TATA CONSULTANCY SERVICES
Experience certainty.

General Data Protection Regulation (GDPR)

and implications for Storage

Point of View by
Sachin Patil,
Delivery Manager, Storage Product Engineering services
Tata Consultancy Services Ltd

31-May-18

General Data Protection Regulation

25th May 2018 → EU's GDPR enforceable

- In April 2016, European Parliament adopted **REGULATION (EU) 2016/679**
- Transition from EU European Data Protection Directive 95/46/EC
- Binding Act applicable across all 28 EU member states

Why are business organizations worried?

- Potential reputation damage resulting due to the Data Breaches
- Non Compliant Organizations can be fined up to 4% of annual global turnover or €20 Million (whichever is greater)
- Restriction on how data can be utilized

Reference, more reading…

European Commission **http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32016R0679**

Alternately, look for sites of Information Commissioner Office (ICO) of 11 “adequately” protected countries

EU GDPR Portal https://www.eugdpr.org/

Data Protection in EU https://ec.europa.eu/info/law/law-topic/data-protection_en

SNIA Data Protection and Capacity Optimization (DPCO) Committee
https://www.snia.org/forums/dpco

Tata Consultancy Services Ltd (TCS)
https://www.tcs.com/gdpr-preparing-for-the-new-privacy-regime
http://sites.tcs.com/blogs/agile-business/gdpr-compliance-improves-data-governance/

General Data Protection Regulation

- EU Regulation to protect **Natural Persons in EU (data subjects)** from privacy and data breaches in an increasingly data-driven world

- Applies **directly** to businesses **(controllers)** including public and private sector, established in EU or not, that offer goods or services to, or monitor the behavior of, individuals resident in the EU.

- In addition, controllers transferring personal data to businesses (controllers or **processors**) will require those businesses to comply with the requirements of the GDPR in respect of those inward transfers

Definitions (some…)

An identifiable natural person	• one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person;
Data Subject	• An Identifiable Natural Person
Personal data	• Any information enabling identification of the Data Subject
Data Processor	• Entity processing data on behalf of the controller under contract
Data Controller	• Determines the purposes and means of processing data • implements appropriate technical and organizational measures in compliance of GDPR

General Data Protection Regulation

Applies to:

- the processing by an **individual, a company or an organization** of **personal data** relating to **individuals** in the EU

- the processing of personal data wholly or partly **by automated means** as well as to **non-automated processing**, if it is part of a structured filing system

Does not apply to:

- personal data of deceased persons or of legal entities

- data processed by an individual for **purely personal reasons** or for activities carried out **in one's home**, provided there is no connection to a professional or commercial activity

7 Principles of GDPR

- Purpose Limitation
- Data minimization
- Lawful, fair & transparent
- Accuracy
- Integrity and confidentiality
- Storage Limitation
- Accountability
  - The controller shall be responsible for and, be able to demonstrate compliance with the GDPR principles

Key GDPR tenets

Explicit Opt-in	Data Subjects need to give an informed consent and, by free will
	Data Controller cannot take inferred consent by use of default opt-in or by ambiguity
Access to Information	Data Subjects can request what personal data is stored and the purpose it is retained for Data controller to also maintain the recipient list, log of access and processing of the data
Rectification	Data Subject can request to rectify inaccurate or incomplete data Data Controller must notify each recipient of the data rectification for update
Breach Notification	The local supervisory authority must be informed of any data loss within 72 hours Data Subjects should be informed “as soon as possible.”
Erasure	Data Subjects have the right to be forgotten and have their information removed on demand Any request for data to be deleted has to be complied with, within a specified time Data to be erased after the period of need including from backup & archive copies

Key GDPR tenets

Data Portability	Data Subject can request to transfer the earlier provided personal data to another data controller if technically feasible Data Controllers to maintain a machine readable data and in a commonly used structure
Objection to processing	Data Subject can complain if the data is processed for a purpose more than consented to, Data Subject can object to having the data processed for the purposes of marketing or profiling
International Transfer	Transfer outside EU to 11 non EU countries with adequate Data Protection laws in place or if Processor has appropriate Binding Corporate Rules and Contractual Obligations
Data Security	Data Controllers and Processors to implement appropriate technical and organizational measures to ensure a level of security appropriate to the risk

Steps to Compliance by Organizations

- Identify a Data Protection Officer (DPO)
- Identify the data being asked for, processed & stored
- Identify the processes & controls in place
- Update Contractual obligations with your partners/suppliers
- Regularly do Data Protection Impact Assessments, including DR testing & simulation
- Bring in the Culture “Data Protection by Design and by Default”
- Implement the “state of art” and “appropriate” technical and organizational security measures

Abilities to enable compliance by Technology

- Identify & Map the data
- Identify Users, Groups and Access Controls
- Search specific data, classify Personal data including Unstructured data
- Export, restore, update specific information
- Secure the data at a multi levels to prevent infiltration & exfiltration
- Monitor the data access patterns and act for malicious activities
- Show the compliance & ability to comply

Support from Developers

- Embrace the Culture “Data Protection by Design and by Default”
  - Architecturally Significant Requirement / Non Functional Requirement
    - Do we soft delete or erase data from? Memory location? Memory/USB/SSD Scrubbing
    - Are we storing user information for manageability solutions?
    - Are the handheld devices using personal data for logins?
  - Data interfaces/flows
    - Are support logs exported with/stored in easily readable format?
    - Data minimization? Minimal Access privileges given by default?
  - Vulnerability Management
    - Would vulnerabilities like Spectre/Meltdown have enabled Data breach?
    - Check & remediate for vulnerabilities in code base

Capabilities and Implications

- Paper Storage / Manual Filing
  - Papers are easy to file, difficult to search & retrieve
  - Need to
    - Secure and manage the papers used
    - Catalog, search the existing paper files quickly
    - Maintain access rights and record the access to files
    - Convert/Digitize Information into machine encoded text (Type/Scan/OCR/…)

- Physical Storage (Tapes, CD/DVDs,…)
  - Newer generation LTO Tapes provide 256-bit Advanced Encryption Standard (AES) to enable secure archiving and off-site transportation
  - In case of Active archive usage, LTFS helps with search, retrieve and update specific data quickly if requested
  - For older tape archives, evaluate if data to be de-archived, updated and perhaps migrated
  - In case of existing tape archives, need to review retention times, geography and any legal formalities in moving tapes or retention

Capabilities and Implications

- Backup Applications, Data Centre Infrastructure, Cloud need to have:-
  - Reduction in Easy identifiable information (Email addresses, Mobile phones are used as logins!)
  - Identity management with dual-factor authentication
  - Strict role-based access control
  - Stringent audit trails with monitoring for the patterns
  - High level of physical security with biometric locks on the equipment cages
  - Multi-tenancy with complete networking and resource separation among tenants
  - Increase process visibility in case of cloud

  - Data at-rest encryption with customer-owned keys
  - Data in-flight encryption for any data movement
  - Secured management communication that is always encrypted
    - Use of TLS and AES256 amongst other techniques

  - Data Pseudonymization and Data Anonymization (Dev, Staging) techniques

Capabilities and Implications

- Backup Applications, Data Centre Infrastructure, Cloud need to have:-
  - Selection of the region where the data can be kept
  - Classify user data to segregate user's personal data
  - Be aware of stored data, including geographic region of that storage
  - Integrate with applications & contextualize the data
    - make the data visible, so that the location of the data can be identified
  - Modification of existing appliances or Solution deployments for data classification

  - Monitoring of applications to manage continual GDPR compliance
  - Software Tools that are Data Aware and act on Pattern Recognition, Messaging Cue from emails and Social Media
  - Search Unstructured Data to identify Data & act using Policy driven actions like defensible deletions and moving data into storage that supports unstructured data analysis

  - Focus on elimination of data loss, i.e. a data breach and concern for access request
  - Data Erasing rather than deletion when the data is to be removed
  - Control over removable media like USB drives

Thank You!

Sachin Patil