FORUM: Legal Committee (GA6)

QUESTION OF: Establishing a legal framework for data protection and privacy

SUBMITTED BY: Japan

CO-SUBMITTED: Australia, Costa Rica, Cyprus, Denmark, Egypt, Finland, Germany, Israel, Jordan, Malta, Portugal, Republic of the Congo, Sweden, Switzerland, Ukraine, United Kingdom, United States of America

THE LEGAL COMMITTEE,

Acknowledging the increasing importance of data privacy and protection as fundamental rights under Article 12 of the Universal Declaration of Human Rights (UDHR),

Noting with regret the rise in illegal data collection, processing, sharing, storage, and recognising that the need for data protection and privacy has increased dramatically,

Further agreeing that there must be some legal baseline of data information that must be collected to prevent criminal activities such as money laundering and terrorism, cyber attacks, phishing and stealing of data, which pose a significant risk to individuals and governments organisations,

1. Calls for the creation of an international legal framework run by the United Nations (UN), which will outline clear rules for data collection, usage, and storage while granting individuals the right to access, amend, and delete their data and will also emphasize the importance of obtaining informed consent before data collection to maintain transparency and accountability, in order to:

    a) protect personal data and prevent misuse and unauthorized access by:

        i. establishing strict penalties for unauthorized data and misuse such as but not limited to fines, sanctions and legal prosecutions to deter violations,

        ii. requiring security measures such as multi-factor authentication to help keep data safe from breaches and cyberattacks,

        iii. having a group of trained professionals regularly review if there is a breach of the rules and regulations,

    b) ensure individuals have rights to access, correct, and delete their data,

    c) require clear and informed consent for data collection by ensuring that all data collection forms are written in clear language and are easily accessible;

2. Urges Member States and relevant stakeholders to enhance capacity building in all Member States, by providing financial aid through the UN fund and governmental funds to incorporate the following strategies:

    a) creating infrastructure for data protection, including:

        i. digital identification systems, that secure identification incorporating safeguards,

        ii. biometric authentication for governmental and citizen data protection,

    b) incorporating encryption systems that ensures unauthorized users do not have access to data in transit, such as but not limited to:

        i. transport Layer Security, for internet communication,

        ii. end-to-end encryption,

    c) establishing Intrusion/Violation Detection and Prevention Systems (IDPS) for governmental and international data;

3. Recommends the implementation of suitable strategies to ensure monitoring and accountability in citizen and governmental data management, such as but not limited to:

    a) assessing regularly Member States compliance with international and national data protection standards, by:

        i. composing an analytical report sent to the General Assembly every six months, including progress and challenges faced,

        ii. sending representatives in case of suspicions of flawed management,

    b) providing recommendations and modifications for improvement in national frameworks of Member States;

4. Calls for Member States to ensure ethical and responsible use of citizen and governmental data by:

    a) encouraging proper use of personal data by organizations and Member-States governmental bodies, by providing them with detailed guidelines regarding:

        i. refraining from profiling and discrimination based on sensitive personal data including gender, race, ethnicity, etc. within governmental data management,

ii. committing to responsible use of Artificial Intelligence (AI) technologies especially those involved in the processing of personal data,

b) ensuring that governments take responsibility for wrongful and harmful use of citizen data so that member states are more selective in their use of it, and participate in organizations such as the Information Commissioner's Office (ICO,) which as aforementioned oversees and certifies the correct use of data

5. Encourages all Member States to raise public awareness in LEDCs (Less Economically Developed Countries) regarding data protection and privacy through methods such as but not limited to:

a) empowering and encouraging individuals to participate in simulation platforms that align values, attitudes, and behaviors with ethical principles,

b) providing seminars and workshops to inform and educate individuals about protecting their personal data, and recognizing phishing attempts,

c) allocating training, resources, and technical assistance to understand and adopt data protection standards,

d) form international partnerships between developing and developed countries to enhance technical infrastructure;

6. Further encourages all member states to collaborate by creating shared databases and exchanging data to develop effective strategies and best practices, and to ensure the following:

a) cross-border data transfers should only occur to countries that have strong data protection laws, including:

i. assessing whether a country’s data protection laws meet international standards,

ii. reviewing legal frameworks to ensure they align with global data protection principles,

b) Member States and organizations should regularly review their data flow maps to understand where data is being transferred, making sure to:

i. ensure transparency about where data is going,

ii. identify any potential risks or gaps in how data is protected,

c) full assessment should be conducted to ensure the jurisdictions involved in data transfers have adequate data protection laws, by:

i. checking if sufficient safeguards are in place to protect data during transfer,

ii. identifying areas where extra measures might be needed for compliance;

7. Further urges the UN to create a new body, namely the Global Data Protection Framework (GDPF), to coordinate global privacy standards, this framework would thus:

a) safekeep Universal Privacy Principles by:

i. ensuring that transparency between countries is kept,

ii. taking proper accountability for actions,

iii. conducting research on d+ata minimization and guaranteeing that standards are

iv. met,

b) set standards and make decisions regarding disputes in order to assist countries with laws regarding privacy,

c) provide adaptable templates for nations to ensure consistency of laws while simultaneously respecting differences in governance so that every nation follows a certain guideline while still having its own laws catered to itself;

8. Calls upon the United Nations to establish a working group of legal experts and diplomats to comprehensively review and develop an international legal framework concerning political immunity, with the aim of enhancing clarity,consistency, and mutual understanding of this concept in the context of diplomatic and consular ones:

a) stresses that the working group should prioritise human rights and prevention of impunity for grave crimes,

b) suggests that the group consider regional legal frameworks and best practices to ensure global application,

c) Recommends that reports from the working group include timelines for implementations and monitoring mechanisms.