Working Group on Ethics and Data Protection in Artificial Intelligence

Report – July 2021

Office of the Privacy Commissioner for Personal Data (PCPD), Hong Kong, China

Commission Nationale de l'Informatique et des Libertés (CNIL), France

European Data Protection Supervisor (EDPS), European Union

Table of Contents

Executive Summary

In early 2021, the AI Working Group (the Group) agreed on its objectives for the year and organised itself in teams of rapporteurs and co-rapporteurs for the implementation of its work packages. While the unexpected challenges of the COVID-19 pandemic required reviews of priorities and resource allocation for many organisations, work on a number of work packages proceeded so that deliverables can be made available and presented to the GPA Closed Session 2021. For others, the scheduling of deliverables is under review.

Among the work projects and deliverables of the Working Group, we are pleased to present a quick summary of the key outputs of the Group:

- **A repository of AI related documents accessible by all GPA Members and Observers**: this is regularly updated with new documents, and all members and observers of the GPA are invited to inform the Group's Secretariat at the EDPS with information of new documents to be added to the repository.
- **A repository of AI use cases**, aiming at obtaining a meaningful overview of real life applications of AI technology, which are relevant for ethics and data protection.
- **Preparation of an analysis of the risk to data protection, especially data minimisation, as brought about by the demands to maximise personal data collection on the grounds of 'eliminating' bias and discrimination**: while the work on this item is still ongoing and will be presented in 2022, the aim of the analysis is to also cover other relevant risks considered in the Declaration on Ethics and Data Protection in Artificial Intelligence, in particular risks for the whole society, giving basic indications for managing these risks with reference to the various stakeholders involved. The inclusion of the risks to sustainability and inequality at global level will also be evaluated. The WG is committed to present a draft version of the document at the Closed Session of the 2021 GPA with the objective to involve other active Members on this activity.
- **A survey on authorities' capacity and expertise in addressing ethical and data protection issues in AI systems applications:** As part of its work programme 2019-2021, the GPA AIWG undertook to conduct a survey on members' capacity and expertise in addressing ethical and data protection issues in AI systems applications. This survey constituted a first step in order to pursue the working group work in the future on capacity and expertise in the field of AI, supporting the development of a gap analysis and relevant recommendations in order to improve knowledge sharing and capacity building within the GPA in this field.
- **IEWG-AIWG FRT sub-group:** The GPA in 2020 adopted a resolution to follow up on its FRT declaration. The resolution tasked the IEWG and AIWG with developing a set of principles and expectations for the use of personal data in FRT. With coordination from the IEWG Secretariat, an IEWG-AIWG FRT sub-group was established in late 2020 to progress work mandated by the resolution. The sub-group comprises the EDPS, the FDPIC (Switzerland), the ICO (United Kingdom), PPC (Japan), the OAIC (Australia), and the OPC (Canada).

Additional information on the work and deliverables of the Group will be presented in more detail in the report. In general, the identified priorities appear still valid. The next work phase of the Group will on the one hand be characterized by the monitoring of concrete legislative initiatives by some national, regional and international entities, and on the other by the need to take account of long term challenges to human rights, such as environmental developments and global inequality. At the

same time, the impact of future developments of Artificial Intelligence (AI) in relation with the monitoring and control of the COVID-19 pandemic will require scrutiny.

In addition to its work on substantial policy orientations, the Group will continue its outreach activities with a focus on international organisations and civil society.

Introduction

The 40th ICDPPC (now Global Privacy Assembly) adopted in October 2018 in Brussels a Declaration on Ethics and Data Protection in Artificial Intelligence[1] (the Declaration), which endorses six guiding principles as core values for the preservation of human rights in the development of Artificial Intelligence. The Declaration establishes the Permanent Working Group on Ethics and Data Protection in Artificial Intelligence and mandates it with promoting the principles of the resolution "*by all relevant parties involved in the development of artificial intelligence systems, including governments and public authorities, standardization bodies, artificial intelligence systems designers, providers and researchers, companies, citizens and end users of artificial intelligence systems"*[2].

With the help of the Executive Committee of the GPA (the ExCo), the Group started in early 2019. PCPD (Hong Kong, China), CNIL (France) and EDPS (EU) agreed to co-chair the Group, with the EDPS providing the secretariat function for the Group.

Member authorities of the Group are:

- AAIP (Argentina);
- OAIC (Australia);
- OPC (Canada);
- OIPC British Columbia (Canada);
- CAI Quebec (Canada);
- SDPD (Colombia);
- Datatilsynet (Denmark);
- DPC (Gabon);
- BfDI (Germany);
- Bavarian DPC (Germany);
- LfDI Rheinland-Pfalz (Germany);
- HDPA (Greece);
- ODPC (Guernsey);
- GPDP (Italy);
- PPC (Japan);
- OIC (Jersey);
- OPC (New Zealand);
- ICO (United Kingdom);
- FTC (USA);
- FDPIC (Switzerland).

The Observers part of the Group are:

- Council of Europe (COE);
- Fundamental Rights Agency (FRA- EU);
- International Committee of the Red Cross (ICRC).

[1] Declaration on Ethics and Data Protection in Artificial Intelligence; 40th ICDPPC, 23rd October 2018, Brussels, http://globalprivacyassembly.org/wp-content/uploads/2018/10/20180922_ICDPPC-40th_AI-Declaration_ADOPTED.pdf.

[2] The Declaration, p. 6.

The Group developed a work programme covering 2019 to 2021, with 11 work packages and corresponding deliverables. Seven work packages are completed or proceeding according to schedule, while for the others the new demands due to the COVID-19 pandemic have required the Group member authorities to review priorities and resource allocations. During this year, the GPA AIWG focussed its activities on Action Points 6 and 8 of the Group's Work Plan. The working group is currently considering the inclusion of an additional action item that focuses on the impact of Artificial Intelligence in the employment context.

As elements of the work programme correspond to work streams identified as priorities in the Assembly's Strategic Plan 2019 – 2021 and associated Policy Strategy, a call with the Strategic Direction Sub-Committee (SDSC) in the second quarter 2021 allowed to identify needs and possibilities for coordination.

Working Group Activities

Implementation of the Work Program

After its establishment in early 2019, the Group discussed a draft work program. A physical meeting alongside the Closed Session was held in Tirana to allow Group's members to review this draft. At the meeting, the Group achieved consensus about the work packages and deliverables scheduled for 2019 and 2020 and agreed to review future work schedules at a later stage. During a teleconference in February 2020, the Group's members and observers fielded resources as rapporteurs and co-rapporteurs for the agreed work packages.

Due to the COVID-19 pandemic emergency in the following months, GPA member authorities were confronted with a huge additional workload. Many organisations had to review their priorities and readjust resource allocations, as well as reconsider the scheduling of committed activities. At the time of writing of this report, the corresponding revision of the work program schedule is still ongoing. The Group's co-chairs intend to use their oral presentation at the Closed Session to provide the latest update to participants.

As a general observation, the first wave of policy orientation initiatives regarding AI seems to be ending, and a new phase of more specific programs and legislative initiatives appears to begin. This new phase will again require the attention of data protection and privacy authorities. The work of the Group should lay the foundations for the more detailed work in the coming years. Focussing on current experiences and sound principles, as well as proven practices, will enable GPA members and observers to make a significant contribution to the forthcoming debates.

While some of the enthusiastic forecasts of the capabilities of systems based on AI technology might have created the expectation that such systems could have a significant effect in the fight against the pandemic, there is little evidence of such impact. While there are reports about successful use of some of the more advanced AI applications (analysis of medical imagery, statistical analysis of mass data, guidance of complex diagnostics, and analysis of complex molecules) in the context of COVID-19, the main effect on AI appears to be increased funding for related research and development, and possibly financial support in the phase of economic recovery.

In the sections below, the report will be presenting the key outputs of the Group's activities.

Repository of documents

As there are many policy initiatives addressing the development of AI, and in particular its impact on human rights, including privacy and data protection, the Group's work program includes the creation of a repository of policy documents issued by GPA member authorities and observers or other entities which are setting the legal and regulatory framework for the development and use of AI technologies and applications and their impact on the rights of individuals.

The repository is constantly updated with new documents, and all members and observers of the GPA are invited to inform the Group's Secretariat at the EDPS with information of new documents to be added to the repository. The repository may be accessed by all members and observers of the GPA. Interested organisations are invited to contact the Group's Secretariat at the EDPS for

instructions on access. If appropriate, the Group may consult the GPA Executive Committee to determine time and format of publication on the GPA's website.

Repository of cases

This work item aims at obtaining a meaningful overview of real life applications of AI technology, which are relevant for ethics and data protection. To collect a first set of relevant cases, the Group asked the GPA members' collaboration and sent them in early August 2020 a use case form. The deadline for this first information gathering exercise is 15 September 2020. Since its goal is to keep track of the dynamic development of the domain, the repository will be a living document. Consequently, GPA members are encouraged to send any meaningful addition or update they will come across in the future.

Analysis of the risk to data protection, especially data minimisation, as brought about by the demands to maximise personal data collection on the grounds of 'eliminating' bias and discrimination (Action Point 6)

The co-rapporteurs reported during the June 2021 AIWG meeting that a first draft will soon be submitted to all AIWG members for a first review. The current draft has gone through a general framework of risk management of AI, in particular as to what are the main risks in terms of threats and the likelihood of such risks in terms of methodology.

The co-rapporteurs have signalled the document's Eurocentric approach as its main current issue. The AIWG agreed it would be better to have a larger contribution from other members of the Group from a non- European perspective. Consequently, the AIWG co-chairs launched a call for expressions of interest among its members, and OPC Canada committed to work on this action point. However, participation from Global South countries remains absent.

As a temporary solution, the co-rapporteurs plan to have an ad-hoc meeting to discuss the document in order to reach a compromise between volunteering for the subgroup while still contributing to the work.

The draft would need further revision with precise planning still to be defined. Therefore, it is unsure whether it could be presented in Mexico. Surely, a general discussion on the document could be done at a round table at the GPA Conference in Mexico 2021.

While the work on this item is still ongoing and will be presented in 2022, the aim of the analysis is to also cover other relevant risks considered in the Declaration on Ethics and Data Protection in Artificial Intelligence, in particular risks for the whole society, giving basic indications for managing these risks with reference to the various stakeholders involved. The risks also include sustainability and inequality at global level.

Survey on authorities' capacity and expertise in addressing ethical and data protection issues in AI systems applications (Action Point 8)

As part of its work programme 2019-2021, the GPA AIWG undertook to conduct a survey on members' capacity and expertise in addressing ethical and data protection issues in AI systems applications. The survey aims at drawing a first overview in terms of GPA members' capacity and expertise in addressing ethical and data protection issues related to the application of AI systems, as well as identifying possible upcoming challenges. In the long run, the survey is a first step towards the development of a 'gap analysis', informing GPA members in terms of resources strategies and

best practices. The survey has been conducted during Q2 2021 and the AIWG received a total of 38 responses.

The co-rapporteurs presented during the last AIWG meeting a preliminary summary of the answers and discussed with members possible issues to be further analysed and highlighted in the final survey report.

While most replies come from European authorities, other world regions are also represented. The sample of authorities having responded to the survey reflected a fair balance in terms of staffing and financial resources, thus allowing the development of future analysis on the basis of these criteria. The vast majority of respondents considered relevant to increase knowledge sharing and capacity building between authorities at regional or international level.

The co-rapporteurs plan to present a report on the survey results, with some first overall conclusions based on the analysis carried out, at the Closed Session of the 2021 GPA.

AI in the employment context

AIWG discussed in its April meeting the potential to include a new action point focussing on the impact of AI in the employment context. Here it would be possible in particular to conduct a survey and report on the AI systems (services and products) used in the area of AI employee monitoring and the concrete experiences of the GPA members with these products/companies including the exercise of powers as supervisory authorities and the relevant legal grounds. This proposal was welcomed in principle, but currently the necessary volunteers of this new action item are still lacking. Germany and the UK have already signalled their willingness to become co-rapporteurs.

The work on this action point is still in its early stages.

IEWG- AIWG FRT sub-group

Background

The virtual GPA in 2020 adopted a resolution that tasked the IEWG and AIWG with developing a set of principles and expectations for the use of personal data in FRT. With coordination from the IEWG Secretariat, an IEWG-AIWG FRT sub-group was established in late 2020 to progress work mandated by the resolution. The sub-group comprises the EDPS, the FDPIC, the ICO, the PPC, the OAIC, and the OPC.

Project plan

In January 2021, the sub-group developed and agreed on a project plan for delivery of the resolution. The plan sets out three deliverables:

1. A concise and meaningful set of principles that are designed with a focus on usability and application in practice.
2. Plans for promoting the principles via stakeholder engagement and evaluation of industry application of principles.
3. Reflective report on stakeholder engagement and industry application of principles.

The plan also sets out a phased and collaborative approach for delivery of the deliverables:

- a *research phase* to gather relevant material from GPA members and external stakeholders;
- a *development phase* to analyse the information gathered, and draft and consult on the principles; and
- an *adoption phase* to present the principles for adoption by the GPA, and promote and review their application in practice by industry.

State of play

The sub-group is currently making good progress in undertaking the research phase. In February and March 2021, subgroup members each carried out desk-based research to create an initial pool of relevant material reflecting policy and enforcement activity on FRT by the members themselves, as well as court judgements, reports and articles from other bodies that have helped inform that activity.

In April 2021, the subgroup developed a survey to elicit feedback from GPA members on their views and experience of FRT. The survey sought specific input from members on any policy and guidance products they had developed on FRT, any enforcement actions taken, and any stakeholders engaged as part of that work. It also asked members to set out, with brief explanation, their views on the riskiest purposes for deploying FRT, the most significant data protection and privacy risks associated with those purposes, and any real world examples of use cases they were aware of in their jurisdiction.

There was an excellent response rate to this survey, with over 35 replies from a geographically diverse mix of authorities, providing valuable information on their activities and perspectives on use of FRT around the world. It is clear there is significant and important work across the GPA membership on FRT, and the sub-group take this opportunity to spotlight some key policy and enforcement updates from that work here.

Key updates

Australia – Office of the Australian Information Commissioner (OAIC) and Office of the Victorian Information Commissioner (OVIC)

The OAIC's regulatory role includes handling complaints, conducting investigations, monitoring, advice and providing guidance on proposed uses of biometric information under Australia's Privacy Act. The OAIC has conducted assessments of the handling of personal biometric information collected through and used in facial recognition technology.[3]

Australia's proposed Identity-matching Services (IMS) Bill 2019 contains provisions which will permit the use of FRT for several national security and law enforcement purposes. This draft

[3] Seem for example https://www.oaic.gov.au/privacy/privacy-assessments/summary-of-the-oaics-assessment-of-department-of-immigration-and-border-protections-handling-of-personal-information-using-smartgate-systems/ and https://www.oaic.gov.au/privacy/privacy-assessments/summary-of-the-oaics-assessment-of-ibms-handling-of-personal-information-using-smartgate-systems/.

legislation has been reviewed by the Parliamentary Joint Committee on Intelligence and Security (Parliamentary Committee)[4] but has not yet passed into law.

OAIC: The OAIC made a submission to the Parliamentary Committee on the IMS Bill which suggested that the Bill required further consideration to better ensure that any adverse effects of the proposed enactment on the privacy of individuals are minimised.

OVIC: As well as producing general guidance on biometrics and privacy for the public sector in Victoria (which highlights some key privacy challenges including issues around covert data collection and validity of consent) the OVIC has made a number of submissions specific to the IMS Bill, including a public submission to the relevant Parliamentary Committee. The submission highlights OVIC's concerns with the bill, including: a lack of enforceable governance for use of FRT; the potential for scope creep; inadequate reporting / oversight.

Belgium – Supervisory Body for Police Information (COC)

In Belgium, the Federal Police at Brussels Airport (Zaventem) carried out a test using FRT. As part of the test, LFR was deployed on four cameras to match individuals walking through the airport against a wanted list. The COC, which has the role of Data Protection Authority for law enforcement processing of personal data, carried out an investigation into the test and issued a report to summarise its findings and the action taken. The COC found that although the test was partially discontinued due to high margins of error, the LFR system actually remained active in part. Based on an analysis of the test against the legal framework, the COC also found that there was insufficient clarity on the appropriate legal basis for the test, and documents such as risk assessments had not been completed. The COC therefore issued a corrective order to suspend the LFR test project.

Canada – Information and Privacy Commissioners

Data Protection Authorities in Canada have long given detailed thought to the theoretical implications and real-world impact of deployment of FRT, issuing guidance and carrying out investigations that date back to the beginning of the century. Recently, in addition to a joint investigation into Clearview AI (Federal, British Columbia, Alberta and Quebec privacy authorities), a Special Report was tabled in Parliament regarding the outcome of the OPC investigation into the federal police service's use of FRT, as well as the commencement of public consultations on guidance for police force use of FRT. Further, the Atlantic Information and Privacy Commissioners

[4] Please see the Parliamentary Committee's report of October 2019 at: https://parlinfo.aph.gov.au/parlInfo/download/committees/reportjnt/024343/toc_pdf/AdvisoryreportontheIdentity-matchingServicesBill2019andtheAustralianPassportsAmendment(Identity-matchingServices)Bill2019.pdf;fileType=application%2Fpdf.

of Canada joined together to issue a statement on the implications of FRT. In particular, the joint statement highlights the authorities' concerns with the accuracy of FRT systems, the potential for scope creep, and the proportionality of using FRT when less privacy invasive measures may be available.

European Union - European Data Protection Supervisor (EDPS) and European Data Protection Board

In 2020 and 2021, the European Commission took significant steps in progressing plans to establish a legal framework for AI in the EU. The proposals, set out in a White Paper in 2020 and as a draft Act in 2021, include risk-based provisions that limit the use of AI for automated recognition of human features in publicly accessible spaces (such as LFR). The EDPS published an Opinion on the White Paper in 2020, and a Joint Opinion with the European Data Protection Board on the Act in 2021. Both Opinions are based on a comprehensive assessment of the objectives and approach of the proposals, and expert analysis of the potential implications. In its Opinions, the EDPS notes the extremely high risks posed by remote biometric identification of individuals in publicly accessible spaces and, as a starting point, calls for a general ban on any use of AI for automated recognition of human features in publicly accessible spaces, such as recognition of faces, gait, fingerprints, DNA, voice, keystrokes and other biometric or behavioural signals, in any context.

Japan – Personal Information Protection Commission (PPC)

The Ministry of Land, Infrastructure, Transport and Tourism (MLIT) of Japan launched a "FAST TRAVEL" initiative to address increased demand for air travel and shortage of human resources. As part of this initiative, airport companies in the Tokyo metropolitan area are introducing 'One ID', an optional service that streamlines boarding procedures using FRT. A study group was set up to examine the handling of personal data in the One ID service, including a call for public opinion and the development of guidelines for its use by airport companies. The PPC participated in the study group as an observer and provided advice on privacy protection. This led to the publication of a Guidebook in 2020 which, amongst other things, highlighted that: the use of personal data should be limited solely to boarding procedure purposes; personal data should be deleted within 24 hours; and passengers should consent to the One ID service based on an easy-to-understand explanation of the service and how their personal data is used.

Philippines – National Privacy Commission (NPC)

In addition to publication of an Advisory Opinion on the use of FRT for ID systems (which set out the need for a valid lawful basis for processing personal data and transparency obligations to ensure individuals are aware of its use and how to exercise their rights), the NPC has also taken enforcement action against an organisation's deployment of FRT in one of their products. Grab Philippines is an app that provides several services including food delivery and ride hailing. In 2020, the NPC assessed, amongst other things, a pilot run by Grab using FRT for 'passenger selfie verification' as part of its ride hailing service. The NPC found that Grab did not sufficiently identify and assess the risks to the rights and freedoms of data subjects, and failed to identify an appropriate lawful basis or justify its proportionality. As such, the NPC issued a cease and desist order.

United Kingdom - Information Commissioner's Office (ICO)

Following investigations into trials of live facial recognition technology (LFR) by police forces in the UK, the ICO issued its first formal regulatory Opinion on the deployment of LFR by law enforcement in public places. In the Opinion, the ICO clarifies its position on the application of data protection law, including that use of LFR for law enforcement purposes constitutes sensitive processing; data protection impact assessments must be implemented; and those deploying LFR must meet the high bar of strict necessity. Building on this, the ICO issued a further Opinion on the use of LFR in public places by private companies and public organisations. Rooted in law, and informed in part by several ICO investigations into use or planned use of LFR, the Opinion sets out the ICO's expectations for assessing the crucial concepts of fairness, necessity and proportionality, and clarifies that organisations must also demonstrate high standards of governance and accountability, as well as being transparent with individuals about how their data will be used if they decide to go ahead with an LFR deployment.

United State of America – Federal Trade Commission (FTC)

In 2012, recognising the increasing use of FRT by organisations across the US, the FTC issued best practice guidance for use of FRT, highlighting amongst other things the need to ensure consumers are aware of the deployment of FRT, and for consumers to have a choice not to have their biometric data collected and used for FRT. Subsequently, in 2021, the FTC took enforcement action against Everalbum in the form of a proposed settlement for alleged issues in relation to its use of FRT in its Ever app – offering cloud based photo storage. According to the complaint, many consumers were not informed about Ever's default use of FRT to automatically tag photos, they did not have an option to disable this, Everalbum did not inform consumers that it also used their photos to help train its FRT tool in the first place, and in addition, it retained images indefinitely even after account deletions. The FTC's proposed order requires Everalbum, amongst other things, to delete the FRT

models and algorithms it developed, and to obtain users' express consent before using or developing FRT using their personal data.

In progress

The sub-group is currently concluding its plans for the final element of the research phase - engaging with external stakeholders. Relevant questions are finalised for organisations and industry bodies that develop and offer FRT services; organisations that use and deploy FRT products; lawmakers and regulators that set and enforce relevant regulatory frameworks; and civil society and research bodies that advocate or provide independent advice on development and use of FRT. The stakeholder list is being finalised, with the aim of ensuring a broad collection of experiences, views and opinions on FRT from organisations and bodies the world over. The sub-group expects to reach out to stakeholders in the weeks following submission of this report at the end of July 2021.

Next steps

In July 2021, the sub-group set out plans to commence the development phase of the project, beginning with analysis of the materials collated during the research phase. Sub-group members will work collaboratively to extract key themes, commonalities and areas of contrast, with an initial focus during August and September 2021 on documentation obtained from the desk-based research and survey of GPA membership, followed by analysis of responses from external stakeholders in September and October 2021.

Following the GPA in Mexico, the sub-group will work together on an initial draft of the principles by early 2022, using this analysis as an evidence base. The sub-group will undertake stakeholder consultation on the draft principles and iteratively work towards a final draft by mid-2022 for submission to the GPA Closed Session as a resolution for adoption. In parallel, the sub-group will draft engagement plans for promotion of the principles and review of their application by industry for implementation post-adoption.

Outreach activities

While there have been no direct outreach activities carried by the Group this year, several members had the opportunity to raise awareness about past and ongoing activities of the Group during public events and exchanges with government, public authorities and external stakeholders in relation to recent developments in the field of AI and data protection.

Forward looking plan 2021-2022

The challenges of the pandemic have made some of the issues, which are already addressed in the founding Declaration and in the Work Programme, more visible. They have highlighted some of the ethical questions. The potential conflicts or interferences between various individual rights, or between individual freedoms and societal needs, require a thorough analysis at general level. GPA members should consider what guidance they might be able to provide to organisations and individuals faced with such difficult decisions in concrete situations related to the development of AI and its ethical and data protection aspects. The work packages on the relationship between ethics, human rights and data protection and on the capacity and expertise of data protection and privacy authorities in addressing ethical and data protection issues in cases of application of AI systems will allow to look deeper into this context.

The continuous extension of the repositories on documents and on cases will allow a stocktaking exercise to inform the GPA membership community in 2021 about any new developments in AI that may be relevant for its future work. The Group will work with the Executive Committee to determine whether selected information from the repositories may become accessible to the public, and what an appropriate format could be.

As part of its upcoming activities, and in line with the GPA's strategic direction 2021-2023 the Group will also dedicate in the year to come further reflection on how data protection and privacy are essential to sustainable digital growth and AI innovation.

In the light of the GPA's Strategic Direction 2021 - 2023, the Group will conclude the discussion about the challenges on which it had postponed a decision. In particular, in view of the Action on the integral relationship of data protection to other rights and freedoms, the Group will discuss the best way for approaching the analysis of the societal and environmental impact of data intensive technologies and the analysis of the impact of AI technologies on inequality at global and local level. While there seems to be a growing consensus that environmental challenges and social justice need to be taken into account in all fundamental rights contexts, the GPA may consider to address these issues in a broader context than the development of AI technologies and systems.

The Group will further aim to make suggestions to the GPA on a way forward in addressing the future development of AI technologies and their use, considering their impact on data protection and privacy rights.

Lastly, the Group will continue its cooperation with the IECWG on the FRT activities; it will also explore further opportunities in terms of outreach towards external stakeholders.

Conclusion

The rollout of systems using technologies from the domain of Artificial Intelligence has illustrated the need for a strategic approach to the challenges for data protection and privacy as human rights.

The occurrence of the COVID-19 pandemic has accentuated even more the urgency to address complex challenges with a longer-term perspective.

The common work on these matters demonstrates that the Global Privacy Assembly has the unique potential to contribute to the determination of global strategies to address global problems.