European Union
General Data Protection Regulation
The protection of natural persons in relation to the processing of personal data is a fundamental right.
GDPR Overview

- Regulation (EU) 2016/679
- Adopted on 27 April 2016
- Enforceable starting 25 May 2018
- 99 articles (approx 88 pages)
Goals

◉ "harmonize" data privacy laws across Europe - a single set of rules will apply to all EU member states.

◉ give greater protection and rights to individuals
Scope

- **data controller** (organization that collects data from EU residents)
- **data processor** (organization that processes data on behalf of data controller)
- the **data subject** (person) is based in the EU

- offering goods or services to EU citizens (even if no payment)
- the monitoring of behaviour that takes place within the EU
- does not apply to the personal data of deceased persons
‘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.
Penalties

- a warning in writing in cases of first and non-intentional non-compliance
- regular periodic data protection audits
- up to 2% of annual global turnover or €10 Million (whichever is greater)
- up to 4% of annual global turnover or €20 Million (whichever is greater)
The principles of, and rules on the protection of natural persons with regard to the processing of their personal data should, whatever their nationality or residence, respect their [fundamental right and freedoms], in particular their right to the protection of personal data.
Privacy and Security by Design

- data protection impact assessments when the type of processing is “likely to result in a high risk to the rights and freedoms of natural persons” and implementing appropriate technical safeguards
- only personal data which are necessary for each specific purpose of the processing are processed
- implement appropriate technical and organisational measures, such as pseudonymisation, which are designed to implement data-protection principles, such as data minimisation, in an effective manner
Data Protection Officer

- must be appointed on the basis of professional qualities and, in particular, expert knowledge on data protection law and practices
- may be a staff member or an external service provider
- must be provided with appropriate resources to carry out their tasks and maintain their expert knowledge
- must report directly to the highest level of management
- must not carry out any other tasks that could result in a conflict of interest
Data Breach Notification

- mandatory where a data breach is likely to “result in a risk for the rights and freedoms of individuals”
- 72 hours of first having become aware of the breach
- data processors will also be required to notify their customers, the controllers, “without undue delay” after first becoming aware of a data breach.
Consent

- valid consent must be explicit for data collected and the purposes data is used for
- consent must be:
  - clear and distinguishable from other matters
  - provided in an intelligible and easily accessible form
  - using clear and plain language.
- consent for children must be given by the child’s parent or custodian
- consent may be withdrawn - it must be as easy to withdraw as it is to give it
Profiling

- automated processing of personal data
- and using that personal data to evaluate certain personal aspects relating to a natural person
- examples include analyzing or predicting “aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements.”
The processing of personal data should be designed to serve mankind. The right to the protection of personal data is not an absolute right; it must be considered in relation to its function in society and be balanced against other fundamental rights, in accordance with the principle of proportionality...
Right to Access

- right to obtain from the data controller confirmation as to whether or not personal data concerning them is being processed, where, and for what purpose

- requires disclosure of “the existence of automated decision making including profiling” along with “the significance and the envisaged consequences of such processing for the data subject.”

- the controller shall provide a copy of the personal data, free of charge, in an electronic format.
Facts
- **1998**: La Vanguardia newspaper of Spain published two articles concerning an attachment and garnishment action against Costeja González.
- **2009**: he asked Newspaper to remove the articles because they came up in a Google search.
- Newspaper: denied, claiming that the legal action was published pursuant to an order by Spain’s Ministry of Labor and Social Affairs.

Ruling - “Right to be Forgotten” and balancing test
- Individuals may request that the information be removed.
- Rights to privacy and protection of personal data override both economic interest of business and general public access.
- unless in “the preponderant interest of the general public”
Right to Erasure

- data subject can have the data controller:
  - erase his/her personal data
  - cease further dissemination of the data

- conditions for erasure include the data no longer being relevant to original purposes for processing or a data subject withdrawing consent

- controllers required to compare the subjects' rights to "the public interest in the availability of the data" when considering such requests
Right to Data Portability

- **right** for a data subject to receive the personal data concerning them

- both data that has been 'provided' by the data subject and data that has been 'observed'

- data that has been sufficiently anonymised is excluded

- must be provided in a structured and commonly used **Open standard** electronic format
Thanks!

Any questions?

You can find me at

- straley@uci.edu
- https://security.uci.edu

Thanks!
Credits

Special thanks to all the people who made and released these awesome resources for free:

◉ Presentation template by SlidesCarnival
◉ Photographs by Unsplash