania
   e. North America
   f. South or Central America
   g. Other
d) Year of establishment:
e) What is (are) the primary language(s) of your authority? If applicable, what is (are) the secondary language(s) of your authority?

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

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

   i. Website link or user name: …
   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 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? Yes/No
   b. Common? Yes/No
   c. Mixed systems? Yes/No

If Yes, please specify.

d. Other? Yes/No
If Yes, please specify.

B. Data protection law, jurisdiction and exemptions

1. Does the authority oversee privacy protection practices by:
    a. Only the public sector?
    b. Only the private sector?
    c. Both public and private sectors?

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

3. Is 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 data protection or privacy? Yes/No

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

5. In addition to roles under a 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

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?

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. Has your data protection or privacy law been revised in the last 3 years? Yes/No

C. Authority's funding and resources

1. What was your total budget/ income for 2019 in your national currency? (no decimals, please do not put commas or dots to differentiate thousands)

	Income	Currency
2019		

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 this pre-planned or did external factors have a bearing on this?
    a. Pre-planned
    b. Unplanned.

6(a) If unplanned and due to recent external factors please briefly specify reasons.

7. What is your nation's Gross Domestic Product?

8. Would there be any obstacles for your authority in receiving funds from membership fees in the event the Assembly established a funded Secretariat? Yes/ No

    If yes, please select which obstacle(s) from the list below:
    a. Authority's internal constitution or other governance arrangements with Government
    b. Primary legislation
    c. Secondary legislation
    d. Other (please specify)

9. Would there be any obstacle for your authority in disbursing funds for the payment for a membership fee to fund the GPA Secretariat? Yes/ No

    9(a) If yes, please specify:
        i. Budgetary constraints
        ii. Authority's internal constitution or other governance arrangements with Government
        iii. Primary legislation
        iv. Secondary legislation
        v. Other (please specify)

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 accept for investigation in 2019?

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

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

   8.a How many cases were taken on appeal in 2019?

9. Does the authority report publicly on cases it has handled? Yes/No
   If YES:

9.a How many case reports were released in the last year?	
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)?	Yes/No

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

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

    10 (a) If yes, does the authority keep:
    b. all of the fine
    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 in 2019

11. Does your data protection or privacy law provide for the award of compensation caused by breach of the legislation
    Yes/No

12. Which body 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 2019 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 information to other enforcement authorities? Yes/No

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 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. In 2019, has the authority participated in a secondment with another privacy enforcement authority? Yes/No

7. 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. GPA Enforcement Cooperation Arrangement Yes/No
   e. Unsolicited Communications Enforcement Network (UCENet) Yes/No
   f. Other

   Please specify

8. 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)

9. 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

10. Does the authority have any mechanism for cooperating with other regulatory authorities (e.g. consumer protection authorities)?
Yes/No/Not applicable

11. 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

12. In 2019, has your authority been involved with the following coordinated efforts, involving authorities from many countries, to raise awareness of privacy and data protection:
    a. Data Protection Day
    b. Asia Pacific Privacy Awareness Week
    c. GPEN Sweep
    d. Other

13. 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

13a 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)
13b 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)

14. In 2019, has the authority (select all that apply):

a. Undertaken a joint investigation with any other enforcement authority or regulator within the same country?	
b. Undertaken a joint investigation with a privacy enforcement authority from another country?	
c. Provided assistance to an investigation being undertaken by a privacy enforcement authority from another country?	
d. Transferred a complaint to a privacy enforcement authority in another country?	
e. Received the transfer of a complaint from a privacy enforcement authority in another country?	

15. 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. the authority
   - iii. both the data subject and the 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

2.b Do mandatory breach notification requirements recommend notification to:

i. the data subject
ii. the authority
iii. both the data subject and the 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 2019?

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

	Select all that apply	URL/Hyperlink/Name
Authority's annual report		
Authority's website		
Other:		
Other:		
Other:		

G. Other matters

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

- 2.a If yes, please specify:

2. Did the Authority conduct a public opinion survey in 2019?

- 3.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.

END

Appendix 2 – Authorities' social media sites

All social media sites for the GPA members can be found online here:
https://globalprivacyassembly.org/participation-in-the-assembly/members-online/

Appendix 3 – Authorities' constitutional references

Authority name	Country / economy	Constitutional reference
Ombudsman	Cayman Islands	Private and family life 9.—(1) Government shall respect every person's private and family life, his or her home and his or her correspondence. (2) Except with his or her own consent or as permitted under subsection (3), no person shall be subjected to the search of his or her person or his or her property or the entry of persons on his or her premises. (3) Nothing in any law or done under its authority shall be held to contravene this section to the extent that it is reasonably justifiable in a democratic society— (a) in the interests of defence, public safety, public order, public morality, public health, town and country planning, or the development or utilisation of any other property in such a manner as to promote the public benefit; (b) for the purpose of protecting the rights and freedoms of other persons; (c) to enable an agent of the Government or a public body established by law to enter on the premises of any person in order to inspect those premises or anything on them for the purpose of any tax, rate or due or in order to carry out work connected with any property that is lawfully on those premises and that belongs to the Government or that public body; (d) to authorise, for the purpose of enforcing the judgment or order of a court, the search of any person or property by order of a court or the entry on any premises by such order; or (e) to regulate the right to enter or remain in the Cayman Islands.
Commission de l'Informatique et des Libertés	Burkina Faso	article 2 de la constitution du 2 juin 1991 du Burkina Faso reconnait le droit à la vie privé
Autorité de Protection des Données à caractère	Mali	Le domicile, le domaine, la vie privée et familiale, le secret de la correspondance et des communications sont inviolables. Il ne peut y être porté atteinte que dans les conditions prévues par la loi.

Personnel (APDP)		
Persónuvernd - Icelandic Data Protection Authority	Iceland	Article 71 of the Icelandic Constitution: https://www.government.is/lisalib/getfile.aspx?itemid=71b52917-fd28-11e7-9423-005056bc4d74
Autoridad Nacional de Protección de Datos Personales	Perú	Artículo 2,numeral 6, de la Constitución Política del Perú
The Hessian Commissioner for Data Protection and Freedom of Information	Germany, Hesse	There is no explicit reference to data protection or data privacy in our country's constitution, the Basic Law for the Federal Republic of Germany. However, the protection of personal data is recognized as part of the right to informational self-determination, which is derived from Article 2(1) in conjunction with Article 1(1) of the Basic Law of the Federal Republic of Germany. On occasion of the 1983 census, the German Federal Constitutional Court ruled that "[...] in the context of modern data processing, the protection of the individual against unlimited collection, storage, use and disclosure of his/her personal data is encompassed by the general personal rights of the German constitution. This basic right warrants in this respect the capacity of the individual to determine in principle the disclosure and use of his/her personal data. Limitations to this informational self-determination are allowed only in case of overriding public interest."
Agência Nacional de Protecção de Dados Pessoais	São Tomé e Príncipe	Artigo 24 - Direito à Identidade e à Intimidade Artigo 25 - Inviolabilidade do domicílio e da correspondência Artigo 27- Liberdade de Consciência, de Religião e do Culto
Landesbeauftragte für Datenschutz und Informationsfreiheit Nordrhein-Westfalen (North Rhine-Westphalia Commissioner for Data Protection and Freedom of Information)	North Rhine-Westphalia (Germany)	Article 4 (2) Verfassung für das Land Nordrhein-Westfalen https://recht.nrw.de/lmi/owa/br_bes_detail?sg=0&menu=1&bes_id=3321&anw_nr=2&aufgehoben=N&det_id=462326

Turkish Personal Protection Authority	Turkey	IV. Privacy and protection of private life A. Privacy of private life ARTICLE 20- Everyone has the right to demand respect for his/her private and family life. Privacy of private or family life shall not be violated. (Sentence repealed on May 3, 2001; Act No. 4709) (As amended on October 3, 2001; Act No. 4709) Unless there exists a decision duly given by a judge on one or several of the grounds of national security, public order, prevention of crime, protection of public health and public morals, or protection of the rights and freedoms of others, or unless there exists a written order of an agency authorized by law, in cases where delay is prejudicial, again on the above-mentioned grounds, neither the person, nor the private papers, nor belongings of an individual shall be searched nor shall they be seized. The decision of the competent authority shall be submitted for the approval of the judge having jurisdiction within twenty-four hours. The judge shall announce his decision within forty-eight hours from the time of seizure; otherwise, seizure shall automatically be lifted. (Paragraph added on September 12, 2010; Act No. 5982) Everyone has the right to request the protection of his/her personal data. This right includes being informed of, having access to and requesting the correction and deletion of his/her personal data, and to be informed whether these are used in consistency with envisaged objectives. Personal data can be processed only in cases envisaged by law or by the person's explicit consent. The principles and procedures regarding the protection of personal data shall be laid down in law.
Information and Data Protection Commissioner	Albania	Article 35 of the Constitution 1. No one may be obliged, except when the law requires it, to make public the data connected with his person. 2. The collection, use and making public of data about a person is done with his consent, except for the cases provided by law. 3. Everyone has the right to become acquainted with data collected about him, except for the cases provided by law. 4. Everyone has the right to request the correction or expunging of untrue or incomplete data or data collected in violation of law.
The Office for Personal Data Protection of	Slovak Republic	Please see Art. 16 of the Constitution of the Slovak Republic https://www.prezident.sk/upload-files/46422.pdf

the Slovak Republic		
Préposé fédéral à la protection des données et à la transparence (PFPDT)	Suisse	Art. 13 Protection de la sphère privée 1 Toute personne a droit au respect de sa vie privée et familiale, de son domicile, de sa correspondance et des relations qu'elle établit par la poste et les télécommunications. 2 Toute personne a le droit d'être protégée contre l'emploi abusif des données qui la concernent.
Gibraltar Regulatory Authority ('GRA')	Gibraltar	The Gibraltar Constitution Order 2006 ("Constitution"): The Constitution provides for the protection for privacy of home as a fundamental right and freedom. See for example section 1(c) of Chapter 1 of the Constitution, found here: https://www.gibraltarlaws.gov.gi/papers/gibraltar-constitution-order-2006-6
Superintendencia de Industria y Comercio	República de Colombia	Artículo 15 de la Constitución Política de Colombia 1991
Centro de Protección de Datos Personales	Argentina	La Constitución de la Ciudad Autónoma de Buenos Aires ha legislado en su art. 16 la acción de hábeas data en forma más amplia: "Toda persona tiene, mediante una acción de amparo, libre acceso a todo registro, archivo o banco de datos que conste en organismos públicos o en los privados destinados a proveer informes, a fin de conocer cualquier asiento sobre su persona, su fuente, origen, finalidad o uso que del mismo se haga. También puede requerir su actualización, rectificación, confidencialidad o supresión, cuando esa información lesione o restrinja algún derecho. El ejercicio de este derecho no afecta el secreto de la fuente de información periodística". Y también es su art. 13 inc. 8 "La Ciudad garantiza la libertad de sus habitantes como parte de la inviolable dignidad de las personas. Los funcionarios se atienen estrictamente a las siguientes reglas: 8. El allanamiento de domicilio, las escuchas telefónicas, el secuestro de papeles y correspondencia o información personal almacenada, sólo pueden ser ordenados por el juez competente".
European Data Protection Supervisor (EDPS)	International Organisation	The protection of natural persons in relation to the processing of personal data is a fundamental right. Article 8(1) of the Charter of Fundamental Rights of the European Union (the 'Charter') and Article 16(1) of the Treaty on the Functioning of the European Union (TFEU) provide that

		everyone has the right to the protection of personal data concerning him or her. This right is also guaranteed under Article 8 of the European Convention for the Protection of Human Rights and Fundamental Freedoms.
Consejo para la Transparencia	Chile	Artículo 19 numeral 4 de la Constitución Política de la República que señala: 'La Constitución asegura a todas las personas: (...) El respeto y protección a la vida privada y a la honra de la persona y su familia, y asimismo, la protección de sus datos personales. El tratamiento y protección de estos datos se efectuará en la forma y condiciones que determine la ley;'.
Commission for Personal Data Protection	Republic of Bulgaria	Art. 32. (1) The privacy of citizens shall be inviolable. Everyone shall be entitled to protection against any illegal interference in his private or family affairs and against encroachments on his honour,dignity and reputation. (2) No one shall be followed, photographed, filmed, recorded or subjected to any other similar activity without his knowledge or despite his express disapproval, except when such actions are permitted by law. rt. 34. (1) The freedom and confidentiality of correspondence and all other communications shall be inviolable. (2) Exceptions to this provision shall be allowed only with the permission of the judicial authorities for the purpose of discovering or preventing a grave crime.
National Privacy Commission	Philippines	ARTICLE III Bill of Rights SECTION 1. No person shall be deprived of life, liberty, or property without due process of law, nor shall any person be denied the equal protection of the laws. SECTION 2. The right of the people to be secure in their persons, houses, papers, and effects against unreasonable searches and seizures of whatever nature and for any purpose shall be inviolable, and no search warrant or warrant of arrest shall issue except upon probable cause to be determined personally by the judge after examination under oath or affirmation of the complainant and the witnesses he may produce, and particularly describing the place to be searched and the persons or things to be seized. SECTION 3. (1) The privacy of communication and correspondence shall be inviolable except upon lawful order of the court, or when public safety or order requires otherwise as prescribed by law. (2) Any evidence obtained in violation of this or the

		preceding section shall be inadmissible for any purpose in any proceeding.
Belgian Data Protection Authority	Belgium	Article 22 of the Belgian Constitution stipulates that: "Everyone has the right to the respect of his private and family life, except in the cases and conditions determined by the law. The laws, federate laws and rules referred to in Article 134 guarantee the protection of this right.". There is no explicit reference to data protection but the Constitutional court systematically interprets this provision as also cover the fundamental right to data protection. Furthermore, the Charter of fundamental rights of the EU (which applies in Belgium) protects the rights of data protection and privacy separately: Article 7 "Respect for private and family life Everyone has the right to respect for his or her private and family life, home and communications." Article 8 Protection of personal data "1. Everyone has the right to the protection of personal data concerning him or her. 2. Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified. 3. Compliance with these rules shall be subject to control by an independent authority."
Commission d'accès à l'information du Québec (CAI)	Québec (province du Canada)	Article 8 de la Constitution du Canada.
supervisory body for police information management	belgium	Article 22
Datatilsynet	Norway	The Constitution of the Kingdom of Norway Section 102 https://lovdata.no/NLE/lov/1814-05-17/a102
OFFICE OF THE COMMISSIONER FOR INFORMATION OF PUBLIC IMPORTANCE AND PERSONAL	Republic of Serbia	Article 42

DATA PROTECTION		
DATA PROTECTION COMMISSION	GHANA	The 1992 Constitution of Ghana
Commission de L'INFORMATIQUE et des Libertés (CIL)	BURKINA Faso	Constitution du 11 juin 1991
Data Protection Authority	Principality of Liechtenstein	Art. 32 Constitution
Commission Nationale pour la Protection des Données à Caractère Personnel (CNPDCP)	Gabon - Afrique Centrale	- Préambule; - Titre préliminaire, article premier des principes et droits fondamentaux, points 5 et 6.
Office of the Privacy Commissioner for Personal Data, Hong Kong, China	Hong Kong Special Administrative Region of the People's Republic of China	Article 30 of the Basic Law of Hong Kong Special Administrative Region provides, inter alia, that the freedom and privacy of communication of Hong Kong residents shall be protected by law. Article 39 of the Basic Law provides that the provisions of the International Covenant on Civil and Political Rights (which include the right to privacy under article 17 of ICCPR) shall remain in force. For the full text of the Basic Law, please see https://www.basiclaw.gov.hk/en/basiclawtext/images/basiclaw_full_text_en.pdf.
Hellenic Data Protection Authority	Greece	Article 9A of the Hellenic Constitution (see here https://www.hellenicparliament.gr/UserFiles/f3c70a23-7696-49db-9148-f24dce6a27c8/001-156%20aggliko.pdf)
DIFC Authority	United Arab Emirates	Article 31 of the UAE Constitution addresses privacy by providing that "freedom of communication by post, telegraph or other means of communication and the secrecy thereof shall be guaranteed in accordance with the law".
Informacijski pooblaščenec (eng. Information Commissioner)	Slovenia	Art. 38; https://www.us-rs.si/legal-basis/constitution/?lang=en
Personal Data Protection Agency in	Bosnia and Herzegovina	Constitution of Bosnia and Herzegovina - Article 2, paragraph 3, item f) All persons in the territory of Bosnia and Herzegovina enjoy

Bosnia and Herzegovina		the human rights and freedoms referred to in paragraph 2 of this Article, which include: f) The right to private and family life, home and correspondence.
AUTORITAT CATALANA DE PROTECCIÓ DE DADES	ESPAÑA	ARTÍCULO 18 CONSTITUCIÓN ESPAÑOLA. 18.1: SE GARANTIZA EL DERECHO AL HONOR, A LA INTIMIDAD PERSONAL Y FAMILIAR Y A LA PROPIA IMAGEN. 18.4: LA LEY LIMITARÁ EL USO DE LA INFORMÁTICA PARA GARANTIZAR EL HONOR Y LA INTIMIDAD PERSONAL Y FAMILIAR DE LOS CIUDADANOS Y EL PLENO EJERCICIO DE SUS DERECHOS.
Commissioner for Data protction and Freedom of Information Rhineland-Palatinate	Germany	Art. 4 Constitution of Rhineland-Palatinate
The State Inspector's Service	Georgia	Constitution of Georgia includes a reference to privacy. Namely, article 15 on Rights to personal and family privacy, personal space and privacy of communication: Article 15 – Rights to personal and family privacy, personal space and privacy of communication 1. Personal and family life shall be inviolable. This right may be restricted only in accordance with law for ensuring national security or public safety, or for protecting the rights of others, insofar as is necessary in a democratic society. 2. Personal space and communication shall be inviolable. No one shall have the right to enter a place of residence or other possessions, or to conduct a search, against the will of the possessor. These rights may be restricted only in accordance with law for ensuring national security or public safety, or for protecting the rights of others, insofar as is necessary in a democratic society, based on a court decision or without a court decision in cases of urgent necessity provided for by law. In cases of urgent necessity, a court shall be notified of the restriction of the right no later than 24 hours after the restriction, and the court shall approve the lawfulness of the restriction no later than 24 hours after the submission of the notification.
Office of the Privacy Commissioner for Bermuda	Bermuda	Chapter 1, Section 1, 'Fundamental rights and freedoms of the individual': '1. Whereas every person in Bermuda is entitled to the fundamental rights and freedoms of the individual, that is to

		say, has the right, whatever his race, place of origin, political opinions, colour, creed or sex, but subject to respect for the rights and freedoms of others and for the public interest, to each and all of the following, namely: '(a) life, liberty, security of the person and the protection of the law; '(b) freedom of conscience, of expression and of assembly and association; and '(c) protection for the privacy of his home and other property and from deprivation of property without compensation...' These rights are further described in subsequent sections of the Constitution's Chapter 1.
Federal Trade Commission	United States of America	Amendment IV: The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized. https://www.archives.gov/founding-docs/bill-of-rights-transcript
Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales	México	Artículo 16 de la Constitución Política de los Estados Unidos Mexicanos.
The Danish Data Protection Agency	Denmark	The Danish Constitution § 72.
Estonian Data Protection Authority	Estonia	Article 26 of Estonian Consitution: § 26. Everyone has the right to the inviolability of private and family life. State agencies, municipalities and their officials shall not interfere with the family or private life of any person, except in the cases and pursuant to a procedure provided by a law to protect health, morals, public order, or the rights and freedoms of others, to prevent a criminal offence or to apprehend a criminal offender.
Hungarian National Authority for Data Protection	Hungary	The fundamental law of Hungary, Article VI section (1) “Everyone shall have the right to have his or her private and family life, home, communications and good reputation respected.”

and Freedom of Information		
State Data Protection Inspectorate (hereinafter referred to as SDPI)	Lithuania	Article 22 of the Constitution of the Republic of Lithuania The private life of a human being shall be inviolable. Personal correspondence, telephone conversations, telegraph messages, and other communications shall be inviolable. Information concerning the private life of a person may be collected only upon a justified court decision and only according to the law. The law and the court shall protect everyone from arbitrary or unlawful interference in his private and family life, from encroachment upon his honour and dignity. https://www.e-tar.lt/portal/en/legalAct/TAR.47BB952431DA/itvNOwWAhd
Autoriteit Persoonsgegevens (English/International: Dutch Data Protection Authority)	Netherlands	Article 10 Dutch Constitution
Privacy Protection Authority	Israel	https://www.knesset.gov.il/laws/speciaL/eng/basic3_eng.html
Office for Personal Data Protection	Czech Republic	https://public.psp.cz/en/docs/laws/constitution.html
Berlin Commissioner for Data Protection and the Freedom of Information	Germany	The German Basic Law (German Constitution) does not provide a specific reference to data protection. However, according to the ruling of the Federal Constitutional Court in 1983 the right to informational self-determination and thus data protection is contained in Article 2 subsection 1 (Personal freedoms) in conjunction with Article 1 subsection 1 (Human dignity) of the German Basic Law. Articles 10 (Privacy of correspondence, posts and telecommunications) and 13 (Inviolability of the home) of the German Basic Law provide further specifications for privacy protection. The Berlin Constitution includes a specific reference to data protection in Article 33. Articles 16 (Privacy of correspondence, posts and telecommunications) and 28 subsection 2 (Inviolability of the home) of the Berlin Constitution refer to privacy protection.
The Federal Commissioner	Germany	The German legal system classifies data protection and data security having constitutional status as being important

for Data Protection and Freedom of Information		elements of free democratic principles on the basis of the constitutional 'Right to informational self-determination', which the Federal Constitutional Court defined with its census verdict of 1983. The general personality right as laid down in Article 2 in conjunction with the principle of respecting human dignity pursuant to Article 1 of German Basic Law (Grundgesetz) serves to protect the Right to informational self-determination.
National Center for Personal Data Protection of the Republic of Moldova	Moldova	Art. 28
Personal Data Protection Office (UODO)	Poland	The Constitution of the Republic of Poland of 7 April 1997 (articles 47 and 51): https://uodo.gov.pl/en/594
Data Protection Commission	Ireland	THERE IS NO EXPLICITLY STATED RIGHT TO PRIVACY IN THE IRISH CONSTITUTION HOWEVER THE IRISH COURTS HAVE HELD THAT THERE IS AN UNENUMERATED RIGHT TO PRIVACY UNDER ARTICLE 40.3 OF THE IRISH CONSTITUTION AS ONE OF THE PERSONAL RIGHTS OF THE CITIZEN. ARTICLE 40.3: “THE STATE GUARANTEES IN ITS LAWS TO RESPECT, AND,AS FAR AS PRACTICABLE, BY ITS LAWS TO DEFEND AND VINDICATE THE PERSONAL RIGHTS OF THE CITIZEN.”

Appendix 4 – Authorities' annual reports

Authority name	Country / economy	Link to annual report
European Data Protection Supervisor (EDPS)	International Organisation	https://edps.europa.eu/sites/edp/files/publication/2020-03-17_annual_report_2020_en_0.pdf
The Office of the Australian Information Commissioner (OAIC)	Australia	https://www.oaic.gov.au/about-us/our-corporate-information/annual-reports/
Data Protection Commissioner of the Council of Europe	International Organisation	https://www.coe.int/en/web/data-protection/data-protection-commissioner
Österreichische Datenschutzbehörde (Austrian Data Protection Authority)	Austria	https://www.dsb.gv.at/download-links/dokumente.html

Appendix 5 – List of laws available online

Authority name	Country / economy	Link to laws online
San Marino Data Protection Authority	San Marino	https://www.consigliograndeegenerale.sm/on-line/home/archivio-leggi-decreti-e-regolamenti/scheda17161069.html
Data Protection Commissioner	International Organisation	https://www.oecd.org/general/OECD-Decision-Processing-Personal-Data.pdf
Ombudsman	Cayman Islands	https://ombudsman.ky/resources
Commission de l'Informatique et des Libertés	Burkina Faso	http://www.cil.bf/index.php/legislation/legislation-nationale
Autorité de Protection des Données à caractère Personnel (APDP)	Mali	https://apdp.ml
Persónuvernd - Icelandic Data Protection Authority	Iceland	https://www.personuvernd.is/media/uncategorized/Act_No_90_2018_on_Data_Protection_and_the_Processing_of_Personal_Data.pdf
Autoridad Nacional de Protección de Datos Personales	Perú	https://www.minjus.gob.pe/legislacion/
Jersey Data Protection Authority	Bailiwick of Jersey	https://www.jerseylaw.je/laws/revised/Pages/15.240.aspx https://www.jerseylaw.je/laws/revised/Pages/15.245.aspx
The Hessian Commissioner for Data Protection and Freedom of Information	Germany, Hesse	https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&from=DE https://www.gesetze-im-internet.de/englisch_bdsg/englisch_bdsg.pdf https://www.rv.hessenrecht.hessen.de/jportal/recherche3doc/DSIFG_HE_jlr-DSIFGHErahmen.pdf?json=%7B'format'%3A'pdf'%2C'docId'%3A'jlr-DSIFGHErahmen'%2C'portalId'%3A'bshe'%7D&_=%2FDSIFG_HE_jlr-DSIFGHErahmen.pdf (no English version available)
Agência Nacional de Protecção de Dados Pessoais	São Tomé e Príncipe	www.anpdp.st
Landesbeauftragte für Datenschutz und Informationsfreiheit Nordrhein-Westfalen (North	North Rhine-Westphalia (Germany)	Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection

Rhine-Westphalia Commissioner for Data Protection and Freedom of Information)		Regulation) https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv%3AOJ.L_.2016.119.01.0001.01.ENG&toc=OJ%3AL%3A2016%3A119%3ATOC Federal Data Protection Act (BDSG) https://www.gesetze-im-internet.de/englisch_bdsg/ Data Protection Act North Rhine-Westphalia / Datenschutzgesetz Nordrhein-Westfalen (DSG NRW) https://recht.nrw.de/lmi/owa/br_text_anzeigen?v_id=35200071121100436275 Telemediengesetz (TMG) https://www.gesetze-im-internet.de/tmg/BJNR017910007.html
Turkish Personal Protection Authority	Turkey	https://www.kvkk.gov.tr/Icerik/6649/Personal-Data-Protection-Law
Unidad Reguladora y de Control de Datos Personales	Uruguay	https://www.gub.uy/unidad-reguladora-control-datos-personales/institucional/normativa
Office of the Privacy Commissioner Te Mana Mātāpono Matatapu	New Zealand	https://privacy.org.nz/privacy-act-2020/privacy-act-2020/
Information and Data Protection Commissioner	Albania	https://www.idp.al/wp-content/uploads/2019/10/LDP_english_version_amended_2014.pdf
The Office for Personal Data Protection of the Slovak Republic	Slovak Republic	https://dataprotection.gov.sk/uoou/sites/default/files/2019_10_03_act_18_2018_on_personal_data_protection_and_amending_and_supplementing_certain_acts.pdf#overlay-context=sk/content/182018#overlay-context=sk/content/182018%22
Office of the Information and Privacy Commissioner of Nova Scotia	Canada	https://oipc.novascotia.ca/legislation
Préposé fédéral à la protection des données et à la transparence (PFPDT)	Suisse	https://www.fedlex.admin.ch/eli/cc/1993/1945_1945_1945/fr et la future loi qui entrera en vigueur en 2022: https://www.fedlex.admin.ch/eli/fga/2020/1998/fr
Gibraltar Regulatory Authority ('GRA')	Gibraltar	https://www.gra.gi/data-protection/legislation

Superintendencia de Industria y Comercio	República de Colombia	https://www.sic.gov.co/repositorio-de-normatividad
Centro de Protección de Datos Personales	Argentina	http://cpdp.defensoria.org.ar/
European Data Protection Supervisor (EDPS)	International Organisation	https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32018R1725&from=EN
Consejo para la Transparencia	Chile	Ley 19.628 sobre Protección de la Vida Privada, disponible en https://www.bcn.cl/leychile/navegar?idNorma=141599
Isle of Man Information Commissioner	Isle of Man	https://inforights.im/organisations/data-protection-law-2018/legislation-and-case-law/the-legislation/
Commission for Personal Data Protection	Republic of Bulgaria	https://www.cpdp.bg/en/index.php?p=element&aid=1194
National Privacy Commission	Philippines	https://www.privacy.gov.ph/wp-content/uploads/DPA-of-2012.pdf
Belgian Data Protection Authority	Belgium	National organic law of 3 December 2017 (constitution of BE DPA) - http://www.ejustice.just.fgov.be/eli/wet/2017/12/03/2017031916/justel National privacy law of 30 July 2018 - https://www.gegevensbeschermingsautoriteit.be/publications/kaderwet.pdf General data protection regulation - https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1584346533528&uri=CELEX:02016R0679-20160504
Commission d'accès à l'information du Québec (CAI)	Québec (province du Canada)	Secteur public : Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels : http://legisquebec.gouv.qc.ca/fr/showdoc/cs/A-2.1 Secteur privé : Loi sur la protection des renseignements personnels dans le secteur privé : http://legisquebec.gouv.qc.ca/fr/showDoc/cs/P-39.1?&digest
supervisory body for police information management	belgium	http://www.ejustice.just.fgov.be/eli/wet/2018/07/30/2018040581/justel
Datatilsynet	Norway	https://lovdata.no/dokument/NL/lov/2018-06-15-38
OFFICE OF THE COMMISSIONER FOR INFORMATION OF PUBLIC	Republic of Serbia	www.poverenik.rs/sr/заштита-података/pravni-okvir-zp.html

IMPORTANCE AND PERSONAL DATA PROTECTION		
DATA PROTECTION COMMISSION	GHANA	https://www.dataprotection.org.gh/index.php/resources/downloads/data-protection-act/38-data-protection-act-2012-act-843
The Information Commissioners Office	Uniter Kingdom	Data protection - GOV.UK (www.gov.uk) Guide to the General Data Protection Regulation - GOV.UK (www.gov.uk) (We are regulators in relation to more than one data protection and privacy law. A full list of the legislation we cover is also listed on the ICO's own website here: https://ico.org.uk/about-the-ico/what-we-do/legislation-we-cover/)
Office of the Information and Privacy Commissioner of Ontario	Ontario, Canada	Freedom of Information and Protection of Privacy Act: https://www.ontario.ca/laws/statute/90f31 Municipal Freedom of Information and Protection of Privacy Act: https://www.ontario.ca/laws/statute/90m56 Personal Health Information Protection Act: https://www.ontario.ca/laws/statute/04p03 Child, Youth and Family Services Act Part X: https://www.ontario.ca/laws/statute/17c14#BK381
Office of the Information and Privacy Commissioner of NL	Newfoundland, Canada	https://www.assembly.nl.ca/legislation/sr/statutes/a01-2.html https://assembly.nl.ca/legislation/sr/statutes/p07-01.html
Commission de L'INFORMATIQUE et des Libertés (CIL)	BURKINA Faso	www.cil.bf
Data Protection Authority	Principality of Liechtenstein	- National Data Protection Act: https://www.datenschutzstelle.li/application/files/4515/8641/2923/DSG_English_final.pdf - National Data Protection Ordinance: https://www.datenschutzstelle.li/application/files/7916/1043/6564/DSV_Uebersetzung.pdf - GDPR: https://www.datenschutz-grundverordnung.eu/wp-

		content/uploads/2016/05/CELEX_32016R0679_EN_TXT.pdf
Office of the Privacy Commissioner of Canada	Canada	Privacy Act (public sector): https://laws-lois.justice.gc.ca/ENG/ACTS/P-21/index.html PIPEDA (private sector): https://laws-lois.justice.gc.ca/ENG/ACTS/P-8.6/index.html
Commission Nationale pour la Protection des Données à Caractère Personnel (CNPDCP)	Gabon - Afrique Centrale	www.cnpdcp.ga
Office of the Privacy Commissioner for Personal Data, Hong Kong, China	Hong Kong Special Administrative Region of the People's Republic of China	https://www.elegislation.gov.hk/hk/cap486
Hellenic Data Protection Authority	Greece	https://www.dpa.gr/sites/default/files/2020-08/LAW%204624_2019_EN_TRANSLATED%20BY%20THE%20HDPA.PDF
DIFC Authority	United Arab Emirates	https://www.difc.ae/files/6115/9358/6486/Data_Protection_Law_DIFC_Law_No.5_of_2020.pdf https://www.difc.ae/files/9315/9358/7756/Data_Protection_Regulations_2020.pdf
Informacijski pooblaščenec (eng. Information Commissioner)	Slovenia	https://ec.europa.eu/info/law/law-topic/data-protection/data-protection-eu_en https://www.ip-rs.si/en/legislation/
Office of the Information and Data Protection Commissioner	Malta	https://legislation.mt/eli/cap/586/eng/pdf
Personal Data Protection Agency in Bosnia and Herzegovina	Bosnia and Herzegovina	http://azlp.ba/propisi/Default.aspx?id=5&langTag=en-US&template_id=149&pageIndex=1
AUTORITAT CATALANA DE PROTECCIÓ DE DADES	ESPAÑA	HTTPS://APDCAT.GENCAT.CAT/CA/AUTORITAT/NORMATIVA

Commissioner for Data protction and Freedom of Information Rhineland-Palatinate	Germany	http://landesrecht.rlp.de/jportal/?quelle=jlink&query=DSG+RP&psml=bsrlpprod.psml https://dsgvo-gesetz.de/bdsg/ https://dsgvo-gesetz.de
The State Inspector's Service	Georgia	At the moment, an updated version of Georgian Law on Personal Data Protection is available only in national language. The older version of the Law is available at the following link: https://www.matsne.gov.ge/ka/document/view/1561437?impose=translateEn&publication=9
Garante per la protezione dei dati personali	Italy	https://www.garanteprivacy.it/documents/10160/0/Data+Protection+Code.pdf/7f4dc718-98e4-1af5-fb44-16a313f4e70f?version=1.3
Office of the Privacy Commissioner for Bermuda	Bermuda	http://www.bermudalaws.bm/laws/Annual%20Laws/2016/Acts/Personal%20Information%20Protection%20Act%202016.pdf
Federal Trade Commission	United States of America	https://www.ftc.gov/enforcement/statutes/federal-trade-commission-act
Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales	México	https://home.inai.org.mx/?page_id=1870
Office of the Information and Privacy Commissioner for British Columbia	Canada	- FIPPA: https://www.bclaws.gov.bc.ca/civix/document/id/complete/statreg/96165_00 - FIPPA Regulation: https://www.bclaws.gov.bc.ca/civix/document/id/complete/statreg/155_2012 - PIPA: https://www.bclaws.gov.bc.ca/civix/document/id/complete/statreg/00_03063_01 - PIPA Regulations: https://www.bclaws.gov.bc.ca/civix/document/id/complete/statreg/10_473_2003
The Office of the Australian	Australia	https://www.legislation.gov.au/Details/C2020C00237

Information Commissioner		
Office of the Victorian Information Commissioner	Australia	https://www.legislation.vic.gov.au/in-force/acts/privacy-and-data-protection-act-2014/026
The Danish Data Protection Agency	Denmark	https://www.datatilsynet.dk/english/legislation
Estonian Data Protection Authority	Estonia	GDPR National data protection act: https://www.riigiteataja.ee/en/eli/523012019001/consolide
Hungarian National Authority for Data Protection and Freedom of Information	Hungary	https://njt.hu/translated/doc/J2011T0112P_20200101_FINrev.pdf https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016R0679&from=HU
State Data Protection Inspectorate (hereinafter referred to as SDPI)	Lithuania	- Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation): https://eur-lex.europa.eu/legal-content/LT/TXT/?uri=CELEX%3A32016R0679 - Law of the Republic of Lithuania on Legal Protection of Personal Data: https://www.e-tar.lt/portal/en/legalAct/TAR.5368B592234C/sqyPjSiFfg Unofficial translation to English can be found here (not the newest consolidated version): https://vdai.lrv.lt/en/legislation - Law of the Republic of Lithuania on Legal Protection of Personal Data, Processed for the Purposes of Prevention, Investigation, Detection or Prosecution of Criminal Offences, or the Execution of Criminal Penalties, or National Security, or Defence (hereinafter – Law on Law enforcement) which transposes Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA:

		https://www.e-tar.lt/portal/en/legalAct/TAR.299D835159BE/amtbLRwHvC Unofficial translation to English can be found here (not the newest consolidated version): https://vdai.lrv.lt/en/legislation
Autoriteit Persoonsgegevens (English/International: Dutch Data Protection Authority)	Netherlands	The Dutch DPA supervises the correct application of (certain aspects of) the following laws/acts: 1. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), Official publication: OJ L 119, 4.5.2016, p. 1–88. Available in all EU languages at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32016R0679 2. Wet van 16 mei 2018, houdende regels ter uitvoering van Verordening (EU) 2016/679 van het Europees Parlement en de Raad van 27 april 2016 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens en tot intrekking van Richtlijn 95/46/EG (algemene verordening gegevensbescherming) (PbEU 2016, L 119) (Uitvoeringswet Algemene verordening gegevensbescherming). Freely translated title: Act of 16 May 2018, containing rules for the implementation of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (OJ 2016, L 119) (Implementation Act GDPR). Available in Dutch at: https://wetten.overheid.nl/BWBR0040940/2018-05-25 3. Wet van 21 juli 2007, houdende regels inzake de verwerking van politiegegevens (Wet politiegegevens). Freely translated title: Act of 21 july 2007, containing rules with regard to the processing of police data (Police Data Act). Available in Dutch at: https://wetten.overheid.nl/BWBR0022463/2020-01-01 4. Wet van 7 november 2002 tot wijziging van de regels betreffende de verwerking van justitiële gegevens en het

		stellen van regels met betrekking tot de verwerking van persoonsgegevens in persoonsdossiers (Wet justitiële gegevens) Freely translated title: Act of 7 november 2002 amending rules concerning the processing of judicial data and data pertaining to criminal procedure and putting in place rules with regard to the processing of personal data in criminal records (Judicial Data and Criminal Records Act). Available in Dutch at: https://wetten.overheid.nl/BWBR0014194/2020-01-01 5. Wet van 28 september 1989, houdende nieuwe bepalingen inzake het kiesrecht en de verkiezingen (Kieswet). Freely translated title: Act of 28 September 1989, containing new rules on the right to vote and elections (Elections Act). Available in Dutch at: https://wetten.overheid.nl/BWBR0004627/2020-07-01 6. Wet van 3 juli 2013 houdende nieuwe regels voor een basisregistratie personen (Wet basisregistratie personen). Freely translated title: Act of 3 July 2013 containing new rules for a key register of persons (Act on the Key Register of persons). Available in Dutch at: https://wetten.overheid.nl/BWBR0033715/2019-02-03 7. Wet van 5 juni 2019, houdende regels ter implementatie van richtlijn (EU) 2016/681 van het Europees Parlement en de Raad van 27 april 2016 over het gebruik van persoonsgegevens van passagiers (PNR-gegevens) voor het voorkomen, opsporen, onderzoeken en vervolgen van terroristische misdrijven en ernstige criminaliteit (PbEU 2016, L 119) (Wet gebruik van passagiersgegevens voor de bestrijding van terroristische en ernstige misdrijven). Freely translated title: Act of 5 June 2019, containing rules for the implementation of Directive (EU) 2016/681 of the European Parliament and of the Council of 27 April 2016 on the use of passenger name record (PNR) data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime (OJ 2016 L 119) (Use of Passenger Name Record Data For Combating Terrorist Offences and Serious Crime Act). Available in Dutch at: https://wetten.overheid.nl/BWBR0042301/2019-06-18 8. Wet van 19 oktober 1998, houdende regels inzake de telecommunicatie (Telecommunicatiewet). Freely translated title: Act of 19 October 1998, containing

		rules regarding telecommunications (Telecommunications Act). Available in Dutch at: https://wetten.overheid.nl/BWBR0009950/2020-12-21
Data Protection Commissioner of the Council of Europe	France	https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=090000168073dc0c
Privacy Protection Authority	Israel	https://www.gov.il/BlobFolder/legalinfo/legislation/en/ProtectionofPrivacyLaw57411981unofficialtranslatio.pdf
Office for Personal Data Protection	Czech Republic	www.uoou.cz/en/vismo/zobraz_dok.asp?id_org=200156&id_ktg=1420&archiv=0&p1=1105
Berlin Commissioner for Data Protection and the Freedom of Information	Germany	https://gesetze.berlin.de/bsbe/document/jlr-DSGBE2018V1IVZ
Commission nationale de l'informatique et des libertés - CNIL	France	Oui https://www.cnil.fr/fr/la-loi-informatique-et-libertes
The Federal Commissioner for Data Protection and Freedom of Information	Germany	General Data Protection Regulation http://data.europa.eu/eli/reg/2016/679/oj Federal Data Protection Act https://www.gesetze-im-internet.de/englisch_bdsg/
National Center for Personal Data Protection of the Republic of Moldova	Moldova	https://datepersonale.md/en/legislation/national-legislation/law/
Personal Data Protection Office (UODO)	Poland	The Act of 10 May 2018 on the Protection of Personal Data: https://uodo.gov.pl/en/594
Data Protection Commission	Ireland	http://www.irishstatutebook.ie/eli/2018/act/7/enacted/en/html NOTE THE PREVIOUS LEGISATION WHICH APPLIED PRIOR TO THE DATA PROTECTION ACT 2018 (DATA PROTECTION ACTS 1988 AND 2003) CONTINUES TO APPLY TO LIMITED CASES SUCH AS COMPLAINTS REGARDING MATTERS WHICH OCCURRED PRIOR TO 25 MAY 2018 AND CONTRAVENTIONS OF DATA PROTECTION LAW WHICH OCCURRED PRIOR TO THAT DATE: https://www.lawreform.ie/_fileupload/Restatement/First%20Programme%20of%20Restatement/EN_ACT_1988_0025.PDF

		ALSO APPLICABLE ARE E-PRIVACY REGULATIONS CONCERNING ELECTRONIC COMMUNICATIONS (STATUTORY INSTRUMENT 336 OF 2011): http://www.irishstatutebook.ie/eli/2011/si/336/
Commission de protection des Données Personnelles du Sénégal (CDP)	Sénégal	Loi 2008-12 du 25 janvier 2008 portant sur la protection des données à caractère personnel : https://www.cdp.sn/content/loi-n%C2%B0-2008-12-du-25-janvier-2008-portant-sur-la-protection-des-donn%C3%A9es-%C3%A0-caract%C3%A8re
The Office of the Australian Information Commissioner (OAIC)	Australia	https://www.legislation.gov.au/Details/C2020C00237
Data Protection Commissioner of the Council of Europe	International Organisation	https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=090000168073dc0c
Österreichische Datenschutzbehörde (Austrian Data Protection Authority)	Austria	https://www.ris.bka.gv.at/Dokument.wxe?Abfrage=Erv&Dokumentnummer=ERV_1999_1_165

Appendix 6 – List of 'other' enforcement cooperation networks or arrangements where authorities participate

Enforcement cooperation networks or arrangements	
1. African Network of Data Protection Authorities (RAPDP) 2. Asia Pacific Privacy Authorities 3. Council of Europe's Convention 108 4. COVID taskforce (New Zealand) 5. Domestic Enforcement Collaboration Forum (Canada) 6. Eurodac supervision coordination group 7. European Case Handling Workshop 8. European Data Protection Board (EDPB) 9. European Spring Conference 10. Ibero-American Data Protection Network 11. International Conference of Information Commissioners (ICIC)	12. OECD working party on data governance and privacy 13. Privacy Authorities Australia 14. Privacy Authorities Australia Cooperation and Enforcement Group 15. Privacy Authorities Australia Policy Group 16. The Association of Francophone Data Protection Authorities (AFAPDP) 17. The British, Irish and Islands Data Protection Network (BIIDPA) 18. The Common Thread Network 19. The GDPR's one-stop-shop OSS mechanism. 20. Visa supervision coordination group (EU) 21. Working Group on Data Protection in Technology (Berlin Group)