CHSVMUN

UNITED NATIONS HUMAN RIGHTS COMMISSION

BACKGROUND GUIDE

PRIVACY LAW:

Privacy law refers to the laws that deal with the regulation, storing, and using of personally identifiable information, personal healthcare information, and financial information of individuals, which can be collected by governments, public or private organizations, or other individuals. It also applies in the commercial sector to things like trade secrets and the liability that directors, officers, and employees have when handing sensitive information.
Privacy laws are considered within the context of an individual's privacy rights or within reasonable expectation of privacy.

Classifications of Privacy Laws:

Privacy laws can be broadly classified into:

1) General privacy laws that have an overall bearing on the personal information of individuals and affect the policies that govern many different areas of information.
    a) Trespass
    b) Negligence
    c) Fiduciary Duty
    d) Contract
    e) Unfair and Deceptive Trade Practices

2) Specific privacy laws that are designed to regulate specific types of information. Some examples include:
    a) Communication privacy laws
    b) Financial privacy laws
    c) Health privacy laws
    d) Information privacy laws
    e) Online privacy laws
    f) Privacy in one's home

STATUS OF PRIVACY LAWS AROUND THE WORLD:

1) Asia-Pacific Economic Cooperation (APEC)

APEC created a voluntary Privacy Framework that was adopted by all 21 member economies in 2004 in an attempt to improve general information privacy and the cross-border transfer of information. The Framework consists of nine Privacy Principles that act as minimum standards for privacy protection: Preventing harm, Notice, Collection limitation, Use of personal information, Choice, Integrity of personal information, Security safeguards, Access and correction, and Accountability.

In 2011, APEC implemented the APEC Cross Border Privacy Rules System with the goal of balancing "the flow of information and data across borders ... essential to trust and confidence in the online marketplace." The four agreed-upon rules of the System are based upon the APEC Privacy Framework and include self-assessment, compliance review, recognition/acceptance, and dispute resolution and enforcement.

2) Council of Europe

Article 8 of the European Convention on Human Rights, which was drafted and adopted by the Council of Europe in 1950 and currently covers the whole European continent except for Belarus and Kosovo, protects the right to respect for private life: "Everyone has the right to respect for his private and family life, his home and his correspondence." Through the huge case-law of the European Court of Human Rights in Strasbourg, privacy has been defined and its protection has been established as a positive right of everyone.

The Council of Europe also adopted Convention for the protection of individuals with regard to automatic processing of personal data in 1981 and addressed privacy protection in regards to the Internet in 1998 when it published "Draft Guidelines for the protection of individuals with regard to the collection and processing of personal data on the information highway, which may be incorporated in or annexed to Code of Conduct." The Council developed these guidelines in conjunction with the European Commission, and they were adopted in 1999.

3) European Union (EU)

The 1995 Data Protection Directive (officially Directive 95/46/EC) recognized the authority of National data protection authorities and required that all Member States adhere to universal privacy protection standards. Member States must adopt strict privacy laws that are no more relaxed than the framework provided by the directive. Additionally, the Directive outlines that non-EU countries must adopt privacy legislation of equal restriction in

order to be allowed to exchange personal data with EU countries. Furthermore, companies in non-EU countries must also adopt privacy standards of at least equal restriction as provided in the Directive in order to do business with companies located in EU countries. Thus, the Directive has also influenced the development of privacy legislation in non-European countries. The proposed ePrivacy Regulation, which would replace the Privacy and Electronic Communications Directive 2002, also contributes to EU privacy regulations.

The General Data Protection Regulation has replaced the Data Protection Directive of 1995 when it came to effect on 25 May 2018. A notable contribution that has come from the General Data Protection Regulation is its recognition of a "right to be forgotten", which requires any group that collects data on individuals to delete the data related to an individual upon that individual's request. The Regulation was influenced by the aforementioned European Convention on Human Rights.

4) Organization for Economic Co-operation and Development (OECD)

In 1980, the OECD adopted the voluntary OECD Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data in response to growing concerns about information privacy and data protection in an increasingly technological and connected world. The OECD Guidelines helped establish an international standard for privacy legislation by defining the term "personal data" and outlining fair information practice principles (FIPPs) that other countries have adopted in their national privacy legislation.

In 2007, the OECD adopted the Recommendation on Cross-border Co-operation in the Enforcement of Laws Protecting Privacy. This framework is based on the OECD Guidelines and includes two cooperation-based model forms to encourage the enforcement of privacy laws among member states. The Recommendation is also notable for coining the term "Privacy Enforcement Authority."

5) United Nations (UN)

Article 17 of the International Covenant on Civil and Political Rights of the United Nations in 1966 also protects privacy: "No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honor and reputation. Everyone has the right to the protection of the law against such interference or attacks."

On December 18, 2013, the United Nations General Assembly adopted resolution 68/167 on the right to privacy in the digital age. The resolution makes reference to the Universal Declaration of Human Rights and reaffirms the fundamental and protected human right of privacy.

The Principles on Personal Data Protection and Privacy for the United Nations System were declared on 11 October 2018.

Right to Privacy with respect to Data Protection

It is important to distinguish between the concept of Data Protection Law from the Fundamental Human right to Privacy. Privacy is a right whilst data protection is the legislation which implements that right. The Right to Privacy as a European concept extends to one's personal or family activities which should not be scrutinized by Public authorities. One could look at it as Privacy being a protection from possible abuses of personal information or searches by the state, while Data Protection is the tool the law uses to make sure that an individual is protected from abuse of his personal information by another individual. Basically, one always has to keep in mind that Privacy protects one against the actions of the state while Data Protection will only work against any private individual. To clarify, a private individual can also include a company since Maltese law provides that a data controller can be either an individual or a group of individuals. To illustrate, Data protection law includes the right of the individual to be informed that he can refuse direct marketing from a company or other trader he has given his personal details to.

Another area that should be mentioned in this area is the concept of Freedom of Information, not to be confused with Freedom of Speech. This particular area mainly concerns information that is in possession of the government of a state. It is commonly referred to as 'the right to know' and basically empowers individuals to access information that is being kept by the state. The main issue is one of transparency. The laws laid down in the Freedom of Information Act, once they come into force will allow access to government information by any individual considered as eligible. The whole idea is to make sure that the government remains accountable to individuals in the way it carries out its functions. The laws will not however grant access to any and all documents as there are some areas like the Electoral Commission and the Office of the Attorney General which still will not be affected by this law. With regard to the concept of Data Protection, the fact remains that freedom of information will not in any way water it down as the information is still protected by the Data Commissioner and excludes disclosing any information protected by the Data Protection Act. This means that even though disclosure might be necessary, the information released can never be sensitive personal information since this remains protected under the Data Protection Act. Such information will always be kept safe by the government or even private individuals unless it falls under one of the exceptions in the Data protection Act. An example of these exceptions is when using the data is necessary to save the life of the individual.

Role of Governments in Data Protection

Different Countries have different policies towards Data collection and protection of citizens data.