**Data Privacy Legislations**

Table of Contents

[EU General Data Protection Regulation 2](#_Toc63379716)

[Definitions 2](#_Toc63379717)

[Requirements 3](#_Toc63379718)

[Practical Implications 5](#_Toc63379719)

[Conclusion 6](#_Toc63379720)

[Personal Data Protection Act 7](#_Toc63379721)

[Objectives 7](#_Toc63379722)

[Main Concepts 8](#_Toc63379723)

[Applicability of the PDPA 9](#_Toc63379724)

[Digital Security Act of Bangladesh 10](#_Toc63379725)

## EU General Data Protection Regulation

The European Union (EU) General Data Protection Regulation (GDPR) is a set of rules drafted by the EU that all EU member states must follow. It sets out rules for data protection and privacy of individuals within the EU. Any companies operating within the EU must follow these rules when handling any personal data of its users so as to ensure that the data is being handled with honesty. The entire set of rules is extremely large and can be found in the resources section. A brief overview will be given here.

The purpose of the GDPR is to ensure that there is a uniform and harmonized level of protection for personal data throughout the EU. This ensures that the data can move freely anywhere inside the EU. If a uniform set of rules had not been made, the differences in regulations would have prevented this free movement.

### Definitions

Under article 4 of the GDPR, personal data is defined as any information that, either directly or indirectly, can identify a living person. Names, phone numbers, and addresses are obvious examples, but interests, history of purchases, health data and online behaviour are also considered personal data under the GDPR since they could be indirectly used to identify the person.

The processing of personal data refers to the complete data lifecycle, collection, structuring, organization, usage, storage, sharing, disclosure, erasure and destruction of data.

The organization that uses the data is called the data controller and the people from whom the data is collected are called the data subjects. Any data controller within the EU that processes personal data must ensure that they fulfil the requirements set by the GDPR.

### Requirements

The requirements of the GDPR include:

* The same rules must be followed throughout the EU.
* Personal data must be used with integrity, that is, there needs to be a well thought out process of how the data will be handled once it is collect before collection can begin.
* Personal data must be used in a legal manner.
  + Consent to use the data must be obtained from the customers. This can be done with a contract that mentions how the data will be used and any conditions related to the contract.
  + Personal data can only be collected if it serves some purpose, i.e. if the collection has some purpose to the organization or the customers or even the general public. There are ethical committees that are required to oversee the reasoning behind personal data collection, and their approval is required before personal data can be collected.
* Use of personal data must be respectful to the individual’s rights.
  + Individuals have the right to know exactly how their data is being processed. The way personal data is processed must be properly and rigorously documented.
  + They have the right to access all the data being collected about them.
  + They have the right to make objections and take legal action against the organization.
  + Personal data can only be stored for as long as necessary. Once it is not being used anymore, it must be erased.
  + The process of handling personal data must not be risky.
* Personal data breaches or loss of sensitive data must be reported to the data protection authority of the country within 72 hours.
* Businesses are responsible for their suppliers. They will face the consequences of any breaches of the rules by organizations processing personal data on their behalf. The business is obligated to periodically check for and report any breaches of the GDPR rules by its suppliers.

Organizations that fail to follow any of the guidelines may face fines up to of their global sales for the last months or , whichever is higher.

### Practical Implications

Practically, these rules lead to some obligations for companies processing personal data. These include:

* Informing citizens and customers about their activities in a transparent manner.
* Assigning a Data Protection Office (DPO) who works as the main operator and expert on the organization’s privacy measures. This person is not an employee of the company, but is assigned by the data protection authority. If they find any breaches of the data protection laws, they will report it to that authority.
* Managing the citizens’ and individuals’ rights efficiently.
* Regulating responsibilities between buyers (the organizations actually using the data, also called data controllers) and suppliers (the organizations processing the data, also called the data processors).
* Keeping a data inventory to document what data is being collected and how it is being used.
* Setting up a process to manage personal data breaches within the 72-hour time limit.
* Analysing possible risks and impacts on citizens’ rights for the intended use of personal data. This review process is called the Data Processing Impact Assessment.

### Conclusion

Personal data is valuable. It makes it possible to develop business models, gain an understanding of customers, conduct effective marketing campaigns and develop products and services. However, there is a need to use the data responsibly, based on some common rules. In the age of artificial intelligence, not even the people who create the systems that process people’s personal data fully understand what exactly is going on. This not only leads to a reflection of unacknowledged human biases in the system, but also new and unpredictable biases and errors with sometimes deadly consequences. Further, data breaches are all too common, even in large companies, and they compromise vital personal information of hundreds of millions of people, like social security numbers, addresses, credit card numbers, etc.

The GDPR not only ensures that the individual’s data always belongs to the individual and that they know exactly what is being done with their data, it also threatens substantial fines on anyone not following the rules. Privacy and data protection are considered vital components of a substantial democracy in the EU. The GDPR is designed to safeguard these components.

## Personal Data Protection Act

The Personal Data Protection Act (PDPA) is a set of data protection laws establish by the Singaporean government that comprises of various rules governing the collection, use, disclosure and care of personal data. It recognizes both the rights of individuals to protect their personal data, including their rights to access and correction, and the needs of organizations to collect, use and disclose personal data for legitimate and reasonable purposes.

### Objectives

In the current world, a very large amount of data is collected, used and even transferred to third party organizations for a variety of reasons. This trend will most likely keep growing as the processing and analysis of this data becomes easier with more sophisticated technology.

Because of this, a data protection act is necessary to govern the collection, use and disclosure of personal data, so as to address concerns about the handling of the data and maintain individuals’ trust in the organizations that handle the data.

By regulating the flow of personal data among organizations, the PDPA aims to strengthen and entrench Singapore’s competitiveness and position as a trusted world-class hub for business.

### Main Concepts

According to the PDPA, personal data refers to any information, true or false, about individuals who can be identified either directly by that data or by a combination of the data and other information to which the organization has or is likely to have access. This data could be both electronic or non-electronic.

The PDPA does not apply to situations where individuals are willingly sharing information with each other in strictly personal environments, such as between friends and family. Rather, it is meant for organizations that are collecting personal data from their users. The PDPA is designed to work alongside existing laws for the specific industry in which the organization acts. It provides a baseline standard for the protection of personal data across the economy.

The main concepts behind the PDPA are:

* Consent - Organizations may collect, use and disclose personal data only if the individual is aware of it and they have given their consent. This requirement can only be waived in some specific exceptional cases. An example of a specific exceptional case is the one stated before, where personal information is being shared in a strictly personal environment.
* Purpose - Organizations are also required to inform individuals about the purpose for the collection, use or disclosure of the data they are collecting.
* Reasonableness - Finally, the purposes for the collection, use or disclosure have to be appropriate from the perspective of a reasonable person in the given circumstances. This part is somewhat subjective. As such, it is possible that some people will find the purposes provided by a particular organization are not reasonable. In that circumstance, they are able to appeal the reasonableness of it. Such appeals are handled by the Data Protection Appeal Panel.

### Applicability of the PDPA

The PDPA does not generally apply to:

1. Individuals acting in a personal or domestic environment. This refers to the situation explained earlier, where people share personal information in personal environments.
2. Any information shared by employees with the business in which they are employed in the course of their work.
3. Any public agencies or organizations working on behalf of public agencies that are acting for the betterment of the general public. However, such agencies or organizations do have to disclose their purposes.
4. Professional information regarding an individual such as their name, post in an organization, official contact information etc.

## Digital Security Act of Bangladesh

The Digital Security Act of Bangladesh is not designed to protect the personal data of individuals, but rather to protect VIPs from defamation and security threats, prevent cyber-crime and prevent the spread of false information. As such, there is no information regarding personal data protection.

However, there is still one section (Section 26) that can be somewhat related to the protection of personal data. It declares that if any person that does not have the legal authority to do so collects, sells, takes possession of, supplies or uses any person’s identity information, they will be charged.

A shortcoming of this section is that the specific information that is considered identity information is limited to things like a person’s name, address, NID, etc. i.e., static data. It does not cover any of the dynamic data that we generate every day that is indirectly identity information.