Significance of GDPR Compliance

Why in news?

\n\n

The European Union has declared the deadline for the compliance of General Data Protection Regulation (GDPR)

\n\n

What is GDPR?

\n\n

\n
- The GDPR redefines the understanding of the individual's relationship with their personal data.
\n
- It relates to an identifiable living individual and includes names, email IDs, ID card numbers, physical and IP addresses.
\n
- This law grants the citizen substantial rights in his/her interaction with\n
\n
1. **Data controllers -** Those who determine why and how data is collected such as a government or private news website.
\n
2. **Data processors -** Those who process the data on behalf of controllers, such as an Indian IT firm to which an E.U. firm has outsourced its data analytics.
\n
\n
\n

\n\n

How GDPR works?

\n\n

\n
- **Definition of Data and Entities -** Any company offering back-end services to companies operating in the EU or elsewhere, if they are receiving EU resident data, may fall within the definition of a processor under the GDPR.

\n

\n\n

\n

- Under GDPR a data controller will have to provide consent terms that are clearly distinguishable.
\n
- The GDPR also requires data collectors to provide information on the ‘who’ and ‘how.’
\n
- Individuals will also have the right to have personal data deleted under certain conditions.
\n
- **Stronger obligations -** Under GDPR, data breaches have to be reported within 72 hours and failure to comply with the new laws could result in a fine up to 4% of global turnover or maximum amount of fine 20 million Euros.
\n
- It mandates the concept of ‘privacy by design and default’ and creates categories of data privacy compliance that never existed earlier.
\n
- **Higher Autonomy -** The GDPR has global implications as it applies to those outside the E.U. who either monitor the behaviour of EU residents or sell goods and services to them.
\n
- By which it empowers EU statutory authorities to impose heavy administrative fines and to impose bans on data processing, ordering rectification, restriction or erasure of data and suspending transfers to certain countries.
\n

\n\n

How GDPR differs from Indian IT laws?

\n\n

\n

- Under India’s existing data protection regime, only one legislation, the Information Technology Act, 2000 (the IT Act) has attempted to deal with data protection in a comprehensive manner.
\n
- The IT (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules 2011 (The IT-RS Rules) under the IT Act seek to address data privacy issues.
\n
- However, the granularity of detail at which the GDPR addresses data

protection compliance is hard to compare to the approach taken by the IT-RS Rules.
\n
- The GDPR commits five detailed provisions to the essentiality of lawful consent for processing data and factors to determine whether consent was lawfully obtained.
\n
- The language of the GDPR indicates that consent is interwoven through most of its important provisions, making it a key foundation of GDPR compliance.
\n
- Thus there are certain aspects of the GDPR which are not reflected anywhere in the IT-RS, such as the adoption of a rights-based approach to data privacy.
\n

\n\n

Why GDPR is relevant to India?

\n\n

\n
- The GDPR is being adopted at a time where SC recognised the concept of informational privacy and noted that legislation should be enacted to ensure enforceability against non-State actors (private entities).
\n
- By this there are indications that a future data protection legislation in India will share several commonalities with the GDPR.
\n
- From this perspective, GDPR compliance may be considered an opportunity for Indian companies to achieve early compliance with a potential Indian data privacy legislation.
\n

\n\n

\n\n

Source: Business Line

\n

