General Data Protection Regulation (GDPR) for Enterprises

By

Samant Khajuria

Associate Professor

The problem …

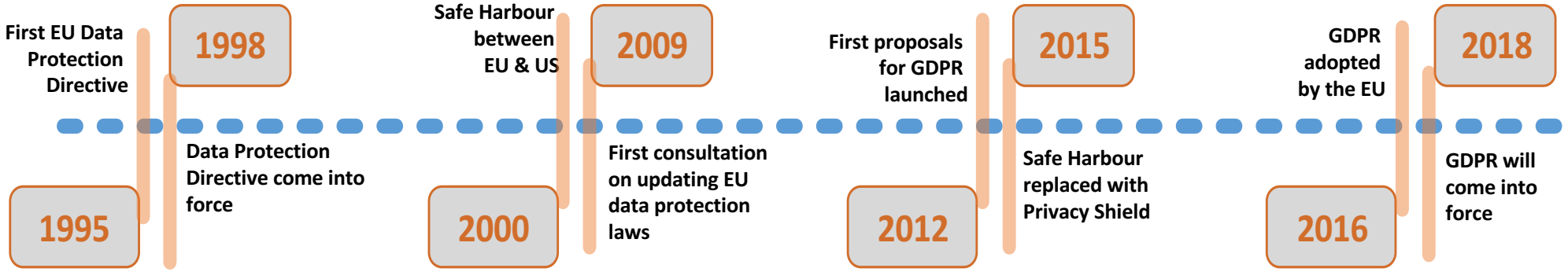
*It is impossible to keep the **data secure and private** when one can't keep track of what they have, where it is and what its value is ..*

Privacy Issue

- Due to the **digitization** of all kinds of records in public and private sector
  - Medical records, citizen data at the municipality, student data at the schools and universities, clients data in enterprises, messages and micro-posts send by people every day.
- This raises serious privacy concerns not only to the organized groups but also to the average user of technology – who have keen interest in the processing and handling procedures of personal data by the organizations.
- **Westin** defines privacy as*" claim of individuals, groups and institutions to determine for themselves when how and to what extent information about them is communicated to others*"
- Privacy is multifaceted, multidisciplinary, and complex issue of the digital world
  - Usually understood and valued differently by different individuals, data holders, courts and legislations
- The notion of privacy is human made and it evolves around them and the society they live in.

AALBORG UNIVERSITY
DENMARK

Timeline: From Directive to Regulation …..



First European Union Data Protection Directive to General Data Protection Regulation

A more definitive meaning of privacy; especially information privacy

AALBORG UNIVERSITY
DENMARK

Regulation

- The main goal of the regulation is to build and/or increase trust in the EU citizens in using digital services.
- The regulation is carefully designed in coherence with **EU Digital Market Strategy**
  - Ambition: To produce right incentives for the services to flourish by providing trustworthy infrastructure supported by the right regulation.
- The regulation is seen as as a modernization of the protection of the processing of personal data to cover the legislative gaps created by the rise of social media, big data and increasingly digital world.
- The regulation extends the definition of personal data to any information relating to an individual, such as name, photo, an email address, bank details, posting on social networking websites, medical information or a computer's IP address.

AALBORG UNIVERSITY
DENMARK

New initiatives in the Regulation

- Most of the legal practices in the new regulation are based on new legislation.
- A number of new initiatives are introduced:
  - New rights to data subject
  - New obligations to data controller and processor
  - Partial harmonization across European countries
  - One-stop-shop: where the main establishment of the company interacts with only one supervisory authority
  - Fines: Failing to comply the regulation
    - Fine up to **10 Million EUR or up to 2% of the annual worldwide turnover** of the preceding financial year in the case of an enterprise, whichever is greater

AALBORG UNIVERSITY
DENMARK

Preliminaries of the Regulation

- **Personal data:** "Any information relating to an identified or identifiable natural person"
  - Personal data is categorized as *Common Data* and *Sensitive or Special Categories of personal data* ex., Ethnic origin, religious belief and even political opinions
- **Controller:** " Natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purpose and means of the processing of personal data"
  - A controller is usually a service provider to which the user provides their information.
  - A controller decides the *type of data collection, kind of processing and the storage of data*.
  - If any 3rd party data processors are involved, controller makes sure that they comply with the regulation.
- **Processor:** "Natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller"
  - The entities are contracted by the controllers to process personal data information
- **Processing:** any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means,
  - such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction;"

AALBORG UNIVERSITY
DENMARK

Implementing General Data Protection Regulation (GDPR)

- Where one starts?
- Who should be responsible?
- How to prove that one is compliant to all the requirements?

AALBORG UNIVERSITY
DENMARK

Privacy Frameworks

- Guidelines and practices that put together all the requirements that can be applied to an organization
  - Processes, policies and controls that are necessary to meet those requirements.
- Tools that can help organizations think about and frame discussions about privacy and understand privacy requirements related to **personally identifiable information (PII).**

- **Under Article 24 GDPR: *"Responsibility of the Controller"***
  - "the controller shall implement appropriate technical and organizational measures to ensure and to be able to demonstrate that processing is performed in accordance with this regulation"
- Several Privacy Frameworks publically available:
  - COBIT – Control objectives for information and related technologies
  - AEPC – Asia Pacific economic corporation
  - NIST – National Institute of Standards and Technology
  - OECD – Organization for economic corporation and development
  - ISO 2700XX - International Standards for Organizations

AALBORG UNIVERSITY
DENMARK

OECD Privacy Framework

- Guidelines on the protection of privacy and trans-border flows of personal data are internationally accepted for processing personal data.
- Framework could also be used for the governance of personal data collected and processed by enterprises over the course of their business.
- Eight Privacy Principles

Collection Limitation	Collection of any personal data can only occur under the consent and knowledge of the data subject (user)
Data Quality	The data should be relevant and purpose specific
Individual Participation	Data Subject should have the right to access personal data and have the data erased, rectified, completed or amended.
Purpose Specification	Data Subject should know the purpose of information collected
Use Limitation	Any personal data should in principle not be used for purposes other than those specified at the time of the collection, except in certain cases
Security Safeguards	Reasonable security objectives should be in place ex., unauthorized use/access, modification of data etc.
Openness	Data controllers and processers should be transparent to data subjects
Accountability	Data collectors should be held accountable for compliance

ISO 27001

- Internationally recognized framework and cover key areas of privacy i.e., *policies and procedures, the privacy principles and governance, risk management and compliance objectives.*
- The framework describes the requirements for information security systems management (ISMS) which help protect information, including privacy aspects.
- The framework only gives the requirements, the tools to fulfil those are up to enterprises.
- The main goal of ISO 27001 is to ensure the “confidentiality, integrity and availability (CIA)” of information by applying risk management processes.
    - Preserving authorized restrictions on information access, guarding against improper modification or destruction and ensuring timely access to and use of information can be done

ISO 27001 – Version 2013:

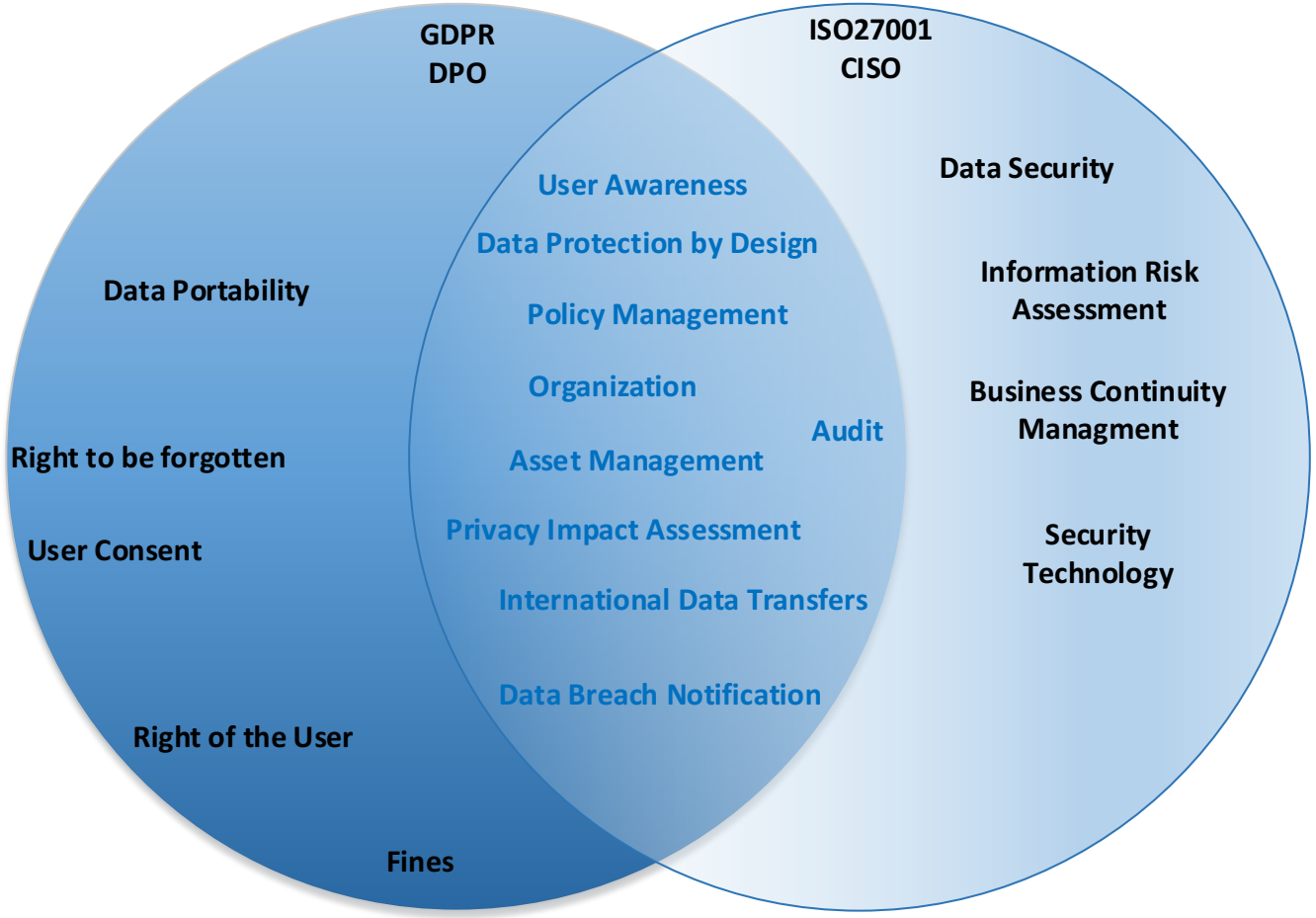
- consists of 114 controls in 14 domains

- Information Security Policies
- Organization of Information Security
- Assert Management
- Cryptography
- Communications Security
- System Acquisition, Development, and Maintenance
- Supplier Relationships
- Physical and Environmental Security
- Human Resource Security
- Compliance
- Access Control
- Information Security Aspect of Business Continuity Management
- Operations Security
- Information Security and Incident Management

(ISC)² Common Body of Knowledge 10 security domains	ISO 27001 / 27002 v2013 114 controls in 14 domains	NIST SP800-53v4 224 controls in 18 families	Council on Cyber Security Critical Security Controls - 20 controls
1. Access Control 2. Telecommunications and Network Security 3. Information Security Governance and Risk Management 4. Software Development Security 5. Cryptography 6. Security Architecture and Design 7. Security Operations 8. Business Continuity and Disaster Recovery Planning 9. Legal, Regulations, Investigations, and Compliance 10. Physical (Environmental) Security	1. Information Security Policies 2. Organization of Information Security 3. Human Resource Security 4. Asset Management 5. Access Control 6. Cryptography 7. Physical and Environmental Security 8. Operations Security 9. Communications Security 10. System Acquisition, Development, and Maintenance 11. Supplier Relationships 12. Information Security Incident Management 13. Information Security Aspect of Business Continuity Management 14. Compliance	1. Access Control 2. Awareness and Training 3. Audit and Accountability 4. Security Assessment and Authorization 5. Configuration Management 6. Contingency Planning 7. Identification and Authentication 8. Incident Response 9. Maintenance 10. Media Protection 11. Physical and Environmental Protection 12. Planning 13. Personnel Security 14. Risk Assessment 15. System and Services Acquisition 16. System and Communications Protection 17. System and Information Integrity 18. Program Management	1. Inventory of Devices 2. Inventory of Software 3. Secure Configurations for Computers 4. Continuous Vulnerability Assessment and Remediation 5. Malware Defenses 6. Application Software Security 7. Wireless Device Control 8. Data Recovery Capability 9. Security Skills Assessment and Training 10. Security Configurations for Network Devices 11. Network Ports, Protocols, and Services 12. Control of Administrative Privileges 13. Boundary Defense 14. Security Audit Logs 15. Need-to-Know Access Control 16. Account Monitoring and Control 17. Data Loss Prevention 18. Incident Response Capability 19. Secure Network Engineering 20. Penetration Testing and Red Team Exercises

Overlap between Regulation and Framework

- Enterprises ie., data controllers and processors, must designate a
- Data protection officer (DPO) to comply with the GDPR
- Chief Information security officer (CISO) oversees ISO 27001



AALBORG UNIVERSITY
DENMARK

General Data Protection Regulation (GDPR)

- The roots of GDPR goes to "first European union data protection directive ”
- Many concepts and principles in the regulation are much as same as in the directive.
- If the enterprises are in compliance with the directive and/or follow privacy frameworks then most of principles mentioned will remain valid and can be a very good starting point.

- Article 5 of the regulation discusses six privacy principles (decedents from Data Protection Directive) to guide how enterprises can manage personal data.
  - These principles can be seen as duties of enterprises to comply with the regulation

AALBORG UNIVERSITY
DENMARK

Six Privacy Principles of GDPR and comparison with the directive

AALBORG UNIVERSITY
DENMARK

Lawfulness, fairness and transparency

- Personal data should be processed fairly and legally ie., User should be informed what their personal data will be used for.
- Article 6, EU data directive: “Personal data should be processed fairly and lawfully”
- Article 5, GDPR: “Personal data must be processed lawfully, fairly and in a transparent manner in relation to the data subject”
- Difference: Additional care when designing and implementing data processing activities.
- Lawful processing and conditions for processing data
  - Data subject have given explicit *consent*
  - Data subject has to fulfil the conditions or it is necessary for the performance of the *contact*
  - Legal obligation; necessary for compliance
  - *M*edical situation; processing is necessary to save someone’s life
  - P*ublic function*; processing is necessary for public interest
  - *Legitimate interest* pursued by the controller or 3rd party

AALBORG UNIVERSITY
DENMARK

Limited for its purpose

- Data collected for one purpose should not be used for any other purpose.
- The principle states same in directive and in the regulation

"Personal data may only be collected for specified, explicit and legitimate purposes and must not be further processed in a manner that is incompatible with those purposes."

AALBORG UNIVERSITY
DENMARK

Data minimization

- An enterprise should only process the personal data that it actually needs to process in order to achieve its processing purposes.
- Article 6, EU data directive: “Personal data must be adequate, relevant and not excessive in relation to the purposes for which those data are collected and/or further processed”.
- Article 5, GDPR: Updates the principle from “not excessive...” to “limited to what is necessary ...”.
- Difference: From implementation perspective, enterprises will carefully need to look into their data processing operation to check if they process any personal data that are not strictly necessary in relation to the purposes.

AALBORG UNIVERSITY
DENMARK

Accuracy

- Data controllers should take appropriate steps to maintain the accuracy of personal data and keep it up to date.
- No change from directive to regulation.
- Principle states that:

"Personal data must be accurate and, where necessary, kept up to date. Every reasonable step must be taken to ensure that personal data that are inaccurate are either erased or rectified without delay"

AALBORG UNIVERSITY
DENMARK

Retention

- Any data that can identity data subjects should not be kept longer than is necessary for the purposes for which the personal data are processed.

Get rid of data, if you no longer need it.

- Directive states

"Personal data must be kept in a form that permits identification of data subjects for no longer than is necessary for the purposes for which the data were collected or for which they are further processed. Member States are obliged to implement appropriate safeguards for personal data stored for longer periods for historical, statistical or scientific use."

- Regulation added to two new factors,
  - Specific provisions on the processing of personal data for historical, statistical or scientific purposes
  - "Right to be forgotten" where data subject have the right to erasure of personal data.

AALBORG UNIVERSITY
DENMARK

Integrity and Confidentiality

- Controller needs to take appropriate measures to keep personal data secure against any external or internal threats.
- No change in the principle from the Directive to Regulation.

  "Personal data must be processed in a manner that ensures appropriate security of those data, including protection against unauthorized or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organizational measures."

- GDPR explicitly mentions data security is a fundamental obligation of all controllers.
- Sort of 7th Principle : *Accountability*
  - *Principle states that the data controller is responsible and must be able to demonstrate, compliance with the six privacy principles.*

AALBORG UNIVERSITY
DENMARK

New Initiatives

New Initiatives

- *Consent &Transparency* - "Any freely given specific informed and unambiguous indication of the data subject's wishes by which he or her, by a statement or by clear affirmative action, signifies agreement to the processing of personal data relating to him or her"
  - One of the most important elements for ensuring compliance with the regulation.
  - Change from Directive : unambiguous, where the users perform an affirmative action for the actual processing of personal data for the specific purpose.
  - "consent and children" where the regulation states that for online services which rely on consent to processing, verifiable parental consent is required for use of a child's (under 16) personal data
- *Data Sensitivity* – Classification of data into two categories common data or special categories of data also referred to as sensitive data (Genetic and Biometric).
  - Significant changes from the directive to regulation: Member states classified data based on their own local data protection regulations ex:, ., in Denmark personal data was classified into three different categories: normal, sensitive and semi-sensitive data
- *Pseudonymisation – A method of securing personal data.* A privacy enhancing technique of processing personal data in such a way that it can no longer be attributed to a specific data subject.

New Initiatives

- *Enhanced Data Subjects Rights*
  - *The right to be forgotten* (Article 17)
    - Data subject has the right to have their information deleted in certain situations.
    - Once the subjects exercise their rights, controller is obliged to delete their personal data.
    - If the data is on the public domain then its controllers' duty to ensure that other controller who also process same data, must delete the data.
  - *Data Portability:* Allows data subjects to request copies of their personal data in a useful electronic format.

    "The data subject shall have the right to receive the personal data concerning him or her, which he or she has provided to a controller, in a structured, commonly used and machine-readable format and have the right to transmit those data to another controller without hindrance from the controller to which the personal data have been provided."
  - *The right not to be profiled* : automatic processing of personal data, which is intended to evaluate certain personal aspects.
    - Regulation introduces a new right where data subjects will not be automatically profiled.

New Initiatives

- *Duties of controller and processor* : Entities involved in personal data handling ie., collection, processing, storing requires to implement a variety of measures.
  - *Privacy by design & privacy by default* : "the controller should adopt internal policies and implement measures which meet in data protection by design and data protection by default".
    - Technical solution includes pseudonymisation and encryption of data.
  - *Privacy impact assessments:* A process that helps organizations identify and minimize privacy risks.
    - Regulation requires PIA to include
      - **Description** of the processing activities and **assessment** processing, identify risks, mitigate those risks, security techniques to protect data and compliance with the regulation.
  - *Data Protection officer* (DPO)
    - A person with the responsibility to ensure protection of personal data and compliance with the regulation
    - A controller or a processor shall appoint a DPO if they Public authorities, an enterprise whose core activity is regular and systematic monitoring of data subjects or an enterprise whose core activity is processing of sensitive data or criminal records.
  - *Data Breach Notification*: Controller is obligated to notify supervisory authority in case of any data breaches, which could comprise personal data
  - *Obligation for Processor:* assist controller to fulfil a number of the controller's obligations
    - The relationship between a controller and processer is contractual.

New Initiatives

- *Transfer to 3rd Countries:* Personal data of EU citizens can be transferred to 3rd countries by using standard contracts.
  - EU- US privacy shield, a framework between united states and European union for transatlantic exchanges of personal data for commercial purposes.
- *One-stop-shop and Consistency mechanism*: Concept where businesses are established in more than one Member state
  - Lead authority determined by the place of its main establishment in EU.
  - In the case of enterprises under investigations, they do not have to submit to multiple investigations for the same case.
- *Fines & Penalties*: The supervisory authorities are empowered to impose significant fines to the controllers and processors failing to comply with the regulation.
  - Two tiers of fines
    - lower level of fine can be up 10 million euro or in the case of an undertaking up to 2% of the total worldwide annual turnover, whichever is the greater
    - higher level can be up to 20 million euro or, in the case of an undertaking, up to 4% of the total worldwide annual turnover, whichever is the greater

AALBORG UNIVERSITY
DENMARK

Checklist and Guidelines for Enterprises

Awareness	Decision makers and the key people in an enterprise are aware that the law is changing to GDPR
Information you hold	Documentation of any personal information enterprise holds. Does data fall into Common personal data or special category personal data.? How data is collected, stored, processed? Is data shared with anyone else?
Communicating privacy information	From current law to GDPR, there is some additional information that enterprises need to share with the data subjects. Ex., explanation of legal basis for processing the data, retention period etc. This information is shared though privacy notices.
Individual' rights	The right to be forgotten, Data portability and the right not to be profiled. Enterprises should make sure that they cover all the rights individuals have.
Subject access requests	Due to new timescales, enterprises need to update their procedures and plan how they will handle requests.
Legal basis for processing personal data	Documentation about various types of data processing carried out in enterprises and identifying legal basis for carrying to processing
Consent	Revising how enterprises are getting consents from the data subjects.
Children	Systems should be placed in enterprises for verifying subjects' age. In case of children, enterprises should gather parental consent got data processing
Data Breaches	Right procedures should be in place for detecting, reporting and investigate a personal data breach.
Data Protection by Design and Data Protection Impact Assessment	A privacy impact assessment should be implemented in the enterprises to identify and minimize risks.
Data protection offices	A DPO should be appointed to ensure protection of personal data and compliance with the regulation
International	Multinational enterprises should determine which data protection supervisory authority they should come under.

AALBORG UNIVERSITY
DENMARK

Conclusion

- One of the top priorities for European Union is Digital Single Market.
- Union claims to create up to 415 billion euro in revenue and hundreds of thousands of new jobs.
- Today citizens do not trust online services, which means they will not use all the opportunities presented by technologies.
- The main aim of the GDPR is to build or increase trust in EU citizens in using digital services.
- GDPR is seen as a **modernization of the protection of the processing of personal data** to cover the legislative gaps created by the rise of social media, big data and increasingly digital world.

- GDPR and the new initiatives taken in the regulation were discussed .
- The discussion compared regulations' six fundamental privacy principles with the Data protection directive and also implementation guidelines/ checklists for the enterprises.

AALBORG UNIVERSITY
DENMARK

Thank you!!