46th Closed Session of the Global Privacy Assembly

1 November 2024

Resolution on Data Free Flow with Trust and an effective regulation of global data flows

SPONSORS:

- European Data Protection Supervisor (EDPS);
- Federal Data Protection Commissioner (BfDI), Germany

CO-SPONSORS:

- Federal Data Protection and Information Commissioner (FDPIC), Switzerland;
- Dubai International Financial Centre Authority (DIFC), Dubai;
- National Institute for Transparency, Access to Information, and Personal Data Protection of México (INAI), Mexico;
- Information Commissioner's Office (ICO), United Kingdom;
- Office of the Privacy Commissioner of Canada (OPC), Canada;
- Garante per la Protezione dei Dati Personali (GPDP), Italy;
- Information Regulator, South Africa;
- Personal Information Protection Commission (PPC), Japan;
- Data Protection Commissioner of the Council of Europe;
- National Privacy Commission (NPC), Philippines;
- Agencia de Acceso a la Información Pública (AAIP), Argentina;
- Commission for Personal Data Protection (CPDP), Bulgaria;
- Commission nationale de l'informatique et des libertés (CNIL), France

The 46th Annual Closed Session of the Global Privacy Assembly:

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 whose personal data are processed;

RECOGNISING that jurisdictions around the world have been developing data protection laws that share a number of commonalities with respect to substantive requirements as well as independent oversight and effective redress, and FURTHER RECOGNISING the need for international efforts to continue to build upon these commonalities, complementarities and elements of convergence in order to foster future interoperability between them;

CONSCIOUS THAT rapidly developing digital economies and societies globally result in increased sharing of data across borders; AND THAT such global data flows are crucial for an inclusive information society, science, research, technology, economy, commerce and trade, as well as for the achievement of other public policy objectives;

TAKING INTO ACCOUNT THAT such data flows may impose risks and potential harms to privacy, data protection and other fundamental rights when personal data are concerned, and need to be duly considered and addressed through appropriate safeguards;

FURTHER EMPHASISING THAT in order to facilitate data to flow across borders, frameworks and mechanisms based on comparable high standards should ensure robust and consistent protection of individuals' enforceable rights and THAT a lack of trust in the protection provided to data when they flow across borders may hinder productivity, innovation and economic growth, or the achievement of public policy objectives;

ACKNOWLEDGING THAT the complexity and fragmentation of transfer mechanisms in different jurisdictions can present challenges to organizations, in particular small and medium sized enterprises (SMEs);

CONVINCED that mechanisms to frame data flows need to be predictable, ensure legal certainty, be consistent across sectors and focused on providing effective protection to individuals;

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;

[1] https://globalprivacyassembly.org/wp-content/uploads/2015/02/The-Madrid-Resolution.pdf

REITERATING the importance of the Resolution on "Achieving global data protection standards: Principles to ensure high levels of data protection and privacy worldwide"[2], adopted in 2023, which aims at positively impacting developments on global data protection laws, policies and practices, by setting out the key principles, rights and other elements that GPA members agree are important to achieve high data protection standards in today's digital economy and that should be implemented in data protection laws, policies and practices worldwide;

RECOGNISING that Data Free Flow with Trust (DFFT) is a common objective for like-minded countries and in various international fora, and FURTHER EMPHASISING that ensuring "trust", including a high standard of protection of personal data, is a fundamental requirement and prerequisite to facilitate the free flow of data;

WELCOMING the ongoing various efforts to work towards elements of convergence in order to foster future interoperability of data protection frameworks and transfer mechanisms in relevant international fora, in particular under the notion of DFFT, which was originally proposed by the Japanese Government in 2019 and supported by G7 and G20 Members;

WELCOMING specifically the G7 Industry, Technology and Digital Ministerial Declaration of 15 March 2024[3], in which G7 Ministers reaffirmed their commitment to operationalize DFFT and to build upon commonalities, complementarities and elements of convergence between existing regulatory approaches and instruments enabling data to flow with trust in order to foster future interoperability. FURTHER WELCOMING the support by Ministers for the G7 data protection authorities (DPAs) to further cooperate on knowledge sharing through the Roundtable of G7 DPAs;

ACKNOWLEDGING that Annex I (Operationalising DFFT)[4] of the G7 Digital and Tech Ministerial Declaration 2023[5], which was endorsed by the G7 Leaders in the Hiroshima Leaders' Communiqué on 20 May 2023, draws particular attention to DPAs' regulatory cooperation including identifying commonalities in regulatory approaches to cross-border data transfers and data protection requirements, as well as facilitating cooperation on Privacy-Enhancing Technologies (PETs), model contractual clauses, certification, access to regulatory information and good regulatory practices, such as enhancing transparency;

[2] https://globalprivacyassembly.org/wp-content/uploads/2023/10/3.-Resolution-Achieving-global-DP-standards.pdf

[3] https://assets.innovazione.gov.it/1710505409-final-version_declaration.pdf

[4] https://www.digital.go.jp/assets/contents/node/information/field_ref_resources/efdaf817-4962-442d-8b5d-9fa1215cb56a/3ca4c780/20230430_news_g7_results_01.pdf

[5] https://www.digital.go.jp/assets/contents/node/information/field_ref_resources/efdaf817-4962-442d-8b5d-9fa1215cb56a/f65a20b6/20230430_news_g7_results_00.pdf

HIGHLIGHTING the importance of the initiatives aimed at operationalizing DFFT, as underlined in the Communiqué 2024[6] and the Action Plan 2024[7] of the Roundtable of G7 DPAs as a driving force for advancing DFFT and promoting concrete actions having an operational impact;

SUPPORTING the valuable efforts made by the G7 DPA DFFT Working Group in advancing the international discussion on the concept of DFFT and sharing knowledge on tools for secure and trustworthy transfers, in particular through the comparative analysis of existing data transfer tools such as certification;

TAKING NOTE of the Institutional Arrangement for Partnership (IAP), launched in 2023 by G7 Ministers to advance the concept of DFFT by bringing together stakeholders and the broader multidisciplinary community of data governance experts including the relevant DPAs, currently in the form of the DFFT Expert Community at the OECD;

UNDERLINING that DPAs should play a key role in these discussions on DFFT, including within the IAP/OECD DFFT Expert Community, to ensure that high standards of data protection and privacy continue to be upheld;

ACKNOWLEDGING the efforts in other international fora on DFFT and encouraging their further development,;

TAKING NOTE also of the European Commission's and other initiatives to strengthen cooperation with countries that benefit from an adequacy decision and RECALLING that cooperation among DPAs from adequate countries is of key importance in such initiative;

CONSCIOUS that there is now a specific momentum to discuss current approaches in different data protection and privacy legal systems and international frameworks;

UNDERLINING the current need for a range of cross-border transfer tools that provide appropriate safeguards to address the particular risks linked to data transfers and provide data subjects with enforceable rights and effective legal remedies while also taking into account the needs for legal certainty of entities and organizations;

CONVINCED that transfer tools should provide appropriate safeguards while also addressing the practical needs of entities and organizations and be clear and user-friendly for the parties relying on them;

[6] https://g7privacy2024.gpdp.it/wp-content/uploads/2024/10/G7-DPAs_Rome-Roundtable_Draft-Communique_FIN_11_10.pdf

[7] https://www.ppc.go.jp/files/pdf/G7roundtable_202306_actionplan.pdf

CONSCIOUS that issues related to disproportionate governmental access to personal data held by private entities constitute an important obstacle to global data flows; Taking note of recent developments in some jurisdictions on the importance of protecting sensitive data from access by adversarial actors and from malicious activities;

REITERATING the strategic importance of the 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", adopted in 2021[8];

WELCOMING also the OECD Ministerial Declaration on Government Access to Personal Data held by Private Sector Entities adopted in December 2022 in Gran Canaria and in light of its global nature ENCOURAGING Governments from non-OECD countries to consider adherence to the Declaration and reflect on its principles in their own policymaking;

SUPPORTING also the efforts of other multinational fora on these aspects, for instance within the framework of the Consultative Committee of Convention 108 of the Council of Europe, in particular on the interpretation of Article 11 of the Modernised Convention 108 on exceptions and restrictions and CALLING for a swift and prompt entry into force of this Modernised Convention accompanied by an effective evaluation and follow up mechanism;

TAKING NOTE of ongoing discussions and progress being made on transfer tools, for instance on model contractual clauses (by the European Union, Council of Europe, Association of Southeast Asian Nations (ASEAN), and the Ibero-American Data Protection Network (RIPD)) and certification (Global Cross-Border Privacy Rules (CBPR) Forum and instruments developed by the European Data Protection Board (EDPB);

ENCOURAGING dialogue between these organisations and networks to develop convergent and enforceable transfer mechanisms in order to foster future interoperability whilst having in mind the specificities of the respective legal frameworks;

RECALLING the ongoing work undertaken by the Global Frameworks and Standards Working Group of the GPA to aid further understanding of current and emerging transfer mechanisms, monitor developments in the field and foster engagement with global networks, multilateral organisations and other key stakeholders;

RECALLING in particular the comparison of standard or model contractual clauses identified as the most prominent tool currently available in several regions and member countries of the GPA[9]; and HIGHLIGHTING the close convergence between several existing model clauses;

[8] https://globalprivacyassembly.org/wp-content/uploads/2021/10/20211025-GPA-Resolution-Government-Access-Final-Adopted_.pdf

[9] See https://globalprivacyassembly.org/document-archive/working-group-reports/

The 46th Global Privacy Assembly therefore resolves to:

- Advocate for and promote the initiatives developed under the concept of DFFT as a banner **to promote high standards for data protection and privacy for an efficient regulation of global data flows.**

- **Call on lawmakers, policy makers and regulators** to:

  - foster convergence on high standards and future interoperability when developing or updating data transfer tools, by paying particular attention to the principles set out in the Resolution on "Achieving global data protection standards: Principles to ensure high levels of data protection and privacy worldwide" and in particular to the following **high-level elements the Assembly regards as essential to achieve secure and trustworthy cross-border data flows** and which are already addressed by several data transfer tools:

    - **Key data protection principles**: Data transfer tools should provide for core data protection principles, in particular the principles of necessity, proportionality, lawfulness, purpose limitation, limited data retention, data minimisation, data accuracy and transparency. Where relevant, they should also provide for additional safeguards for the protection of particularly sensitive categories of data, taking into account the specific risks involved in their processing. Such tools should be based on legally binding and enforceable instruments.

    - **Individual Rights:** Data transfer tools should ensure enforceable rights for individuals. Individuals should have the right to obtain confirmation whether or not their personal data is being processed and to be informed about the main elements of the processing (such as the identity of the controller, the purpose of the processing and the rights of the individual in relation to the processing). Individuals should also have the right to access their data, obtain rectification where data is inaccurate or incomplete, and request erasure of their data when their processing is unlawful or no longer necessary. Restrictions to individual rights should be limited to what is provided for by law, necessary, reasonable and proportionate for important public interest reasons shared and recognised in both the jurisdiction of the data exporter and the data importer. In case the data importer refuses such requests, individuals should have access to appropriate channels and remedies to effectively enforce their rights.

- **Security**: Data transfer tools should ensure that both the data exporter and data importer adopt appropriate measures to ensure confidentiality, integrity and availability of data, including protection against accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access to, personal data transmitted, stored or otherwise processed which may in particular lead to a risk of physical, material or non-material damage. These measures might encompass, but are not limited to, robust encryption protocols, regular security audits, and compliance with suitable and internationally recognized data protection and privacy standards.

- **Onward Transfers**: Onward transfers by the data importer to a third party should be allowed only if the level of protection provided by the data transfer tool is appropriate, so that the level of protection and safeguards established for the initial transfer are not undermined.

- **Government Access**: Given the possibility of disproportionate access to transferred personal data by public authorities for national security or law enforcement purposes, data transfer regulations and tools should address how to deal with such access and set up mechanisms to protect against access which is not prescribed by law and that goes beyond what is necessary and proportionate in fair and transparent political and social systems.

- **Independent Oversight**: Compliance with the provisions of the data transfer tool should be subject to the supervision of independent and impartial authorities with effective investigative, monitoring and enforcement powers. Transfer tools may for instance establish obligations to cooperate with the competent supervisory authorities of the data exporter and adhere to their decisions.

- **Legal Remedies and Redress**: Transfer tools should provide individuals with avenues to exercise their rights and enforce compliance through effective legal remedies and administrative and judicial redress, including for compensation due to damage suffered.

- consult data protection and privacy authorities when enacting and amending data protection, privacy and related laws with respect to data transfers;

- support the efforts towards a swift entry into force of the Modernised Convention 108 (CETS No. 223) of the Council of Europe as currently the sole international binding convention on privacy and data protection open to the ratification of countries from all over the world and support establishing a strong and robust evaluation and follow-up mechanism;

- support the OECD to continue its work on trusted government access including considering further steps to promote its Declaration on Government Access to Personal Data held by Private Sector Entities adopted at the OECD Ministerial meeting in December 2022 and encourage non-OECD members to consider adherence to the OECD Declaration and reflect its principles in their policy making.

- Commit to support efforts to bridge differences in regulatory systems and in particular to:

    - explore as a matter of priority ways to achieve the **possible interoperability of model or standard contractual clauses from different regions or jurisdictions that present a sufficient level of convergence** as demonstrated by the GPA comparison of model contractual clauses, for instance among the models developed at the levels of the European Union, the Council of Europe or the Ibero-American Network, and consider the expected benefits and challenges of such interoperability to facilitate compliance with cross-border transfer rules for companies operating across different regions of the world, including on the possibility to explore possible global model contractual clauses;

    - support the development of **adequacy decisions or mutual adequacy arrangements ensuring a high level of data protection and privacy** to increase their network effect and the development of a broad network where data can flow freely, including development of an adequacy network;

    - support efforts to promote and where relevant develop **certification tools[10],** as well as other tools for secure and trustworthy transfers, such as codes of conduct, or model administrative arrangements;

    - discuss and explore whether **Privacy Enhancing Technologies** such as synthetic data, homomorphic encryption, differential privacy or tokenisation could play a role in complementing effective transfer tools on data transfers and contribute to ensure more trustworthy data governance globally.

- Commit to encourage a dialogue between GPA members and various stakeholders in the field, including by consulting the Reference Panel of the GPA;

- Mandate the Global Frameworks and Standards Working Group to develop a report on the evolutions linked to DFFT and actions taken by GPA members and report back with some additional follow-up actions at the 47th Global Privacy Assembly.

[10] See also the resolution Endorsing and Encouraging the Use of Data Protection Certification Mechanisms adopted by the Global Privacy Assembly in 2024