Working Group on Data Sharing for the Public Good

Report – July 2023

Office of the Information Commissioner, Bailiwick of Jersey

Table of Contents

Executive Summary

I am very pleased to present my second annual report on the activities of the GPA Data Sharing Working Group.

Following the adoption of the GPA Resolution on Data Sharing for the Public Good in Mexico, in October 2021, and developing upon the Annual Report of July 2022, the GPA Working Group on Data Sharing for the Public Good (DSWG) has continued to work towards identifying practical solutions for data sharing where there is a public benefit.

In terms of the actions of the DSWG, the adopted resolution on the Assembly's Strategic Direction (2021-23) provides that the objective of the Data Sharing Working Group is to:

- *Deliver and promote best practices on data sharing for the public good, for data protection and privacy authorities to use in conversations with governments and other stakeholders to demonstrate what good data sharing practice looks like, and to highlight key principles.*

This objective links to 3 strategic priorities of the GPA:

1. SP1 – Advancing global privacy in an age of accelerated digitalisation.
2. SP2 – Maximise the GPA's voice and influence.
3. SP3 – Capacity building for members.

Whilst it has been frustrating to find membership for the DSWG and challenging to be inclusive of all Data Protection Authorities, we have been able to further our progress during 2023. It remains the case that the subject of data sharing is vast, and as such it has continued to be the priority of the DSWG to identify the main data sharing issues affecting each of the membership jurisdictions. We have continued to meet on average once a month to ensure momentum is maintained.

At the time of my last Annual Report, work was underway to create a survey for DSWG members, with the aim of identifying the key issues affecting Data Protection Authorities. The survey was completed, distributed to the DSWG membership, the results assessed, and a work plan for 2023 was established. The results of the survey are detailed in Appendix 1.

Introduction

The Data Sharing Working Group (hereafter "the DSWG") was established by the Resolution on Data Sharing for the Public Good during the 42nd GPA Conference in Mexico City, 2021.

That Resolution resolved to:

Acknowledge the need to continue and broaden the work of the Covid-19 Working Group and evolve its mandate to focus on data protection and privacy issues and concerns related to sharing of personal data as the global pandemic response shifts towards economic recovery.

Establish a Working Group on data sharing for the public good. The new Working Group will continue the work of the Covid-19 Working Group and will:

i. Focus on identifying practical and pragmatic approaches on how personal data can be shared and used to enable innovation and growth while protecting individual rights and promoting public trust and provide principles and best practices on key components of data sharing for public good;

ii. Collaborate with relevant stakeholders, such as international networks, civil society organisations, and privacy advocates, on efforts geared towards strengthening capacity of GPA members and observers to tackle emerging challenges related to data sharing;

iii. Develop proactive responses on any emerging data protection and privacy concerns relative to the sharing of personal data, for example, on areas of concern identified in the surveys on emerging data protection and privacy issues, such as health passports, health monitoring of incoming travellers and returning nationals, contact tracing measures, handling of children's or student data in e-learning technologies;

iv. Consult with the GPA Reference Panel on emerging policy ideas to consider integrating into future approaches towards data sharing; and

v. Report on the progress of the Working Group, and the scope of any related considerations for future working arrangements, to the 2022 closed session.

The DSWG is composed of the following members:

- Jersey, Office of the Information Commissioner **(JOIC) (Chair)**
- Office of the Australian Information Commissioner **(OAIC)**
- National Privacy Commission of the Philippines **(NPC)**
- Data Protection Commission of the Dubai International Finance Centre **(DIFC)**
- Organisation for Economic Development and Cooperation **(OECD)**
- European Data Protection Supervisor **(EDPS)**
- Germany, Bundesbeauftragte für den Datenschutz und die Informationsfreiheit (**BfDI**)
- Office for Personal Data Protection of Macao **(GPDP)**
- Israeli Privacy Protection Authority **(IPPA)**
- Canada, Office of the Privacy Commissioner (**OPC**)

- Ontario Office of the Information and Privacy Commissioner **(OIPC)**
- Burkina Faso, Commission de l'Informatique et des libertés (**CIL**)
- Japan, Personal Information Protection Commission **(PPC)**
- UK, Information Commissioner's Office (**ICO**)
- Hong Kong, Office of the Privacy Commissioner for Personal Data **(PCPD)**
- Switzerland, Federal Data Protection and Information Commissioner **(FDPIC)**
- US Federal Trade Commission **(FTC)**
- UN Global Pulse **(UNGP)** (Observer)

The composition of the DSWG reflects the geographical diversity of the GPA.

At the time of writing, the DSWG has met six times by videoconference since the GPA Annual Meeting in Istanbul.

During these meetings, the DSWG has:

- Concluded and analysed the survey of DSWG members;
- Identified 3 key areas for further investigation:
    - Big data sharing frameworks
    - Data sharing across Government agencies
    - Barriers to the access, use and sharing of digital health data.
- Heard representations on key objectives from the DIFC, EDPS and UK ICO;
- Resolved to create a sub-group to work on creating guiding principles for data sharing;
- Resolved to create a second sub-group later in the year to work on either adapting the DIFC's Ethical Data Management Risk Index, or International Transfers of Health Data for Research Purposes.

Working Group Activities

In conformity with the objectives of the Resolution, the members of the DSWG have set themselves the following general goals:

- to focus on identifying practical and pragmatic approaches on how personal data can be shared and used to enable innovation and growth while protecting individual rights and promoting public trust and provide principles and best practices on key components of data sharing for public good;

- to develop proactive responses on any emerging data protection and privacy concerns relative to the sharing of personal data, for example, on areas of concern identified in the surveys on emerging data protection and privacy issues (conducted by the former GPA Covid-19 Working Group), such as health passports, health monitoring of incoming travellers and returning nationals, contact tracing measures, handling of children's or student data in e-learning technologies.

In order to achieve these two goals, the DSWG decided to implement the following activities:

- Understand the data protection and privacy issues faced by Data Protection Authorities in relation to data sharing for the public good;

- Establish relationships with relevant actors and organisations, to maximise the reach of the GPA's voice in relation to data sharing;

- Collaborate with other relevant Working Groups of the GPA, produce documents and advocacy tools for better consideration of data protection and privacy;

- Build the capacity of Data Protection Authorities when dealing with issues of data sharing for public benefit.

Since the last annual meeting of the GPA in October 2022, the DSWG has met six times at the time of writing and has conducted the following activities:

1. Concluded and analysed the survey of DSWG members;
2. Identified 3 key areas for further investigation:

    - Big data sharing frameworks
    - Data sharing across Government agencies
    - Barriers to the access, use and sharing of digital health data.

3. Heard representations on key objectives from the DIFC, EDPS and UK ICO;
4. Resolved to create a sub-group to work on creating guiding principles for data sharing;
5. Resolved to create a second sub-group later in the year to work on either adapting the DIFC's Ethical Data Management Risk Index, or International Transfers of Health Data for Research Purposes.

In relation to point 1 above, the DSWG Chair and Secretariat analysed the results of the survey and compiled a report of the findings in November 2022 for the DSWG membership. The Chair would like to sincerely thank those Authorities that took the time to respond to the survey.

The purpose of the survey was to understand and assess the issues and concerns facing Data Protection Authorities in terms of personal data sharing. The results of the survey identified 3 key themes the membership agreed warranted further investigation. These 3 areas were:

- Big data sharing frameworks
- Data sharing across Government agencies
- Barriers to the access, use and sharing of digital health data.

The DSWG decided to explore these areas in more detail and conduct a 'deep dive' into the issues to identify practical and pragmatic approaches on how personal data can be shared and used for public benefit.

In February 2023, Lori Baker of the DIFC presented to the DSWG on the subject of Big Data Sharing Frameworks, and spoke specifically about their own journey and experiences in the DIFC following the implementation of their revised law in 2020. Lori spoke of the desire of the DIFC to share information with others with fewer restrictions whilst maintaining compliance with privacy regulations, thus making it easier and more practical for the Dubai business community. Part of this process was to build in a specific article on Government data sharing which focused on exercising reasonable caution and diligence, assessed the impact of proposed transfers of personal data and obtained assurances regarding the upholding of data subject rights.

Another objective was to examine the adequacy status of all those countries deemed to be EU-adequate, and emphasising the importance of conducting the appropriate due diligence prior to sharing personal data. As a result, the DIFC created the Ethical Data Management Risk Index (EDMRI), which was later published along with guidance reflecting DIFC's view of the data protection landscape.

Veronique Cimina of the EDPS also gave a presentation which highlighted that the GDPR does not define the term 'data sharing'. However, she also talked about frameworks such as the recently adopted EU Data Governance Act which covers data sharing based on voluntary agreements, the European Strategy for Data and the Public Sector Information Re-use Directive.

Both presentations gave a valuable insight into some of the data sharing frameworks available and how they work in practice, as well as highlighting the challenges faced by different jurisdictions who are trying to navigate the complexities of data sharing.

In terms of data sharing across government agencies and the barriers to the access, use and sharing of digital health data, representatives from the UK ICO presented to the DSWG in April 2023.The DSWG were informed about the UK ICO's 'ICO25' strategic plan on data sharing, including information rights, empowerment and safeguarding and promoting consumer growth. They referred to the UK's National Data Strategy and gave examples of data sharing in education and the Welsh accord on the sharing of personal information. The UK ICO also talked about the Digital Economy Act 2017 which enables public sector data sharing around public sector delivery. Whilst it includes data sharing for research purposes, it does not yet include the sharing of health data.

The UK ICO explained their desire to dispel the myth that data protection law is a barrier to data sharing, and that organisations should feel confident sharing data where necessary. They promote the law as a framework for data sharing and increasing trust and confidence, whilst maintaining

appropriate safeguards to protect the data. They use surveys to research what issues organisations encounter when sharing health data in order to identify common problems and work closely with public sector stakeholders, such as NHS England. In this example, they referred to the NHS's 'Data Lock' portal through which health data can be safely shared.

The UK ICO also helpfully pointed the DSWG to some of their resources, such as the ICO Code of Practice on Data Sharing which is designed to give confidence to controllers and includes practical guidance and case studies. The UK ICO also has a data sharing page on their website which contains further data sharing resources.

Action Plan 2023-2024

The work of the DSWG will focus on the advancement of privacy protection worldwide, the promotion of high data protection standards as stated in the GPA Resolution on the Assembly's Strategic Direction (2021-23). It will also work towards maximising the GPA's voice and influence by strengthening relations with other international bodies and networks.

To this end, the DSWG intends to focus essentially on:

- Developing guiding principles for data sharing;
- Adapting the DIFC's Ethical Data Management Risk Index for the wider GPA membership;
- International Transfers of Health Data for Research Purposes;
- Health data sharing for the public good;
- Identifying practical and pragmatic approaches and developing proactive responses on any emerging data protection and privacy concerns relative to the sharing of personal data;
- Developing a compendium of best practices on data sharing for the public good and updating the Covid-19 compendium of best practices, if members identify such a need;
- Capacity building of Data Protection Authorities in reference to data sharing approaches and practices.
- Continuing to explore possible synergies with other GPA Working Groups and external stakeholders;
- Continue to promote the work of the GPA and the DSWG by actively participating in various meetings, conferences, training sessions related to the objectives of the DSWG with external stakeholders in order to maintain and continue to explore possible synergies.

The action plan will be discussed and adopted at the first DSWG meeting following the GPA Annual Meeting in Bermuda in October 2023.

Conclusion

As Chair of the DSWG it continues to be an honour to lead on this important topic. Whilst it is disappointing that we have been unable to increase our active membership, I am confident that as a small group we can make significant progress and improve data sharing practices for public benefit.

Sharing personal data in a privacy protective manner can inform policy and decision-making, improve trust and confidence and provide for efficiencies in service delivery for citizens across the globe, as well as improving public services and business effectiveness. However, the importance of establishing appropriate and pragmatic privacy and data security safeguards as part of any data sharing initiatives cannot be underestimated.

With specific regard to health data sharing, there remain difficult challenges for organisations across the globe in this area. The small survey conducted of the DWSG membership identified many different frameworks, both legal and in practice, which on their own have tried to assist organisations in their respective jurisdictions and provide some clarity around data sharing. However, they also cause difficulties when it comes to cross-border data sharing and creating any kind of consistency. Without agreeing on some common principles, it is hard to see how this situation will improve.

The DSWG will continue to work hard to change this narrative for the better, providing guiding principles and focusing on the complex challenges of health data sharing faced by organisations working in this sphere. We look forward to presenting the outcomes of our work in the coming year ahead.

Paul Vane
Information Commissioner, Bailiwick of Jersey

GPA
Global Privacy Assembly

Appendix 1:
DSWG Survey Results

GPA DATA SHARING WORKING GROUP

Survey results on data sharing for the public good

QUESTION 1:

How would you describe data sharing for the public good?

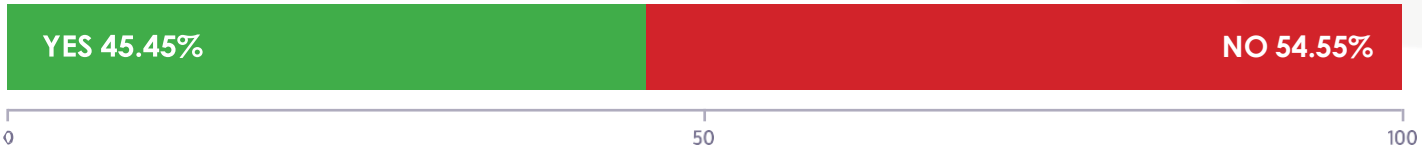
Summary

The general consensus is that the focus should be on data sharing where it is done for the wider societal benefit, whilst also allowing space for innovation and the incorporation of ethical standards.

A couple of respondents went further by suggesting that there should be no commercial or proprietary interest attached to such data sharing activities.

QUESTION 2:

Does your data protection law or applicable regulation / issuance define data sharing?



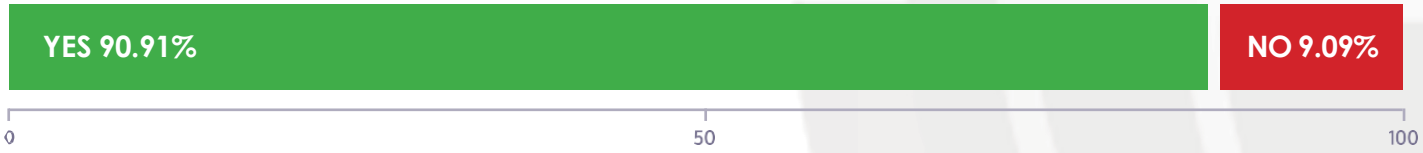
Summary

From our limited sample, less than half of respondents confirmed the availability of specific provisions in their domestic laws around data sharing.

Interestingly however, the EU Data Governance Act appears to provide an avenue for data stewardship services, which could provide an opening for innovative ways in which data could be utilised for public or societal benefit, where

QUESTION 3:

Has your jurisdiction put in place any laws/ frameworks/policies/strategies which facilitate or promote sharing of personal data and data directly or indirectly related to an individual?

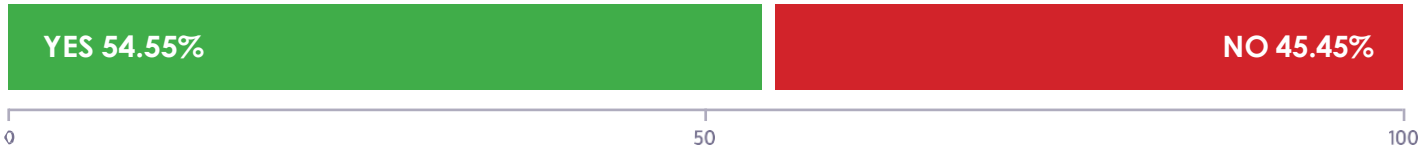


Summary

Whilst frameworks do exist in the majority of respondent jurisdictions, they are generally either sector specific, or relate to Government data sharing only. However, in terms of the broader picture, the UK ICO has developed a data sharing hub, thus recognising the complexities faced by organisations in respect of data sharing, and the European Commission have commenced work on a Europe-wide data strategy which intends to ensure the best use of data for societal benefit, whilst maintaining the privacy rights of individuals.

QUESTION 4:

Has your jurisdiction put in place any laws/ frameworks/policies/strategies which facilitate or promote sharing of big data in the private sector?

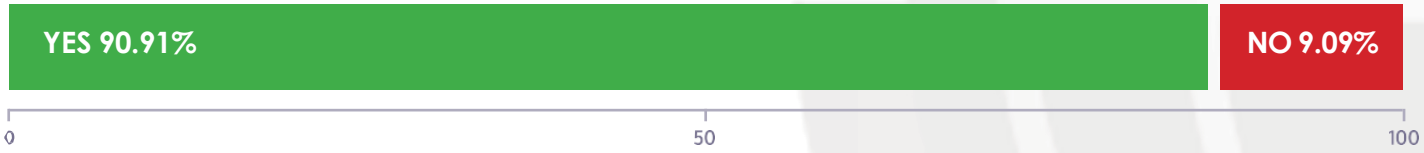


Summary

The main initiatives highlighted were from the UK ICO and the EDPS in terms of facilitating the sharing of big data in the private sector, with a key emphasis placed on harnessing the potential of data for the benefit of the European economy and society.

QUESTION 5:

Has your jurisdiction put in place any laws/ frameworks/policies/strategies which facilitate or promote sharing of public sector data (e.g. open data initiatives)?



Summary

Most respondents commented on having frameworks/policies/strategies which facilitate or promote sharing

of public sector data. Open data frameworks are in place in Ontario, Canada, and the Philippines. The UK, Israel, Europe and Hong Kong all have mechanisms in place to facilitate the use of public sector data for other commercial or non-commercial uses.

QUESTION 6:

What are the major issues/regulatory concerns in your jurisdiction in relation to data sharing, where the sharing is for the public good?

Summary

This question attracted a variety of responses from members. One common concern was around the definition of 'public good' and what constitutes data sharing for the public good, and the potential for misuse for gains other than societal ones.

Another common concern was around the lack of awareness around data sharing requirements, for example, lawful bases for sharing, the need for DPIAs, secondary processing, and issues over supervision of data sharing practices.

QUESTION 7:

What changes, if any, in relation to data sharing for the public good, are necessary in your Authority's view, to make to your jurisdiction's current legal framework?

(Please refer to any public statements you have made about this).

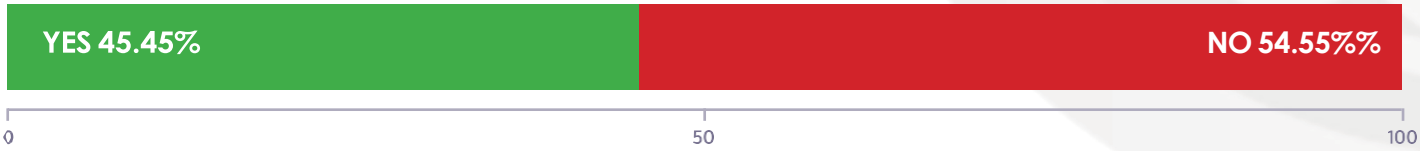
Summary

Again, this question resulted in a variety of responses, with some suggesting there was no need for a legal framework, with others suggesting that more explicit provisions for data sharing would be an advantage, with detailed ethical guidance as an accompaniment. Questions were asked as to what else regulators could do to assist smaller businesses with less expertise in data protection rules, and how growth and innovation can be fostered whilst maintaining a high standard of data protection rights for individuals. There was also a common theme regarding more consistency of definitions across jurisdictions which would help reduce legal uncertainty.

QUESTION 8:

For data sharing in the public sector, does your jurisdiction have a consistent approach across government agencies to information sharing/management? For example, is there an established framework of principles as a guide for all agencies?

If yes, please elaborate or if no, are there any issues experienced by the government agencies? (e.g. the need for repeated consent and increase of administrative costs)



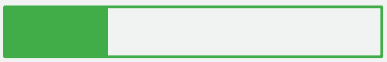
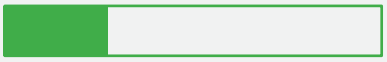
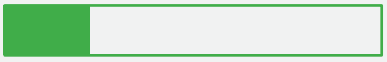
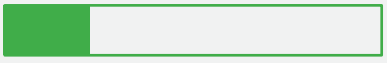
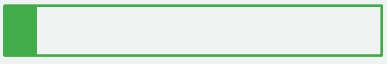
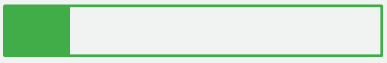
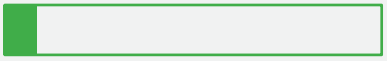
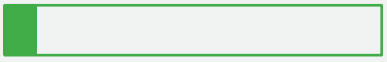
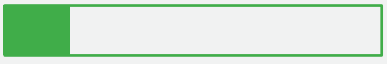
Summary

Interestingly, more than half of respondents state they do not have a consistent approach across government agencies to information sharing. Some discussed a 'patchwork' approach to public sector data sharing, with interoperability problems impeding data sharing and causing a risk averse culture, and less sharing that would be lawfully permitted.

Those respondents that do have a framework referred to their own legislative provisions, best practice codes or frameworks laid out in other legislation.

QUESTION 9:

In your jurisdiction, what are the most common purposes applied for data sharing?

Answers			Response Percentage	Response Total
1	Law enforcement/crime prevention		54.55%	6
2	Investigations (criminal, tax, administrative, etc.)		45.45%	5
3	Social welfare		36.36%	4
4	Tax administration/revenue generation		45.45%	5
5	Border management/security		36.36%	4
6	Legislative/policy development		27.27%	3
7	Research		54.55%	6
8	General KYC requirements		27.27%	3
9	Direct marketing/other advertising activities		9.09%	1
10	Labour/employment-related		18.18%	2
11	As an incident of mergers and acquisitions		9.09%	1
12	As an incident of providing goods/services		9.09%	1
13	Profiling		18.18%	2
14	Other (please specify):		45.45%	5
			Answered	11
			Skipped	1

Other categories mentioned:

- Local Government inc provision of services to the public, social care eg safeguarding and supporting vulnerable people inc children (this applies to some other sectors listed below as well)
- General Businesses (private sector)
- Charities/Not-for-profits
- Education
- Central Government - sharing across government, provision of services to the public
- Health and Social Care
- Legal (Law societies and firms)

Summary

The top two most common purposes for data sharing (from those jurisdictions who collect this type of data) was for law enforcement purposes, or conducting research. Tax investigations or administration was another popular response. However, outside of the options available, public sector data sharing for exercising public functions was deemed the most common purpose by some jurisdictions. For example, social and health care, safeguarding of vulnerable persons, children's services including education and other numerous public services.

QUESTION 10:

What are the most common lawful bases for data sharing involving personal data held by public authorities?

Answers		Response Percentage	Response Total
1	Contract	27.27%	3
2	Legal obligation/law	54.55%	6
3	Vital interests of data subjects	18.18%	2
4	Legal claims	36.36%	4
5	Public interest - health	54.55%	6
6	Public interest - research	54.55%	6
7	Other (please specify):	36.36%	4
		Answered	11
		Skipped	1

Summary

For those jurisdictions that collect this kind of data, the most popular legal bases for data sharing are where there is a legal obligation to share, or where sharing data is in the public interest for health or research purposes. One jurisdiction commented that there is a surprising amount of sharing based on individual consent, particularly in public sector areas which may result in an imbalance of power.

QUESTION 11:

In your Authority's opinion, what are the privacy and data protection concerns you have encountered regarding data sharing?

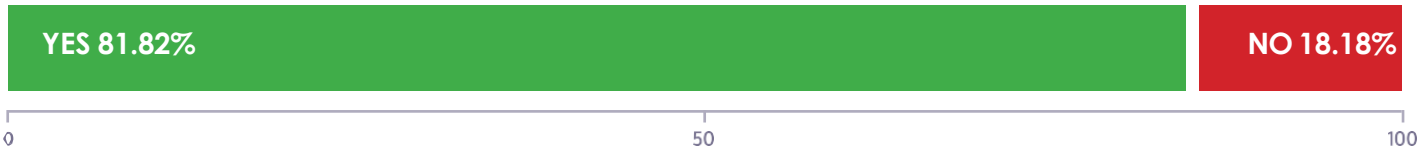
Summary

This was another question that elicited a wide range of responses. One DPA stated that there were no privacy concerns with data sharing in their jurisdiction. However, most DPAs responded with similar concerns around fear and lack of awareness of organisations in terms of how to share information whilst still protecting the rights of the individual.

The most common concerns were around establishing the correct lawful basis for sharing, lack of transparency, anonymisation/pseudonymisation, lack of control around third party processing, purpose limitation, security, excessive data sharing and retention, accountability and inadequate governance documentation, for example, Data Sharing Agreements, and individuals not being able to exercise their rights.

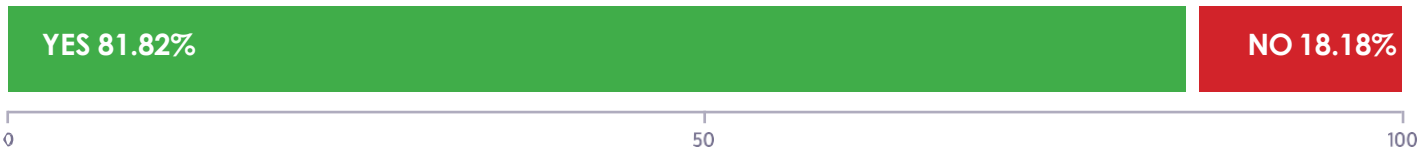
QUESTION 12:

Does your Authority have the power/mandate to review, on its own initiative, data sharing arrangements/agreements?



QUESTION 13:

Does your Authority accept requests from stakeholders (public/private) to review data sharing arrangements/agreements?



QUESTION 14:

In your jurisdiction, privacy impact assessments for data sharing are:

Answers		Response Percentage	Response Total
1	Required / mandatory	0.00%	0
2	Encouraged / best practice	45.45%	5
3	Other (please specify)	54.55%	6
		Answered	11
		Skipped	1

Summary

In most cases, DPIAs are only mandatory where the processing of personal data involves a high risk to the rights and freedoms of individuals in respect of their personal data. However, most Authorities recommend the use of DPIAs as a best practice tool to help mitigate any potential risk to individuals.

QUESTION 15:

In your jurisdiction, what are the common issues and/or challenges raised by personal information controllers with respect to their proposed data sharing initiatives? Select all that apply:

Answers		Response Percentage	Response Total
1	Perception that data sharing is prohibited	72.73%	8
2	Interpretation that all data sharing arrangements are consent-based	45.45%	5
3	Uncertainty as to what personal data can be shared	72.73%	8
4	Appropriate security measures for shared data	63.64%	7
5	Existing compliance check / case / complaint / investigation involving a data sharing arrangement	18.18%	2
6	Other (please specily):	45.45%	5
		Answered	11
		Skipped	1

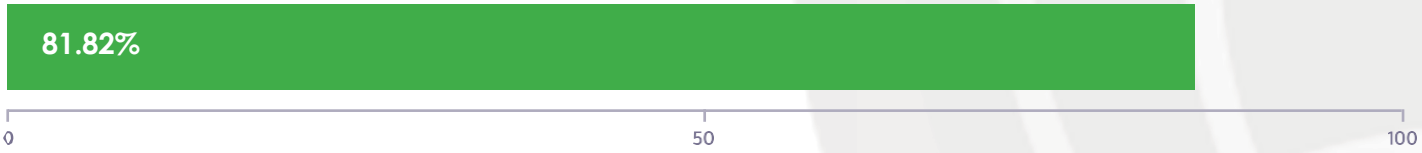
Summary

The majority of respondents stated that there was a perception amongst Controllers that data sharing is prohibited, despite numerous gateways being available in respective legislation. Equally, many Controllers felt uncertainty as to what personal data could be shared. It is possible that this uncertainty leads to the negative perception that data cannot be shared. Others quoted difficulties in meeting security obligations when data sharing was an issue.

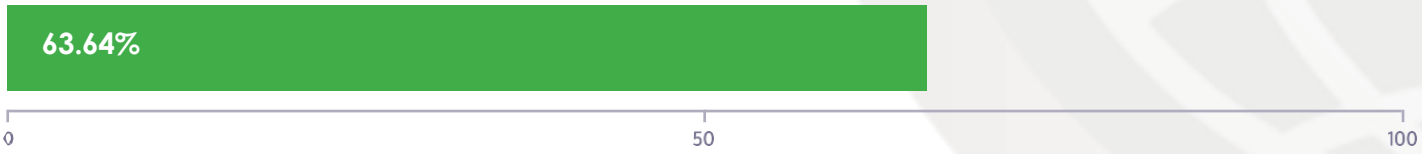
QUESTION 16:

What are the ways through which data protection authorities can encourage data sharing for the public good? Select all that apply:

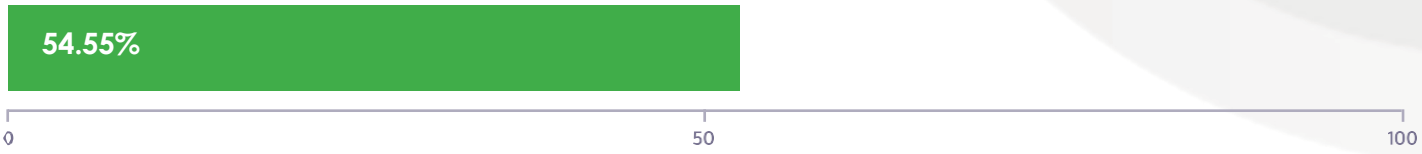
1: ISSUE ADDITIONAL GUIDELINES/REGULATIONS



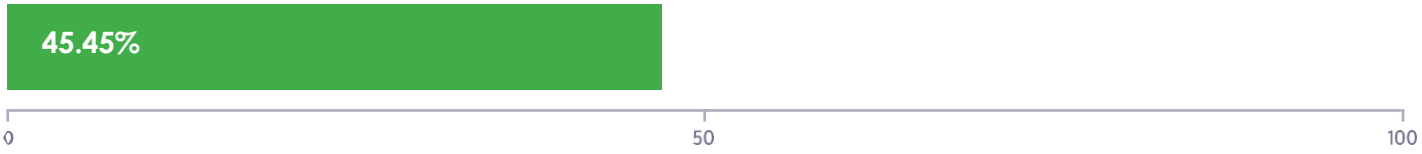
2. OFFER A REGULATORY SANDBOX



3. OTHER



4. INCENTIVISE DATA SHARING & ISSUE CERTIFICATIONS



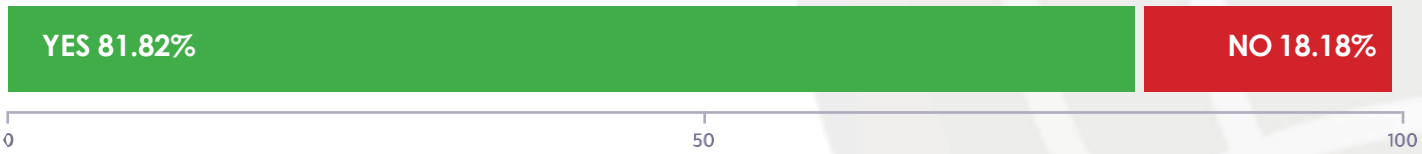
Summary

Overwhelmingly, respondents suggested that additional guidance and/or regulations would help to encourage the sharing of personal data for public good. One respondent suggested lobbying parliament with a view to modernising privacy laws to facilitate the appropriate and accountable use and sharing of personal data. However, practical guidance and clarification of existing rules could also assist.

The UK ICO also echoed those sentiments and have found their data sharing code and guidance on anonymisation and Privacy Enhancing Technologies has helped to provide greater regulatory certainty. They also suggest certification mechanisms may help reduce uncertainty.

QUESTION 17:

Perspective 1: State of play of data protection laws and enforcement concerns. Does your jurisdiction's privacy law recognise the importance of allowing personal data to be reused or shared for public good?



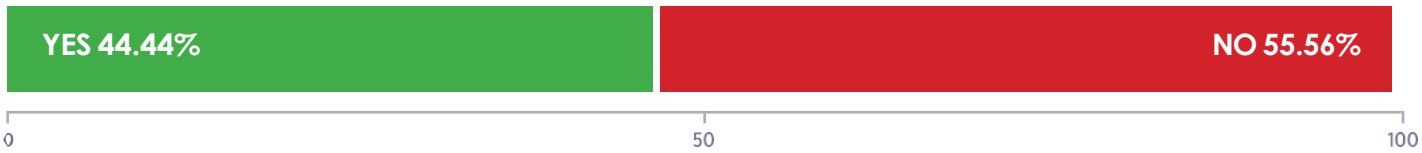
Summary

Most respondents said they have privacy laws that recognise the importance of allowing personal data to be reused or shared for public good. However, from the respondents that commented further, only one jurisdiction appears to have a specific provision for the re-use of personal data for purposes which are considered to be in the 'public good'.

For other jurisdictions, more general provisions for data sharing or disclosure of personal data are included, which

QUESTION 18:

If you answered yes to the question above, has your Authority encountered issues in enforcing the relevant legal provisions?

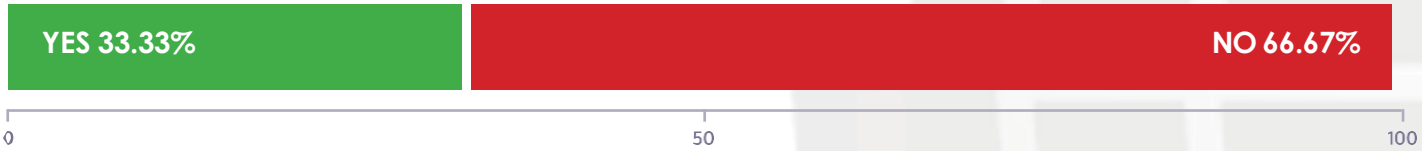


Summary

This question resulted in a fairly even split from respondents, with just under half having encountered problems enforcing the relevant legal provisions.

QUESTION 19:

Has your Authority received any feedback from the public regarding the issues in applying the relevant legal provisions?



Summary

Two thirds of respondents had not received any feedback from the public regarding the issues in applying the relevant legal provisions. However, a Canadian public survey highlighted that there was a moderate to high level of concern regarding the possibility of sharing of individuals' personal data by the Government of Canada, either between Government departments or by private companies, if the sharing was either without consent or not compatible with the service they signed up for.

QUESTION 20:

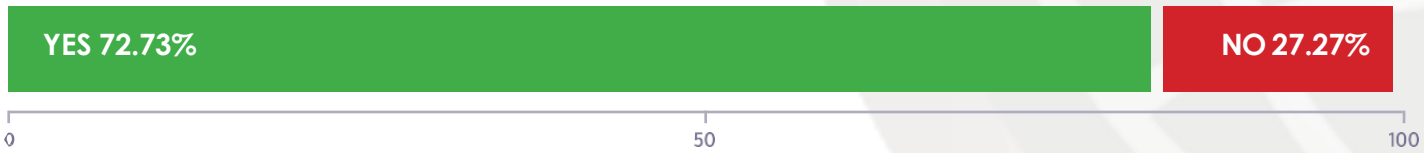
If you answered 'No' in question 17, has your Authority encountered any general issues in assessing the legality of data sharing for the public good?

Summary

Two thirds of respondents had not encountered any general issues in assessing the legality of data sharing for the public good. Germany explored the issue of whether data can be *sold* when it is being disclosed for the public good (e.g. health information sold to a research firm). Their general finding was that this is permissible, but must be made very transparent. Jersey stated they experienced issues during the Covid pandemic where many Controllers, particularly in the health and hospitality sectors were unsure what data could be shared and in what circumstances.

QUESTION 21:

Does the privacy law and/or other data related laws in your jurisdiction contain any provisions requiring, facilitating and/or regulating the sharing of data? e.g. the right to data portability, data sharing obligations imposed to organisations, etc.



Summary

Nearly three quarters of respondents have legislative provisions requiring, facilitating and/or regulating the sharing of data.

QUESTION 22:

With a focus on the broader issue of global data governance and responsible data flow across borders, please give examples of domestic good practice that could be applied internationally. How can the GPA promote good practice in this area?

Summary

Again, this question promoted a varied response from members. Canada suggested, for example, that exceptions to consent were needed to facilitate legitimate commercial processing of data that was in the public interest, recognising that any override of consent would have to balance the interests of the organisation against those of the individual.

The DIFC suggested their EDMRI+ due diligence assessment, which includes documenting decision making around using certain importers and providing guidance about filling gaps in the importer's compliance preparedness.

The EDPS suggested the GPA could promote good practice in this area by firstly assessing and comparing the different legislative initiatives promoting data sharing and data reuse, which would allow identification of common principles and practices for the effective sharing and reuse of data while at the same time safeguarding the right to privacy and data protection.

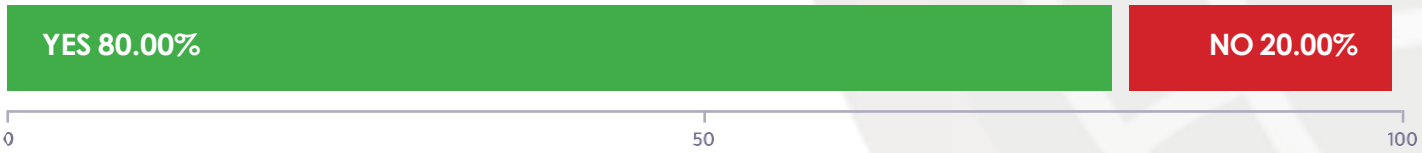
Hong Kong identified good practices such as having robust policies and procedures in place in respect of data sharing, conducting DPIAs for systemic or large-scale data sharing, and appropriate security measures and transparency for data subjects.

Ontario, Canada suggested model clauses for cross-border data flows could be adapted for data sharing, and suggested the GPA could start by providing a library of tools that DPAs or other oraganisations have created - such as model contractual clauses, or even arrangements such as sandboxes, as well as an analysis of the key elements of these tools should other DPAs want to create new ones.

QUESTION 23:

Perspective 2: Data Sharing in the Health Sector

For health/medical data sharing, does your jurisdiction have an established framework for sharing (electronic) health/medical data (be it public or private organisations)?



Summary

Most respondents said they have an established framework for sharing (electronic) health/medical data. Dubai have a separate 'Health Data' Law, whereas the UK Department of Health and Social Care has produced a strategy outlining the future of health data in England. The document promotes data sharing for research purposes within the health sector.

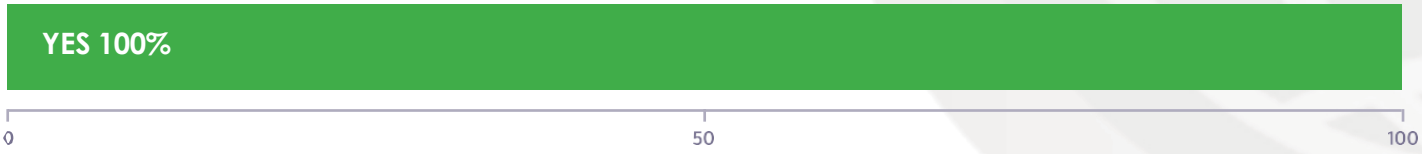
In Israel, regulations oblige each public body to establish an internal committee for data transfers, whose members include the director general of the public body, the legal advisor, and a data management and security specialist.

In Europe, the European Commission has published a Proposal on the European Health Data Space (EHDS) which aims to support individuals in taking control of their own health data, as well as supporting the use of health data for better healthcare delivery, better research, innovation and policy making. This will enable the EU to make full use of the potential offered by a safe and secure exchange, use and reuse of health data.

The Philippine Health Information Exchange (PHIE) is a platform for secure electronic access and efficient exchange of health data and/or information among health facilities, health care providers, health information oraganisations, and government agencies in accordance with set national standards in the interest of public health.

QUESTION 24:

In your jurisdiction, are there barriers (regulatory or non-regulatory) that prevent the access, use and sharing of digital health data and information for the public good? If so, what changes can be made to reduce barriers to the access, use and sharing of digital health data and information for the public good?



Summary

All respondents alluded to barriers preventing access to, use and sharing of health data for the public good.

As expected, this question provoked a range of responses from member DPAs. Jersey mentioned the lack of collaboration and communication between private General Practitioners and Government Health Services. Canada bemoaned its patchwork of information laws, interoperability issues and aversion to risk as being a significant problem.

The UK referred to concerns of commercial organisations sharing health data for profit, while the EDPS discussed problems of individuals having limited control over their health data at national and cross-border level. Hong Kong suggested individuals may be concerned to share their own medical data, even if for the public good.

In terms of possible remedies, Ontario, Canada suggested getting everyone on the same page regarding motivations and overall framework for data sharing, as well as finding funding to allow all health providers to transition to whatever new

QUESTION 25:

With specific reference to the sharing of health data for research purposes, please identify the key data protection and privacy issues to address and/or prioritise eg. transparency, privacy enhancing technologies, etc.

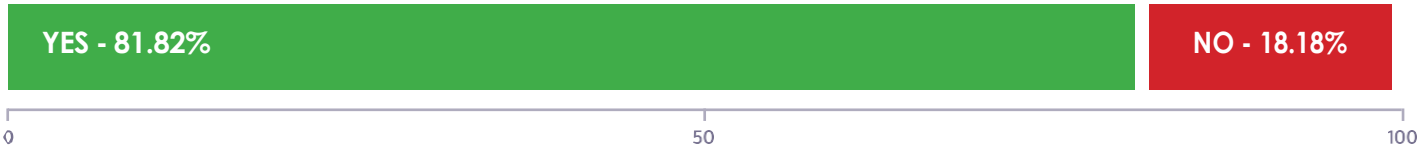
Summary

The transparency of the data processing, together with accountability proved to be the overwhelming common response from respondents. The secondary use of personal data by third party private sector companies was also a common cause for concern. In terms of addressing those concerns, a number of respondents identified Privacy Enhancing Technologies (PETs) as a potential solution, as well as anonymisation, better security controls and data minimisation.

QUESTION 26:

Perspective 3: Data Sharing and the COVID-19 Pandemic

Has your jurisdiction created a data sharing framework/policy/strategy for facilitating data sharing during the COVID-19 pandemic?



Summary

Most respondents implemented guidance of some description specifically relating to data sharing during the Covid-19 pandemic. In addition, the EDPS issued its Formal Comments on a package of three legislative proposals for a European Health Union which aims to improve the protection, prevention, preparedness and response to human health hazards at EU level.

QUESTION 27:

How can measures introduced to fight the pandemic be used sustainably for the public good?

Summary

This question provoked a varied response from member Authorities. It was suggested that some of the guidance included within the Covid-19 Compendium of Best Practices could be adapted for wider use in relation to data sharing for the public good, as could other frameworks and agreements, as long as they balance data sharing with the need to protect personal privacy.

Canada referred to the key principles in their Framework for the Government of Canada to assess privacy- impactful initiatives in response to Covid-19 as a starting point for further development, while the UK ICO referred to the lessons learned from the pandemic and the UK's Data Saves Lives strategy, which builds on measures with recommendations including investment in secure data environments to power life-saving research and treatments; using technology to allow staff to spend more quality time with patients; and giving people better access to their own data through shared care records and the NHS App.

The EDPS highlighted the importance of distinguishing between 'emergency measures', which should by definition be limited in time, and 'emergency preparedness measures', whereby we have the right governance framework/infrastructure etc. in place to enable reuse of data as needed to respond to similar public health emergencies in the future. They also suggested stronger data governance, including the clarification of key concepts that would simplify data protection compliance would be a benefit to the scientific research community. This was also a point of concern for Ontario, Canada, who suggested there is a lot of public mistrust about the "temporary" nature of many of these measures, so making them permanent could be very problematic.

QUESTION 28:

Where COVID-19 measures have been decommissioned, please list three issues in relation to data sharing that have been the greatest concerns for data protection compliance.

Summary

There were a variety of answers to this question. Proper deletion of data after Covid measures terminate, continued and excessive sharing outside the requirements coupled with poor data security, data minimisation and data retention were highlighted as key issues for data compliance.

QUESTION 29:

Perspective 4: Case Study Examples

Please outline some examples of good practice in utilising privacy protective measures/ regulations/guidance to facilitate data sharing for the public good.

Summary

The UK ICO gave examples of funding from the UK Government's Regulators' Pioneer Fund to explore barriers to adoption and explore ways to address data sharing challenges. They have also recently consulted on guidance for PETs and are supporting CDEI with the US-UK Prize Challenge focused on advancing the maturity of PETs for privacy-safe data sharing to combat financial crime and healthcare issues.

Hong Kong have privacy protecting measures adopted in the 'HA Go' application, e.g., validation and encryption.

QUESTION 30:

Have you conducted any research into challenges to data sharing for the public good?

Summary

Whilst only a third of respondents have conducted any research into challenges to data sharing for the public good, some authorities have been very active in researching this area. The UK ICO has conducted a survey of DPOs working in healthcare organisations to understand the most common data sharing challenges they faced, the EDPS has organised a webinar on 'Data for the public good: Building a healthier digital future', and one jurisdiction has found the biggest challenge to be defining the key terms and the areas to focus on. For example, is data sharing the same as data transfer/ data disclosure? How to define 'public good'? What are the key use cases of data sharing that data protection authorities should focus on (e.g., public sector open data, public-private sector data sharing, private sector bilateral or multi-lateral data sharing, local or cross-border data sharing) and are there different good privacy practices in different use cases?

GPA

Global Privacy Assembly