A COMPREHENSIVE ANALYSIS OF GDPR AND ITS RELEVANCE WITH ISO 27701 STANDARD

Aakarshna CG, SASTRA Deemed University, Thanjavur, Tamil Nadu, India

ABSTRACT:

The gold rate in India today is about 5490 per gram. Interestingly, what is even more valuable today, perhaps something which cannot be even quantified in money, is Data. Data includes any information or fact, including numbers which have wide applications; right from scientific inventions to making decisions in a corporate field to using it as evidence in the court. Right to privacy has been understood as a fundamental right under Article 21 since the infamous Puttaswamy judgment. With technology becoming our oxygen to breathe, data privacy inevitably becomes the need of the hour. Data privacy generally means the ability of a person to determine for themselves when, how, and to what extent personal information about them is shared with or communicated to others. This personal information can be one's name, location, contact information, or online or real-world behavior. This paper aims to make a comprehensive analysis of the international law- the GDPR and its relevance with ISO 27701/2022 Standard

Keywords: Data privacy, GDPR, Data Protection, ISO 27701

INTRODUCTION

International Data Privacy and Protection Laws and Data Standards:

The rights to privacy plays a foundational role in a democratic set up of the society.

Data privacy laws specify how data should be collected, stored, and shared with third parties.[1] Data standards are documented agreements on representation, format, definition, structuring, tagging, transmission, manipulation, use, and management of data.

International Declarations on Data Privacy

Article 12 of the Universal Declaration of Human Rights provides that "No one shall be subjected to arbitrary interference with his privacy, family, 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"[2]. Article 17 of the International Covenant on Civil and Political Rights provides "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."[3]

They further state that "everyone has the right to the protection of the law against such interference or attacks." While the right to privacy under international human rights law is not absolute, any instance of interference must be provided by law and subject to a careful and critical assessment of its necessity and proportionality. Moreover, Since 2013, the United Nations General Assembly and the Human Rights Council have adopted numerous resolutions on the right to privacy in the digital age.[4] GDPR: The European Union's General Data Protection Regulation (GDPR) is the most comprehensive data privacy law in effect. For the purpose of the research paper, it is important to discuss the intricacies of GDPR in detail.

---

[1] *What is data privacy? definition and compliance guide* (no date) *Talend*. Available at: https://www.talend.com/resources/data-privacy/#:~:text=Data%20privacy%20laws%20specify%20how,data%20privacy%20law%20in%20effect (Accessed: 29 November 2023).

[2] Article 12, UDHR

[3] Article 17, ICCPR

[4] *OHCHR and privacy in the Digital age | OHCHR - UN human rights office*. Available at: https://www.ohchr.org/en/privacy-in-the-digital-age (Accessed: 29 November 2023).

GENERAL DATA PROTECTION REGULATION

The General Data Protection Regulation is the finest Information Privacy law drafted yet, by the European Union that was passed in the year 2016 by the European Parliament.It came into effect in the year 2018. With the development in technology and invent of the Internet, the European union formulated the European Data Protection Directive in 1995, deriving its objective from the European Convention on Human Rights, which states, "Everyone has the right to respect for his private and family life, his home and his correspondence"[5]. However, later with the emergence of Internet Banking, Various Social media apps such as Facebook, Instagram, whatsapp, etc and with increasing use of Email, the Data Protection Authority contemplated stronger laws. The issue aggravated or in an optimistic perspective, paved the way for a comprehensive Data protection regulation, when a case was filed by a Google user for scanning her Emails in 2011. The purpose of the General Data Protection Regulation is to bring about protection of the privacy of Residents of EU and to update the rules for data protection with the update and increasing use of technology and digitalized society[6]

Scope of GDPR:

GDPR aims to create a uniform standardized norm for personal data protection within the EU. GDPR applies to all the organizations that either automated or manually process[7] the Personal data of the EU Residents. This will include both organizations situated inside the EU as well as organizations outside the EU which process the personal information of the residents of the EU.

GDPR applies to individuals or a group of individuals like companies, organizations, associations, some authorities and in some cases, private individuals.

[5] European Convention on Human Rights

[6]Svobodová, K. (2023) *What is GDPR? the scope, purpose, fines and how to comply*, *Safetica*. Available at: https://www.safetica.com/blog/what-is-gdpr#:~:text=The%20Scope%20of%20GDPR,is%20based%20outside%20the%20EU. (Accessed: 29 November 2023)

[7] *Integritetsskyddsmyndigheten: IMY* (no date) *IMY (to startpage)*. Available at: https://www.imy.se/en/organisations/data-protection/this-applies-accordning-to-gdpr/the-purposes-and-scope-of-gdpr/ (Accessed: 29 November 2023).

Thus, there are three category of people who are governed by GDPR[8],

Data subject- Owner of personal data.

Data controller- the person or entity choosing what personal information to gather and how to use it.

Data processors- organizations that process personal data for the controller.

All member states of the European Union as well as those that are part of the European Economic Area, including Iceland, Lichtenstein, Norway, and the United Kingdom, are subject to GDPR. Thus essentially, GDPR applies to anyone processing the personal data of European Residents and there are two scenarios in which a non-EU organization might have to comply with the GDPR: firstly, for offering goods and services and secondly, for monitoring the behavior of the EU residents. However there are two exceptions to the same, the regulation need be followed when there is "purely personal or household activity" and secondly when an organization has less than 250 employees. Small and Medium Enterprises are not totally exempt form the but they have no obligation of record-keeping in most cases.

GDPR manages to define a number of terms relating to data and information with an aim to make the regulation a comprehensive one, some of the major and very important definitions among others include definition of Personal data, Data processing , Data subject Data controller Data processor etc.

What does the GDPR protect?

GDPR 'personal data' as information relating to "an identified or identifiable natural person" -- referred to as a "data subject." this includes Name, Location data, Any information that is specific to "the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person, Biometric data that is acquired through some form of technical process, such as facial

[8]Castagna, R. and Lavery, T. (2021) *What is GDPR? an overview of GDPR compliance and conditions*, *WhatIs.com*. Available at: https://www.techtarget.com/whatis/definition/General-Data-Protection-Regulation-GDPR#:~:text=Under%20GDPR%2C%20companies%20can't,steps%20to%20enter%20a%20contract. (Accessed: 29 November 2023).

imaging or fingerprinting, Information relating to a person's health or healthcare, Racial or ethnic information of an individual, Political opinions or religious beliefs, Union membership.

KEY ELEMENTS OF GDPR

General Principles Under GDPR:

Article 5 (1-2) of the GDPR Provides Principles relating to processing of personal data: Processing of personal data should be done following these principles to avoid penalties.

1. Personal data shall be:

    a. *processed lawfully, fairly and in a transparent manner in relation to the data subject ('lawfulness, fairness and transparency');*

    b. *collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall, in accordance with* ***Article 89****(1), not be considered to be incompatible with the initial purposes ('purpose limitation');*

    c. *adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation');*

    d. *accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay ('accuracy');*

    e. *kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with* ***Article 89(****1) subject to*

implementation of the appropriate technical and organisational measures required by this Regulation in order to safeguard the rights and freedoms of the data subject ('storage limitation');

f. *processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures ('integrity and confidentiality').*

2. *The controller shall be responsible for, and be able to demonstrate compliance with, paragraph 1 ('accountability')*[9].

Lawfulness of Processing[10] Data:

Article 6 of the Regulation provides for certain conditions for processing data. Usage of data will be deemed to be legal only if those conditions are fulfilled and thus when no such conditions aree fulfilled, data cannot be shared/ processed. They are as follows.

Article 6-

1) *"Processing shall be lawful only if and to the extent that at least one of the following applies:*

a) *the data subject has given consent to the processing of his or her personal data for one or more specific purposes;*

b) *processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract;*

c) *processing is necessary for compliance with a legal obligation to which the controller is*

[9] Article 5, GDPR,
[10] Article 6, GDPR

subject;

d) *processing is necessary in order to protect the vital interests of the data subject or of another natural person;*

e) *processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;*

f) *processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.*

Point (f) of the first subparagraph shall not apply to processing carried out by public authorities in the performance of their tasks.

The Basis for the processing referred to in point (c) and (e) of paragraph 1 shall be laid down by:

a) Union law; or

b) Member State law to which the controller is subject……"

Consent under GDP:

For legal processing of Data, there should be a very clear and unambiguous consent[11].Article 7 of the GDPR, states the Conditions for consent. It provides that :

1. *Where processing is based on consent, the controller shall be able to demonstrate that the data subject has consented to processing of his or her personal data.*

2. *If the data subject's consent is given in the context of a written declaration which also*

[11] *GDPR – Key Provisions* (2018) *GDPR – Key Provisions | Dixon Wilson*. Available at: https://www.dixonwilson.com/technical-updates/gdpr-key-provisions (Accessed: 29 November 2023).

concerns other matters, the request for consent shall be presented in a manner which is clearly distinguishable from the other matters, in an intelligible and easily accessible form, using clear and plain language. Any part of such a declaration which constitutes an infringement of this Regulation shall not be binding.

3. *The data subject shall have the right to withdraw his or her consent at any time. The withdrawal of consent shall not affect the lawfulness of processing based on consent before its withdrawal. Prior to giving consent, the data subject shall be informed thereof. It shall be as easy to withdraw as to give consent.*

4. *When assessing whether consent is freely given, utmost account shall be taken of whether, inter alia, the performance of a contract, including the provision of a service, is conditional on consent to the processing of personal data that is not necessary for the performance of that contract.*[12]

Rights of Individuals:

Chapter 6 of the GDPR mentions the rights of individuals who are subject to the regulation[13].

- The right of access-
- The right to rectification,
- The right to erasure,
- The right to restrict processing,
- The right to data portability,
- The right to object

[12] Article 7, GDPR

[13] *Rights of the individual* (no date) *European Data Protection Supervisor*. Available at: https://edps.europa.eu/data-protection/our-work/subjects/rights-individual_en#:~:text=The%20GDPR%20has%20a%20chapter,decision%20based%20solely%20on%20automated (Accessed: 29 November 2023).

- The right not to be subject to a decision based solely on automated processing

The right to be forgotten/ the right to erase is the right of the subjects to get their information erased on the request of the same. A new right introduced by the GDPR is "data portability." The right to have data transferred in a machine-readable format to a third-party service provider is now granted to data subjects. This right, however, only applies when personal information is given and processed with consent or when it's required to carry out a contract.

Privacy Impact Assessment under GDPR:

The privacy impact assessment under GDPR is the duty of the controller to conduct an impact assessment for the data that is proposed to be processed. The same is introduced under Article 35 of the GDPR[14]

Article 35(1) *Where a type of processing in particular using new technologies, and taking into account the nature, scope, context and purposes of the processing, is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall, prior to the processing, carry out an assessment of the impact of the envisaged processing operations on the protection of personal data.*

The Controller can opt for advice from the Data protection office while conducting the same. The assessment is conducted especially for the 'high- risk' projects that involves processing a huge amount of personal data with high risk to rights of privacy and freedom The supervisory authority may also establish and make public a list of the kind of processing operations for which no data protection impact assessment is required and supervisory authority shall communicate those lists to the board.

Essentials of the Privacy Impact Assessment Article 35(7)

a. *A systematic description of the envisaged processing operations and the purposes of the*

[14] *Privacy impact assessment* (2021) *General Data Protection Regulation (GDPR)*. Available at: https://gdpr-info.eu/issues/privacy-impact-assessment/ (Accessed: 29 November 2023).

processing, including, where applicable, the legitimate interest pursued by the controller;

b. *An assessment of the necessity and proportionality of the processing operations in relation to the purposes;*

c. *an assessment of the risks to the rights and freedoms of data subjects referred to in paragraph 1; and*

d. *the measures envisaged to address the risks, including safeguards, security measures and mechanisms to ensure the protection of personal data and to demonstrate compliance with this Regulation taking into account the rights and legitimate interests of data subjects and other persons concerned.*[15]

Privacy Impact Assessment shall be conducted in for example, in cases where there is usage of new technologies, the organization tracks object's location or behavior, If there is systematic monitoring of a publicly accessible place on a large scale If you're processing children's data, If the data you're processing could result in physical or legal harm to the data subjects if it is leaked or if it related to racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation"[16].

Data Protection Officer:

The main responsibility of the data protection officer (DPO) is to make sure that the organization complies with applicable data protection regulations when processing the personal data of its employees, clients, suppliers, or any other individuals (also known as data subjects)[17].

Article 37, 38 and 39 Designation of the data protection officer, Position of the data protection

[15] Article 35(7) GDPR
[16] *Data Protection Impact Assessment (DPIA)* (2023) *GDPR.eu*. Available at: https://gdpr.eu/data-protection-impact-assessment-template/ (Accessed: 29 November 2023).
[17] *Data Protection officer (DPO)* (2023) *European Data Protection Supervisor*. Available at: https://edps.europa.eu/data-protection/data-protection/reference-library/data-protection-officer-dpo_en (Accessed: 29 November 2023).

officer, *and* Tasks of the data protection officer respectively.

Designation of the data protection officer:

The DPO is an integral part of the organization, with an important objective of ensuring compliance with GDPR . Although it isn't stated clearly anywhere, the Article 29 Working Party on Data Protection Officers (WP 243) Guidelines state that the level of specialist knowledge expected of the DPO should be proportionate with the kind, complexity, and volume of data processed within the unit[18]. It is to be noted that there should not be any conflict of interest between the duties of the individual as a DPO and other duties if she/he has a different role in the organization if any. To avoid such conflicts, it is recommended that a DPO does hold positions of a controller of processing activities (Example HR Manager) ,the DPO should not be an employee.

The term of appointment and unambiguous conditions for dismissal must be given by the entity for a DPO post. The appointment is usually for a period between three and five years, may be reappointed and can be dismissed only with the consent of the EDPS (In Europe).

Position of the data protection officer:

Data subjects may contact the data protection officer with regard to all issues related to processing of their personal data and to the exercise of their rights under this Regulation. The data protection officer is bound by secrecy or confidentiality concerning the performance of his or her tasks, in accordance with concerned law.

He shall directly report to the highest management level of the controller or the processor.The controller and the processor shall ensure that the data protection officer is involved, properly and in a timely manner, in all issues which relate to the protection of personal data.They shall support the data protection officer in performing the tasks as provided in Article 39 by providing necessary resources including access to personal data and processing operations.The data protection officer may carry out other responsibilities. Any such jobs and responsibilities must be

[18] *Should the DPO be appointed based on the same qualifications as the administrator of is?* (no date) *UODO*. Available at: https://uodo.gov.pl/en/679/1545 (Accessed: 29 November 2023).

avoided by the controller or processor to avoid a conflict of interest.

Tasks of Data Protection Officer:

The primary role of the DPO is to ensure that the data protection rules are followed by the institution. These are the tasks listed by Article 39 of GDPR:

It is his duty to make sure that controllers and data subjects are aware about their data protection rights, obligations and responsibilities. His/ she has the duty to advise and recommend to the institution about the interpretation or application of the data protection rules.

Create a document of processing operations within the institution and notify the EDPS risks,if encountered and thus ensure data protection compliance within the institution by improving accountability of the organization.

He/she should be able to handle queries or complaints on request by the institution, the controller, other person(s), or on her own initiative and on the other hand Cooperate with the EDPS to respond to those queries and investigation.

Fines in GDPR:

Article 83- General conditions for imposing administrative fines of the GDPR provides for fines for non compliance that provides for determination of fines based on size and scale of the firm.[19] The GDPR provides for a two tier system of fines. The less grave non- compliances could result in a fine of up to €10 million, or 2% of the firm's worldwide annual revenue from the preceding financial year, whichever amount is higher, these shall include violation of Article 8,11,25-39, 41,42,43.

The more severe infringements are the cases where there principles of GDPR are not followed These infringements may lead to fines up to €20 million, or 4% of the firm's worldwide annual revenue from the preceding financial year, whichever amount is higher. These violations include violation of basic principles in article 5, violation of Article 6, 9 Article 7-violation of conditions

[19] *What are the GDPR fines?* (2023) *GDPR.eu*. Available at: https://gdpr.eu/fines/ (Accessed: 29 November 2023).

for consent etc.

The penalties are decided the GDPR Data Protection Regulator who decides the penalty based upon certain criteria, which includes Gravity and nature of the infringement , Intention behind it Mitigation steps and Precautionary measures taken by the organization, Organisation's history with data protection infringement, compliance with past administrative corrective actions under the GDPR, The extent of cooperation of the supervisory authorities while spotting and mitigating the infringement, type of data involved, Notification by the organization or their individuals about the same to concerned authorities, Certification for the organization for their conduct and other aggravating/ mitigating factors.

ISO – Introduction to ISO 27701

In 1946, after World War II, ISA members and the United Nations Standards Coordinating Committee held a meeting on International Standards. Their work led to the formation of ISO as a nongovernmental organization the following year[20].The goal of ISO 2770- **PRIVACY INFORMATION MANAGEMENT SYSTEM** CERTIFICATION, which was published in August 2019, is to offer a genuinely global approach to privacy protection as a part of information security[21].

Building on ISO 27001(INFORMATION SECURITY MANAGAEMENT), ISO 27701 is a framework for data privacy. In order to comply with the GDPR and other data protection/privacy regulations and laws, organizations should implement policies and procedures that are outlined in this most recent privacy best practice.ISO 27701 can be implemented by any organization irrespective of its size.

The GDPR is one of the many regulations that can be tailored to a comprehensive set of operational checklists provided by the ISO 27701 standard, a PIMS (Privacy Information Management

[20] Loshin, P. and Steele, C. (2021) *What is the ISO (International Organization for Standardization)?*, *Data Center*. Available at: https://www.techtarget.com/searchdatacenter/definition/ISO#:~:text=In%201946%2C%20after%20World%20War,nongovernmental%20organization%20the%20following%20year. (Accessed: 29 November 2023).

[21] *ISO 27701 – the standard for Privacy Information Management* (no date) *ISMS.online*. Available at: https://www.isms.online/iso-27701/ (Accessed: 29 November 2023).

System) standard. Businesses follow the operational checklists in the standard when documenting their policies, procedures, protocols, and activities. Internal and external auditors then audit these records, providing comprehensive documentation of the standard's compliance. Companies can lower privacy risks and maintain an efficient information security and privacy system with the support of ISO 27701.

The scope of this standard is information security , privacy data protection and cyber security.

Key Benefits of ISO 27701

- Safeguarding reputation of a company by protecting it's consumers' personal information.
- Aim for adherence to data protection laws.
- Identify and reduce risk by putting strict privacy controls in place.
- Establishing data protection as a core business practice to win over stakeholders.

Implementation of ISO 27701 –

The standard has a total of 10 clauses, clause 6 providing for planning, 8 for evaluation etc. . There are about 93 controls in detail, as per 2022 version of the standard that are to be implemented in the organization to achieve the scope of the standard, these controls are categorized into 4, organization controls, people controls, physical controls and technical controls.Various roles such as the Lead Implementer/ Project Manager Chief Privacy Officer / Data Protection Officer, Privacy Manager/Data Protection Manager, Internal Auditor, External Auditor, Privacy Analyst- for taking functional requirements and converting to technical implementation and Database and Software Professionals are needed for implementation of the standard after adhering to the requirements of the standard.

ISO 27701 and GDPR

Under the UK Data Protection Act of 2018 and the General Data Protection Regulation (GDPR), organizations are required to secure and guarantee the integrity of any sensitive data they handle

(DPA). Nevertheless, neither the DPA nor the GDPR specify the steps that businesses need to take to protect customer data. Here's where ISO 27701 is useful. The specifications and recommendations for a best-practice procedure for managing a privacy information management system (PIMS) with strong data security and privacy capabilities are provided by ISO 27701.While more than 35 countries have signed up with Europe to implement GDPR, ISO 27701 helps them with the same.

Businesses can strengthen their security measures to guard against any risk that might result in harm by implementing ISO 27001. It is intended to prioritize the needs of the business over the personal data that it processes. In contrast, the GDPR aims to shield data subjects' rights from companies[22].

Conclusion

Implementation of ISO 27701 is not enough to comply with GDPR though it provides for extensive implementation procedures, since GDPR has its own procedures and norms. However, the scope still remains the same. On the other hand, both these standards are not mandatory in India (In case of GDPR- as long as India Company does not process the data of European Resident) and ISO 27701 is only for the companies that prefer to improve the customer satisfaction through promise of privacy, since the same is an International Standard.

[22] Mohan, V. (2023) *Difference between GDPR and ISO 27001*, *Sprinto*. Available at: https://sprinto.com/blog/difference-between-gdpr-and-iso-27001/#:~:text=ISO%2027001%20helps%20businesses%20enhance,a%20data%20subject%20from%20businesses. (Accessed: 29 November 2023).