FORUM: Legal Committee (GA6)

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

STUDENT OFFICER: Vasiliki Lentoudi

POSITION: Co-chair

INTRODUCTION

As more social and economic activities have taken place online, the importance of privacy and data protection is increasingly recognized. Both terms data privacy and data protection are often utilized interchangeably; however, they have a significant difference. Data privacy defines who has access to data, while data protection provides tools and policies to restrict access to the data.[1] Data protection is closely connected to the fundamental human right of privacy, which every individual has, according to Article 12[2] of the Universal Declaration of Human Rights (UDHR). Although attempts to combat the issue of data privacy and protection have been made in the past, the frameworks that exist are regional and do not apply to the majority of countries. Some examples of such attempts and frameworks are the California Consumer Privacy Act (CCPA)[3] and the Asia Pacific Economic Cooperation (APEC) Privacy Framework[4].

Privacy and protection of personal data is a key concern for individuals, organizations, and regulators. Individuals expect organizations and countries to handle their personal information as private and confidential, safeguard their personal data, and make use of it only to provide and operate financial services, and for other purposes as required by law or regulation. However, most of the time, the security of individuals' personal data is jeopardized, since their personal data is often shared or sold to third parties. Thus the creation of a legal framework on data privacy and protection is a matter and Act of utmost

---

[1] Ross, Jeremy. "Data Protection and Privacy: How to Protect User Data." *Cloudian*, cloudian.com/guides/data-protection/data-protection-and-privacy-7-ways-to-protect-user-data/amp/.

[2] "Universal Declaration of Human Rights | United Nations." *United Nations*, www.un.org/en/about-us/universal-declaration-of-human-rights.

[3] Anna. "California Consumer Privacy Act (CCPA)." *Cookiebot*, 4 Aug. 2023, www.cookiebot.com/de/ccpa-konformitaet.

[4] *APEC PRIVACY FRAMEWORK (2015)* _____ *CONTENTS*.

importance. It is going to enhance some already legal frameworks like CCPA or UDHR and add to them crucial characteristics for a legal framework.

The topic of establishing a legal framework for data privacy and protection can be easily associated with the topic of the conference, namely "Ethos Versus Progress – Reassessing our values in a fragile world." To begin with, the topic of data privacy and protection has ethical foundations since it emphasizes how crucial it is to respect individuals' privacy and protect their personal information. Additionally, in reassessing our values privacy and data protection must be upheld as a human right, while ensuring that the utilization of personal data will be ethical involves considerations of fairness and accountability. Last but not least, in a fragile society and world establishing frameworks about data privacy and protection contributes to the security of digital infrastructures. More specifically it gives individuals, businesses, companies, organizations and pretty much everyone the chance to make use of the enhanced and new technological advancements, without having the fear of the mishandling of their personal data and information.

DEFINITION OF KEY TERMS

Data privacy

"Data privacy is a guideline for how data should be collected or handled, based on its sensitivity and importance." [5]

Data protection

"Data protection signifies the strategic and procedural steps undertaken to safeguard the privacy, availability, and integrity of sensitive data, and is often interchangeably used with the term 'data security."[6]

Right to access

[5] Ross, Jeremy. "Data Protection and Privacy: How to Protect User Data." *Cloudian*, cloudian.com/guides/data-protection/data-protection-and-privacy-7-ways-to-protect-user-data/amp/.

[6] Cloudian. "Data Protection and Privacy: Definitions, Differences, and Best Practices." *Cloudian*, 2022, cloudian.com/guides/data-protection/data-protection-and-privacy-7-ways-to-protect-user-data/.

The right to access refers to the right of individuals to be provided with a copy of their personal data or other personal information. [7]

Right to rectification

"If an individual's personal data is inaccurate, they have the right to have the data rectified, by the controller, without undue delay."[8]

Sensitive data

"It refers to information that, if disclosed, misused, or accessed without authorization, could result in harm, discrimination, or adverse consequences for the individual to whom the data pertains."[9]

Personal data

"Personal data is any information that relates to an identified or identifiable living individual."[10]

Processing

"Data processing occurs when data is collected and translated into usable information."[11]

[7] https://gdpr-info.eu/issues/right-of-access/

[8] "The Right to Rectification | Data Protection Commission." *The Right to Rectification | Data Protection Commission*, www.dataprotection.ie/en/individuals/know-your-rights/right-rectification.

[9] "What Is Sensitive Data?" *Palo Alto Networks*, www.paloaltonetworks.com/cyberpedia/sensitive-data.

[10] "What is personal data?" *European Commission*, commission.europa.eu/law/law-topic/data-protection/reform/what-personal-data_en.

[11] Pearlman, Shana. "What Is Data Processing? Definition and Stages - Talend Cloud Integration." *Talend Real-Time Open Source Data Integration Software*, 2018, www.talend.com/resources/what-is-data-processing/.

BACKGROUND INFORMATION

Historical Background of data privacy and protection

The history of data privacy and protection goes back to "the U.S. Constitution[12], which came into effect in 1789, and while not explicitly guaranteeing the right to privacy, the Supreme Court has found that the Constitution does provide for a right to privacy in its First, Third, Fourth, and Fifth Amendments.[13] After that, the right to privacy, a law review article, was published in the 1890 Harvard Law Review[14]. It was the first publication in the US that advocated the right to privacy, articulating that right primarily as a right to be let alone, which set the foundation of other rights, such as the right to property and the right to prevent the publication of personal data and private information. The authors also requested the existence of a right to privacy based on the jurisdictional justifications used by the courts to protect material from publication, which is the closest version of what is nowadays considered in this context data privacy. Under the term data privacy exists nowadays issues related to collecting, storing and retaining data as well as data transfers within applicable regulations and laws, such as GDPR.[15]

In 1914, the Federal Trade Commission Act (FTCA) established the Federal Trade Commission and outlawed unfair or deceptive commercial practices[16]. In 1948, the United Nations Organization (UN) established the UN Declaration of Human Rights, which states in the 12th Article "No one shall be subjected to arbitrary interference with his privacy, family,

[12]"The Constitution | Bill of Rights Institute." Bill of Rights Institute, www.googleadservices.com/pagead/aclk?sa=L&ai=DChcSEwii793y-5eIAxVjlYMHHVcuAmoYABABGgJlZg&co=1&ase=2&gclid=CjwKCAjwlbu2BhA3EiwA3yXyu6_ZdxZOIMQJa9weDeoDlm8G8TaR1OcASy_HqgnXz1LUKxIky4IWdBoCnTcQAvD_BwE&ohost=www.google.com&cid=CAESVuD2QnOHOYosRwvtZBBKvAl3-iITjm9TxzsW4cdg9dTl7ZAVKg9hs2t__KS3oFFmiZ8jJ4zViofZ4ws9wVLTdb_IqVUcKv-bDUiHQQZIlF3rN9nxEdgu&sig=AOD64_1ZHmDQuC7jkKX3kaTn9ji80iqebw&q&nis=4&adurl&ved=2ahUKEwjU3dTy-5eIAxUUhP0HHR8LK2cQ0Qx6BAgGEAE.

[13] "History of Privacy Timeline / Safecomputing.umich.edu." *Safecomputing.umich.edu*, safecomputing.umich.edu/protect-privacy/history-of-privacy-timeline.

[14] https://archive.org/details/jstor-1321160/page/n1/mode/2up

[15] "What Is Data Privacy? - Definition from TechTarget.com." *CIO*, www.techtarget.com/searchcio/definition/data-privacy-information-privacy#:~:text=Data%20privacy%20focuses%20on%20issues.

[16] "Federal Trade Commission Act (FTCA) | Britannica Money." *Encyclopædia Britannica*, 2024, www.britannica.com/money/Federal-Trade-Commission-Act#:~:text=Federal%20Trade%20Commission%20Act%20(FTCA)%2C%20federal%20legislation%20that%20was. Accessed 1 Sept. 2024.

home or correspondence, nor to attacks upon his honor and reputation. Everyone has the right to the protection of the law against such interference or attacks."[17]

In addition to that, since the Declaration includes the right to privacy and is recognized on an international level the right to privacy is a fundamental right in all member States, thus the establishment of an international framework would be much easier because there has already been a basis for the framework.

In 1973, "the Department of Health, Education, and Welfare (HEW) Secretary's Advisory Committee on Automated Personal Data Systems (SACAPDS) in the US developed the landmark 1973 Records, Computers and the Rights of Citizens, Report of the Secretary's Advisory Committee on Automated Personal Data Systems"[18], which set the basis for modern privacy legislation, since it was the first connection of the protection of privacy in the context of technology. Some other Acts that were implemented in a variety of places around the world are for example the adoption of the Personal Information Protection Law, by China on 20 August 2021 which is the first national-level law comprehensively regulating issues in relation to personal information protection in this country[19] or the Australia's Notifiable Data Breaches Scheme NDB which came into effect and applies to all agencies and organizations that collect and hold people's personal information[20]. Countries and organizations worldwide began to take action after recognizing the significant importance of data privacy and protection through some incidents that have taken place throughout the years. Examples of such incidents are first of all the fact that a British consulting firm, Cambridge Analytic, collected personal data belonging to millions of Facebook users without their consent, predominantly to be used for political advertising in 2010. This caused extreme Action and individuals started to understand the importance of the topic and their right to privacy.

---

[17] United Nations. "Universal Declaration of Human Rights." *United Nations*, 1948, www.un.org/en/about-us/universal-declaration-of-human-rights.

[18] "History of Privacy Timeline / Safecomputing.umich.edu." *Safecomputing.umich.edu*, safecomputing.umich.edu/protect-privacy/history-of-privacy-timeline.

[19] Law, Bloomberg. "China's Personal Information Protection Law (PIPL) - Bloomberg Law." *Bloomberg Law*, 9 Jan. 2024, pro.bloomberglaw.com/insights/privacy/china-personal-information-protection-law-pipl-faqs/#:~:text=China's%20PIPL%2C%20adopted%20on%20Aug,relation%20to%20personal%20information%20protection.

[20] "Notifiable Data Breaches Bill - Australia." *Fortinet*, 2023, www.fortinet.com/solutions/industries/notifiabledatabreach#:~:text=The%20NDB%20came%20into%20effect. Accessed 9 Aug. 2024.

Current Situation of Data Privacy and Protection

The new and advanced technologies are extremely helpful, and profitable and bring a variety of social and economic advantages and benefits to people, governments and businesses. Such advantages include providing consumers with a variety of options, market expansion, productivity, education, communication and product innovation. [21] Although these technologies make it much faster and cheaper to collect, analyze and utilize large quantities of information, their design often makes them undetectable to individuals and thus more difficult for them to retain a measure of control over their personal information and data. That is because advanced technologies collect a massive quantity of information and data in a short amount of time, while the risk of data breaches increases as long as even more data gets stored and processed by advanced technologies. Consequently, it is a matter of great importance to enforce and encourage ethical and trustworthy ways of handling personal data, not only online but also offline ones, so that people and businesses feel more comfortable and less jeopardized to share their data and information when needed.

After many years and a variety of regional frameworks, there is still no Data Protection and Privacy legislation that applies worldwide. 137 out of 194 Member States had put in place legislation to secure the protection of data and privacy. 71% of countries have legislation, 9% have draft legislation, 15% have no legislation and 5% have no data. [22]

Importance of the establishment of a framework for data privacy and protection

The establishment of a legal framework for Data Privacy and Protection is a matter of great importance for several reasons. To begin with, it will contribute to the implementation of proper privacy safeguards for personal information, especially by protecting individuals from the negative consequences of privacy breaches and the misuse of their personal information and data. Individuals will be informed about what kind of information is collected about them and why since one of the goals of the new legal framework on data privacy and protection is to set a clear view of which data and why should be collected. In addition, the goal of the framework is to become a national piece of legislation and thus apply to all Member States, which makes it easier for every country to have legislation on data privacy and protection. Thus, the residents of each country will automatically not only

[21] (*APEC PRIVACY FRAMEWORK (2015)* _____ *CONTENTS*)
[22] UNCTAD. "Data Protection and Privacy Legislation Worldwide | UNCTAD." *Unctad.org*, 14 Dec. 2021, unctad.org/page/data-protection-and-privacy-legislation-worldwide.

have the right to privacy but also the right to be protected by law, some of the main purposes and goals of the legal framework on data privacy and protection.

Furthermore, the establishment of a new legal framework on data privacy and protection is a matter of utmost importance, since it will cover crucial aspects of the topic, which haven't yet been covered by any other legal document, due to the rapid development and evolution. To begin with, it will be a very important aspect of promoting the right to data privacy as a fundamental human right and thus reform and add to the UN Declaration of Human Rights, which was put into effect in 1948 and thus only states in its 12th Article that "no one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honor and reputation." The legal framework will also be able to add to the General Data Protection Regulation (GDPR) that was put into effect by the European Union on May 25, 2018, which is nowadays the toughest security and privacy law in the world. It not only applies to Europe but it imposes obligations onto organizations anywhere as long as they collect data from European citizens. Firstly the new legal framework should in contrast with the GDPR cover every citizen around the world, while some other changes should be implemented too. For example, the new data privacy and protection framework, in contrast to the GDPR, states that children above 13 can be their one data subject and "Children under 13 can only give consent with permission from their parent"[23]. Only adults should be able to give consent for their personal information, while for individuals, who are under 18, their parents are going to be the ones who handle their data. This move could make such a difference since adults have their responsibility and they can understand and decide more carefully whether they should give consent to organizations to handle their personal data. Additionally, it would be very helpful if every organization got obliged to keep drafts of the consent of every individual that agrees with the collection and handling of their data. Consequently not only the individuals and data subjects would have documentary evidence of consent.

Data privacy principles

One of the main Data Privacy principles is directed toward ensuring that individuals know what information is collected about them and for what purpose it is to be utilized. One of the main principles of the Framework recognizes that one of

[23]Wolford, Ben. "What Is GDPR, the EU's New Data Protection Law?" GDPR.eu, 29 Aug. 2024, gdpr.eu/what-is-gdpr.

the most crucial and primary objectives is to prevent the mishandling of personal data and information. Very important is also the principle about collection limitation. This principle limits the collection of personal information by reference to the purposes for which it is collected. In addition to that it is really important to set a clear set of instances, in which data processing is allowed and legal. Such instances could be that the data subject has given documentary consent for the processing of his or her data, to handle personal data to even save somenones' life etc. Furthermore, individuals should be provided with clear, prominent, easily understandable, accessible and affordable mechanisms to exercise their right of choice and say in relation to the collection, use and disclosure of their personal information. This provides the basis for the creation and establishment of a trustful relationship between the data subject and the data processor. The idea of the Choice Principle is very important for individuals since they are to have the chance to have a say in the collection, disclosure and transfer of their personal data and information. Consequently, they will have the right to exercise one of their main privacy rights too, namely the right to delete personal data that has been already collected.

Limitations of establishing a legal framework

The establishment of a legal framework on data privacy and protection is accompanied by a variety of limitations and difficulties. Firstly, such a framework requires rapid technological development in the majority of countries. The whole framework is going to be based on technological systems, which will make the cooperation of all Member States easier and faster. However, not all Member States have had the same technological development throughout the years and can't maybe support the whole process easily and rapidly. Furthermore, one of the most important limitations according to the establishment of a legal framework on data privacy and protection is the national and regional legal frameworks, legislations and policies of countries and regions that differ from region to region and country to country. Thus, it is extremely challenging to set and establish a legal framework that meets the policy of every country and could be implemented in all Member States. Another important limitation is balancing privacy and innovation. In today's digital age, Artificial Intelligence (AI) has become a very powerful and crucial tool,

drastically revolutionizing various industries, including healthcare and finance.[24] Consequently, it is for sure that it will also be utilized in the framework of data privacy and protection. Despite the vast and transformative promises of AI, there is a critical concern regarding its potential implications for data privacy.

MAJOR COUNTRIES AND ORGANIZATIONS INVOLVED

United States

The United States has implemented a variety of regional Acts on data privacy and protection throughout the years. To begin with, there is the California Consumer Privacy Act (CCPA). It went into effect on January 1, 2020[25] and gives consumers more control over the personal information that businesses collect about them and the CCPA regulations provide guidance on how to implement the law. This Act secured new privacy rights for individuals such as the right to know, namely the right to become informed about what information is collected about them and why, and the right to delete, which is the ability they have to delete information that was collected about them, the right to opt-out of the sale of sharing their personal information and the right to exercise their CCPA rights freely without any discrimination.[26] This Act has been a significant Act not only for the State of California but also for the US as a whole since it has been the most recent one and has set a basis for other ones that are going to be implemented soon. While the United States lacks a national legal data privacy and protection law a variety of efforts have been made to enforce and implement one. One of them is the American Data Privacy and Protection Act.

ADPPA was introduced during the 117th Congress in 2021-2022. Although it has yet to receive a vote, its provisions could become law by being included in another bill."[27] If it were to be enacted into law, it would have regulated how organizations keep and use consumer data. One of the other acts that have been already implemented is the Health Insurance Portability and Accountability (HIPAA), which was enacted by the 104th United States Congress and signed into law by President Bill Clinton on August 21, 1996 and protects

[24] "AI and Data Privacy: Balancing Innovation with Security - SmartDev." *SmartDev*, 23 Mar. 2024, www.smartdev.com/ai-and-data-privacy-balancing-innovation-with-security/. Accessed 9 Aug. 2024.

[25] CCPA. www.cloudflare.com/learning/privacy/what-is-the-ccpa.

[26] "California Consumer Privacy Act (CCPA)." State of California - Department of Justice - Office of the Attorney General, 13 Mar. 2024, oag.ca.gov/privacy/ccpa.

[27] "U.S. Data Privacy Protection Laws: 2024 Guide." *Security*, www.techtarget.com/searchsecurity/tip/State-of-data-privacy-laws#:~:text=While%20the%20U.S.%20currently%20doesn.

information held by a covered entity that concerns health status, provision of healthcare or payment for healthcare that can be linked to an individual. Its Privacy Rule regulates the collection and disclosure of such information, and its Security Rule imposes requirements for the secureness of this information and data. In addition, there is the Gramm Leach Bliley Act (GLBA), enacted on 12 November 1999 by the 106th United States Congress[28] and governs the protection of personal information in the hands of banks, insurance companies and other companies in the financial service industry. This statute addresses "Nonpublic Personal Information" (NPI), which includes any information that a financial service company collects from its customers in connection with the provision of its services."[29] In a nutshell, NPI is any information an individual provides to get a financial product or service.

Japan

In Japan, The Act on the Protection of Personal Information Act No. 57 of 2003 (APPI) [30] is the primary legislation that applies to the collection and processing of personal data, which also went through substantial revision both in 2017 and 2022. "The APPI establishes the PPC (Personal Information Protection Commission), a regulatory body that can issue guidance on the application and interpretation of the Law and its requirements."[31] Some important regulations of this Act are first of all that before making use of personal information and data a clear purpose must have already been identified. In case someone gets to handle sensitive information, such as data related to race, religion and medical records, prior consent is required and after the achievement of the specified purpose the data that has been collected has to be deleted. These and others are important achievements of this Act. Furthermore, there are unfortunately no laws or regulations that target artificial intelligence (AI) at this time in Japan.

[28]"Gramm-Leach-Bliley Act." Federal Trade Commission, 23 May 2024, www.ftc.gov/business-guidance/privacy-security/gramm-leach-bliley-act.

[29] ICLG. "Gambling Singapore Chapter." *Gambling 2019 | Laws and Regulations | Singapore | ICLG*, 2024, iclg.com/practice-areas/gambling-laws-and-regulations/singapore.

[30] "Japan Data Protection Law: Everything You Need to Know | Didomi." *Didomi.io*, 2024, www.didomi.io/blog/japan-data-protection-law-appi-everything-you-need-to-know#:~:text=In%20Japan%2C%20The%20Act%20on. Accessed 1 Sept. 2024.

[31] "Japan Data Protection Law: Everything You Need to Know | Didomi." *Blog.didomi.io*, blog.didomi.io/japan-data-protection-law-appi-everything-you-need-to-know.

European Union

The General Data Protection Regulation (GDPR)[32] is the most stringent security and privacy law in the world. It was drafted and passed by the European Union, however, it applies to organizations globally in case they collect or handle data of individuals in the European Union. [33] The regulation was put into effect on 25 May 2018 and it imposes fines to those who violate the privacy and security standards. Through the establishment of GDPR Europe makes it clear that it takes data privacy and protection as a matter of great importance especially as even more people handle their personal data with cloud services and could face data breaches. One of the most crucial articles of the GDPR is Article 6[34], which states clearly the instances in which it is legal to process someone's personal data. Such examples of instances are when the data subject gave unambiguous consent when someone needs to process it to comply with a legal obligation and when to perform a task in the public interest etc.[35] The GDPR was also a Regulation of utmost importance since it has set new rules about what constitutes consent from a data subject to process their information. Two of them are that children under 13 can only give consent with permission from their parents and that every individual needs to keep documentary evidence of consent.[36]

The Asia Pacific Economic Cooperation

Asia Pacific Economic Cooperation members recognize the fact that the digital economy has a huge potential to raise more business opportunities, reduce costs, boost efficiency and enhance the quality of life. Thus, the APEC established a framework to protect privacy within and beyond economies and to enable regional transfers of personal information to benefit consumers, businesses, and governments. "APEC economies do not underestimate the importance of [37]protecting information privacy while maintaining information flows among economies in the Asia Pacific region and among their trading partners." It has set out principles that have to do with preventing harm, acknowledging the

[32]Wolford, Ben. "What is GDPR, the EU's new data protection law?" *GDPR.eu*, 29 Aug. 2024, gdpr.eu/what-is-gdpr.

[33]Ibid

[34] "ibid"

[35]"ibid"

[36] "ibid"

[37]*APEC PRIVACY FRAMEWORK (2015)* _____ *CONTENTS*.

risk of mishandling personal data, and collection limitations, namely setting a clear set of proper purposes for data collection, uses of personal information, the right of individuals to choose and have a say in the collection of their data, the use of personal information, and accountability. The framework was developed and updated due to some important, mainly evolutionary reasons. To begin with, the members of the cooperation found it extremely crucial to implement proper privacy safeguards for personal data, especially from harmful intrusions and the misuse of personal information. In addition to that the cooperation wanted to ensure the free flow of information to trade, and to economic and social growth in both developed and developing market economies.

TIMELINE OF EVENTS

Date	Description of Event
25 May 2018	"The EU adopted the General Data Protection Regulation (GDPR), one of its greatest achievements in recent years, which replaces the 1995 Data Protection Directive, which was adopted at a time when the internet was in its infancy."[38]
2010	British consulting firm Cambridge Analytica collected personal data belonging to millions of Facebook users without their consent by, predominantly to be used for political advertising.
14 August 2020	The California Department of Justice implemented the CCPA which was [39]
1979	In 1979 the establishment of the Global Privacy Assembly took place, which has been the premier global forum for data protection and privacy authorities for more than four decades[40]
20 August 2021	China adopted the Personal Information Protection Law, which is the first national-level law comprehensively regulating issues in relation to personal information protection[41]

[38] "The History of the General Data Protection Regulation." *European Data Protection Supervisor*, 25 May 2018, www.edps.europa.eu/data-protection/data-protection/legislation/history-general-data-protection-regulation_en.

[39] "California Consumer Privacy Act (CCPA)." *State of California - Department of Justice - Office of the Attorney General*, 15 Oct. 2018, oag.ca.gov/privacy/ccpa#:~:text=Are%20there%20any%20CCPA%20regulations. Accessed 9 Aug. 2024.

[40]Global Privacy Assembly. globalprivacyassembly.org.

[41]Law, Bloomberg. "China's Personal Information Protection Law (PIPL) - Bloomberg Law." Bloomberg Law, 9 Jan. 2024, pro.bloomberglaw.com/insights/privacy/china-personal-information-protection-law-pipl-faqs/#:~:text=China's%20PIPL%2C%20adopted%20on%20Aug,relation%20to%20personal%20information%20protection.

February 2018	Australia's Notifiable Data Breaches Scheme NDB came into effect, which applies to all agencies and organizations that collect and hold people's personal information [42]
25 May 2018	The UK Data Protection Act updates data protection laws in the UK, supplementing the General Data Protection Regulation, implementing the EU Law Enforcement Directive (LED), and extending data protection laws to areas that are not covered by the GDPR or the LED[43]

UN INVOLVEMENT: RELEVANT RESOLUTIONS, TREATIES AND EVENTS

Adoption of the Principles by the High Level Committee on Management (HLCM)

The High-Level Committee on Management adopted at its 36th meeting on 11 October 2018 the set of Personal Data Protection and Privacy Principles, which published a framework upon the process of personal data by, or on behalf of, the United Nations System Organizations in carrying out their mandated activities. The purpose of these principles is first of all to set clear and mutual standards for the protection of personal data across the UN System. In addition, they aim to facilitate the accountable processing of personal data and promote respect for the human rights and fundamental freedoms of individuals, more specifically the right to privacy. The total of these principles applies to personal data, contained in any form. [44]

Resolution adopted by the General Assembly on 18 December 2013 on the right to privacy in the digital age

The resolution adopted by the General Assembly on 18 December 2013 on the right to privacy in the digital age "reaffirms the right to privacy, according to which no one should

[42] "Notifiable Data Breaches Bill - Australia." *Fortinet*, 2023, www.fortinet.com/solutions/industries/notifiabledatabreach#:~:text=The%20NDB%20came%20into%20effect. Accessed 9 Aug. 2024.

[43] Introduction to the Data Protection Bill. ico.org.uk/media/2614158/ico-introduction-to-the-data-protection-bill.pdf.

[44] Personal Data Protection and Privacy | United Nations - CEB. unsceb.org/privacy-principles.

be subjected to arbitrary or unlawful interference with his or her privacy, home, family or correspondence and the right to the protection of the law against such interference". In addition, it acknowledges the new, global and accessible nature of the internet as well as the rapid development of communication and information technologies as a crucial factor in the acceleration of progress towards development in its various forms. Furthermore ,it encourages the United Nations High Commissioner for Human Rights to provide a report protecting and promoting the right to privacy especially concerning domestic and extraterritorial surveillance or the interception of digital communications and the collection of personal data.[45]

World Summit on the Information Society (WSIS)

"The World Summit on the Information Society (WSIS) is a unique two-phase United Nations (UN) summit that was initiated in order to create an evolving multi-stakeholder platform aimed at addressing the issues raised by information and communication technologies (ICTs)."[46] The World Summit on the Information Society (WSIS) aims to achieve a common vision, desire and commitment to build a people-centric, inclusive and development-oriented Information Society where everyone can create, access, utilize and share information. The establishment of the World Summit on the Information Society (WSIS) took place in two phases, in Geneva in 2003 and Tunis in 2005. The World Summit on the Information Society (WSIS) set twenty years ago the framework for worldwide digital cooperation, aiming to build people-centric, inclusive and development-oriented information and knowledge societies.[47]

The International Covenant on Civil and Political Rights (ICCPR)

[45]UNODC. documents.un.org/doc/undoc/gen/n13/449/47/pdf/n1344947.pdf?token=5vMIv4uFGwHDTxRjNF&fe=true.

[46]World Summit on the Information Society (WSIS). sustainabledevelopment.un.org/index.php?page=view&type=30022&nr=102&menu=3170.

[47] "World Summit on the Information Society (WSIS)." *Who.int*, 2024, www.who.int/news-room/events/detail/2024/05/27/default-calendar/world-summit-on-the-information-society-(wsis). Accessed 9 Aug. 2024.

The International Covenant on Civil and Political Rights (ICCPR) is an international agreement that obligates member States to uphold the civil and political rights of individuals, such as the right to life, freedom of religion and speech, freedom of assembly and most importantly in this context the right to privacy. It was adopted by United Nations General Assembly Resolution 2200A (XXI) on 16 December 1966. More specifically its 17th Article mandates the right to privacy and aims to protect people against unlawful attacks to their honor and reputation. Additionally, it requires that the State has to limit and safeguard the storage and use of personal information. It promises individuals the right to have access to their already stored personal data so that they can correct any inaccuracies.

PREVIOUS ATTEMPTS TO SOLVE THE ISSUE

California Consumer Privacy Act (CCPA)

"The California Consumer Privacy Act (CCPA) is a state statute intended to enhance privacy rights and consumer protection for residents of the state of California in the United States."[48] The Act gives consumers more control over the personal information that businesses collect about them and the CCPA regulations guide how to implement the law. The privacy rights for California consumers are mainly the right to be informed about the personal data a business collects about them and the way it is utilized and shared, the right to have the option to delete personal information, the right to opt-out of the sale or sharing of their personal information and the right to be free to exercise theirs CCPA rights without any discrimination and other difficulties.[49]The CCPA only applies to individuals who are residents of the State of California.

The Asia Pacific Economic Cooperation Privacy Framework

"The Asia Pacific Economic Cooperation (APEC) economies recognize the importance of protecting information privacy while maintaining information flows among economies in

[48] State of California Department of Justice. "California Consumer Privacy Act (CCPA)." *State of California - Department of Justice - Office of the Attorney General*, 13 Mar. 2024, oag.ca.gov/privacy/ccpa.

[49] "ibid"

the Asia Pacific region and among their trading partners." Therefore, the Asia Pacific Economic Cooperation (APEC) established a framework to "protect privacy within and beyond economies and to enable regional transfers of personal information benefits consumers, businesses, and governments." The Framework especially highlights how crucial it is to safeguard privacy, while at the same time ensuring that information flows free and ensuring to tackle issues that are extremely relevant to APEC economies. One of the main principles of the Framework is the limitation of the collection. According to the APEC Privacy Framework, only information and data that is relevant to the purpose of the collection should be collected, while any such information should be acquired by lawful and fair means. The framework also states that information should only be collected to fulfill the purposes of collection and other compatible or related purposes. [50]

POSSIBLE SOLUTIONS

Creation of a legal framework

It is a matter of great importance to draft and implement comprehensive data protection laws that cover every aspect of the issue, data privacy and protection that are based on universally accepted principles. Since the law differs in all countries and regions it is crucial that the new framework on Data Privacy and Protection could be implemented by all member States and all policies. The principles of the framework are to be accepted worldwide, and because of that, research and international cooperation of member states should be implemented, so that the framework meets every policy of every country. This will be easily achieved by basing the whole framework and its principles on already accepted ones from other legal and national documents that were also implemented to combat the issue of data privacy and protection, thus setting legal docs, like the Universal Declaration of Human Rights or the International Covenant on Civil and Political Rights

Creation of a UN body to ensure the compliance with the legal framework

It would be a really efficient and effective idea to promote the establishment of an UN body, that is to have the responsibility of overseeing compliance, investigating breaches and enforcing the law. That way it is to be sure that the laws established by the framework

[50] *APEC PRIVACY FRAMEWORK (2015)* _____ *CONTENTS.*

will be implemented and followed by every individual and country. This body is also going to have the capability to impose fines and other penalties on those who overlook the law and framework. It will also be responsible when data breaches are reported. That specific UN body is going to be consulted by a special authority, which will be responsible for having representatives and agents in every country around the world to ensure its compliance with it.

Collaboration of all member States aiming the creation of a mutual database

It is a matter of utmost importance to encourage the collaboration of all member States and the creation of mutual databases and data sharing to ensure that they create good strategies and practices. As a general rule, cross-border transfers are permitted when transferring data to a country with sufficient data protection laws. Organizations and countries should review their data flow maps to understand where cross-border transfers occur. “Once the assessment is complete, organizations should review if the jurisdictions are adequate as deemed by data protection laws.” If not, they should ensure sufficient due diligence is conducted as well as incorporate appropriate safeguards and contractual clauses into agreements.

BIBLIOGRAPHY

A Practical Guide: Establishing a Privacy and Data Protection Framework. 2021.

“AI and Data Privacy: Balancing Innovation with Security - SmartDev.” *SmartDev*, 23 Mar. 2024, www.smartdev.com/ai-and-data-privacy-balancing-innovation-with-security/. Accessed 9 Aug. 2024.

APEC PRIVACY FRAMEWORK (2015) _____ *CONTENTS*.

“California Consumer Privacy Act (CCPA).” *State of California - Department of Justice - Office of the Attorney General*, 15 Oct. 2018, oag.ca.gov/privacy/ccpa#:~:text=Are%20there%20any%20CCPA%20regulations. Accessed 9 Aug. 2024.

"History of Privacy Timeline / Safecomputing.umich.edu." *Safecomputing.umich.edu*, safecomputing.umich.edu/protect-privacy/history-of-privacy-timeline.

ICLG. "Gambling Singapore Chapter." *Gambling 2019 | Laws and Regulations | Singapore | ICLG*, 2024, iclg.com/practice-areas/gambling-laws-and-regulations/singapore.

"Japan Data Protection Law: Everything You Need to Know | Didomi." *Blog.didomi.io*, blog.didomi.io/japan-data-protection-law-appi-everything-you-need-to-know.

"Notifiable Data Breaches Bill - Australia." *Fortinet*, 2023, www.fortinet.com/solutions/industries/notifiabledatabreach#:~:text=The%20NDB%20came%20into%20effect. Accessed 9 Aug. 2024.

Pearlman, Shana. "What Is Data Processing? Definition and Stages - Talend Cloud Integration." *Talend Real-Time Open Source Data Integration Software*, 2018, www.talend.com/resources/what-is-data-processing/.

Ross, Jeremy. "Data Protection and Privacy: How to Protect User Data." *Cloudian*, cloudian.com/guides/data-protection/data-protection-and-privacy-7-ways-to-protect-user-data/amp/.

State of California Department of Justice. "California Consumer Privacy Act (CCPA)." *State of California - Department of Justice - Office of the Attorney General*, 13 Mar. 2024, oag.ca.gov/privacy/ccpa.

"The Right to Rectification | Data Protection Commission." *The Right to Rectification | Data Protection Commission*, www.dataprotection.ie/en/individuals/know-your-rights/right-rectification.

"U.S. Data Privacy Protection Laws: 2024 Guide." *Security*, www.techtarget.com/searchsecurity/tip/State-of-data-privacy-laws#:~:text=While%20the%20U.S.%20currently%20doesn.

UNCTAD. "Data Protection and Privacy Legislation Worldwide | UNCTAD." *Unctad.org*, 14 Dec. 2021, unctad.org/page/data-protection-and-privacy-legislation-worldwide.

Wolford, Ben. “What Is GDPR, the Eu’s New Data Protection Law?” *GDPR.eu*, 2020, gdpr.eu/what-is-gdpr/.

“World Summit on the Information Society (WSIS).” *Who.int*, 2024, www.who.int/news-room/events/detail/2024/05/27/default-calendar/world-summit-on-the-information-society-(wsis). Accessed 9 Aug. 2024.