7 – Data Privacy under GDPR regulation

Michele.mastroianni@unicampania.it
mmastroianni@unisa.it

Università degli Studi della Campania *Luigi Vanvitelli*

Dipartimento di Matematica e Fisica

Presentation Summary

- Aim and Scope of GDPR
- Defintions
- The Key Principles
- The right of Data Subjects
- Anonymization and Pseudonimization
- Q & A

GDPR

- The General Data Protection Regulation (EU) 2016/697 (GDPR) is a regulation in EU law on data protection and privacy in the European Union (EU) and the European Economic Area (EEA).
- It also addresses the transfer of personal data outside the EU and EEA areas.
- The GDPR's primary aim is to give control to individuals over their personal data and to simplify the regulatory environment for international business by unifying the regulation within the EU

Territorial Scope

GDPR applies to the processing of personal data in the context of the activities of an establishment of a controller or a processor in the Union, regardless of whether the processing takes place in the Union or not.

GDPR applies to the processing of personal data of data subjects who are in the Union by a controller or processor not established in the Union, where the processing activities are related to:

- (a) the offering of goods or services, irrespective of whether a payment of the data subject is required, to such data subjects in the Union; or
- (b) the monitoring of their behaviour as far as their behaviour takes place within the Union.

GDPR: Processing of Personal Data

For the purposes of GDPR:

- Processing means 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, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction

GDPR: Processing of Personal Data

For the purposes of GDPR:

- Personal data means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is 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;

Personal data

Any information relating to an identified or identifiable living person

- Human Resource records
- Patient medical record/file
- CCTV images of a student
- Photograph of a person
- DNA of a person
- Email

Automated and manual filing systems

Personal data processing: lawful basis

When is it legal to process personal data?

- Consent: by data subject, specific purpose, written, withdrawal at any time, parental consent children under 16
- Necessity of processing: Contracts, legal obligations, legitimate reason, public interest, vital interest for registered

Special Categories is generally prohibited

- …unless strictly regulated consent or necessity

Special Category Personal Data (art. 9)

AKA Sensitive Personal Data

- Racial / ethnic origin
- Political opinions
- Religious / Philosophical beliefs
- Trade Union membership
- Genetic or biometric data
- Health
- Sex life / sexual orientation

Criminal offences / convictions not now included but separated out and similar extra safeguards put in place at Article 10

Lawfulness in processing Special category of P.D.

- Explicit consent
- Necessary
- To protect vital interests
- Data made manifestly public by subject
- Related to Legal claims
- Substantial public interest (basis in law, proportionate…)
- Preventive or occupational medicine
- Public health
- Archiving, scientific or historical research

GDPR:
Data Controllers and Processors

- Controllers are the main decision-makers – they exercise overall control over the purposes and means of the processing of personal data. University of Campania is a Data controller.
- Processors act on behalf of, and only on the (written) instructions of, the relevant controller. A cloud provider may be a data processor.
- Data Subjects: identifiable natural persons whose personal data are processed by a data controller or processor (in many cases: the user/patient)
- If two or more controllers jointly determine the purposes and means of the processing of the same personal data, they are joint controllers. However, they are not joint controllers if they are processing the same data for different purposes.

GDPR
Key Principles

The GDPR sets out seven key principles:

- Lawfulness, fairness and transparency:
- Purpose limitation: The purpose of processing must be clear and known to the user. The data collected is usable for a new purpose if either this is compatible with your original purpose.
- Data minimization: The personal data you are processing must be adequate, relevant and limited to what is necessary – It is unfair to hold more than you need for that purpose.
- Accuracy
- Storage limitation: The data must be kept for as long as necessary, and no longer (there are exception due to the law)
- Integrity, Accessibility (Access) and Confidentiality (security)
- Accountability: The company must take responsibility for personal data processing, and must have appropriate measures and records in place to be able to demonstrate the compliance.

Accountability Details

- adopting and implementing data protection policies;
- taking a 'data protection by design and default' approach;
- putting written contracts in place with organisations that process personal data on your behalf;
- maintaining documentation of your processing activities;
- implementing appropriate security measures;
- recording and reporting personal data breaches;
- carrying out data protection impact assessments for uses of personal data that are likely to result in high risk to individuals' interests;
- appointing a data protection officer;
- adhering to relevant codes of conduct and signing up to certification schemes.

Right of the data subjects

- The right to be informed
- The right of access
- The right to rectification
- The right to erasure
- The right to restrict processing
- The right to data portability
- The right to object
- Rights related to automated decision making and profiling

Key points

- Access control/Authorization: "means to ensure that access to assets is authorized and restricted based on business and security requirements"
- Integrity: "protection against accidental loss, destruction or damage"
- Confidentiality: "Protection against unauthorized or unlawful processing“
- Data minimization: "adequate, relevant and limited to what is necessary"

Key points

- Information/transparency: "processed in a transparent manner".
- Storage limitation: storing data "no longer than is necessary for the purposes for which the personal data are processed"
- Purpose limitation: "collected for specified, explicit and legitimate purposes"
- Accountability: "demonstrate that processing is performed in accordance with the regulation"

GDPR
Other key points

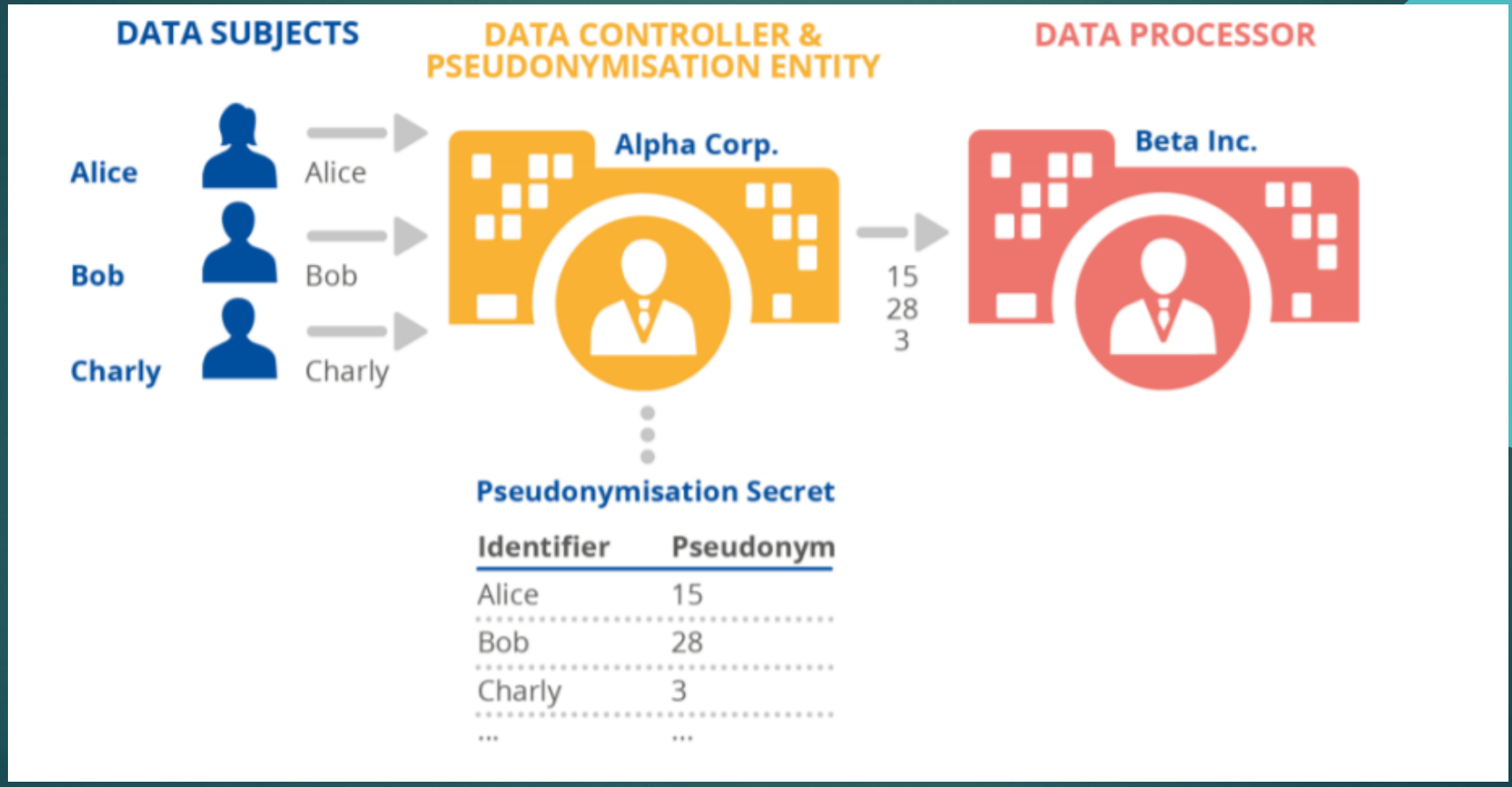
- Data Breach: The GDPR introduces a duty on all organisations to report certain personal data breaches to the relevant supervisory authority. You must do this within 72 hours of becoming aware of the breach, where feasible. In some cases, the data breach must be communicated to all data subjects involved.

- Data transfer outside EU: Any transfer of personal data to a third country or to an international organisation shall take place only if certain condition are met (EU approval of specific Country, appropriate safeguards, approved corporate rules)

Anonimization and pseudonimization

- Pseudonymization is a de-identification process that has gained additional attention following the adoption of GDPR, where it is referenced as both a security and data protection by design mechanism. In addition, in the GDPR context, pseudonymisation can reduce the risk severity if properly applied.
- Pseudonymization is a process that allows you to switch the original data set (for example data subject's e-mail or a name) with an alias or pseudonym. Pseudonymization is a reversible process, that de-identifies data but allows the reidentification later on if necessary.
- Pseudonimization is NOT anonymization, due to the reversibility of the process.

Pseudonimisation Example



Reference: [3]

Anonymization

- Personal data are made up of information and assessments that can be linked to a specific person.
- It can be difficult to draw the line between personal data and anonymous data. It is therefore important to have some understanding of what personal data are.
- Anonymous data fall outside the scope of the GDPR. For this Act not to apply, it is crucial that the anonymisation of data is real. In other words, it must be impossible to recreate any link between the data and the individual concerned, taking into account the means that may reasonably be envisaged used.
- The advantage of anonymisation is that the further processing of the data can take place without incurring any form of processing liability.

Anonymization techniques

- Mask/substitute/delete the personal data (is possible? age may be deleted?)

- Generalization: This technique has the purpose of reducing the granularity of the data. As a result, the data that is disclosed is less precise than the original data and therefore makes it difficult if not impossible to retrieve the exact values associated with an individual. For example, the exact ages of the concrete individuals would be replaced with age groups, e.g. 55-65, 65-75, etc.
- WARNING: in case of patients with rare pathology is difficult to obtain anonymization

Anonymization challenges

- The danger of re-identification: When data from several sources are compared against each other, there is a risk that individuals in what are nominally anonymous data sets may be identified.
- Two known data points, e.g. postcode and birthdate, could be enough to re-identify individuals from a data set.
- Pseudonymous data must not be confused with anonymous data. Pseudonymous data are personal data, and their processing falls within the scope of the Personal Data Act.
- Encryption is not the same as anonymization. The objective of encryption is to protect the data, not make them unidentifiable.

Useful other techniques

- Pseudonymity/Non-identifiability: "Processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information"
- Unlinkability: "Inability of an attacker to determine whether two items of interest (IOI) are related or not."
- Encryption: "protection measures that render data unintelligible to any person who is not authorised to access it"

Thanks for your attention

Q & A Session

References

1. EU Parliament, "Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data (GDPR)", available: https://eur-lex.europa.eu/eli/reg/2016/679/2016-05-04 (16.11.2020)
2. ICO (Information right authority of UK), "Guide to Data Protection", available: https://ico.org.uk/for-organisations/guide-to-data-protection/
3. ENISA, "Pseudonymisation techniques and best practices", November 2019, available: https://www.enisa.europa.eu/publications/pseudonymisation-techniques-and-best-practices/at_download/fullReport
4. Datatilsynet, The anonymisation of personal data https://www.datatilsynet.no/en/regulations-and-tools/reports-on-specific-subjects/anonymisation/