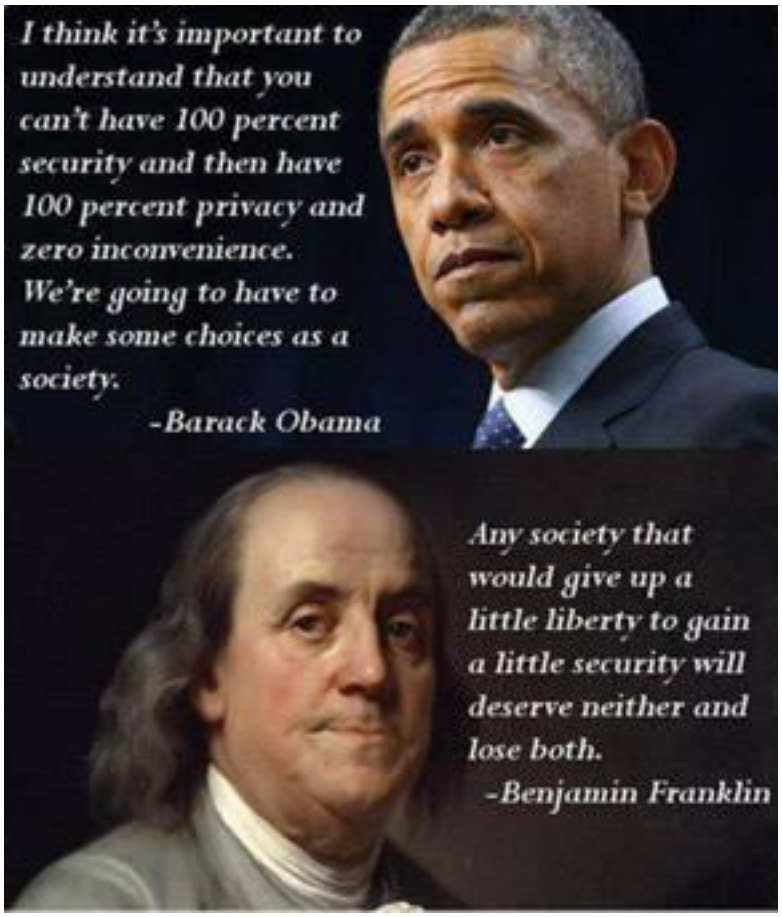
Data Privacy – Yesterday, Today & Tomorrow – An Overview

Mr. Ramkumar Ramachandran
Founder & Principal Consultant
Ascentant Corporation
ram@ascentantcorp.biz



The most of vocal Data Privacy advocates would've been shocked when they first time saw the details captured by Google in terms of their movements. The image below is slightly hashed detail of my own Google account communicating where I've been travelling in a given month.

Like any other technology giant, Google 'technically' complies to law since somewhere somehow we have ticked that box providing our acceptance to track our movements. If you never knew this, right now log into your google account under accounts.google.com and have fun.

Privacy is becoming a hot debate in the current tech world. As it is told 'Privacy in Internet' is an oxymoron. Enough has been discussed on how our mobiles track us even if the GPS is switched off. Enough has been discussed about the types of data that is shared from our mobile that results in that call from a service provider, that mail for a loan, that search for a grey colored puppy.

This article is going throw light on the evolution of data privacy globally, specifically in US, EU and India. While privacy concerns has been there been long in the western world, India is catching up with its own Data Privacy law now. The next privacy demand from California Consumer Privacy Act (CCPA) is another monster waiting to prey on privacy violators.

McAfee study on Data Explosion in 2016 has given the following forecast: -

- There is huge data generated globally
- McAfee analysis tells 8.8 ZB in 2015 to 44.02 ZB in 2020
- Governments want to stop the abuse on data privacy
- Spam emails and Cold calls are taken seriously
- Data breaches leads to heavy financial loss
- Suits by victims due to data breaches is heavy
- Protectionism, is the name of the game

So, the rush in data collection has not attained any plateau, and is only conquering more new peaks.

Where it all Started in US

In US, Privacy Act 1974 was the first initiative towards securing the privacy of individuals data. Modern tort law, as first categorized by William Prosser, includes four categories of invasion of privacy

- **Intrusion of solitude**: physical or electronic intrusion into one's private quarters
- **Public disclosure of private facts**: the dissemination of truthful private information which a reasonable person would find objectionable
- **False light**: the publication of facts which place a person in a false light, even though the facts themselves may not be defamatory
- **Appropriation**: the unauthorized use of a person's name or likeness to obtain some benefits

The essence of the law is a person to have the 'right for privacy', which is defined 'the right to be let alone'. The privacy of US residents is addressed by more than 600 state laws and 12 Federal laws to address data pertaining health, student information and limiting surveillance electronically. Recently San Francisco became the first city to ban facial recognition technology. This means individuals cannot be identified by using facial recognition technology for any service provision.

US does not have a comprehensive data privacy law like EU. The protection of data varies from public to private sector. For governmental access of people data there are there are sweeping legislations like Privacy Act, Electronics Communication Privacy Act etc. In private sector there are few sector specific norms that exist like the Federal Trade Commission Act

After the May – July 2017 Equifax breach of 145.5 million US consumers, there was an attempt to improve the consumer privacy in US, which failed in Congress.

Evolution of EU Data Privacy

EU Directive on personal data 95/46 EC 1995 was the first European adoption of privacy law. This became EU Data Protection Act 1998. EU Data Protection Directive 1995 demands: -

- Comprehensive protection of personal information
- Clear restrictions of data transfer
- Allows data transfer to third country subject to adequate level of protection

A need for change in protection laws of EU was evidenced due to following reasons: -

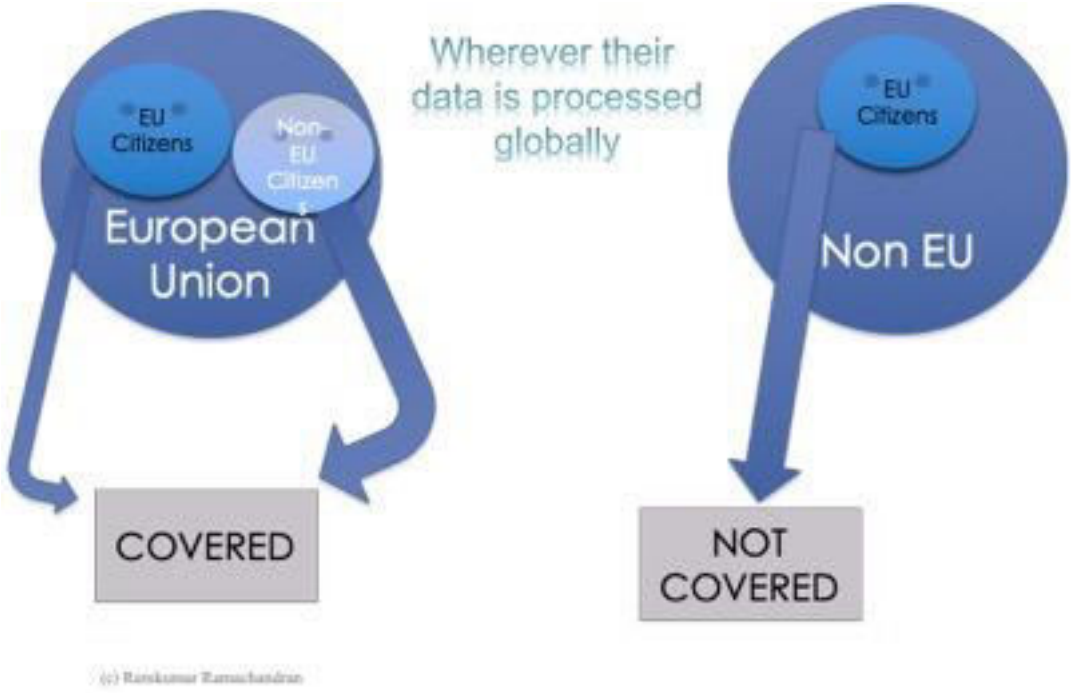
- Evolution of technology
- Internet
- Social Media

There was need to be more explicit in terms used, which led to the design of GDPR. GDPR chronological events happened as follows: -

The General Data Protection Regulation (GDPR) (Regulation (EU) 2016/679) is a regulation

- By which the European Parliament, the Council of the European Union and the European Commission
- Intended to strengthen and unify data protection for all individuals within the European Union (EU)

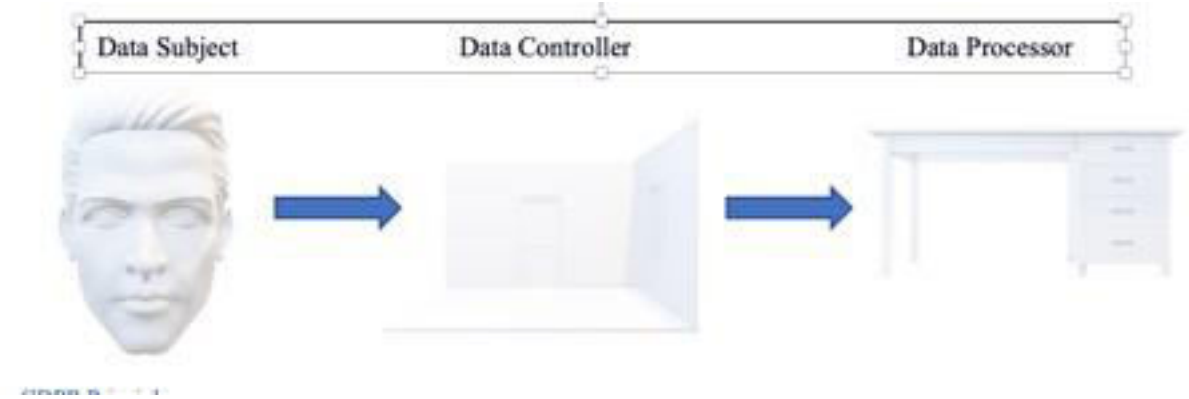
This updated Regulation applies to all member states of EU. It applies to all organization processing the data of EU data subjects – wherever the organization is geographically based. This Regulation will supersede national laws. Is meant to unify data protection and ease flow of personal data and all organizations processing PII of EU residents must comply.



GDPR talks about three distinct roles: -

1) Data Subject
2) Data Controller
3) Data Processor

Data Subject is the living person who gives their data for processing to Data Controller with formal conditions. Data Controller holds the personal data and commits to its safety. This data is processed internally by Data Processor or outsourced to another entity called Data Processor. Data Processor, based on the understanding with Data Controller processes the personal data.



GDPR Principles

GDPR operates with certain principles that are clear no-no for violation. In case of any breaches in an Organization, if it is evidenced that they've violated the GDPR principles, that may lead to maximum penalty. GDPR lists out six principles that are the core of the regulation: -

Rule # 1: Lawfulness, fairness, and transparency
Personal data must be processed in lawful manner, fairly and transparently. It shall be maintained with respect to the data subject.

Rule # 2: Limitation of purpose
Personal data must be collected for specific, explicit and legitimate purpose. Processing must be limited to the legitimate purpose only. Data collected to issue movie tickets should not be used to canvas for Star Nite celebration.

Rule # 3: Data Minimization
Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed. To issue ticket for cricket match only name should be taken, and additional data like age, sex, occupation should not be collected.

Rule # 4: Accuracy
Personal data shall be accurate and, where necessary, kept up to date. All stored data shall be ensured for accuracy and provision for the Data Subject to correct the same should be allowed.

Rule # 5: Storage Limitation
Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes. The data collected for issuing IPL match ticket should not be used to sell World Cup tickets

Rule # 6: Integrity and Confidentiality
Personal data shall be processed in a way that ensures security, including protection against un-authorized and un-lawful processing, damage or loss. Safety of personal data should be ensured and the controls should be implemented after analyzing all possible risks to the same.

Data Subject Rights

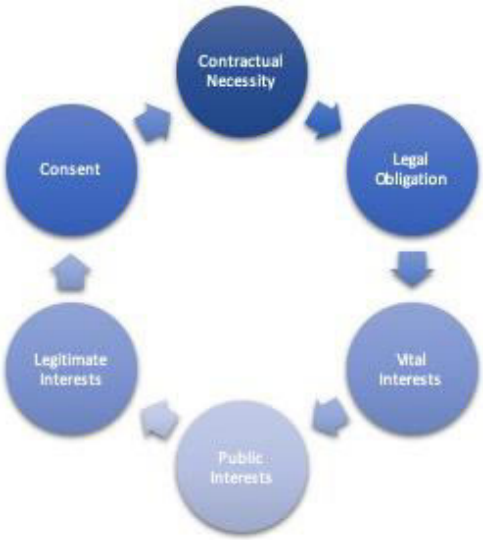
GDPR lays very high importance to the rights given to the Data Subjects whom's personal data is stored. The empowerment of Data Subject is very high and if he/she properly uses the same they can ensure the highest safety for their personal data. The Data Subject Rights are as following: -

1. **Right to information -** Right to ask what personal data of theirs is processed and with whom it is shared. Data Subject can ask which of their personal data is processed, which should sync with the consent taken from them
2. **Right to access -** Right to access their own data as well as request copies of the same. Data subject can demand access to their personal data any point in time.
3. **Right to rectification -** Right to request for change to their data if it not accurate. Data Subject may want to modify the data any point in time for any valid reasons.
4. **Right to withdraw consent -** Right to withdraw the previously given consent, so that company does not process their data anymore. Data Subject may want the consent given for processing to be stopped. The mechanism to withdraw consent should be clearly communicated to the Data Subject prior and cannot be turned down
5. **Right to object -** Right to object when his/her data is processed in variance to committed purposes. This is similar to 'Withdraw Consent'. The data collected for a given purpose being used for a different purpose can be objected by the Data Subject.
6. **Right to object to automated processing -** Right to demand only manual processing to understand the uniqueness of the data subject. Data Subject can request for their personal data from being included in automated processing which profiles individuals and decides on what to communicate to them
7. **Right to be forgotten -** Right to request for deletion of their data. To be in conjunction with retention period and retention schedule in-line with applicable laws. Data Subject can inform that their data need not be included for processing any more.
8. **Right for data portability -** Right to return the data or transfer it to another controller. Data Subject may want their data to be removed and given to another Data Controller.

Lawful Processing

GDPR provides six lawful way of processing the personal data of the Data Subjects. While many GDPR Practitioners talk about Consent as the only way, GDPR is clear and gives six possible channels to lawfully process personal data of Data Subject.

The six lawful ways of processing personal data are: -



1) Performance of Contractual Agreement
   - You can rely on this lawful basis if you need to process someone's personal data:
     - To fulfil your contractual obligations to them; or
     - Because they have asked you to do something before entering into a contract (eg provide a quote)
2) Legal Obligation
   - You can rely on this lawful basis if you need to process the personal data to comply with a common law or statutory obligation
   - Ex. An employer needs to process personal data to comply with its legal obligation to disclose employee salary details to Income Tax Department. The employer can point to the IT website where the requirements are set out to demonstrate this obligation. In this situation it is not necessary to cite each specific piece of legislation
3) Vital Interests
   - You are likely to be able to rely on vital interests as your lawful basis if you need to process the personal data to protect someone's life.
   - Ex: An individual is admitted to the Emergency department of a hospital with life-threatening injuries following a serious road accident. The disclosure to the hospital of the individual's medical history is necessary in order to protect his/her vital interests
4) Public Interest
   - You can rely on this lawful basis if you need to process personal data:
   - 'In the exercise of official authority'. This covers public functions and powers that are set out in law; OR
   - To perform a specific task in the public interest that is set out in law
5) Legitimate Interest
   - Legitimate interests is the most flexible lawful basis for processing
   - It is likely to be most appropriate where you use people's data in ways they would reasonably expect and which have a minimal privacy impact, or where there is a compelling justification for the processing.
6) Consent
   - The GDPR sets a high standard for consent. But you often won't need consent. If consent is difficult, look for a different lawful basis.
   - Consent means offering individuals real choice and control. Genuine consent should put individuals in charge, build trust and engagement, and enhance your reputation

Penalties for Violation

GDPR treats data breaches in two categories viz.1) Minor and 2) Major breach The penalty for less important (minor) breaches will be 10 million Euros or 2% of global turnover, whichever is higher. In case of major breach the penalty will be 20 million Euros or 4% of global turnover, whichever is higher.

The penalty is decided after considering various factors. GDPR checks the intent of the organization that has failed in safeguarding the personal data and then decides the penalty. Following are the considerations done before a penalty is decided: -

- The *nature, gravity and duration of the infringement* taking into account the nature scope or purpose of the processing concerned as well as the number of data subjects affected and the level of damage suffered by them;
- The *intentional or negligent* character of the infringement;
- Any *action taken by the controller* or processor to mitigate the damage suffered by data subjects;
- The degree of responsibility of the controller or processor taking into account technical and *organizational measures implemented* by them pursuant to Articles 25 and 32;
- Any relevant *previous infringements* by the controller or processor;
- The *degree of cooperation with the supervisory authority*, in order to remedy the infringement and mitigate the possible adverse effects of the infringement

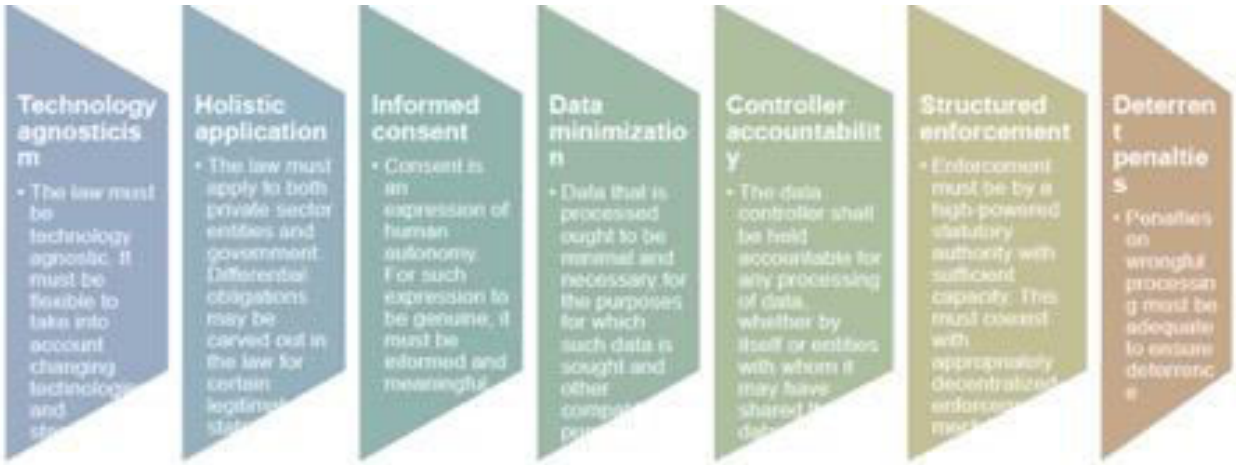
Security By Design

GDPR expects organizations to foresee risks and implement appropriate controls. Based on the type of data that is handled and other related parameters, the risks to the data should be identified and effectively mitigated. This ensures that the security is implemented by default than reacting as and when the breach happens.

This effectively means that 'data protection' should be built-into the business processes and should not operate in silos. Data Protection by design effectively means considering data protection and privacy anything you do. Ex. We create a new product campaign, then discuss about whom you are going to approach and their consent for the same. New privacy measures should not be invented for each data that comes in, but data privacy principles should be automatically applied during the same

The Indian Context

Currently protection of personal data in India is governed by SPD Rules (Sensitive Personal Data information, 2011). This is becoming very inadequate, due to which the latest personal data protection bill is getting tabled. Data Protection in India is based on the following principles: -



Justice Srikrishna Committee submitted the report on Data Protection and Draft Personal Data Protection Bill 2018 to MeITY on 27th July 2018. This bill predominantly reflects the GDPR requirements.

Features of Indian Privacy Law

Certain salient points of the Indian Personal Data Protection Bill 2018 are: -

1) All the organizations who need to protect personal data needs to appoint Data Protection Officer
2) Exemptions have been provided for processing data for journalistic purpose, or for purely personal / domestic purposes
3) Penalties range from 2% to 4% of company's global turnover or INR 5 Crores to INR 15 Crores, whichever is higher
4) Data Protection Authority of India will be the equivalent of Supervisory Authority in EU
5) Organizations should store atleast one copy of the personal data in India
6) Critical personal data shall be processed only in a server or data centre in India
7) Part of the penalties would go the Data Protection Fund and Data Protection Awareness Fund

Demands of California Consumer Privacy Act

The California legislature passed AB 375, the California Consumer Privacy Act of 2018, on Thursday, June 28, 2018, effective January 1, 2020 (the "CCPA").

It is important to look into the last 40+ years history of California to understand the privacy legislation of California. Way back in 1972, California voted to include privacy amongst the 'inalienable' rights to all people. This gave the individuals the ability to control the use and sale of their personal data.

The state followed with adopting privacy measures that include:

1) Online Privacy Protection Act
2) Privacy Rights for California Minors in the Digital World Act
3) Shine the Light, a California law intended to give Californians the "who, what, where, and when" of how businesses handle consumers' personal information

It's quite logical that California has now come up with the upgraded privacy law that considers the latest technological developments.

Under the new law, residents of California will be able to:

- Know what personal information is being collected about them
- Access that information
- Know if their personal information is disclosed, and with whom
- Know if their personal information is sold and the right to opt out of the sale
- Receive equal service and price whether or not they exercise their privacy rights

CCPA would apply to organizations that would fall in one or more of the following categories: -

- Has annual gross revenues in excess of $25 million;
- Possesses the personal information of 50,000 or more consumers, households, or devices; or
- Earns more than half of its annual revenue from selling consumers' personal information

Sanctions that is possible under CCPA are: -

- Companies that become victims of data theft or other data security breaches can be ordered in civil class action lawsuits to pay
    - statutory damages between $100 to $750 per California resident and incident, or
    - actual damages, whichever is greater, and
    - any other relief a court deems proper, subject to an option of the California Attorney General's Office to prosecute the company instead of allowing civil suits to be brought against it
- A fine up to $7,500 for each intentional violation and $2,500 for each unintentional violation

Where will we be in 2025 on Data Privacy

In the years to come Data Privacy will mature and could transform into controls that are reasonable to comply. The data privacy laws could also change based on regional demands, where 'exhibitionism' could lead to lesser control of privacy and 'conservatism' could lead to stronger controls.

The judicial activists crowd may exploit organizations through class suits and make more money, while organizations could build a strong compliance framework to prove they are right. With increase of data by the second, it could become more costlier to safeguard data.

Data Privacy is here to stay, it could evolve into a new animal, but it will remain an animal that should be tamed…!

About the author

Ramkumar 'Ram' Ramachandran is a veteran in the IT industry with global service delivery experience across 10+ countries, which includes US, UK, France, China, Singapore, Malaysia, Indonesia, Thailand, Taiwan, Philippines, Kuwait, Bahrain, Qatar, Saudi etc. He is a IIM-Calcutta Alumni and a qualified PMP, CISA and CSQA. He is also a Lead Auditor for QMS, ISMS, BCMS and ITSM. He is a certified Systems Thinker from MIT Sloan Institute of Management. He provides services in the areas of Information Security, Data Privacy, Agile, DevOps, CMMI and ISO standards. He also happens to be the past President of SPIN Chennai and currently on its Board. He runs his Consulting Firm 'Ascentant Corporation' which is primarily into IT consulting. Prior to starting his own Firm, he has worked with organizations like HCL, Polaris, KPMG and Renault-Nissan. He started his career as a Programmer and has been in various responsibilities in software delivery. He later moved into Software Quality and Security. He has taken many organizations into successful ISO and CMMI journeys. He is an avid reader of books and boasts a great collection of fiction and non-fiction in physical and e-forms. He loves travelling and would like to visit places of heritage importance. He loves music and his Alexa helps him get the best.

7 principles of the GDPR and what they mean

1. Lawfulness, fairness and transparency: Obtain the data on a lawful basis, leave the individual fully informed and keep your word.
2. Purpose limitation: Be specific
3. Data minimization: Collect the minimum data you need
4. Accuracy: Store accurate up-to-date data
5. Storage limitations: Retain the data for a necessary limited period and then erase
6. Integrity and confidentiality: Keep it secure
7. Accountability: Record and prove compliance. Ensure policies

https://www.amara-marketing.com/travel-blog/7-principles-of-the-gdpr-and-what-they-mean

EU GDPR.ORG

The EU General Data Protection Regulation (GDPR) is the most important change in data privacy regulation in 20 years. The regulation will fundamentally reshape the way in which data is handled across every sector, from healthcare to banking and beyond. https://eugdpr.org/