GDPR

Introduction & Overview

GDPR?

- General Data Protection Regulation (GDPR)
- GDPR is the core of Europe's digital privacy legislation
- GDPR is a new set of rules designed to give EU citizens more control over their personal data

GDPR Compliance

- GDPR emphasize handling of personal data gathered for various purposes (e.g. in a forms) are to be managed and used only for legal and relative utility purpose in accordance with the obligation to protect it from misuse and exploitation
- GDPR has enabled organisations to respect the rights of data owners, in case of a misuse or a breach or availability of data in public, to face severe penalties
- GDPR is applied to any organisation within the European Union or to outside the geographical region of EU, towards safeguarding the data belongs to EU citizens

Personal Data Under GDPR

Personal data — Personal data is any information that relates to a person who can be directly or indirectly identified. Names and email addresses are certainly personal data. Location information, ethnicity, gender, biometric data, religious beliefs, web cookies, and political opinions are also personal data. Pseudonymous data can also fall under the definition if it's relatively easy to ID someone from it.

Data processing — Any action performed on data, whether automated or manual. The examples cited in the text include collecting, recording, organizing, structuring, storing, using, erasing… so basically anything.

Data subject — The person whose data is processed. These are your customers or site visitors.

Data controller — The person who decides why and how personal data will be processed. If you're an owner or employee in your organization who handles data, this is you.

Data processor — A third party that processes personal data on behalf of a data controller. The GDPR has special rules for these individuals and organizations.

History of GDPR

- Oct-1995: Directive 95/46/EC is adopted
  - ✓Adoption of the "European Data Protection Directive (Directive 95/46/EC)" for protecting the individuals about the processing of personal data
- June-2011: Data Protection Supervisor Opinion on EC Communication
- Jan-2012: EC proposal to strengthen online privacy rights and digital economy
- Mar-2014: European Parliament (EP) adopts GDPR
- May-2016: The General Data Protection Regulation enters into force, 20 days after publication in the Official Journal of the EU
- **25-May-2018**: The General Data Protection Regulation will apply from this day

Lawful purposes of data usage

As per GDPR, unless a data subject has provided informed consent to data processing for one or more purposes, his/her personal data may not be processed unless there is at least one legal basis to do so. The lawful purposes are listed below:

- ✓If the data subject has given consent to the processing of his or her personal data;
- ✓To fulfill contractual obligations with a data subject, or for tasks at the request of a data subject who is in the process of entering into a contract;
- ✓To comply with a data controller's legal obligations;
- ✓To protect the vital interests of a data subject or another individual;
- ✓To perform a task in the public interest or in official authority;
- ✓For the legitimate interests of a data controller or a third party, unless these interests are overridden by interests of the data subject or her or his rights according to the Charter of Fundamental Rights (especially in the case of children).

7 Key Principles outlined in GDPR

1.Lawfulness, fairness and transparency

✓Processing must be lawful, fair, and transparent to the data subject.

2.Purpose limitation

✓You must process data for the legitimate purposes specified explicitly to the data subject when you collected it.

3.Data minimization

✓You should collect and process only as much data as absolutely necessary for the purposes specified.

4.Accuracy

✓You must keep personal data accurate and up to date.

5.Storage limitation

✓You may only store personally identifying data for as long as necessary for the specified purpose.

6.Integrity and confidentiality

✓Processing must be done in such a way as to ensure appropriate security, integrity, and confidentiality (e.g. by using encryption).

7.Accountability

✓The data controller is responsible for being able to demonstrate GDPR compliance with all of these principles

Lower Level Fines

Failing to adequately integrate data protection by design into business operations.

Fines of up to **10 million Euros or 2% of the previous year's global revenue**, whichever value is greater

REASON FOR LOWER FINES:

- Breaches happening in spite of robust policies and infrastructure
- Extremely low volume of data and/or data that will have minimal impact on customers
- Swift management actions to secure infrastructure and execute preventive actions post a breach
- Being very transparent in explaining what data was breached and the actions taken to the supervisory authorities.

Upper Level Fines

These involve serious infringements on an individual's privacy rights and freedom.

can cost up to **20 million Euros or 4% of the company's global revenue**, whichever is higher.

REASON FOR HIGHER FINES:

- Lack of fundamental security framework or policies
- Lack of management commitment in securing personal data of customers
- Lack periodic of risk assessment and action on identified issues/security lapses.
- Attempts to cover-up data breaches or lack of transparency towards customers and/or regulatory authorities.

Top 3 Fines

Organisation	Amount	Issued by
British Airways	€ 20,24,20,645	UK (ICO)
Marriott International	€ 10,94,91,030	UK (ICO)
Google LLC	€ 5,00,00,000	France (CNIL)

British Airways

Nearly 183 Million GBP for a data breach that took place in 2018. This breach affected 500,000 customers browsing and booking tickets online. Subsequently after an investigation, the ICO concluded that "a variety of information was compromised by poor security arrangements, including login, payment card and travel booking details as well as name and address information"

Marriott International

Hackers stole the records of nearly 339 Million guests. They admitted openly that personal data which includes the following were stolen in a massive hack:

- Credit card details
- Passport numbers
- Date of birth records

Key takeaway: Failure to Integrate acquired IT Systems

Google LLC

Failed to provide enough information to users about its data consent policies and did not give them adequate control over how their information is used.

- Lack of transparency, Inadequate information
- Lack of valid consent for ads personalisation
- People were not sufficiently informed about how Google collected data for personalizing advertisements
- Making the process to obtain key information very complex. For example, relevant information is accessible after several steps (sometimes upto 5 or 6 actions).
- Users are not able to full understand the extent of the processing operations carried out by Google

Key takeaway: Lack of transparency in data processing methods and explicit consent

GDPR– Implications

Positives

Brand Safety

Customer Loyalty & Confidence

Cybersecurity Focus

Data Protection Standardization

Negatives

High Penalties

Cost associated with ensuring Compliance

High Regulation

Conclusion

- Organizations can no longer overlook Risk Management
- Imperative to ensure a robust Information Security Management System
- Focussing on “Privacy by Design”
- Comprehensive Data Protection Impact Assessment