DATA PROTECTION AND PRIVACY
University of Genoa

Lesson 1: Introduction to GDPR

Avv. Manuela Bianchi - manuela.bianchi@bmsfarm.it

WHO AM I?

Manuela Bianchi

Data Lawyer, Data Protection Officer, Teacher, Author

Course Program (legal aspects)

- Introduction to GDPR
- Definitions
- Data breach
- DPIA
- Data transfer
- Cookie
- Other European Data Protection Laws (I.e. E-Privacy Directive, AI Act, Digital Market Act, Digital Service Act etc.)

General Data Protection Regulation (GDPR) UE n. 679/2016

- entry into force: on 25 May 2018
- directly applicable in the member States legal orders
- reinforces the protection of the individual's right to personal data protection, reflecting the nature of data protection as a fundamental right for the European Union
- guarantees the free flow of personal data between EU member States
- new opportunities for companies and business

New opportunities for companies and business (1/2)

- a level-playing field for all companies operating in the EU market
- the principles of data protection by design and by default creating incentives for innovative solutions to address data protection issues form the start
- stronger individuals' rights
- more control over personal data for individuals (a new right of data portability)
- stronger protection against data breaches

New opportunities for companies and business (2/2)

- more flexibility for controllers and processors processing personal data due to unambiguous provisions on responsibility (the accountability principle)
- more clarity on the obligations of processors and the responsibility of controllers when selecting a processor
- the protection of the personal data guaranteed by the Regulation travels with the data outside the EU ensuring a high level of protection

Subject-matters and objectives (art. 1)

1. This Regulation lays down rules relating to the protection of natural persons with regard to the processing of personal data and rules relating to the free movement of personal data.
2. This Regulation protects fundamental rights and freedoms of natural persons and in particular their right to the protection of personal data.
3. The free movement of personal data within the Union shall be neither restricted nor prohibited for reasons connected with the protection of natural persons with regard to the processing of personal data.

Material scope (art. 2) (1/2)

1. This Regulation applies to the processing of personal data wholly or partly by automated means and to the processing other than by automated means of personal data which form part of a filing system or are intended to form part of a filing system

Material scope (art. 2) (2/2)

2. This Regulation does not apply to the processing of personal data:
(a) in the course of an activity which falls outside the scope of Union law;
(b) by the Member States when carrying out activities which fall within the scope of Chapter 2 of Title V of the TEU;
(c) by a natural person in the course of a purely personal or household activity;
(d) by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security.

Territorial scope (art. 3) (1/3)

This Regulation 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. L 119/32 EN Official Journal of the European Union 4.5.2016

Territorial scope (art. 3) (2/3)

2. This Regulation 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.

Territorial scope (art. 3) (3/3)

3. This Regulation applies to the processing of personal data by a controller not established in the Union, but in a place where Member State law applies by virtue of public international law.

Definitions (art. 4)
Personal Data (1/4)

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 (2/4)

Pseudonymization vs Anonymization

Personal Data (3/4)

Examples of Personal Data:

- a name and surname
- a home address
- an email address such as name.surname@company.com
- an identification card number
- an Internet Protocol (IP) address
- a cookie ID (ePrivacy Directive 2002/58/EC and Regulation of the European Parliament and of the Council n. 2006/2004; Italian Data Protection Authority Directive June 2021 enters into force on January 2022)
- the advertising identifier of your phone
- data held by a hospital or doctor, which could be a symbol that uniquely identifies a person

Personal Data (4/4)

Examples of Data not considered Personal Data:

- a company registration number
- an email address such as info@company.com
- anonymized data

Processing (1/2)

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

Processing (2/2)

Examples of processing:

- staff management and payroll administration
- access to/consultation of a contacts database containing personal data
- sending promotional emails (to send direct marketing emails, you also have to comply with the marketing rules set out in the ePrivacy Directive)
- shredding documents containing personal data
- posting/putting a photo of a person on a website
- storing IP addresses
- video recording

Profiling

Any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyze or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behavior, location or movements

Pseudonymization

The 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, provided that such additional information is kept separately and is subject to technical and organizational measures to ensure that the personal data are not attributed to an identified or identifiable natural person

Filing System

Any structured set of personal data which are accessible according to specific criteria, whether centralized, decentralized or dispersed on a functional or geographical basis

Controller

The natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data

Processor

A natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller

Recipient

A natural or legal person, public authority, agency or another body, to which the personal data are disclosed, whether a third party or not

Consent

Any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her

Personal data breach

A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored or otherwise processed

Genetic Data

Personal data relating to the inherited or acquired genetic characteristics of a natural person which give unique information about the physiology or the health of that natural person and which result, in particular, from an analysis of a biological sample from the natural person in question

Biometric Data

Personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images or dactyloscopic data

Data concerning health

Personal data related to the physical or mental health of a natural person, including the provision of health care services, which reveal information about his or her health status