

GENERAL DATA PROTECTION REGULATION

Agustí Verde Parera
Data Protection Officer UAB

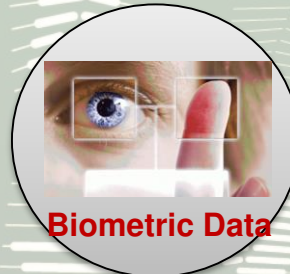
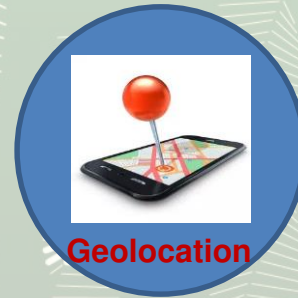
Xavier Rubiralta Costa
IT Responsible for Data Protection UAB



GENERAL DATA PROTECTION REGULATION

- ☐ Principles relating to processing of personal data
- ☐ Lawfulness of processing
- ☐ Consent
- ☐ Data protection by design
- ☐ Processing of personal data in research

PERSONAL DATA



PRINCIPLES RELATING TO PROCESSING OF PERSONAL DATA

- ☐ Lawfulness, fairness and transparency
- ☐ Purpose limitation
- ☐ Minimisation
- ☐ Accuracy
- ☐ Storage limitation
- ☐ Integrity and confidentiality
- ☐ Accountability



LAWFULNESS OF PROCESSING

- ☐ Consent
- ☐ Performance of a contract
- ☐ Compliance of a legal obligation
- ☐ Protection of vital interests
- ☐ Public interest or exercising of official authority
- ☐ Purposes of legitimate interest

CONSENT

- ☐ Freely given
- ☐ Specific
- ☐ Informed
- ☐ Unambiguous



DATA PROTECTION BY DESIGN

- ☐ Risk Analysis
- ☐ Data Protection Impact Assessment
- ☐ Technical measures
- ☐ Organisational measures

PROCESSING OF PERSONAL DATA IN RESEARCH

- ☐ Principles relating to processing of personal data
- ☐ Purpose limitation
- ☐ Publication
- ☐ Information reuse

Balanced protection measures: organisational and technological

- ☐ All the measures are important. Not balanced ones means a weak protection
- ☐ All the protection measures should be based on the identified and analyzed risks
- ☐ Knowledge and awareness of policies and procedures and the use of tools
- ☐ Multidisciplinary teams: different visions

Privacy from design and Privacy by default

- ☐ Data protection should appear in the first step of any project, not later
- ☐ Data protection is not optional, it is compulsory
- ☐ Privacy and Security policies
- ☐ Risk analysis: identify threats, analyze risks and manage risks
- ☐ Risk = impact * likelihood

Risk analysis: relevant scenarios in research environments

- ☐ People of different institutions, countries, legislations, cultures, etc
- ☐ People rotation in the projects
- ☐ Access control: people authorization and authentication
- ☐ Data with bigger risk according to the country
- ☐ Physical location of data and devices
- ☐ Tools for data treatment and conservation
- ☐ De-identification and encryption

Data de-identification (anonymize)

- ☐ Is it possible to de-identify data in any case?
- ☐ Orientations and warranties in de-identification procedures of personal data of the Spanish Data Protection Agency:
 - ☐ <https://www.aepd.es/media/guias/guia-orientaciones-procedimientos-anonimizacion.pdf>
- ☐ List of 18 identifiers of the Health Insurance Portability & Accountability Act (HIPAA)
- ☐ Guide to Protecting the Confidentiality of Personally Identification Information (PII) by the National Institute of Standards & Technology (800-122)

Data processors

- ☐ Data processors selection: key task
- ☐ Audit processes on data processors
- ☐ Accreditation certifications
- ☐ Contract: should detail the data protection issues

Consent and traceability

- ☐ Obligation to be able to prove the reception of the consent
- ☐ Obligation to be able to prove the protection measures on the data
- ☐ Traceability of the accesses to data
- ☐ Validity of the evidences in case of litigation