



مجموعة جامعة
الجميع الذكية
للتعليم القابضة

MIDOCEAN
UNIVERSITY

Data Protection

by Samara Jasim

LAW614

Lecture 4

Data protection is a law that aims to keep your personal information safe. In today's world, it's important for us to have control over our data and be protected from misuse. To achieve this, data protection laws exist to regulate the actions of companies and governments.

Without these rules, these institutions tend to gather, analyze, store, and share our data without informing us. Therefore, data protection laws are necessary to prevent such actions and ensure our privacy.

Whenever you use a service, make an online purchase, sign up for emails, visit your doctor, pay your taxes, or enter any kind of agreement or request, you are required to provide some personal information. It's important to note that even without your awareness, companies and agencies are generating and collecting data about you, often from interactions you haven't intentionally made.

To establish trust in both the government and businesses, it is crucial to have robust data protection practices and effective laws in place. These measures help to limit surveillance and prevent the misuse of data by both state and corporate entities.

Since the 1960s, with the advancement of information technology, personal data has been stored in databases by businesses and government entities. These databases can be searched, edited, cross-referenced, and shared with other organizations around the world.

As the collection and processing of data became more widespread, people began to question what happened to their data once they shared it. They wanted to know who had access to their data, whether it was stored accurately, if it was being collected and shared without their knowledge, and if it could be used to discriminate or violate their fundamental rights.

National laws addressing data protection began to emerge in countries such as Sweden, Germany, and France. By January 2018, more than 100 countries had implemented data protection laws, with an additional 40 countries considering or working on legislation.

Regional legal frameworks were also established over time. In 1980, the Organisation for Economic Cooperation and Development (OECD) developed guidelines that included privacy principles. Shortly after, the Council of Europe introduced the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, which was updated in 2018.

Due to the vast amount of data being generated and the rapid advancement of technology, including profiling, tracking, and artificial intelligence, some existing data protection laws have become outdated and inadequate in addressing current data processing practices. These frameworks fail to account for the new possibilities and challenges presented by evolving technologies integrated into governance systems and business models.

Lecture
04

OVERVIEW OF DIGITAL LAW AND ITS RELEVANCE IN SAFEGUARDING DATA

It has been reported that 90% of the world's data has been created in the past two years alone, and every two days we generate as much data as we did from the beginning of time until 2013. Many data protection laws were drafted before the existence and widespread use of platforms like Google, Facebook, and smartphones.

While a data protection framework may have its limitations, we are actively identifying and addressing them by exploring additional regulations to ensure necessary safeguards. Nevertheless, having a strong data protection framework is crucial as it serves as a fundamental starting point to implement robust regulatory and legal measures for protecting personal data.

A robust data protection framework empowers individuals, curbs harmful data practices, and restricts data exploitation. It is essential to establish comprehensive governance frameworks at both national and global levels, ensuring individuals have strong rights over their data, imposing strict obligations on those handling personal data in public and private sectors, and enabling enforcement powers against those who violate these obligations and protections.

Privacy is an internationally recognized human right. Article 12 of the Universal Declaration of Human Rights (UDHR) proclaims that:

[n]o one shall be subjected to arbitrary interference with his privacy, family, home or correspondence Everyone has the right to the protection of the law against such interference or attacks.

The UDHR has formed the basis for the major international human rights treaties, which similarly enshrine the right to privacy, including the International Covenant on Civil and Political Rights (ICCPR) in Article 17.

As early as 1988, the UN Human Rights Committee, the treaty body charged with monitoring implementation of the ICCPR, recognised the need for data protection laws to safeguard the fundamental right to privacy recognised by Article 17 of the ICCPR:

The gathering and holding of personal information on computers, data banks, and other devices, whether by public authorities or private individuals or bodies, must be regulated by law. ... [E]very individual should have the right to ascertain in an intelligible form, whether, and if so, what personal data is stored in automatic data files, and for what purposes.

Every individual should also be able to ascertain which public authorities or private individuals or bodies control or may control their files. If such files ... have been collected or processed contrary to the provisions of the law, every individual should have the right to request rectification or elimination.

In December 2016, the UN General Assembly passed a resolution (by consensus) on the Right to Privacy in the Digital Age, GA Res. 71/199, which reaffirmed previous General Assembly resolutions on the subject, emphasizing that:

States must respect international human rights obligations regarding the right to privacy [...] when they require disclosure of personal data from third parties, including private companies.

Privacy and data protection go hand in hand. As individuals, whether we are citizens, customers, or consumers, we should have the ability to protect our privacy and our data from misuse. It is crucial that those who handle data understand their responsibilities clearly, taking steps to safeguard personal information, minimize intrusions on privacy, and be held accountable if they fail to fulfill their obligations. This is especially important when it comes to our own personal data.



Personal data refers to information that is processed through automated means or stored in an organized filing system and is related to an individual. Data protection is all about preserving our fundamental right to privacy by regulating how personal data is handled. It grants individuals certain rights over their own data and establishes a framework of accountability and clear obligations for those who control or process the data.

Data protection should ensure the following:

- The purposes for which the data and information is to be used should be specified (at the latest) at the time of collection, and should only be used for those agreed purposes. Personal data can only be disclosed, used, or retained for the original purposes (i.e. the purpose at the time of collection), except with the consent of the individual or under law: accordingly, it must be deleted when no longer necessary for that purpose .

- Personal data, as generated and processed, should be adequate, relevant, and limited to necessity of the purposes for which it is to be used.
- The data should be accurate and complete, and measures should be taken to ensure it is up to date.
- Reasonable security safeguards should be used to protect personal data from loss, unauthorized access, destruction, use, modification, or disclosure.

- There should be no secret processors of data, sources, or processing. Individuals must be made aware of the collection and processing of their data, as well as the purpose of its use, who is controlling it, and who is processing it.
- Individuals have a range of rights which enables them to control their personal data and any processing.

Lecture
04

LEGAL FRAMEWORK FOR DATA PROTECTION

- Those that use personal data must be accountable for and demonstrate compliance with the above principles, and facilitate and fulfil the exercise of these rights, abiding by applicable laws that enshrine those principles.
- There should be limits on the collection of personal data, and it should be obtained by lawful and fair means, as well as being done in a transparent manner.

The Organization for Economic Co-operation and Development (OECD) Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, updated in 2013

1. Collection Limitation Principle
2. Data Quality Principle
3. Purpose Specification Principle

4. Use Limitation Principle
5. Security Safeguards Principle
6. Openness Principle
7. Individual Participation Principle
8. Accountability Principle

Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, No. 108, as amended by 2018

Article 5 (4): Personal data undergoing processing shall be:

- a. processed fairly and in a transparent manner
- b. collected for explicit, specified and legitimate purposes and not processed in a way incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes is, subject to appropriate safeguards, compatible with those purposes

- c. adequate, relevant and not excessive in relation to the purposes for which they are processed
- d. accurate and, where necessary, kept up to date
- e. preserved in a form which permits identification of data subjects for no longer than is necessary for the purposes for which those data are processed

General Directive Personal Data, Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016. Principles presented in Article 5:

1. Lawfulness, fairness and Transparency
2. Purpose limitation
3. Data minimisation
4. Accuracy
5. Storage limitation
6. Integrity and confidentiality
7. Accountability

Any activity that collects, stores, or processes personal data raises certain risks, including, but not limited to:

- Security breaches: Physical or cyberattacks on data in transit or at rest.
- Unauthorized disclosure: Inappropriate transfer of data between government agencies, foreign governments, private companies, or other third parties.

- Function creep: The use (and even sharing) of data for purposes beyond those for which consent was given.
- Identity theft: Identity theft in the digital world can lead to consequences that are at least as serious as those in the “real”, physical world, and, given the global, decentralized nature of the internet, damages that are often more difficult to repair. In a digitized world, impersonation can be undertaken by just about anyone.

- Surveillance risks: The ability to correlate identifying information across databases (e.g., via facial recognition) increases surveillance risks, particularly where biometrics are involved.
- Discrimination or persecution: Identity attributes might be used to discriminate or persecute particular people or groups. Relatedly, reputational attacks (professional and personal) can be launched with significantly greater ease—and to significantly greater effect.

- Exposure of sensitive personal information: Disclosing sensitive personal information (e.g., biometrics, religion, ethnicity, gender, medical histories) for unauthorized purposes.
- Unjust treatment: Incomplete or inaccurate data can lead to mistakes or unjust treatment.

The future evolution of digital technologies and how they are used, particularly for automation and artificial intelligence, will place even greater importance on personal data. How do we prepare for such developments?

In Indonesia, the government has recently enacted a much-anticipated data protection law called Law No. 27 of 2022 on Personal Data Protection (PDP Law). This law applies to personal data protection in all sectors and brings significant changes compared to the previous regulations. The PDP Law largely incorporates principles and provisions from the European Union's GDPR, which means that businesses in Indonesia will need to make substantial adjustments to their current practices of processing personal data.



In New Zealand, the government is reviewing the notification rules regarding the collection of personal information under the Privacy Act 2020. The proposed changes aim to ensure that individuals are notified when an agency collects their personal information indirectly through a third party. Currently, the Privacy Act only mandates notification when the agency collects personal information directly from the individual themselves.

In Greece, digital transformation and the regulation of new technologies have been key priorities on the regulatory agenda. Starting from the second half of 2022, new rules have been introduced, and their enforcement is set to begin in 2023. In the coming months, additional supplementary legislation is expected to provide further clarification on certain areas that may currently lack clarity. These measures aim to assist organizations in navigating the ever-changing legal landscape as technology continues to evolve.

In the last quarter of 2021, the UAE implemented Federal Decree Law 45 of 2021, which focuses on the protection of personal data. This law establishes a comprehensive framework to safeguard the confidentiality of information and protect individuals' privacy within the UAE. Furthermore, the law highlights the forthcoming issuance of an 'implementing regulation,' which will provide additional details on how the law will be applied and enforced.

In conclusion, data protection and digital law play vital roles in safeguarding individuals' privacy and personal information in our modern digital age. Across different countries, we have witnessed the development of data protection laws and regulations aimed at empowering individuals and holding organizations accountable for responsible data handling.





مجموعة جامعة
الجميع الذكية
للتعليم القابضة

MIDOCEAN
UNIVERSITY



Thank You