General Data Protection Regulament

UE 679/2016

We are Here!

Privacy vs Business

- Private data are valuable:
  - Focalize advertising by profile users
    - Car insurances
  - Optimize logistics
    - move goods in the *right* place (Amazon)
    - using personal path optimize delivery avoidin congestion
  - Create new services or implements old service in a new (more efficient) way:
    - signal coverage discovery
    - path optimization (Waze)

Privacy vs Cloud

- More and more personal sensitive data are moved on Cloud
  - Photos
  - Contact
  - Calendars
- More and more businnes data are moved on Cloud
  - Office 365
  - AmazonWS

Security has changed.

Security on the Law

What Is GDPR

- GDPR put some duties on who deals with personal data in order to:
  - enhance personal data protection from data accidental incident and fraudolent activities (accidental incident and fraudolent activity are the same for GDPR)
  - increase comprension on privacy issued and knowledge on how data is treated by dealer
  - Portability of personal data across different dealer

Key Concepts

- Applied to european phisical persons without regarding country bonduaries
  - It must be applied even for european persons outside EU
- Private data are "goods" owned by the user; he can ask to:
  - deny access, destroy, rectify, cancel, export
- User must be fully informed and he have to **explicitly** allow any treatment on his data
  - You must be able to prove this point.

Key Concepts [*contd.*]

- You cannot gather unnecessary data and conserve data indefinitely
  - You have to use only the minimal set of data you needs for the minimal time.
- Dealer have to do anything possible in order to protect data
  - You must be able to prove this point.
- Privacy by design
  - You have to develope your project thinking to privacy

Actors

- Data controller: who treat data, you.
- *(For Italy)* "Responsabile del trattamento dei dati": a external entity which share full or partial of the responsability of the Data controller.
- Data Protection Officer (DPO): the contact point for user in order to enforce its right
- Supervisory Authority (SA): the country Authority

In case of fault…

- Incident notification to the designed Autority within 72 hours
- Evaluation of the fault; if relevant, you must notify incident also to the user.

- *If there has been an infringement on GDPR:* a fine up to 20.000.000€ or up to 4% of the annual worldwide turnover of the preceding financial year in case of an enterprise, whichever is greater.

What you have to do

- GDPR becomes enforceable from **25 May 2018**.
- Prepare an easy undestandable informative on what data you gather and how you use
- Collect explicit aggrement from the user before collect its data.
- Protect the data storage from accidental or fraudolent corruption, accidental or fraudolent dumping using the *state of the art* in security.
  - backup, encription, pseudanonimization, etc., etc
- Create a contact point in which user can enforce its right.