# 43rd Closed Session of the Global Privacy Assembly

## October 2021

# Adopted 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

**SPONSORS:**

- Commission Nationale de l'Informatique et des Libertés (CNIL – France)
- Personal Information Protection Commission (PPC – Japan)
- Office of the Privacy Commissioner of Canada (OPC – Canada)

**CO-SPONSORS:**

- Office of the Privacy Commissioner, Te Mana Mātāpono Matatapu (New Zealand)
- European Data Protection Supervisor (European Union)
- Data Protection Commissioner (Malta)
- Autorità Garante per la protezione dei dati personali (San Marino)
- Autorité de protection des données – Gegevensbeschermingsautoriteit (Belgium)
- Préposé fédéral à la protection des données et à la transparence - Federal Data Protection and Information Commissioner - (Switzerland)
- Information and Privacy Commissioner of Ontario (Canada)
- Commission Nationale pour la Protection des Données (Luxembourg)
- National Privacy Commission (Philippines)
- Commissaire à la protection des données – Data protection Commissioner (Council of Europe)
- Comissão Nacional de Protecção de Dados (Portugal)
- Datenschutzkommission – Data Protection Commission (Austria)
- Information Commissioner's Office (ICO – United Kingdom)
- Instance nationale de protection des données à caractère personnel (INPDP - Tunisia)
- Personal Information Protection Commission (PIPC – Republic of Korea)
- Federal Data Protection Commissioner - Bundesbeauftragten für den Datenschutz (BfDI – Germany)

**The 43rd Annual Closed Session of the Global Privacy Assembly**

*Having regard to the ICDPPC Resolution on the Conference's strategic direction (2019-21)*[1]

*Having regard to the ICDPPC Resolution on privacy as a fundamental human right and precondition for exercising other fundamental rights*[2]

*Having regard to the ICDPPC Resolution on transparency reporting*[3]

*Having regard to the Working Paper of the International Working Group on Data Protection in Telecommunications on 'Towards International Principles or Instruments to Govern Intelligence Gathering' adopted in April 2017*[4]

*Having regard to the AFAPDP Resolution of November 2013 aiming at greater transparency of personal data collection practices by governments*[5]

*Having regard to the communiqué of the roundtable of G7 data protection and privacy authorities of 7-8 September 2021 on data free flow with trust*[6]

**RECALLING** that respect for rule of law, democratic values and human rights lies at the core of data protection regimes and privacy laws,

**CONSIDERING** that data protection and privacy principles applicable to government access to personal data and sensitive information are key elements ensuring respect for the rule of law, democratic values and human rights in relation to the legitimate objective of preserving national and public security,

**CONSIDERING** that the importance of these key elements has been underlined in the case law of high courts in several parts of the world,

**RECOGNIZING** that government authorities seeking access to personal data and sensitive personal information held by the private sector pursue and contribute to a legitimate public policy aim of preserving liberty and security, and that privacy safeguards help to augment the lawfulness, legitimacy and accountability of national security measures and public safety programs,

**POINTING OUT** that the development of a data-driven economy, increasingly relying on personal data processing, entails an ever-expanding volume of personal data and sensitive information held by private sector companies at international level, representing a significant source of information of interest for governments and public authorities in pursuing important objectives of public interest,

**ACKNOWLEDGING** that transparency, including both information to the public and the provision of information to individually affected data subjects, subject to necessary and proportionate

[1] https://globalprivacyassembly.org/wp-content/uploads/2019/10/Resolution-on-the-Conference-Strategic-Direction-2019-2021-FINAL.pdf
[2] https://globalprivacyassembly.org/wp-content/uploads/2019/10/Resolution-on-privacy-as-a-fundamental-human-right-2019-FINAL-EN.pdf
[3] https://globalprivacyassembly.org/wp-content/uploads/2015/02/Resolution-on-Transparency-Reporting.pdf
[4] https://www.datenschutz-berlin.de/infothek-und-service/veroeffentlichungen/working-paper
[5] https://www.afapdp.org/archives/download-view/2013-resolution-sur-la-transparence
[6] https://ico.org.uk/media/about-the-ico/documents/4018242/g7-attachment-202109.pdf

limitations, is an essential element of both government accountability and citizens' ability to exercise their rights in a democratic society,

**STRESSING** the importance of preserving the confidentiality of electronic communication systems and related security features such as cryptographic systems while HIGHLIGHTING the reporting on the alleged use by certain government entities of particularly intrusive technologies made available by private service providers,

**EMPHASIZING** that strong data protections and privacy safeguards are vital for the preservation of public trust, the promotion of market interoperability and the support for international sharing of personal data and cross-border data flow,

**NOTING** that, in addition to the risks posed to privacy as a fundamental human right and to other fundamental rights, the absence of sufficient privacy and data protection safeguards framing government access to personal data held by the private sector also raises serious challenges to the free flow of personal data at international level and may represent a hurdle to the global digital economy,

**RECOGNISING** that different legal systems and traditions co-exist at regional and international level, and that convergence towards key principles and high standards for government access to personal data held by the private sector may contribute to legal certainty and the facilitation of data flows in the global digital economy,

**TAKING INTO ACCOUNT** the important ongoing international initiatives and discussion at a range of fora (e.g. Council of Europe, OECD, G20/G7, United Nations) as well as bilateral negotiations and arrangements in relation to government access to personal data held by the private sector for national security and public safety purposes,

**UNDERLINING** the Global Privacy Assembly objective of enhancing its role and voice in wider digital policy debate at international level for the promotion of high standards and the need to ensure the mainstreaming of data protection and privacy in ongoing developments affecting the digital economy at international level,

**The Global Privacy Assembly therefore adopts the following resolution on government access to data, privacy and the rule of law, advocating for the following principles to be applied for government access to personal data held by the private sector for national security and public safety purposes**, thus laying down conditions ensuring that any type of public authorities' legitimate access for purposes related to national security or public safety also contribute to the preservation of privacy and the rule of law:

1. **Legal basis**: Government access to personal data must be duly authorized by appropriately enacted legislation, after public debate and scrutiny by legislators. The legislation must have respect for the rights to data protection and to privacy, other human rights and be non-discriminatory.

2. **Clear and precise legislation applying to government access**: any legislation authorizing access to personal information should be:

a) publicly available,

b) written in clear, easily understandable language, and,

c) precise and specific as to the scope of personal information for which the law is granting governmental access and the conditions for such access.

3. **General principle of necessity and proportionality**: in order for access to personal data, including sensitive data, by state authorities or any state entity to be justifiable, the specific usage for personal information must be linked to a demonstrably necessary function or activity of government, and the intrusiveness must be proportionate to the goal in question.

4. **Transparency:** Any agreement or arrangement for government access, flowing from authorization in law, should also make proactive, baseline public reporting and publicly available accountability process requirements for government agencies involved, and permit information to be provided to affected individuals, unless limitations to transparency towards individuals constitute a necessary and proportionate measure in a democratic society.

5. **Data subject rights**: while taking into account the national security and public safety requirements, government access to personal data should integrate a specific and dedicated framework for data subjects to exercise their rights, including by addressing directly their requests to public authorities. In particular, individuals should have the right of access and to get personal data corrected or deleted, unless limitations to data subject rights constitute a necessary and proportionate measure in a democratic society.

6. **Independent oversight:** laws authorizing access should consider providing for both independent advance oversight (e.g. prior judicial authorization) as well as retrospective review (e.g. auditing of processing by independent regulatory body), taking into account the gravity and severity of the impact on fundamental rights and freedoms of individuals caused by the specific government access.

7. **Statutory limitation on government's use of data acquired:** law authorizing government access to personal data for one specific purpose should regulate and frame any secondary use or onward transfer for other purposes, also observing general principles in order to ensure a continued protection of personal data.

8. **Effective remedies and redress available to the individuals affected**: any governmental access to personal data should be subject to specific provisions for any individuals affected to seek effective redress and remedies.

Complementary to the principles above, **the Global Privacy Assembly considers the following examples and best practices as relevant illustrations of further accountability in government access to personal data and realisations of key safeguards** ensuring the protection of privacy and personal data of individuals:

- **Ensuring that cryptographic systems are not undermined by government access requirements that could entail exceptional access** via the deliberate introduction of cybersecurity vulnerabilities (e.g. mandated 'backdoors').
- **Transparency reporting** by commercial firms documenting numbers of government requests;

- **Additional avenues** for private sector remedies and redress in relation to government access to personal data in order to support and facilitate the application of the principle of effective remedies and redress mentioned above;
- **International regulatory cooperation** for oversight and supervision of government access to personal data.

**The Global Privacy Assembly resolves to promote and advocate for the above-mentioned principles and best practices for governmental access to personal data held by the private sector for national security and public safety purposes.**

**The Global Privacy Assembly hereby calls on governments and international organisations to observe the above-mentioned principles and to work towards the development of multilateral instruments ensuring adherence to key data protection and privacy principles in relation to government access to personal data.**

**In line with the principles above, the Global Privacy Assembly also calls on governments and international organisations to engage in discussions aiming at regulating the sale, export and use of technologies allowing for particularly intrusive and disproportionate access to individual personal data, in particular electronic communication content and data.**

*The U.S. Federal Trade Commission and the Office of the Privacy Commissioner for Personal Data, Hong Kong, China abstain from this resolution, which relates to matters outside their respective jurisdictions.*