SUMMIT OF THE FUTURE INFORMATION CLEARINGHOUSE BULLETIN

BULLETIN NO 5

Headlines and Key Remarks from the Global Digital Compact Thematic Deep-Dives on "Data Protection" (24 April 2023) and "Human Rights Online" (8 May 2023)

The Summit of the Future (SOTF) Information Clearinghouse Bulletin is an initiative to objectively present the key elements and highlights of the SOTF preparatory meetings taking place at the United Nations.

Note: Excerpts have been quoted directly from the statements made by the stakeholders (non-italicized)

PROJECT TEAM: Eliane El Haber (Lead Author, Bulletin No 5), Mwendwa Kiogora, Jebilson Raja Joslin , Jeffery Huffines, and Fergus Watt.

PROJECT PARTNERS:

DISCLAIMER:

This bulletin is intended to provide an overview of the latest developments and is not a comprehensive summary or record of the SOTF preparatory process. When reporting on statements made by Member States, the bulletin presents key highlights and remarks and the full statements have been hyperlinked if available on the UN Journal website. This information service is a collaborative endeavor supported by Action for Sustainable Development, Coalition for the UN We Need, Global Governance Innovation Network, International Development Law Organization, and the Present and Future Institute. This report was prepared independently with support from project partners. However, the content of the report does not reflect the specific views of any of the partner organizations. Contact Fergus Watt (ferguswatt6@gmail.com) for more information on this information service. Material is not copyrighted and can be distributed freely.

Global Digital Compact Thematic Deep-Dive –
Data Protection (24 April 2023)

Note: This bulletin summarizes the stakeholders remarks only (MS statements are not included).

ABOUT

The third thematic deep dive or informal consultations on the Global Digital Compact (GDC) was held on 24 April 2023 at the Trusteeship Council Chamber . "The deep dives aim to share knowledge and views, as well as allow for contributions on a wide range of digital issues". The Permanent Representative (PR) of Rwanda – H.E. Mr. Claver Gatete and PR of Sweden – H.E. Ms. Anna Karin Eneström are Co-Facilitators of the intergovernmental process negotiating the GDC.

HEADLINES

There is a need to have data that is accurate, safe, accessible, and affordable. It should be up-to-date, standardized, and interoperable. Hence, this kind of data, which determines the way we live, should be highly protected.

RESOURCES

1. Letter from the Co-Facilitators – 18 April 2023

STAKEHOLDERS REMARKS

Co-Facilitator	✚ Inviting all speakers to consider the following guiding questions, 1. Art. 17 ICCPR recognizes the individual right to privacy. How can governments, data protection authorities' private companies, the scientific community and civil society work together to ensure personal data is processed, stored, secured and protected against misuse? 2. What principles would support quality and interoperable data so that governments, international organizations, the private sector, civil society and individuals can contribute to and benefit from digital trade and economy and leave no one behind? 3. Data is a key enabler of innovation and research. How can stakeholders leverage tools such as (pseudo)anonymization, encryption, portability, etc. to drive innovation and interoperability while protecting personal data?

The stakeholders' remarks included contributions from but were not limited to Google, Microsoft, Meta, Youth IGF movement, Association for Progressive Communications, Bangladesh NGOs Network for Radio & Communication, The Royal Society, Digital cooperation organization, Project Omna, International Chamber of Commerce, UNHCR, and Caribbean Telecommunications Union.

- An increasing array of organizations use personal data to provide a growing range of services. Responsible data use can unlock benefits for people, companies, and other organizations around the world.

- Google has synthesized a set of high-level principles called the Framework for Responsible Data Protection Regulation, which can be found online. These principles are based on established privacy regimes and are meant to apply to organizations that make decisions regarding the collection and use of personal information.
- There is a need to strengthen privacy and personal data protection Frameworks so that they effectively address the erosion of collective autonomy that arises from non-consensual data collection, individual and group profiling, recombination of third-party sharing, and downstream processing of anonymized personal data.
- There is a need to ensure that laws and policies for the economic government of data resources maximize social benefit and curtail the market tendency for the concentration of exploitation.
- Everyone has the right to the protection of data that concerns them and to be able to understand, in very simple terms, how that data is processed. No one shall be subjected to arbitrary interference with these rights, and any limitation of this right shall be reasonable, necessary, proportionate, and justifiable. Moreover, any processing of data shall be fair, lawful, and transparent, adhering to the data processing principles set out in international norms and standards.
- There is a need to preserve the robustness of encryption for sensitive data sharing, including end-to-end encryption, and promote the widespread use of end-to-end encryption. The competent operation of trustworthy digital systems relies on many fundamental security technologies including encryption, and these Technologies provide the technical assurance that enables people to entrust their data to digital systems.
- A billion people are online today. Protecting their data has never been more important in today's Digital World. Personal data is constantly collected, processed, and transmitted across borders. This data holds tremendous value and potential for digital trade innovation, research, and development, yet it poses significant risks to individual privacy and security if not handled and protected properly.
- Microsoft believes that privacy is a fundamental human right and that strong data privacy laws are vital for safeguarding it and building trust in technology. There is a need for strong data privacy laws that place accountability where it belongs, which is on the organizations that collect, store, and process data. As the number of privacy laws increases, so does the importance of interoperability.
- Clear, consistent rules across jurisdictions reduce complexity, promote accountability for responsible data practices, and help ensure that everyone's privacy is protected regardless of location.
- Microsoft believes the private sector should take data protection into account. Companies should be transparent about the data they collect and how they use it. There is a need for a right to privacy suited to protect women, girls, and other discriminated-against groups and marginalized people from new harms of abuse that are rooted in the patriarchal structures that fuel gender-based violence.
- The right to privacy in the digital realm is also about safety at its core. The right to privacy protects individuals from intrusion into their own or their family's personal lives by Third parties, creating an expectation of Privacy. That privacy can protect users online from sexual exploitation and abuse, such as having their personal and sexual information shared and distributed without their consent.
- Sharing data may bring many benefits. It has become necessary to share data for everyday tasks and engage with other people in today's society, but it is not without risks. Data can easily be exploited to cause harm and is especially dangerous for vulnerable individuals and communities, such as journalists, activists, human rights defenders, and members of oppressed and marginalized groups, which is why data must be strictly protected.
- The GDC process should employ a human-centric approach. Guided by the international human rights law framework as the basis for protecting such data.

- No one shall be subjected to arbitrary interference with the right to privacy, which is closely linked to the right to data protection; any restriction on these rights must be consistent with the principles of legality, necessity, and proportionality under international law.
- There is a need to adopt a new mentality regarding leadership, harm, and data harm prevention, so there is a need to advance a precautionary approach to data protection. There is a need to focus not only on the inputs and the nature of the data that circulates globally but also on the outcomes and the consequences for social groups. There is a need for robust and open methodologies for data protection impact assessment.
- Asylum claims must respect the confidentiality of Asylum information and regulate data sharing and access, particularly about countries of origin. Upholding the standards is vital to preventing risks for Asylum Seekers and ensuring the humanitarian nature of preservation.
- In the International Covenant on Civil and Political Rights , the Universal Declaration of Human Rights, and the Charter on Fundamental Rights of the European Union, they all established the right of every individual to maintain control over their data, as this is a precondition for the exercise of many other Freedom rights.
- The huge amount of data that's flowing over the internet is an important source of knowledge and economic power as it contributes and creates value to reach Sustainable Development Goals and also because data could be used for the benefit of humanity, but it is also used to provide users with information for marketing campaign purposes and also for malicious and surveillance purposes. That's why it's important and urgent to establish global principles and rules to protect data, regulate the collection, storage, and use of data, and ensure trust and safe transnational transfer of data. What is important is to strike the right balance between the use of data as an economic and social resource and data protection as a fundamental right of the individual. It is essential that data protection rights are guaranteed to protect the digital space and that the GDC includes this principle to defend this right.
- There is a need for governments to guarantee the processing, storage, and protection of their citizens data, placing the right to privacy at the center. There is also a need to analyze this issue from a gender perspective, taking into account that the dissemination of data does not affect all people in the same way.
- More than a billion people use Meta's applications every month, and in doing so, they have access to an interconnected world of people, ideas, news, communities, and commerce unconstrained by local or national boundaries. At its core, Meta wants to preserve an open, universally accessible internet with safety, security, and respect for human rights at its heart.
- While Meta is working to make progress, she should not be doing that alone. That's why Meta supports globally consistent regulations to set clear and fair rules for everyone and a safe and secure open internet where creativity and competition can thrive.
- The internet needs guardrails, not roadblocks. Many are drawn to the idea of digital sovereignty, whereby establishing digital walls at their National borders can better secure data generated by their citizens.
- Governments need to resist protectionist policies that do not further the protection against misuse of how personal data is processed, stored, secured, and protected. Instead, under such policies, the internet becomes a little less free and the digital economy becomes a little bit more constrained.
- It is essential to recognize that international human rights law acts as the basis for protecting the collection, processing, sharing, and use of personal data, which must be considered from the perspective of the younger generations.
- Young people are the generation that will be significantly affected by today's decisions. Today's youth are digital natives, living much of their lives online, and therefore have found the most critical spheres of their lives digitalized. With this digitalization comes a heightened risk and increased vulnerability to

cyberattacks for young people. Their data is an extension of themselves, personal and private, yet beyond their control.

- As the world continues to leverage data as an enabler of innovation and research, it is crucial to prioritize the protection of personal data, ensuring its use is transparent, responsible, and beneficial to all. Innovation and research are essential drivers of progress, yet they must not come at the expense of personal data protection.
- Young people are concerned by the absence of governance and laws concerning digital spaces and data protection. Governments must enact more legislation to incentivize companies to invest in cyber security and treat data responsibly and ethically.