GDPR IN 5 MINUTES: SYNOPSIS FOR BUSINESS LEADERS

Sampurna Sikha,
Chief Information Security Officer, Quadratic Insights Pvt. Ltd.

In today's data-rich world, every one of us has a need that cries out "leave my data alone!" When someone has access to our data without our knowledge, it causes us great discomfort. Many countries realize the individual need for, and business importance of, data privacy and suggest best practices. Some countries have taken the extra step of enforcing data privacy as a law.

European Unions' GDPR (General Data Protection Regulation) is an enforceable guideline. Privacy enforced as a law can benefit both businesses and customers.

1. Better data management & cybersecurity
2. Better loyalty and trust
3. Increased return on investment

Many countries are now following EU's footsteps and referring to EU's GDPR as a guideline. It is mandatory for leaders of global data-driven businesses to understand GDPR at a high level, so we at Quadratyx prepared this note. Let us start with some simple definitions.

- **Personally Identifiable Information (PII):** An individual's data that can be identified directly or indirectly, such as name, id number, location, online id, factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that person.
- **Profiling:** Automation processing used to evaluate an individual, used to analyze or predict aspects like performance at work, economic situation, health, personal preferences, interests, reliability, behavior, location or movements.
- **Data Subjects:** Individuals whose data is referred
- **Data Controllers:** Stakeholders who determine purpose and means for processing PII data
- **Data Processors:** Stakeholders who process PII on behalf of, and in accordance with the instruction of, a data controller
- **Data Lifecycle generally goes through the following stages:** Collection - > Transfer -> Use -> Storage -> Disposal. At each stage, the data controller should ensure that the process adheres to GDPR guidelines and is expected to share details when asked.

GDPR mandates that any processing of PII data should adhere to seven principles:

1. Collect data for a specified, explicit and legitimate purpose.
2. Protect data from unlawful processing, accidental loss, destruction or damage.
3. Process lawfully, fairly and in transparent manner
4. Collect what is adequate, relevant and limited to necessity
5. Maintain data that is accurate, and where necessary, keep up to date
6. Keep data for no longer than necessary
7. Ensure that there is accountability for the entire life cycle of data

GDPR has explicitly provided six rights to individuals (data subjects) to instill confidence in the system and thus, may let individuals share data with confidence.

- Right to access; Right to rectify
- Rights to be forgotten; Right to restrict; Right to withdraw
- Right to move

GDPR is applicable to organizations that meet any one of the following criteria:

— Established in European Union
— Offers goods or services to people in the EU or EU citizens
— Monitor behavior of people in EU or Citizens of EU
— A processor for a controller who must comply to GDPR
— Data processor is in the EU

According to European Commission following 11 countries are considered to have adequate security measures and appropriate privacy laws for personal data to be transferred. These are referred as "Adequate Countries"
Andorra, Argentina, Canada (only commercial organizations), Faroe Islands, Guernsey, Israel, Isle of Man, Jersey, New Zealand, Switzerland, Uruguay and USA (if the recipient belongs to the Privacy Shield). Data transfer to these countries is expressly permitted.

Personal Information Management Systems (PIMS) framework: Plans, establishes, implements and maintains management of personal information. Any organization that needs / wants to comply with GDPR can implement PIMS to guide the process, which involves:

* Drafting a PIMS policy at organizational level that is in line with the law
* Performing risk assessment & treatment considering applicable privacy requirements
* Defining clear objectives that reflect implementation at organizational level
* Measuring and monitoring performance of objectives
* Communicating and updating the policy as required
* Retaining documentation on implementation of PIMS
* Assigning a Data Controller to work as per PIMS policy; share details with customers
* Assign a Data Processing Officer if required, share details with authorities

An organization that has processes to implement privacy laws provides a comfort zone to customers, and keeps fines at bay. Trust strengthens existing relationships & builds new ones.

At Quadratyx, we are committed to securing data of its clientele and their respective customers. Commitment is reflected in the fact that Quadratyx security policies are in line with ISO 27001:2013. A framework that is internationally recognized and recommends best practices for information security management systems.

References:

- https://research.nelson-hall.com/blogs-webcasts/nelsonhall-blog
- https://www.michalsons.com/blog/must-i-comply-gdpr/32482
- https://cis-india.org/internet-governance/files/gdpr-and-india
- https://ec.europa.eu/info/law/law-topic/data-protection_en
- https://eugdpr.org/
- https://gdpr-info.eu/
- https://www.zdnet.com/article/gdpr-an-executive-guide-to-what-you-need-to-know/
- https://www.theguardian.com/technology/2018/may/21/what-is-gdpr-and-how-will-it-affect-you
- https://ico.org.uk/media/for-organisations/guide-to-the-general-data-protection-regulation-gdpr-1-0.pdf
- https://www.ey.com/Publication/vwLUAssets/EY-EU-general-data-protection-regulation-are-you-ready-mar-2017/$FILE/EY-EU-general-data-protection-regulation-are-you-ready-mar-2017.pdf
- http://www.legislation.gov.uk/ukpga/2018/12/pdfs/ukpga_20180012_en.pdf