Working Group on Data Sharing for the Public Good

Report – September 2024

Office of the Information Commissioner, Bailiwick of Jersey

Table of Contents

Executive Summary

I am very pleased to present my third 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.

Over the course of 2024, 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 met on average once a quarter, with more frequent sub-group meetings.

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)**
- Argentina, Agencia de Acceso a la Información Pública **(AAIP)**
- UN Global Pulse **(UNGP)** (Observer)

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

During its recent meetings, the DSWG has continued discussions regarding our previously identified key areas for further investigation:

Further to this, we have:

- Heard representations on key data sharing policies and objectives from the DIFC, EDPS and UK ICO;
- Established a sub-group to work on creating guiding principles for data sharing;
- Established a second sub-group that is working on principles around 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 2023, the DSWG has met three times as a whole group and held additional sub-group meetings at the time of writing this report, and has conducted the following activities:

1. Discussed how to best utilise the results of the 2022/2023 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, as noted above.

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.

Topics addressed at our regular general meetings included:

1) **Priorities for 2024**

The DSWG members considered immediate priorities. Some expressed an interest in joining a sub-group regarding international transfers of health data for research purposes. Others also expressed support for this sub-group. It was established in March 2024 and held meetings in April (vis a vis an invitation to the OECD Health Data Governance Workshop) and May 2024.

The UK Information Commissioner's office informed attendees about their 'Think, Check Share' campaign which aims to raise awareness about responsible data sharing. More information is available at New ICO campaign promotes sharing data to safeguard children | ICO

2) **'Guiding Principles on Data Sharing for the Public Good'**

In preparation for our last GPA conference in Bermuda and ongoing since then, the DSWG prepared a guiding principles document and discussed the programme of work for the year to come. The Guiding Principles on Data Sharing was finalised in March 2024 (please see Appendix 1).

3) **International Transfer of Personal Data for Health Purposes**

This DSWG sub-group progressed to establish the following plans and considerations for its direction:

- Identify risks and benefits of this type of data sharing
- Consider challenges when sharing with government authorities
- 'What does good look like' – seek to prepare guidance / add to guiding principles
- Discuss with group members leading on this, such as OECD, and raise any questions in order to set the main focus of the sub-group

The final point above is in progress at this time.

Action Plan 2024 - 2025

The work of the DSWG will focus on the advancement of privacy protection worldwide and how to enable safe but efficient data sharing, as well as the promotion of high data protection standards as stated in the Resolution on the GPA's Strategic Plan (2023 – 2025). 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 use by the wider GPA membership and developing a governance framework for its contents;
- 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 Jersey in October 2024.

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. We have attempted to create a starting point for this concern with the document at Appendix A.

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 Guiding Principles

GPA DATA SHARING WORKING GROUP

Guiding Principles on Data Sharing for the Public Good

Guiding Principles on Data Sharing for the Public Good

Governments, businesses and citizens need to understand, accept and balance the obligations to protect against threats and prevent crime or other damages with the need to share personal and other data for precisely those purposes while ensuring the right to data protection and privacy of individuals affected by such data operations. Lessons learned from the Covid 19 pandemic provide the most recent, tangible experience of how to find this all-important balance.[1]

The following guiding principles have been produced to give businesses, organisations and individuals throughout multiple jurisdictions the confidence to share data in a safe, fair and transparent manner for the public good.

Data sharing can benefit the public in all jurisdictions. Efficient sharing of data can drive innovation and competition, enhance public service delivery, improve insights, outcomes and choice for members of the public. Another key driver is that of establishing appropriate protocols and safeguards to assure data subjects that their rights and redress options are intact, and that those rights can be exercised effectively by individuals affected.

Any references to 'Data Protection and Privacy laws' refer to the different legislative and regulatory frameworks across the various jurisdictions that govern the protection of individuals' personal data and their privacy.

Whilst the guiding principles we set out here are generally applicable to sharing data within the different Data Protection and Privacy legislative frameworks in each jurisdiction, it will of course be necessary to consult individual Data Protection Authorities and their websites/resources for more detailed information about sharing data within a specific jurisdiction.[2]

You may also wish to review the GPA Resolution on achieving global data protection standards which lists further complementary principles: "Principles to ensure high levels of data protection and privacy worldwide" https://globalprivacyassembly.org/wp-content/uploads/2023/10/3.-Resolution-Achieving-global-DP-standards.pdf

[2] Data sharing may not necessarily be defined in Data Protection and Privacy Laws and may be encompassed by other terminologies such as the 'use', 'disclosure', 'transfer', etc. of data.

Guiding Principles:

- **General principle.** Data Protection and Privacy laws provide useful frameworks through which data can be shared in a fair, secure and proportionate manner, promoting public trust and confidence, while maintaining the fundamental right to data protection and privacy. They are not designed to prevent you from sharing data when you approach it in a fair and proportionate way.

- **Purpose of sharing data.** Ensure that data is shared for a precise and lawful purpose. Be conscious that sometimes it can be more harmful for the public good not to share data, than to share it. Thus, double-check the specificity and legitimacy of any stated purpose of desired data sharing schemes.

- **Fairness and transparency**. You must share data fairly and transparently. You must not share data in ways which would have unjustified adverse effects on members of the public. You must ensure individuals know what is happening to their data, who is processing it and for what specific purpose, and provide clear and accessible information to them. This will help engender public trust in how personal data is being used.

- **Compliance with laws.** Consider legal aspects which may impact your proposed data sharing. This includes ensuring compliance with the relevant Data Protection and Privacy laws that apply to the jurisdiction where the sharing is taking place, but also that the sharing would not breach any other laws. You must also identify if you have a legal power to share, particularly if you are a public sector body.

- **Data sharing agreement.** Consider putting written agreements in place (such as a data sharing agreement or an information sharing protocol/contract) between organisations that are considering sharing data with each other, to make the data sharing arrangements clear to all the parties. Such agreements could cover what types of data will be shared, the purpose of the sharing, what happens to the data at each stage, for how long the data will be shared, information governance arrangements including security measures, what organisations will be involved as well as their respective roles and responsibilities. You should review agreements on a regular basis and update them when appropriate.

- **Privacy / data protection impact assessment.** Consider whether it would be appropriate to conduct a risk assessment

prior to sharing, highlighting any potential risks to individuals and/or the public at large, and any options to introduce safeguards to mitigate such risks. This should help you to promote public trust in your data sharing plans. Such assessments should also factor in the risks involved in not sharing data. Depending on the specific laws in your jurisdiction, you may be obliged to carry out risk assessments in certain situations and possibly liaise with a supervisory authority.

- **Sensitive data/ special categories of data**. You must identify data that is particularly sensitive which could create significant risks when shared, such as data relating to health, as well as data relating to vulnerable members of the public, and ensure adequate safeguards are in place to protect such data. When deciding whether to share children's personal data, you should take into account the best interests of the child, as set out in the United Nations Convention on the Rights of the Child (UNCRC).

- **Special circumstances**. Data Protection and Privacy laws may allow you to share data in an emergency or urgent situation, as is proportionate and necessary. Such situations may include the immediate need to protect the public at large (such as public health), or where there is risk of serious harm to specific members of the public. Processes established under such circumstances should be evaluated, when the special situation is over, and changed as needed and appropriate. You should plan ahead as far as possible for different emergency situations and put contingencies in place. Having a joined-up public service response that enables rapid/urgent data sharing can make a significant difference to public health and safety, as demonstrated by the response to the coronavirus pandemic and other crises.

- **Necessity, proportionality, data minimisation and retention time**. Ensure you are only sharing data that is necessary and proportionate; the minimum personal data needed for the purpose for which it is being shared. Make sure you retain the data only for so long as is necessary.

- **Accuracy.** You must take all reasonably practicable steps to ensure that the data to be shared are accurate, i.e., correct, relevant and actual/up-to-date.

- **Less privacy-intrusive means**. When assessing whether sharing data would be necessary and proportionate, you must consider whether any less intrusive means exist to achieve your purpose. This might involve sharing less data, or not sharing at all.

- **Privacy by design and default**. Ensure you implement a privacy by design and default approach that is embedded into the design and planning phase of any data sharing arrangement, or any system, project or app which involves data sharing. This may also include measures like anonymization or pseudonymisation. In general, consider if Privacy-Enhancing-Technologies (PETs) could be used or helpful to mitigate potential privacy risks.

- **Security**. When sharing data, you must do so securely, having appropriate and sufficient measures in place to safeguard people's data. This includes assessing the general security of the processing and the cyber security risks of any relevant digital systems.

- **Rights of individuals**. Any data sharing arrangement must have procedures and policies in place that allow members of the public to easily exercise any rights they have relating to their personal data, and allow organisations to deal efficiently with incoming queries and complaints. Review that feedback regularly to obtain a clearer understanding of public attitudes to the data sharing you carry out and consider if you should alter your sharing accordingly.

- **Staff training.** Ensure staff in organisations who are likely to make decisions about sharing data have received adequate training to do so appropriately within the relevant jurisdiction. Also new incoming staff should receive appropriate education on data protection and privacy matters.

- **Documentation**. Document your decision to share data and your justification. This will be essential to demonstrate compliance with any relevant data protection or privacy laws that may be in place in a specific national legislation. Bear in mind that a data protection and privacy supervisory authority, if any, may conduct compliance investigations.

Additional Resources:
The GPA Working Group on Data Sharing for the Public Good was created initially as a response to the Covid pandemic and associated data protection considerations. The emergency circumstances requiring collection and processing of personal information across all sectors, public, private, retail, healthcare, education, and so on, as well as the critical decisions to be made based on vast amounts of such data necessitated the establishment of the GPA Covid 19 Task Force in mid-2020.

The Task Force was broken down into two sub-groups, one with the remit to create a compendium of data protection practices and issues for dealing with such recently unprecedented circumstances, and the other to address regulatory capacity building. The resources produced by the sub-groups are available as follows:

- Compendium of Best Practices (Part 1)
- Compendium of Best Practices (Part 2)
- Roundtable Summary – Lessons Learned and the New Future
- GPA C-19 WG and CIPL – Lessons Learned
- COVID 19 regulatory capacity survey results – final Sub-group 2 report

GPA

Global Privacy Assembly