GROVE SCHOOL
OF ENGINEERING

CSE H0240: Law and Policy Issues in Cybersecurity

Position Paper On
International Privacy: General Data Protection Regulation(GDPR)

Created By:

MD ABDUL KADIR

Submitted To:

Professor Benjamin Dynkin & Professor Barry Dynkin

CSE H0240 Course Instructor

Department of Cybersecurity (MS Program)

Grove School of Engineering

The City College of New York

Academic Session- Spring 2023

The enforcement of the GDPR on natural persons' protection regarding personal data treatment and movement, which repeals the Directive 95/46/CE of October 24 1995, poses innumerable challenges to both public and private entities as well as to all the agents whose activities involve the treatment of personal data.

Although the full application of the new GDPR has been set for May 25 2018, date from which the directive 95/46/CE will be effectively repealed, its enforcement on May 25 2016 dictated the need for an adaptation to all the aspects changed or introduced by the regulation. Such adaptation of the present systems and models as well as of best practices regarding personal data treatment and protection by companies is now an imperative stemming from the regulation in order to safeguard its full applicability from May 25 2018.

However, before focusing directly on the new regulation, it is important to clarify exactly how the document defines 'personal data' since its protection is the focus of the act.

The GDPR defines personal data in a broad sense so as to include any information related to an individual which can lead to their identification, either directly, indirectly or by reference to an identifier. Identifiers include

- Names.
- Online identifiers such as social media accounts.
- Identification numbers (e.g., passport numbers).
- Data regarding location (e.g., physical addresses).
- Any data that can be linked to the physical, physiological, genetic, mental, economic, cultural or social identity of a person.

Companies collecting, transferring and processing data should be aware that personal data is contained in any email and also consider that third parties mentioned in emails also count as personal data and, as such, would be subject to the requirements of the GDPR.

The GDPR requirements apply to each member state of the European Union, aiming to create more consistent protection of consumer and personal data across EU nations. The GDPR mandates a baseline set of standards for companies that handle EU citizens' data to better safeguard the processing and movement of citizens' personal data.

The main innovations of the General Data Protection Regulation are :

- New rights for citizens: the right to be forgotten and the right to a user's data portability from one electronic system to another.
- The creation of the post of Data Protection Officer (DPO).
- Obligation to carry out Risk Analyses and Impact Assessments to determine compliance with the regulation.
- Obligation of the Data Controller and Data Processor to document the processing operations.

- New notifications to the Supervisory Authority: security breaches and prior authorisation for certain kinds of processing.
- New obligations to inform the data subject by means of a system of icons that are harmonized across all the countries of the EU.
- An increase in the size of sanctions.
- Application of the concept 'One-stop-shop' so that data subjects can carry out procedures even though this affects authorities in other member states.
- Establishment of obligations for new special categories of data.
- New principles in the obligations over data: transparency and minimisation of data.

Among these points representing the main innovations imposed by the new legislation, I am going to highlight point nine, in which the regulation recognises that health data integrates the 'special categories of data' considering that such data is sensitive and therefore subjected to special limitations regarding access and treatment by third parties.

Health data may reveal information on a citizen's health condition as well as genetic data such as personal data regarding hereditary or acquired genetic characteristics which may disclose unique information on the physiology or health condition of that person. The protection of such health data imposes particular duties and obligations to the companies operating in this sector.

As far as the security of personal data is concerned, the GDPR mandates the application of appropriate technical and organizational measures to ensure an adequate security level, among which:

- The pseudonymisation and encryption of personal data;
- The capacity to ensure the permanent confidentiality, integrity, availability and resilience of data treatment systems and services;
- The capacity to re-establish prompt availability and access to personal data in the event of a physical or technical hazard.

All organizations, including small to medium-sized companies and large enterprises, must be aware of all the GDPR requirements and be prepared to comply by May 2018. By beginning to implement data protection policies and solutions now, companies will be in a much better position to achieve GDPR compliance when it takes effect.