MEDICAL TECHNOLOGY
Med Lab & INTELLIGENT INFORMATION SYSTEMS

Presentation by Michalis Mantzaris, PhD

Introduction to General Data Protection Regulation (GDPR)

TAXINOMISIS

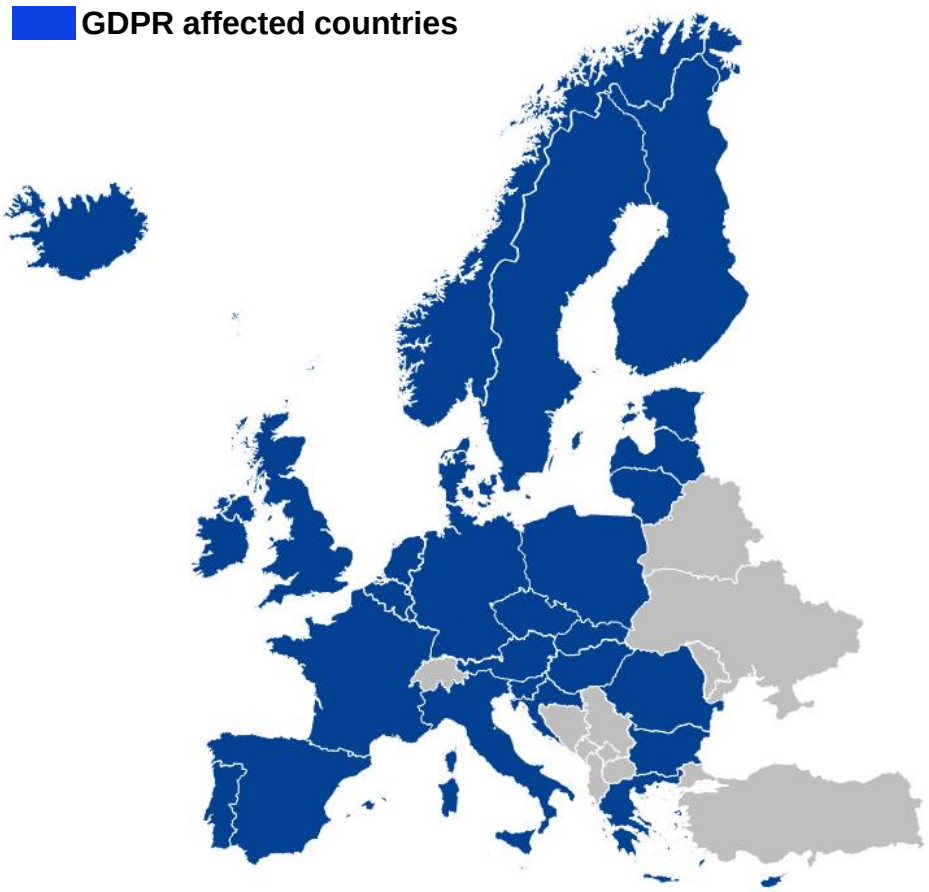
Presentation Structure

- **What is the GDPR?**
  - When and where does it apply?
  - Consisting elements and Guideline provision
  - Key changes and additions compared to the previous EU Data Protection Directive
- **Key definitions in GDPR**
  - Definitions
  - Principles
- **GDPR application in scientific research**
  - Roles, Prospective and Retrospective data, Safeguards
  - A practical “all in one” example of implementation in a research programme.

What is the GDPR?

- The General Data Protection Regulation (GDPR) is the new EU's regulation designed to protect and empower **every subject's data privacy located in the EU** regardless of where the processing is happening.
- GDPR applies to **every organisation located in the EU that processes personal data** regardless of nationality and covers several activities and aspects including data collection, processing, transfer, storage, security and the data subject rights.
- GDPR will be enforced on **May 25th 2018** and non-compliance can be fined up to 4% of annual global turnover or **€20 Million.** Fines will be served by the respective DPAs

GDPR applies to EU and European Economic Area (EEA) members



Austria
Belgium
Bulgaria
Croatia
Cyprus
Czech Republic
Denmark
Estonia
Finland
France
Germany
Greece
Hungary
Iceland (EEA)
Ireland
Italy
Latvia
Liechtenstein (EEA)
Lithuania
Luxembourg
Malta
Netherlands
Norway (EEA)
Poland
Portugal
Romania
Slovakia
Slovenia
Spain
Sweden
United Kingdom (BREXIT, EEA)

GDPR
General Data Protection Regulation

- Every personal data entering or exiting EEA is protected by GDPR

GDPR consisting elements and guidelines

- GDPR comprises **11 chapters** which include **99 Articles** with one or more sub-articles for the protection of personal data
- The 99 Articles were adopted considering **173 Recitals**
- Although Articles and Recitals are complementary to each other, the **Court of Justice of the European Union uses Recitals** to establish any Regulation's or Directive's meaning.
- Guidelines for the consistent implementation of the GDPR is provided by **Article 29 Working Party (WP29)** comprising members of each Member State DPA.
- The WP29 will be renamed to **European Data Protection Board (EDPB)** with enhanced roles on providing guidelines and decisions.

WHAT IS NEW IN THE GDPR?

Key changes to the existing EU Data Protection Directive

- The **Transparency** and **accountability** are now main principles of data protection and **both controllers and processors are liable** under GDPR
- Special provisions for **scientific research**
- Enhanced data subject rights, such as the **right to be forgotten** and the **right to data portability**
- **No need for DPA authorization** but mandatory Data Protection **Impact Assessments (DPIAs)**
- Mandatory appointment of a **Data Protection Officer (DPO)**
- Mandatory procedures for managing **data breaches**
- **European Codes of Conduct**
- **Certification mechanisms** specifically for data protection
- Sanctions and fines.

Key definitions in GDPR

- **Personal data**: any information relating to an identifiable natural person e.g. name, ID, location, online identifier, physical, **health** (Recital 35), **genetic** (Recital 34), biometric, mental, economic, cultural or social data.
- **Genetic data:** personal data relating to the inherited or acquired genetic characteristics of a natural person which **result from the analysis of a biological sample** from the natural person in question, in particular **chromosomal, DNA or RNA analysis**, or from the analysis of another element enabling equivalent information to be obtained.
- **Health data:** 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. **Information derived from the testing or examination of a body part or bodily substance, including from genetic data and biological samples;** and any information on, for example, a disease, disability, disease risk, **medical history**, clinical treatment or the physiological or biomedical state of the data subject independent of its source, for example from a physician or other health professional, a hospital, a medical device or an in vitro diagnostic test.

Key definitions in GDPR

- **Processing:** any operation performed on personal data whether or not by automated means e.g. collection, recording, organization, structuring, storage, alteration, retrieval, consultation, use, disclosure by transmission, dissemination, combination, restriction, erasure or destruction.

- **Pseudonymisation:** the processing of personal data in such a manner that the personal data can no longer be attributed to a person **without the use of additional information** kept separately and secured by means of technical and organisational measures. **Pseudonymized data are still personal data subjected to GDPR.**

- **Anonymous data:** information which does not relate to an identifiable natural person or to personal data rendered anonymous in such a manner that the data subject is not or no longer identifiable. GDPR **does not concern** the processing of such **anonymous information**, including for statistical or research purposes (Recital 26).

Key definitions in GDPR

- **Controller:** the person, authority, or other body which, alone or jointly, determines the purposes and means (**the why and how**) of the processing of personal data.
- **Processor:** a person, authority, or other body which processes personal data on behalf of the controller.
- **Data Protection Officer (DPO):** a staff member or a professional on the basis of a service contract who has **expert knowledge of data protection law and practices**
  - Is able to monitor compliance with GDPR and provide advice
  - Communicates with the supervising authority (DPA)
  - Is accessible to data subjects with regard to the exercise of their rights.

Principles of the GDPR

- ✓ **Lawful, fair and transparent processing** (legal basis e.g. on consent, otherwise purpose compatibility or scientific purpose exemption under appropriate safeguards such as encryption or pheudonymization)
- ✓ **Purpose limitation** (data not further processed in a manner that is incompatible with the initial purposes)
- ✓ **Data minimisation** (limited to what is necessary in relation to initial purposes)
- ✓ **Accuracy** (data updated and rectified where necessary)
- ✓ **Storage limitation** (data kept in a form which permits identification of data subjects for no longer than is necessary for the purposes of the study (exceptions**:** scientific research purposes with the appropriate safeguards including technical and organisational measures required)
- ✓ **Integrity and confidentiality** (protection against unlawful processing, accidental loss, destruction or damage)
- ✓ **Accountability** (controller and processor shall be able to demonstrate compliance with previous points)

GDPR application in scientific research

Data protection by design

- **Controllers:** partners who collect patient data and biological samples.
  - Each controller has full control of the collected data which he has to **pseudonymise** holding the key in separate location.
  - The controller decides “why and how” to process his data. The “how” does not necessarily mean that he would process the data himself, as he can outsource the task to a processor due to his expertise.
- **Processors:** partners who process patient data on behalf of the controllers and under their specific instructions under a **contract**
  - A processor is also liable for the processing of the data
  - A processor can sub-contract part of the processing to a subprocessor **by obtaining controller’s consent** and maintaining liability. Overall control of the data and processing remains to the original controller.

GDPR application in scientific research

Data protection by design

- **Contracts:** Contracts must contain information described in Articles 28,45,47. Contract templates for EU data transfer and Standard Contractual Clauses for non-EU transfers **are available.**
- **Data transfers:** Each controller must implement appropriate pheudonymisation or encryption measures for **data protection by design** (Article 25) and before data is transferred for further processing purposes.
- **Processing records:** Each controller or processor is responsible to maintain a record of processing activities in electronic form with specific information described in Article 30 and provided to supervisor authority or data subject upon request. **Full record templates are available.**

GDPR application in scientific research

Data protection by design

- **Data repositories:** Data should be stored and kept in a form which permits identification of data subjects for no longer than is necessary for the purposes of the study (storage limitation).
  - However, **data may be stored for longer periods** for scientific research purposes with the appropriate safeguards (Article 89, Recital 156).
  - Recital 156 refers to **clinical trials** as a scientific purpose where **processing must comply also with the relevant legislation** such as the ICH GCP guidelines and the EU's Clinical Trial Regulation **witch specify certain archive periods for clinical trials.** This means clinical trials can retain their data even if the data subject requests erasure (**However, the status of observational studies should be addressed**).
  - In addition, appropriate technical and organisational measures for protection against unlawful processing, accidental loss, destruction or damage shall be taken (**data security**) as described in Article 32.

GDPR application in scientific research

Data protection by design

- **Data Protection Officers (DPOs):** Each institution where patient (**health and genetic**) data processing is performed should take appropriate measures to designate a DPO as described in Articles 37, 38, 39.
- **Data Protection Impact Assessment (DPIA):** Controllers (**only**) taking DPO's opinion and advice shall carry out an impact assessment of the risks that may be presented by the processing activities planed, as described in Article 35 (**DPIA templates are available**).
- **Prior Consultation:** If a controller's impact assessment indicates a high risk for data protection, controller shall consult the supervisor authority (DPA), as described in Article 36.
- **Prospective data:** Legal basis for processing in clinical studies is consent. Broader consent in certain research areas (Article 6 and Recital 33) should be useful for future studies. Informed consent procedures must include specific information including the patients' rights (right to withdraw, to access, to rectification, to restriction, to object, to data portability etc) as described in Articles 7, 9, 13, 25, 30, 32.

GDPR application in scientific research

Data protection by design

- **Retrospective data:** Further processing or reuse of retrospective sensitive data from health registries, cohorts and biobanks can be based on consent or broader consent in certain areas of scientific research (Article 6 and Recital 33).
  - If such consent is absent further processing for **scientific purposes** is considered lawful and compatible processing (Article 89 and Recitals 156,157,159).
  - However, data subjects should be informed prior to further processing (Articles 13,14) unless this proves to be impossible or involves a disproportionate effort in particular where processing is carried out for scientific purposes involving a large number of data subjects and data of a certain age (Recital 62). (WP29 guidelines on transparency address this issue and should be considered!)
  - In addition it is important that further processing is coupled with safeguards such as **pseudonymisation** separated storage of codes and respect of ethical standards in the field (Article 89 and Recital 156). Reference to initial ethical approvals from competent ethical committees shall be provided upon request.
  - **Importantly, if data are anonymized GDPR does not apply.**

GDPR application in scientific research

Data protection by design

- **Appropriate safeguards under scientific exemption :** Data processing for scientific purposes shall be subjected to appropriate organisational and technical safeguards and data protection **by design**.
  - Although, **pheudonymisation** is emphasized as a safeguard, GDPR does not elaborate further on such safeguards, **leaving it to Member States** to adopt adequate measures and conditions for processing sensitive data for research purposes.
  - WP29 provides some **safeguards examples for data security** including the introduction of Information Security Managements Systems (e.g., **ISO/IEC standards**) based on the analysis of information resources and underlying threats, measures for **cryptographic protection during storage and transfer** of sensitive data, requirements for authentication and authorization, physical and logical access to data, access logging and others.

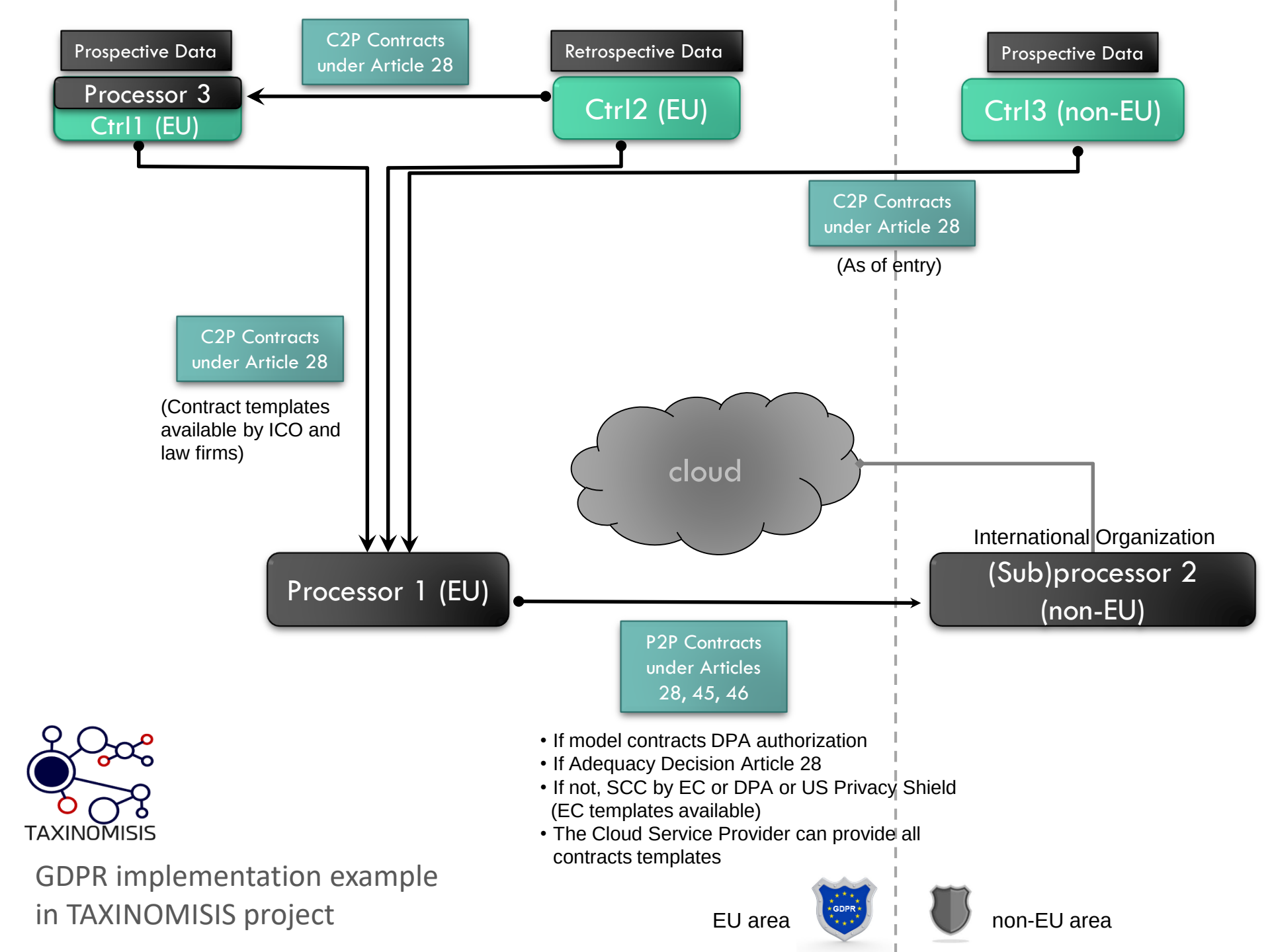
GDPR application in scientific research

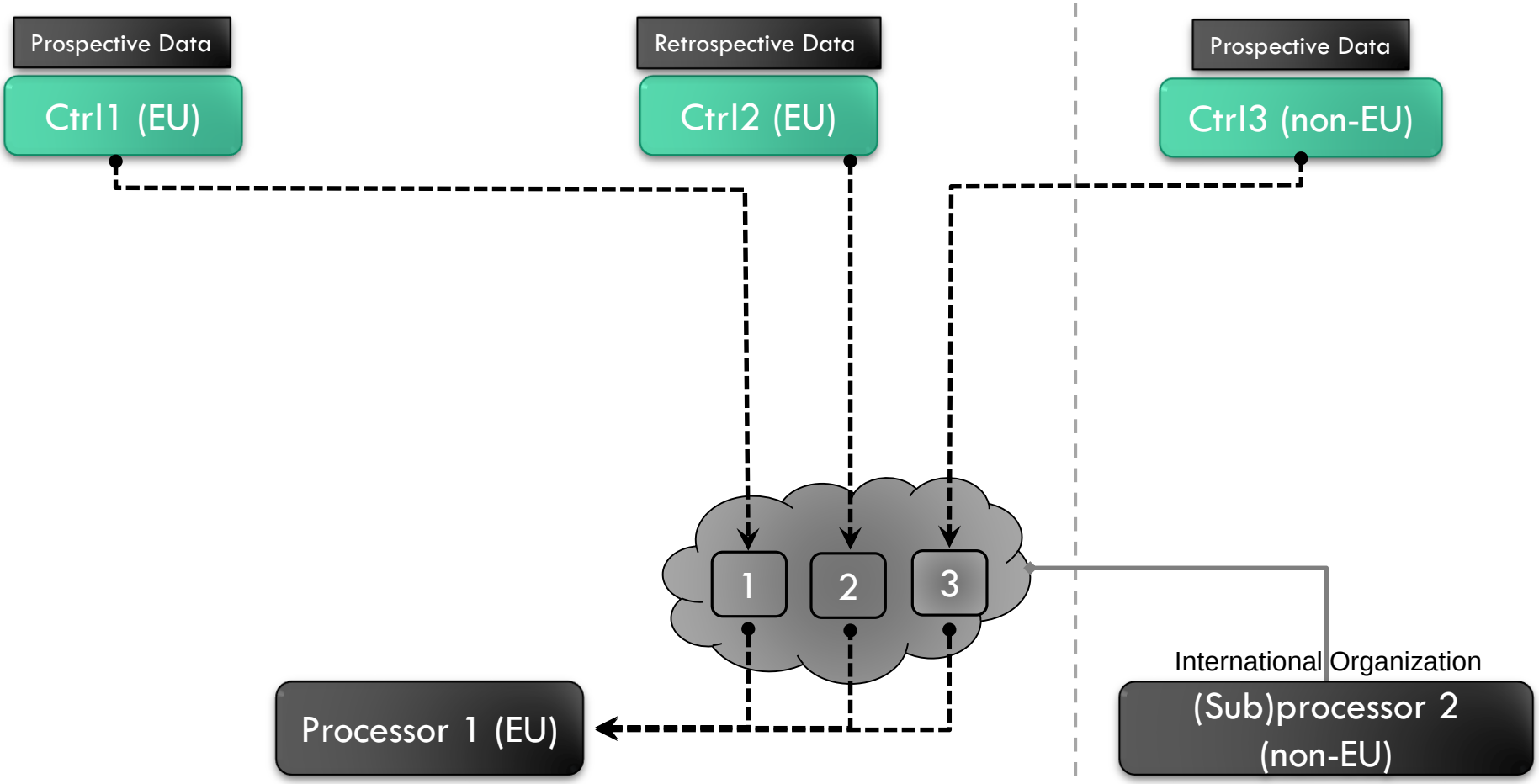
Data protection by design

- **Exemptions regarding specific <u>data subject's rights</u>:** According to Article 89 certain rights of data subjects could not apply if the EU or **member states laws** provide, under certain conditions, legitimate exceptions for **research purposes**. Member States should provide, under specific conditions and subject to appropriate safeguards, specifications and derogations with regard to the rights to rectification, to erasure, to be forgotten, to restriction of processing, and to object as far as these rights render impossible or impair the achievements of the research purposes.

- **Data breach:** Mandatory procedures for managing **data breaches** including communication of the breach to DPA and data subject (Articles 33, 34)**.**

- **Codes of conduct and Certification:** Supervisor authorities **should** establish codes of contacts and data protection certification mechanisms for demonstrating compliance with GDPR.


Prospective Data
Processor 3
Ctrl1 (EU)
C2P Contracts under Article 28
Retrospective Data
Ctrl2 (EU)
Prospective Data
Ctrl3 (non-EU)
C2P Contracts under Article 28
(As of entry)
C2P Contracts under Article 28
(Contract templates available by ICO and law firms)
cloud
International Organization
Processor 1 (EU)
(Sub)processor 2 (non-EU)
P2P Contracts under Articles 28, 45, 46
• If model contracts DPA authorization
• If Adequacy Decision Article 28
• If not, SCC by EC or DPA or US Privacy Shield (EC templates available)
• The Cloud Service Provider can provide all contracts templates
TAXINOMISIS
GDPR implementation example in TAXINOMISIS project
EU area
non-EU area



TAXINOMISIS

GDPR implementation example
in TAXINOMISIS project

EU area

non-EU area

Prospective Data

Ctrl1 (EU)

Data protection by design
- Legal Basis (consent)
- Contracts with Processor
- Safeguards (pseudonymization)
- Records of all processing activities
- DPO (genetic & health data)
- **DPIA**

Retrospective Data

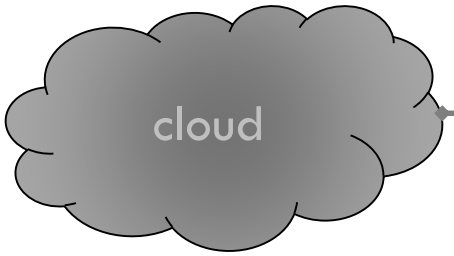
Ctrl2 (EU)

Data protection by design
- Further processing Legal Basis (Broad consent or scientific exemption)
- Contracts with Processors
- Safeguards (pseudonymization)
- Records of all processing activities
- DPO (genetic & health data)
- **DPIA**
- **Information to data subjects**

Prospective Data

Ctrl3 (non-EU)

Data protection by design
- Legal Basis (consent)
- Contracts with Processor
- Safeguards (pseudonymization)
- **Applicable Law**



Processor 1 (EU)

Data protection by design
- Legal Basis for each dataset
- Contracts with Controllers
- **Contract with subprocessor**
- Safeguards (**Access management**)
- Records of all processing activities
- DPO (genetic & health data)
- **Deletion of personal data after the end of the processing**

International Organization

(Sub)processor 2 (non-EU)

Data protection by design
- DPO
- **Contract with processor**
- Safeguards (security and backup)
- **Data storage within EU**
- Records of all processing activities
- Deletion of personal data after the end of the contract.
- **(EU representative)**

TAXINOMISIS

GDPR implementation example in TAXINOMISIS project

EU area

non-EU area

Prospective Data

Ctrl1 (EU)

Data protection by design

1. Preparation of clinical study protocol & Informed Consent procedures (Articles 7,9,13,25,30,32)
2. Preparation of Contract with processor (Article 28) including controller consent for subprocessor
3. DPO consultation on protocol, consent form & contract (Article 39)
4. Clinical study protocol Ethical Approval
5. Signed Contract with processor
6. Documentation of a DPIA (If high risk, prior consultation by DPA, Article 35)
7. Signed Informed Consent & Data Collection
8. Pseudonymization with code separation (Article 25)
9. Data transfer to processor (Article 46) via the cloud
10. Records of all processing activities including purpose, data categories, transfers and safeguards (Article 30) for audits and data subjects upon request.

Retrospective Data

GDPR implementation example in TAXINOMISIS project

TAXINOMISIS

Ctrl2 (EU)

Data protection by design

- **If data anonymized, GDPR does not apply (data can be transferred without the following steps).**

1. If not anonymous, further processing legal basis (Specific/Broad consent or scientific purpose exemption)
2. Further processing information to data subjects unless scientific purpose exception (Articles 13,14,89)
3. Preparation of Contract with processor including controller consent for subprocessor
4. DPO consultation on legal basis & contract
5. Signed Contract with processor
6. Documentation of a DPIA (If high risk, prior consultation by DPA)
7. Pseudonymization with code separation
8. Data transfer to processor via the cloud
9. Records of all processing activities including purpose, data categories, transfers and safeguards for audits and data subjects upon request.

Processor 1 (EU)

Protection by design

1. Legal Basis for each dataset
2. DPO consultation on contracts with controllers and subprocessor
3. Signed Contracts with Controllers including consent for subprocessor (Article
4. Signed Contract with subprocessor outsourcing data storage & security but maintaining liable for personal data processing
5. Safeguards (Cloud Access management)
6. Use of data via the cloud
7. Deletion of personal data after the end of the processing
8. Records of all processing activities including purpose, data categories, transfers and safeguards for audits and data subjects upon request.

Subprocessor 2 (non-EU)

Protection by design

1. Signed Contract with processor for data storage & security within EU.
2. Safeguards & liability (Cloud security and backup)
3. Deletion of personal data after the end of the processing
4. Records of all processing activities for data storage and security

EU area

non-EU area

Concluding Remarks

- GDPR aims at harmonization of data protection laws in EU but this would certainly need a lot of effort from each party involved.
- Every organisation involved in the processing of personal data should prioritize the implementation of appropriate organisational and technical data protection measures including the appointment of a Data Protection Officer (DPO).
- Although GDPR could be viewed as an obstacle in certain areas of scientific research, according to Article 79 of the European Treaty, free flow of data and the formation of a European Area of research is of paramount importance.
- For this reason new guidelines from EDPB, codes of conduct and certification mechanisms are tools to overcome such obstacles and would be urgently needed upon application of the DGPR after 25th of May.

End of Presentation