GDPR

General Data Protection Regulation (EU) 2016/679

General Data Protection Regulation (1)

- GDPR is:
  - a regulation (not a directive)
  - proposed by the European Union
  - on data protection and privacy
  - for all individuals within EU+EEA
  - + export of personal data outside the EU and EEA areas

  - Adopted 2016, April 27th
  - Operative 2018, May 25th

General Data Protection Regulation (2)

- Substitute
  - Europe → Directive 95/46/CE
  - Italy → d. lgs. n. 196/2003 (codice per la protezione dei dati personali)

- The following cases are not covered by the regulation:
  - Lawful interception, national security, military, police, justice
  - Public interest statistical and scientific analysis
  - Deceased persons (national legislation)
  - Employer-employee (dedicated law)
  - Purely personal nature or household activity

Reception/Impact

- Thousands of amendments were proposed in the process of definition
- Over 80 percent of IT professionals surveyed expected GDPR-related spending to be at least *$100,000*
- The total cost for EU companies is estimated at around *€200 billion* while for US companies the estimate is for *$41.7 billion*

- Research indicates that approximately 25% of *software vulnerabilities* have GDPR implications (emphasizes breaches, not bugs)
- After the implementation of the GDPR, the US state of California passed a similar bill called The California Consumer Privacy Act of 2018

Content

- The GDPR consists of 99 *articles*, grouped into 11 chapters, and an additional 173 *recitals* with explanatory remarks. Italian version is 261 pages long.
- Chapters' headings:
  - I - General provisions
  - II - Principles
  - III - Rights of the data subject
  - IV - Controller and processor
  - V - Transfers of personal data to third countries or international organizations
  - VI - Independent supervisory authorities
  - VII - Cooperation and consistency
  - VIII - Remedies, liability and penalties
  - IX - Provisions relating to specific processing situations
  - X - Delegated acts and implementing acts
  - XI - Final provisions

Recitals - 1

Whereas:

(1) [redacted] Article 8(1) of the Charter of Fundamental Rights of the European Union (the 'Charter') and Article 16(1) of the Treaty on the Functioning of the European Union (TFEU) provide that everyone has the right to the protection of personal data concerning him or her.

Article - 1

Subject-matter and objectives

1. This Regulation lays down rules relating to the [redacted] with regard to the processing of [redacted] and rules relating to the [redacted].

2. This Regulation protects [redacted] and in particular their right to the protection of personal data.

3. The free movement of personal data within the Union [redacted] for reasons connected with the protection of natural persons with regard to the processing of personal data.

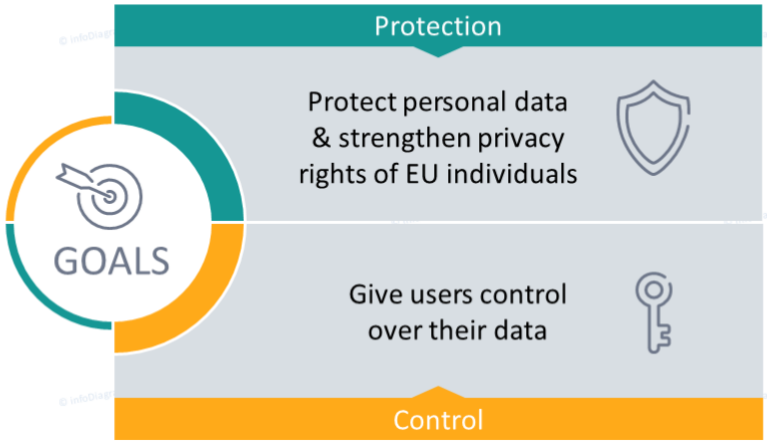
Scope (1)

- The regulation applies if the **data controller** (an organization that collects data from EU residents), or **processor** (an organization that processes data on behalf of a data controller – cloud provides), or the **data subject** (person) is based in the EU.
- The regulation also applies to organizations based outside the EU if they collect or process personal data of **individuals located inside the EU**.
- **Data Protection Officer (DPO)** employed in the organization, has responsibilities for advising on GDPR regulation

Scope (2)

- DPO appointment is **mandatory** for
  - Public bodies (excepts courts) and
  - Data controllers and data processors that, as a core activity, monitor individuals *systematically* and on a large scale, or that process *sensitive* data on large scale
- Appointment, position and tasks of DPO are set out in GDPR
  - Expert knowledge of *data protection law* and practice
  - Be involved in *all data protection issues*
  - Report directly to *highest* level of management
  - Operational independence, no conflicts of interest, confidentiality
  - Inform and advice; monitor compliance; point of contact for individuals

Scope (3)



Scope (4)

Personal Data

- Any information relating to an **individual**, whether it relates to his or her private, professional or public life.
- It can be anything from a name, a home address, a photo, an email address, bank details, posts on social networking websites, medical information, or a computer's IP address."
- The precise definitions of terms such as "personal data", "processing", "data subject", "controller" and "processor", are stated in Article 4 of the Regulation
- any data that are not personal data are outside the scope of the proposed Regulation.

Lawful basis for processing (1)

- **Unless** a data subject has provided informed consent to data processing for one or more purposes, personal data may not be processed unless there is at least one legal basis to do so. According to Article 6, the lawful purposes are:
  - If the data subject has **given consent** to the processing of his or her personal data
    - Consent by default is not valid anymore (EXPLICIT consent)
    - Can be removed and controller cannot refuse
  - To fulfill **contractual obligations** with a data subject;
  - 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 – 16years old).

Lawful basis for processing (2)

- Public Task: you can process personal data, without consent, to carry out your official functions or a task in the **public interest** - and where you have a **legal basic** for the processing
- Legitimate Interest: you can process personal data, without consent, if you have a genuine and legitimate reason to do so
  - Legitimate interest can be for **commercial** benefit
  - GDPR recitals – direct marketing could be a legitimate interest
  - BUT exception if your interests are outweighed by harm to the individual's right and interest

Lawful basis for processing (3)

- Consent may be required if you are:
  - Marketing
  - Selling information
  - Transferring data outside
- Consent will NOT be appropriate:
  - Consent is a pre-condition of using the service
  - You would still process personal data using different basis even if consent was withdrawn
- GDPR sets a higher standard for obtaining consent

Lawful basis for processing (4)

- Consent – Practical changes
  - Identify basis of processing
  - Clear and plain language
  - Keep records
  - Drive Withdrawal
- Don't
  - Don't bundle consent
  - Blanket consent
  - Don't use pre-ticked boxes
  - Penalize withdrawal

Responsibility and accountability

- **Compliance** with the GDPR: the *data controller* must implement measures which meet the principles of **data protection by design and by defaul**t.
- Data protection by design and by default (Article 25) require data protection measures to be designed for products and services.
  - i.e. pseudonymizing personal data, by the controller, as soon as possible (Recital 78).
  - responsibility of the data controller to implement effective measures and be able to demonstrate the compliance of processing activities even if the processing is carried out by a data processor on behalf of the controller (Recital 74)
  - inform the user about collection
  - data protection impact assessments (Article 35)

Data protection by design and by default

- (Article 25) requires **data protection to be designed into the development of business processes** for products and services (At the beginning, for the root → easy task for new process, but what about old process?)
- by default: **Privacy settings at a highest level**
- implement mechanisms to ensure that personal data is not processed **unless necessary** for each specific purpose (touch lesser is better)

- encryption and decryption operations must be carried out **locally**, not by remote service (because of keys) and data must remain in the power of the data owner if any privacy is to be achieved.
- outsourced data storage on remote clouds is practical and relatively safe if only the **data owner**, not the cloud service, holds the decryption keys.

Pseudonymization (1)

- as a process that is required when data is stored (as an alternative to the other option of complete data anonymization) to transform personal data in such a way that the resulting data **cannot be attributed** to a specific data subject without the use of additional information.
- Encryption: decryption key separately!!!
- Tokenization: replaces sensitive data with non-sensitive substitutes (but still possible to link to original owner)

- Nice to have: The definition of personal data lists a number of factors how a person can be identified, e.g. with reference to identification numbers. Here, a general reference to "any other unique identifier" could be added for ensuring comprehensive coverage.

Pseudonymization (2)

- data minimization is a requirement
  - with pseudonymization the regulation provide no guidance on how or what constitutes an effective data de-identification scheme, with a **grey area** on what would be considered as inadequate pseudonymization subject to Section 5 enforcement actions
- anonymization and pseudonymization are two distinct techniques
  - Recital 26 of the GDPR defines anonymized data as "data rendered anonymous in such a way that the data subject is not or **no longer identifiable**."
  - By contrast to anonymization, Article 4(5) of the GDPR defines pseudonymization as "the processing of personal data in such a way that the data can no longer be attributed to a specific data subject without the use of **additional information**."

Pseudonymization (3)

- The risk of re-identification:
  - The effectiveness (and legality) of both anonymization and pseudonymization hinge on their abilities to protect data subjects from re-identification.
  - In Recital 26, the GDPR limits the ability of a data handler to benefit from pseudonymized data if re-identification techniques are "**reasonably** likely to be used, such as singling out, either by the controller or by another person to identify the natural person directly or indirectly."
  - Whether pseudonymized data is "reasonably likely" to be re-identified is a question of fact that **depends on a number of factors** such as the technique used to pseudonymize the data, where the additional identifiable data is stored in relation to the de-identified data, and the likelihood that non-identifiable data elements may be used together to identify an individual.

Pseudonymization (4)

- ANONYMOUS
  - Not possible to identify the user in any way
  - Data can be used in aggregation
- PSEUDO ANONYMOUS
  - Very difficult to identify
    - With current technology
    - With data from other sources
    - In a reasonable time
  - Not direct linked with user profile
- NON ANONYMOUS
  - Identified and linked with user profile
  - Consent for any data types

Right of access

- More generally: data subject right (Article 15).
  - access their personal data and information about how this personal data is being processed
  - A data controller must provide, **upon request**, an overview of the categories of data that are being processed (Article 15-1b) as well as a copy of the actual data (Article 15-3).
  - Furthermore, the data controller has to inform the data subject on **details about the processing**, such as the *purposes* of the processing (Article 15-1a), with whom the data is shared (Article 15-1c), and *how* it acquired the data (Article 15-1g)
  - be able to **transfer** personal data from one electronic processing system to and into another → data portability and data interoperable
  - **review** the collected data

Right to erasure

- Was *right to be forgotten* → became *right of erasure*
- Records of processing activities must be maintained that include purposes of the processing, categories involved and envisaged time limits. The records must be made available to the **supervisory authority** on request (Article 30)
- Supervisory authorities cannot have their eyes on all controllers all the time, so it is crucial **to give data subjects strong rights** for their interactions with controllers.

Data breaches (1)

- the data controller is under a **legal obligation** to notify the supervisory authority without undue delay unless the breach is unlikely to result in a risk to the rights and freedoms of the individuals.
- There is a maximum of **72 hours after becoming aware** of the data breach to make the report (Article 33). **Individuals** have to be notified if adverse impact is determined (Article 34). In addition, the data processor will have to notify the controller without undue delay after becoming aware of a personal data breach (Article 33).
- However, the notice to data subjects **is not required** if the data controller has implemented appropriate technical and organizational protection measures that render **the personal data unintelligible** to any person who is not authorised to access it, such as encryption (Article 34).

Data breaches (2)

- A personal data breach means a breach of security leading to the accidental or unlawful destruction, loss, alternation, unauthorized disclosure of, or access to, personal data. This includes breaches that are the result of both accidental and deliberate causes. It also means that a breach is more than just about losing personal data
- Example: Carphone Warehouse
  - Fined £400.000 in January
  - Records for approximately 3.350.000 customers of a number of mobile phone provider
  - Records for 389 customers across two other companies
  - Historical transaction for period March 2010-April 2010
  - Records of approximately 100 employees

Data breaches (3)

- Vulnerability is a weakness which allow an attacker to reduce a system's information assurance. Vulnerabilities are the intersection of the three elements:
  - a system susceptibility of flaw
  - attacker access to the flaw
  - attacker capability to exploit the flaw
- To exploit a vulnerability, an attacker must have at least one applicable tool or technique that can connect to a system weakness. In this frame, vulnerability is also known as the attack surface
- Example: Carphone Warehouse – how did they get in?
  - Vulnerability?
  - Password

Data breaches (4)

- Example: Uber
  - Details of 2.7 million UK drivers and riders
  - Details of 57 million people worldwide
  - Email address and phone numbers
  - US Driver license numbers
- how did they get in?
  - Password stored on GitHub
  - What is GitHub?
  - Cover up!
  - ICO Response
    - «Uber has confirmed its data breach in October 2016 affected approximate 2.7 million user accounts in the UK. Uber has said the breach involved names, mobile phone numbers and email address. On its own this information is unlikely to pose direct threat to citizens, However, its use may make other scams, such as bogus emails or call appear more credible. People should continue to be vigilant and follow the advice from NCSC»

Data breaches (5)

- It's not only loss of confidentiality or unauthorized processing of personal data
  - It also encompass availability and integrity
- only breaches "likely to affect" data subjects have to be notified to them, and not all breaches
- Nice to have: public register of breaches to educate the public about IT security and provide added insight into trends regarding breaches

Data breaches (6)

- Preventing
  - Vulnerability testing and Penetration testing
  - Password management
    - Risk assess
    - Two Factor Authentication
  - Utilized DLP (Data loss prevention) feature on key documents
    - help a network administrator to control what data end users can transfer
  - Data protection training
    - Employers
    - Users

Sanctions (1)

- a **warning** in writing in cases of first and non-intentional noncompliance
- **regular** periodic data protection **audits**
- a fine up to **€10 million or up to 2% of the annual worldwide turnover** of the preceding financial year in case of an enterprise, whichever is greater, if there has been an infringement of the following provisions: (Article 83, Paragraph 5 & 6)
- a fine up to **€20 million or up to 4% of the annual worldwide turnover** of the preceding financial year in case of an enterprise, whichever is greater, if there has been an infringement of the following provisions: (Article 83, Paragraph 4)

Sanctions (2)

- Data protection Commissioner
  - Investigative powers
    - Conduct *investigations* and audits
    - *Obtain access to data*, premises and equipment
  - Corrective powers
    - Issue warnings and reprimands
    - *Order* compliance
    - Order communication of a data breach to an individual
    - Impose a temporary/permanent ban on processing
    - Order rectification or erasure of personal data
    - Suspend data transfers to a third country
  - Administrative fines
    - May impose fine (effective, proportionate and dissuasive)

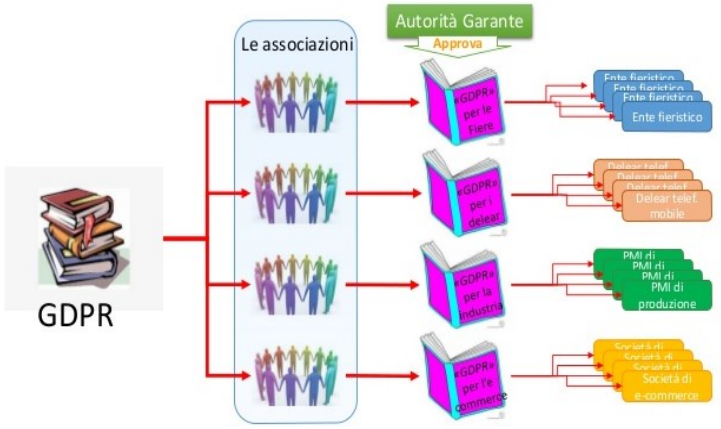
Codes of conduct and certification (section 5, article 40) (1)

- **The Member States, the supervisory authorities**, the Board and the Commission shall encourage the drawing up of codes of conduct intended to contribute to the **proper application** of this Regulation, taking account of the specific features of the **various processing sectors** and the specific needs of micro, small and medium-sized enterprises.
  - Involvement authorities
  - Awareness of the problem
- **Associations and other bodies** representing categories of controllers or processors may prepare codes of conduct, or amend or extend such codes, for the purpose of specifying the application of this Regulation, such as with regard to
  - The association that represent the firms

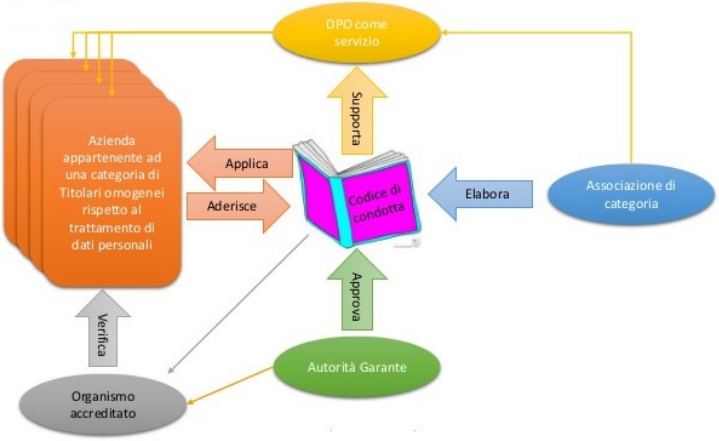
Codes of conduct and certification (section 5, article 40) (2)

- (a) fair and transparent processing;
- (b) the legitimate interests pursued by controllers in specific contexts;
- 5419/16 AV/NT/sr 175 DGD 2 **EN**
- (c) the collection of personal data;
- (d) the pseudonymisation of personal data;
- (e) the **information provided to the public** and to data subjects;
- (f) the exercise of the rights of data subjects;
- (g) the information provided to, and the protection of, children, and the manner in which the consent of the holders of parental responsibility over children is to be obtained;
- (h) the measures and procedures referred to in Articles 24 and 25 and the measures to **ensure security** of processing referred to in Article 32;
- (i) **the notification of personal data breaches** to supervisory authorities and the communication of such personal data breaches to data subjects;
- (j) the transfer of personal data to third countries or international organisations; or
- (k) out-of-court proceedings and other dispute resolution procedures for resolving disputes between controllers and data subjects with regard to processing, without prejudice to the rights of data subjects pursuant to Articles 77 and 79.

Codes of conduct and certification (section 5, article 40) (3)



Codes of conduct and certification (section 5, article 40) (4)



Mapping GDPR to Required Capabilities

- GDPR compliance can be achieved only by applying a combination of controls that can summarized as People, Process, Products:
  - **People** → specific roles, responsibilities and accountability
  - **Processes** → operating principles and business practices
  - **Products** → technologies used for data storage and processing
- Specific set of controls for GDPR:
  - **Discover:** scope data subjects to the regulation
  - **Defend**: implement measure to protect discovered data
  - **Defect**: identify breach against data and remediate security and process gaps

Discover (1)

- *Before* implementing security controls, identify **which** personal data are stored and **how long** the organization is permitted to retain

1. Identification of *IMPACT* to Personal Data: integrate tools that enable controller to quickly and conveniently **review their data content** and to inspect **what additional** data will be captured as new services are under development (Article 35, clause 1)
2. *RETENTION* of Personal Data: capability to **identify personal data**, and **securely erase** once the expiration period has been reached, or an individual specifically requests erasure (Article 13, clause 2a)

- To erase means marking as DELETED
  - for police officer investigation (i.e. 30 days)

Discover (2)

- What 'personal data' do you hold and use?
- Why do you need it or use it? What's the legal basis for processing it?
- How is it processed and shared? How long is it kept for?
- Where is stored and from where is it accessed?
- Identify and understand the data flows (data mapping, data inventory)

Defend (1)

- Implement the controls that will protect data (Article 32, clause 1)

1. *Access Control*: only authorized users can access personal data (Article 25, clause 2 + Article 29). It should be possible to enforce **authentication controls** so that only the clients (users, application, administrations) authorized by the data processor can access the data. The KB should also allow data controllers to define specific *roles, responsibilities and duties* each client can perform against data

Defend (2)

2. *Pseudonymization & Encryption*: in the event of a breach, the **pseudonymization** and **encryption** of data is designed to prevent the identification of any specific individual from compromised data (Clause 28). Pseudonymization via separation of user information from user data + access control. Encryption (Article 32, clause 1 + Article 34 clause 3a) for data *in-transit* using network connections and data *at-rest* using storage and backups
3. *Resilience and Disaster Recovery*: provide system and service + means to restore data in a **timely** fashion + **fault tolerance** to system failures (Article 32)

Defend (3)

4. *Data sovereignty: Data transfer outside of the EU*: To support globally distributed applications, organizations and increasliyng **distributing data to data centers and cloud facilities** located in multiple countries across the globe, it should be possible to enforce data sovereignty policies by only distributing and storing EU citizen data **to region recognized as complying** with the regulation

Detect

- In the event of a data breach, the organization must be able, in a **timely fashion**, to *detect and report* on the issue, and also to generate a record of what activities had been performed against the data

1. *Monitoring and reporting*: The closer to real-time, the better chance of limiting the impact. The KB should offers managements tools that enable constant monitoring of KB behaviour to proactively mitigate threads and that enable the organization to report any breaches (Article 33, clause 1)
2. *Auditing*: Record activities on KB and present that activities for forensic analysis when requested by controller (Article 25, clause 1 + Article 28, clause 3H)

Checklist

- Legal bases for processing
- Policies and procedure
- Privacy notes
- Appropriate technical and organizational measure
- Documentation and record-keeping
- Staff training
- Dealing with Data Subject Rights
- Security and Data breach
- Data Protection Impact Assessments
- Data Processor and contracts
- Appoint a DPO if required, or at least, a lead person
- Privacy by design and by default