Global Privacy Assembly

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