45th Closed Session of the Global Privacy Assembly

October 2023

Achieving global data protection standards: Principles to ensure high levels of data protection and privacy worldwide

This Resolution is submitted by …

SPONSORS:

- Information Commissioner's Office, United Kingdom

CO-SPONSORS:

- National Institute for Transparency, Access to Information and Personal Data Protection (INAI), Mexico – GPA Chair
- Data Protection Commissioner, Council of Europe
- European Data Protection Supervisor, European Union
- National Commission for Informatics and Liberties (CNIL), France
- Federal Data Protection Commissioner (BfDI), Germany
- Data Protection Authority, Bailiwick of Guernsey
- Garante per la protezione del dati personali, Italy
- Federal Data Protection and Information Commissioner (FDPIC), Switzerland
- Regulatory and Control Unit of Personal Data, Uruguay

The 45th Global Privacy Assembly 2023:

EMPHASISING the importance of high standards in both upholding data protection and privacy as a fundamental right and protecting the rights and interests of individuals through the appropriate processing of personal data;

RECOGNISING that consistent interpretation between jurisdictions is important for maintaining high standards and fostering a clear regulatory environment. That, in turn, ensures people's personal data is protected and their rights are upheld, organisations earn people's trust, and innovative products and services for the digital economy can develop.

RECALLING the Madrid Resolution[1] adopted in 2009, which specified a set of principles and rights guaranteeing the effective protection of privacy with regard to the processing of personal data, and *ACKNOWLEDGING* its contribution and global influence;

RECOGNISING THAT jurisdictions around the world have been developing their own data protection laws and regimes which reflect the values, priorities and needs of their culture and society, and *FURTHER RECOGNISING* the need for international efforts to continue to build upon commonalities, complementarities and elements of convergence in order to foster future interoperability between them;

EMPHASISING THAT the context in which data protection and privacy principles and laws must be applied has changed, and continues to evolve, as developments in technology, innovation and digitalisation lead to new activities and business models which increasingly rely on processing large volumes of personal data in new and progressively complex ways, and *ACKNOWLEDGING THAT* laws, principles and the way in which they are implemented must continue to provide a high level of protection;

NOTING THAT such developments range from generalised digitalisation of services to widespread development and deployment of artificial intelligence, the use of automated decisions and innovations using biometric technologies;

CONCERNED THAT such developments can pose new challenges for the implementation and enforcement of data protection and privacy laws, as they present risks relating to data minimisation, security, transparency, accuracy, that can cause significant negative effects such as unfair, discriminatory and biased outcomes for individuals, or affect their ability to exercise their data protection and privacy rights;

CONCERNED THAT this broad context inevitably includes more intrusive processing of personal data, including sensitive personal data, especially those of children and vulnerable people, where the need to ensure rights are upheld and able to be exercised is particularly acute / important;

NOTING THAT these concerns have led GPA members in various jurisdictions to take enforcement action such as issuing fines, requiring the deletion of unnecessary data and algorithms, and issuing orders to stop processing. Members have also raised concerns relating to transparency, fairness, bias and discrimination;

WELCOMING the efforts of GPA members in various jurisdictions to identify the data protection and privacy implications of emerging and future technologies;

NOTING the importance of taking a human-centred and ethical approach to emerging technologies, and *EMPHASISING THAT* data protection and privacy are fundamental to foster

[1] 14302 STANDARDS.qxp:Maquetación 1 (globalprivacyassembly.org)

data governance, in order to safeguard the recognition of rights and interests of individuals in the digital environment;

EMPHASISING THAT the context of a rapidly developing global digital economy also highlights the need to send and receive data across borders in a way that protects people's data protection and privacy rights;

FURTHER EMPHASISING THAT in order to enable data to flow across borders, there is a need for frameworks and mechanisms with comparable high standards to ensure consistent protection of individuals' rights while facilitating the international flow of personal data needed in a globalised world;

HIGHLIGHTING the importance of cooperation to identify and work towards convergence between the protections in legal frameworks and instruments to achieve a high level of data protection and privacy, foster future interoperability and facilitate Data Free Flow with Trust;

AFFIRMING the ability of GPA member authorities to act as trusted expert advisers, and the importance of policymakers, authorities and other stakeholders working together to protect personal data and uphold people's rights in the context of today's global digital economy;

The GPA acknowledges the value of global standards regarding data protection and privacy and therefore recognises and promotes the following high-level principles, rights and other elements as important to achieve high standards of personal data protection and privacy in the context of today's global digital economy:

1. **Lawfulness and fairness**

The processing of personal data must be lawful in accordance with applicable national legislation and international agreements. We also highlight the principle of fairness, and emphasise that personal data must not be obtained by deceitful or fraudulent means, prioritising the protection of the data subject's interests and the reasonable expectation of privacy, ensuring that the processing does not result in unfair, discriminatory or biased outcomes.

2. **Purpose specification**

Processing should be limited to the fulfilment of specific, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes.

3. **Necessity and proportionality**

We reaffirm the principle of data minimisation, according to which personal data should be limited to that which is adequate, relevant and not excessive in relation to the purposes of

the processing. We also emphasise the importance of overall proportionality and necessity in the context of the overall objective of the processing, in relation to people's information rights, to enable appropriate decisions to be made about the use of newer types of processing and technologies, such as those which process sensitive / special category data or biometric data.

4. **Data quality**

All reasonable steps should be taken to ensure that personal data processed is accurate, and kept up to date as necessary to fulfil the purposes. This is particularly important when the risks of significant decisions about individuals being made on the basis of incorrect information are exacerbated by the use of automated decisions, algorithms and AI, which in turn can result in serious implications for decisions relating to, for example, finance, research and criminal offences. Automated decisions must be based upon accurate information, and systems trained by accurate and unbiased information.

5. Retention / storage limitation

Personal data should be retained only as long as is necessary to fulfil the purposes for which it is processed, and should be deleted or anonymised when it is no longer needed for those purposes.

6. **Transparency**

We emphasise the importance of clarity, accessibility, and ease of understanding so that people are properly informed about how their personal data is processed, and are able to exercise their rights. Information should be actively provided to ensure people are aware of the processing, which might require different mechanisms depending on the context.

7. **Accountability**

We emphasise the importance of accompanying practical elements to demonstrate compliance with the high-level principles and operationalise the principle of accountability, such as, but not necessarily limited to, the proactive measures set out below.

8. Security

Controllers and processors must have appropriate measures in place to ensure confidentiality, integrity and availability of personal data. Security is an increasingly important requirement as security risks can be heightened as technology advances, as participation in the digital environment increases, and as volumes of personal data processed in the global digital economy increase.

In particular, this can lead to increased cybersecurity risks. Noting that cybersecurity crosses regulatory spheres, we emphasise the importance of clear and consistent laws and regulatory

approaches, and of cooperation between regulators, cybersecurity bodies and other relevant stakeholders to effectively address global security risks.

9. **Legitimacy and bases for processing**

We emphasise the importance of providing a range of appropriate and proportionate legal bases for processing, for example contract, public interest, legal obligation, legitimate interest, as well as consent, depending on the purposes and context of the processing. Where consent is available as a basis, we emphasise the importance of the requirement for it to be meaningful and valid, that it offers real choice and control, and that it should be the freely given, specific, unambiguous and informed will of the data subject, with their agreement signified by statement or clear affirmative action.

10. **Sensitive data**

Extra protections should be put in place for personal data relating to certain aspects and characteristics, such as racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, data relating to health and sex life, or criminal offences. We also emphasise the need to review the types of personal data included in this category, to keep up with technological developments that enable the identification of personal data and may pose risks relating to its sensitive nature (for example data relating to biometric or genetic information, and to neurotechnology). We further note that data that is not sensitive in its own right can become so when combined with other data. This can include inferred data where in certain circumstances, records relating to, for example, browsing or viewing habits may be used to infer an individual's ethnicity, beliefs, political views, health status or sexual orientation.

11. **Protection for children and vulnerable people**

As children and vulnerable people may be less aware of the risks involved in the processing of their personal data, and might therefore be less able to exercise their data protection and privacy rights, we emphasise the importance of making specific provisions for their protection. We welcome the efforts of GPA members and others in complementing legal requirements with codes of practice and guidance.

12. **Controllers and processors**

It is important that clear arrangements are in place between controllers and processors/service providers acting on behalf and under the instructions of controllers, with respective obligations and responsibilities, specified details about the processing, and instructions set out in a contract.

13. **International transfers of personal data**

We emphasise the importance of providing for the protection of personal data across borders with a range of transfer mechanisms, such as adequacy, model clauses, certifications and administrative arrangements, to ensure that protection travels with the data. We note the benefits of building on commonalities, complementarities and elements of convergence in order to foster future interoperability between existing regulatory approaches and mechanisms enabling safe, trustworthy cross border data flows. We welcome the work of the G7 and its Roundtable of Data Protection and Privacy Authorities on developing and operationalising Data Free Flow with Trust, and recognise the importance of work on this topic as the global digital economy generates increased flows of data.

We reaffirm the GPA Resolution on Government Access to Data, Privacy and the Rule of Law: Principles for Governmental Access to Personal Data held by the Private Sector for National Security and Public Safety Purposes, and welcome the Organisation for Economic Co-operation and Development (OECD) Declaration on Government Access to Personal Data Held by Private Sector Entities.

14. Right to information

We emphasise the importance of a right for people to be informed about what personal data is being processed, how, by whom and for what purposes – and about what rights they have in relation to that processing. We note the link with the principle of transparency, and emphasise the increasing importance of individuals being properly informed as automated processing operations can be increasingly complex and opaque.

15. Rights of Access, Rectification, Deletion and Objection

We emphasise the importance of data subject rights of access, rectification, deletion, and objection and particularly highlight the importance of the right of access, as a key enabler of people's other data protection rights.

16. Restriction

We would also emphasise the importance of a right to restriction of processing, to limit the use of personal data and protect people from the risk of inaccurate, discriminatory and unfair decisions made when that data is inaccurate, processed unlawfully, objected or in dispute.

17. Data portability

We note the importance of data subjects being able to obtain from a controller a copy of their personal data in a structured and commonly used electronic format, to allow them to reuse their data across different services and transfer to another controller as needed.

18. Rights relating to profiling and automated decisions

We highlight the importance of ensuring that rights are provided for data subjects where profiling is carried out, or decisions significantly affecting them are made, based on automated means without human intervention. These rights may for instance include rights to obtain information about the logic involved in the processing, to obtain human intervention or to contest a decision.

19. Ability to exercise rights

We would also highlight the importance of providing **simple, efficient ways for people to exercise rights**. This is especially important as personal data types evolve and processing operations become more complex. Any restriction or limitation of rights should be provided for by law and must be applied to the extent necessary and proportionate to safeguard a public interest objective or the rights and freedoms of others.

20. Proactive measures

We emphasise the need for proactive measures to be put in place to implement data protection and privacy on a practical level. Linked closely to the **accountability principle**, we emphasise the importance of practical implementation and compliance with data protection and privacy requirements, and of demonstrating compliance to both regulators and the people whose data is being processed.

In particular we highlight the importance of:

- **Privacy and personal data protection by design**, as new, innovative products, technologies and ways of processing personal data develop it is vital to build in data protection and privacy from the start of such projects to identify, prevent and mitigate harms, and to ensure that rights can be upheld and exercised. This could include elements such as privacy-enhancing technologies and the use of regulatory sandboxes;
- **Privacy and personal data protection by default** should apply in programs, services, computing systems or platforms, electronic applications or any other technology that process personal data;
- **Proactive compliance measures**, such as:
  - **Privacy / data protection impact assessments** to identify and mitigate data protection and privacy risks
  - **Independent audits** to identify and take appropriate action on non-compliance as needed to protect people's data protection rights
  - **The adoption and implementation of internal data protection policies** which staff must comply with
  - **Training, education and awareness-raising** as appropriate to staff who process personal data, and the existence of data protection officers or equivalent responsible staff to oversee compliance

- **Breach prevention, detection and response measures**, including **notification** to regulatory authorities and to the people affected, as appropriate
- **Privacy management programmes** and other similar approaches to provide for and demonstrate effective safeguards and compliance with data protection and privacy requirements
- **Codes of practice or conduct,** to develop specific guidelines within sectors that effectively address key data protection and privacy issues within those sectors
- **Certification** for organisations to demonstrate their compliance with data protection and privacy requirements via approved schemes
- **Mechanisms to assist data subjects in submitting queries and complaints** regarding the processing of their personal data.

21. Supervisory authority

We emphasise the importance of the existence of an independent supervisory authority. Authorities should be independent, provided with sufficient powers to investigate and take action, sufficiently resourced to be able to effectively perform their duties, and their leaders and staff should have appropriate levels of expertise and technical competence. We recognise the importance of authorities having sufficient jurisdiction to supervise public as well as private sectors, to ensure consistency of application of data protection and privacy legislation. We reaffirm the GPA Global Frameworks and Standards Working Group's analysis and report on the Key features of independent data protection / privacy authorities.[2]

We also emphasise the importance of authorities, in addition to monitoring and enforcing compliance, undertaking awareness-raising and proactive, preventive engagement with controllers where possible and as appropriate, for example by producing guidance, undertaking stakeholder consultation, and projects to promote compliance such as regulatory sandboxes.

22. Cooperation

We emphasise the importance of cooperation by supervisory authorities, **both with other data protection and privacy authorities, and with other sectoral regulators,** such as competition, consumer, financial, and cybersecurity. We recognise the importance of provisions to authorise data protection and privacy authorities to share necessary information with authorities in other jurisdictions to strengthen cooperation among them. We highlight the benefits of cooperation in terms of capacity building, knowledge sharing,

[2] 1.3b-version-4.0-Policy-Strategy-Working-Group-Work-Stream-1-adopted.pdf (globalprivacyassembly.org) (Annex B, page 28)

efficiency, the prevention of duplication of work, better and more consistent regulatory decisions – particularly in relation to investigations of the same companies and issues in different global jurisdictions, and in relation to different regulatory aspects of organisations' actions in the global digital economy.

We would highlight that common approaches from regulators where possible can communicate a stronger message to organisations and get better regulatory results, and better outcomes for global citizens.

23. Liability and redress

We also highlight the importance of having **appropriate liability frameworks in place**, and the ability of data subjects to **enforce their rights directly through the courts.**

The 45th Global Privacy Assembly therefore resolves to:

- Advocate for, promulgate and promote the principles, rights and other elements set out in this resolution, to ensure they can be effectively implemented and applied in all contexts, particularly in the processing of data with new and emerging technologies and innovations; and

- Call on law and policy makers to consult data protection and privacy authorities as trusted expert advisers when enacting and amending data protection, privacy and related laws.

Explanatory note:

The GPA's current members acknowledge the contribution and global influence of the Madrid Resolution, which was adopted by the GPA in 2009, and which specified a set of data protection and privacy principles and rights, many of which remain familiar today. However, in today's context of increasing digitalisation, innovation and technological development, of a global digital economy that sees more data processed across borders, this resolution sets out at a high level current expectations of the principles, rights and other important elements that are important to ensure high data protection and privacy standards in 2023, and which we would advocate for policymakers to consider including as their jurisdictions' laws are introduced and revised.

GPA member authorities are pleased to note that jurisdictions across the world are increasingly enacting new privacy and data protection laws, and reviewing older ones, often

building on similar elements. This includes increasing development of specific international transfer regimes. We welcome existing global frameworks and approaches, such as the Convention 108 of the Council of Europe, an international legally binding instrument open to ratification of all countries and now modernised in Convention 108+, the OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, the OECD Declaration on Government Access to Personal Data Held by Private Sector Entities and the OECD Recommendation on Cross-Border Cooperation in the Enforcement of Laws Protecting Privacy, UN Guidelines for the Regulation of Computerized Personnel Data Files, and Standards for personal data protection for Ibero-American States and welcome efforts to build upon these in order to implement high standards of data protection and privacy globally.

The GPA's work under its current Strategic Plan 2021-23[3] has furthered cooperation between authorities across its regions to ensure high standards of data globally. Our work in recent years has noted, and has sought to highlight, the broad commonality in global frameworks in terms of core principles, rights and other elements – such as in the Global Frameworks and Standards Working Group's 2020 analysis of ten global frameworks[4], and 2021 analysis of transfer mechanisms[5].

Although different jurisdictions have different legal systems, so the approach and detail of their privacy and data protection laws differs, commonality and convergence can be seen, especially in core principles and rights. In this resolution, the GPA aims to highlight the importance of overarching principles and standards and the benefit they can bring in encouraging convergence and interoperability, and in turn supporting international cooperation to protect people's personal data globally. We would also highlight the positive contribution that can be made to this end by international and multilateral organisations such as the OECD and Council of Europe, the G7 and G20, other data protection organisations and networks such as the Ibero-American Data Protection Network (RIPD), Association of Southeast Asian Nations (ASEAN), Asia-Pacific Economic Cooperation (APEC), the European Data Protection Board (EDPB), Network of African Data Protection Authorities (NADPA / RAPDP), Association francophone des autorités de protection des données personnelles (AFAPDP) and standards bodies such as the International Organization for Standardization (ISO).

[3] 2021022-ADOPTED-Resolution-on-the-Assemblys-Strategic-Direction-2021-23.pdf (globalprivacyassembly.org)
[4] Day-1-1_2a-Day-3-3_2b-v1_0-Policy-Strategy-Working-Group-WS1-Global-frameworks-and-standards-Report-Final.pdf (globalprivacyassembly.org)
[5] 1.3b-version-4.0-Policy-Strategy-Working-Group-Work-Stream-1-adopted.pdf (globalprivacyassembly.org)