資料１－３

45th Closed Session of the Global Privacy Assembly

October 2023

Resolution on Generative Artificial Intelligence Systems

SPONSORS:

- European Data Protection Supervisor (EDPS);

CO-SPONSORS:

- Agencia de Acceso a la Información Pública (AAIP, Argentina);
- Defensoría del Pueblo de la Ciudad de Buenos Aires (Argentina)
- Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit (BfDI, Germany);
- Der Landesbeauftragte für den Datenschutz und die Informationsfreiheit Rheinland-Pfalz (DRLP, Germany);
- Commission for the Control and the Protection of Personal Data (CNDP, Morocco);
- Commission nationale de l'informatique et des libertés (CNIL, France);
- Council of Europe (CoE);
- Federal Data Protection and Information Commissioner (FDPIC, Switzerland);
- Garante per la Protezione dei Dati Personali (GPDP, Italy);
- Information Commissioner's Office (ICO, United Kingdom)
- National Institute for Transparency, Access to Information, and Personal Data Protection of México (INAI, Mexico);
- Office of the Information and Data Protection Commissioner of Malta (IDPC, Malta);

- Office of the Information and Privacy Commissioner of Ontario (IPC, Canada);
- Office of the Privacy Commissioner of Canada (OPC, Canada);
- Office of the Privacy Commissioner for Personal Data (Hong Kong, China);
- Personal Information Protection Commission (PPC, Japan);
- Personal Information Protection Commission (PIPC, Korea);
- Privacy Protection Authority of Israel (PPA, Israel);
- Unidad Reguladora y de Control de Datos Personales (AGESIC, Uruguay)

The 45th Annual Closed Session of the Global Privacy Assembly:

ACKNOWLEDGING the rapid development of artificial intelligence (AI) technologies, which often process personal data on a large scale;

NOTING the widespread deployment of generative AI technologies and applications and their increasing adoption across various domains as well as the widespread proliferation of uses around the world;

ACKNOWLEDGING the various concerns expressed in the public debate regarding the ethical and legal implications of generative AI technologies, including their impact on fundamental rights and freedoms, notably in relation to the fundamental right to privacy and protection of personal data;

CONCERNED by the release - often with insufficient pre-deployment assessment - of generative AI systems to the wider public, which may present risks and potential harms to data protection, privacy and other fundamental human rights if not properly developed and regulated;

CONCERNED about the indiscriminate collection of personal data from publicly accessible areas and sources to be fed into such technologies without legal authority;

RECOGNISING about the environmental impact of developing and deploying generative AI models that dedicates substantial computational resources to process large amounts of data;

RECALLING that data protection and privacy principles and current laws, including data protection and privacy laws, bills, statutes and regulations, apply to generative AI products and services, even as different jurisdictions continue to develop AI-specific laws and policies;

ACKNOWLEDGING the ongoing policy making, investigative and enforcement actions taken by various data protection authorities in relation to services using generative AI, in particular with regard to the processing of personal data and transparency for data subjects, including minors;

WELCOMING the Roundtable of G7 Data Protection and Privacy Authorities (DPAs) statement on Generative AI[1] of 21 June 2023 which draws specific attention to key areas where privacy and data protection risks may arise and data protection and privacy principles apply to the development and use of generative AI tools;

ACKNOWLEDGING that continuous global discussion and collaboration is needed on promoting common values in the context of generative AI, not only from a legal perspective but also from an ethical, social and technical one;

[1] https://www.ppc.go.jp/files/pdf/G7roundtable_202306_statement.pdf.

STRESSING that public entities, including DPAs, around the world have an essential role to play to ensure that the foundation models giving origin to generative AI tools are built in full respect for the individual's rights and freedoms, including data protection and privacy, as well as preventing unfair, unethical or discriminatory treatment contrary to human rights law;

RECOGNIZING the unique risks and potential harms of generative AI systems in the context of automated decision-making or in high-risk usages, particularly on vulnerable populations and children;

RECALLING the 40th Global Privacy Assembly's *Declaration on Ethics and Data Protection in Artificial Intelligence* call for an "ethics by design" approach, where artificial intelligence systems should be designed and developed applying the principles of privacy by design and privacy by default*;*

REAFFIRMING the 41st Global Privacy Assembly's *International Resolution on Privacy as a Fundamental Human Right and Precondition For Exercising Other Fundamental Rights* that to build trust in our digital society, accelerate innovation, and protect human dignity, generative AI be human centric, based on democratic values, and should recognize privacy as a fundamental human right, vital to the protection of other rights and freedoms.

The **45th Global Privacy Assembly emphasises** that:

As any other AI systems, generative AI must be designed, developed and deployed in a manner that is responsible and trustworthy, based on the principles of data protection, privacy, human control, transparency and democratic values;

Developers, providers and deployers of generative AI systems should embed data protection and privacy in the conception, design, operation and management of new products and services using generative AI systems, based on the principles of data protection and privacy by design and document their choices and analyses in a data protection and privacy impact assessment;

Moreover, developers, providers and deployers of generative AI systems should understand the risks, harms, and potential impact on affected individuals and society at large as the basis to develop ethical, trustworthy and responsible generative AI;

In addition, developers, providers and deployers of generative AI systems should also put in place measures to ensure compliance with data protection and privacy obligations. These stakeholders should cooperate to ensure that individuals whose data are processed by generative AI systems have the ability to exercise their data protection and privacy rights and;

Close attention should be paid by developers, providers and deployers of generative AI systems to the legal requirements and guidance from DPAs on how to interpret such legal requirements.

Where appropriate, close communication with DPAs can contribute to the responsible design, development and deployment of products and services based on generative AI systems.

In this regard, the **45th Global Privacy Assembly endorses** the existing data protection and privacy principles as core elements for the development, operation, and deployment of generative AI systems:

1. **Lawful basis for processing**

Generative AI systems must have a legal basis and be lawful in accordance with applicable legislation even when personal data is publicly accessible. Developers must establish that generative AI systems are both legal and safe before the systems are launched.

Where required under relevant legislation, developers, providers and deployers of generative AI systems must identify at the outset the legal basis for the processing of personal data related to:

a) collection of data used to develop generative AI systems;
b) training, validation and testing datasets used to develop or improve generative AI systems;
c) individuals' interactions with generative AI systems;
d) content generated by generative AI systems.

2. **Purpose specification and use limitation**

Developers, providers and deployers of generative AI systems shall ensure that they process personal data for specific, explicit and legitimate purpose(s) and not process them further for incompatible purpose(s) or beyond the affected individuals' reasonable expectations. These purpose(s) must be appropriate, reasonable or legitimate in the circumstances.

Developers, providers and deployers of generative AI systems must neither develop nor put into operation generative AI, the use of which is illegal or has a considerable potential to lead to unfair, unethical or discriminatory treatment, particularly where this would lead to significant violations of fundamental rights and freedoms. This is even more fundamental where AI systems are used to make or assist in decision-making about individuals.

Developers, providers and deployers of generative AI systems should carefully evaluate the compatibility —ethical, legal, social, and technical—with the purpose for which the personal data used in their development were collected.

3. **Data minimisation**

Developers, providers and deployers of generative AI systems should limit the collection, sharing, aggregation, retention and further processing of personal data only to what is necessary to fulfil

the legitimate identified purpose(s). Personal data should not be collected and processed indiscriminately.

In addition, inclusion of personal data in training sets poses privacy and other risks to individuals , including, inter alia, that information in training data could foreseeably be produced as part of a generative AI system's output. Therefore, personal data must only be used as training data if required to achieve the intended purpose(s) of the generative AI system and only after a Data Protection and Privacy Impact Assessment has been carried out.

Developers, providers and deployers of generative AI systems should aim to support environmental objectives by developing computational targets that reduce energy consumption, through tactics like data minimization, more efficient computational methods, and architectures that are less reliant on data growth.

4. Accuracy

In their development stage, generative AI systems often use vast amounts of training, testing and validation data, including personal data. The accuracy of the output of generative AI systems highly depends on the quality and representativeness of such large datasets. To safeguard affected individuals from discriminatory, unlawful or otherwise detrimental consequences, it is paramount that developers, providers and deployers of generative AI systems rely on accurate, reliable and representative data. Developers, providers, and deployers must take measures to review and filter the content of the data to exclude information that is false or misleading. In addition, developers must refrain from making unsupported or premature claims related to the accuracy of their systems.

Even when trained with representative high quality data, the content generated by generative AI systems may contain inaccurate or false information including personal data, commonly known as “hallucinations.”

To mitigate the risks posed by the potential lack of accuracy of generative AI systems, developers, providers and deployers of generative AI systems should implement appropriate data governance procedures (e.g. recording of training dataset sources) and technical safeguards (e.g. use of filters in input and output data). Moreover, once deployed, it is essential to ensure adequate cooperation to monitor the behaviour and responses of generative AI systems and fine-tune the behaviour of generative AI systems to produce accurate responses.

5. Transparency

Lack of transparency as to training data used has already fuelled concerns over the impact on individuals’ data protection and privacy. Deployers of generative AI systems must implement adequate transparency measures ensuring the openness of generative AI tools, including

information on how, when, and why personal data is collected and used in the process of training generative AI systems.

Providers who put generative AI systems on the market or in operation must inform deployers about the potential data protection and privacy risks for using such systems and how providers address these issues through adequate policies and practices. These risks and policies must be clear, easy to understand, and readily available to deployers, both before and during use of the system.

If a generative AI system is being used to make or assist in decision-making, developers, providers and deployers must clearly communicate these practices to the affected parties.

Developers, providers and deployers of generative AI systems should provide transparent documentation about their datasets, including the sources of the datasets, the legal authority and licenses of the datasets, and any modification, filtering or other curation practices on the datasets.

6. Security

In the design, conception and operation of generative AI systems, developers, providers and deployers must put in place effective security measures, especially where the system has access to external data sources. In particular, these measures should aim at:

- Integrating traditional cybersecurity controls with specific security controls tailored to generative AI system vulnerabilities (e.g. indirect prompt injection attacks);
- Preventing model inversion attacks that could allow an attacker to extract and reproduce personal data included in the datasets used to train the model;
- Ensuring that the safeguards put in place to foster compliance with data protection and privacy requirements are not undermined.

Developers, providers and deployers of generative AI systems should assess and mitigate the risk of misuse of their systems, such as creating deep fakes or generating text for phishing attacks. Priority should be given to identifying and mitigating the root cause of these risks in order to prevent future harm.

7. Privacy by Design and Default

The capacities and limitations of generative AI systems are evolving rapidly. For example, certain generative AI systems that previously accepted just text, images or sound as input recently have been expanded to become multimodal and accept different types of input. New risks will arise as a result of these evolutions in the technology. In line with the privacy by design and by default principle, developers, providers and deployers of generative AI systems should conduct a data

protection and privacy impact assessment to identify, assess and address the risks posed by these systems at every stage of their life cycle.

Privacy by design and by default aims at protecting data throughout the entire life cycle of data processing, starting from the design stage. By complying with this principle, based on a risk-oriented approach, the threats and risks that AI may create can be minimised by considering them sufficiently in advance.

Developers, providers and deployers of AI systems need to carefully assess the envisaged processing activities, the risks they may pose for the data subjects, the possible measures available to ensure compliance with data protection principles and the protection of individual rights. Privacy-oriented approaches should be favoured at all stages, including in particular through strong privacy by-default options and user-friendly options and controls. Any major change to the functionality of generative AI systems represents a 'stage' in their lifecycle and would warrant a Data Protection and Privacy Impact Assessment.

8. Rights of data subjects

Developers, providers and deployers of generative AI systems must ensure that individuals are granted the right to be informed about the collection and use of their personal data, particularly where such data is obtained from a variety of sources and when personal data is being used to make or assist in decisions. In addition, developers, providers and deployers of generative AI systems shall implement appropriate technical and organisational measures in order to ensure that affected individuals are able to exercise their rights, where provided by law, including:

- The right to access their personal data;
- The right to rectify any inaccurate personal data;
- The right to erase their personal data and;
- The right not to be subject to automated decisions that result in a significant effect for the individuals.

The capacity of affected individuals to exercise their rights is especially relevant when generative AI systems process special categories of data or personal data of minors.

9. Accountability

Developers, providers and deployers of generative AI systems shall be responsible for and must be able to demonstrate compliance with applicable national legislation and international agreements. The principle of accountability requires responsibility to be clearly identified and respected among the various actors involved in the generative AI model supply chain.

Such compliance should be demonstrated by making available technical documentation throughout the lifecycle of systems in order to enable data protection and privacy authorities to

assess compliance of generative AI tools with data protection and privacy requirements. Developers, providers and deployers of generative AI systems should include in their documentation how their models work, what data was used to train their models, and the potential data protection and privacy impacts before putting their services on the market or in operation.

Developers, providers and deployers of generative AI systems should also allow for external audits that can independently assess how a model works, test outputs for inaccuracies and biases, and recommend effective measures to mitigate potential risks. Accountability also requires developers, providers and deployers of generative AI systems to implement sound data governance procedures and tools.

The 45th Global Privacy Assembly therefore resolves to:

- Commit to ensure the application and enforcement of data protection and privacy legislation in the context of generative AI technologies, including the applicable principles and rights set out in this resolution;

- Commit to collaborate on ensuring personal data protection and privacy within the context of generative AI from an ethical, legal, social, and technical perspective;

- Commit to sharing ongoing developments within jurisdictions regarding the data protection and privacy risks of generative AI systems within the Ethics and Data Protection in Artificial Intelligence Working Group;

- Call on developers, providers and deployers of generative AI systems to recognise data protection and privacy as a fundamental human right and to build responsible and trustworthy generative AI technologies that protects data protection, privacy, human dignity and other fundamental rights and freedoms;

- Encourage developers, providers and deployers of generative AI systems to provide training to employees and personnel to understand development and deployment of the generative AI systems regarding data protection, privacy and the rights of data subjects;

- Encourage GPA members to raise awareness of the risks to data protection, privacy and other human rights as well as the applicable legal obligations and principles of data protection and privacy in the context of the generative AI systems;

- Continue monitoring emerging risks and potential harms to fundamental rights and freedoms as they arise in the context of generative AI;

- Aim to advocate and advise on ongoing and forthcoming legislative and regulatory initiatives and approaches;

- Call on GPA members to coordinate their enforcement efforts on generative AI systems;

- Consider presenting, at the 46th Global Privacy Assembly, an interim report on the work conducted by the GPA AIWG members on generative AI systems, and further consider additional policy documents or resolutions to be presented at the 47th Global Privacy Assembly.