GDPR implementation…

…and its impact on the conduct of clinical trials in the Nordic region

Alan Yeomans Quality Manager, PCG Solution ,Viedoc

Presentation Agenda

- Important GDPR concepts
- Applicable regulations
- Data controller / Data Processor
- CTR ICF vs GDPR consent
- Legal basis for data processing
- Subjects' rights
- Pseudonymisation
- Accountability
- Data transfers
- Code of Conduct

Reminder… What is personal data?

GDPR art. 1 §1:

‘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

Applicable regulations

- GDPR – EU Regulation 2016/679, applicable since 2018-05-25 (2018-07-20 in Norway)
- CTR – EU Regulation 2014/536, not yet applicable (2020)
- Opinion 3 – European Data Protection Board opinion, dated 2019-01-23
- Recommendation on the protection of health-related data – European Council Committee of Ministers CM/Rec(2019)2, dated 2019-03-27
- Question and Answers on the interplay between the Clinical Trials Regulation and the General Data Protection Regulation – EC, Directorate-General for Health and Food Safety, dated 2019-04-10

Data Controller, Data Processor

- GDPR – the data controller is the natural or legal person who defines the purpose and the means of the data processing
- Clinical Research – the purpose and means are defined in the study protocol, which GCP defines as the responsibility of the sponsor
- Investigator (site) collects patient data for the purpose of patient care
- Sponsor – Data Controller for the clinical trial
- Investigator – Data Processor for the clinical trial
- Investigator – Data Controller for patient care (in part using the same data)

Possible conflicts?

- The sponsor does not always define the purpose and means – sometimes delegated to a CRO
- Joint controllers?
- No clear rules
- Should be covered by contracts

Informed Consent

GDPR Consent / CTR Informed Consent

- Data subject provides consent to data processing
  Can be supplied by authorised caretakers in more cases than GDPR
- Consent gives more legal rights to subject
  Portability not a legal right in Clinical Trials, access, correction and deletion also restricted
- Withdrawal of consent for data processing stops further processing even of already collected data (exceptions exist)
  Withdrawal does not affect the legal right to process data already collected
- Must be provided by all users in a clinical trial (including site and sponsor personnel)
  Consent is typically only formally provided by data subjects

Legal basis - CTR

- Gather reliable and robust data
- Report results to the authority
- AE and SAE reporting
- ALCOA+ (Attributable, Legible, Contemporaneous, Original, , Accurate, Complete, Consistent, Enduring, Available)
- investigator must record, process, store and handle data in such a way that it can be accurately reported, interpreted and verified while confidentiality remain protected
- Archive data for at least 25 years
- Allow inspectors access to the data
- GDPR applies to the processing of the data

Conclusions

Legal basis for processing of personal data in CTR:

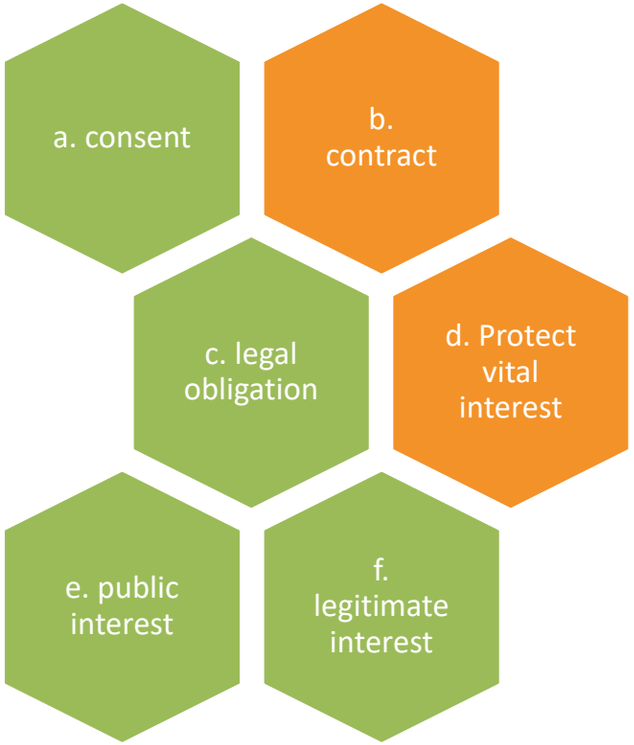
- Processing activities related to research
  Purpose: build robust and reliable data
- Processing activities related to safety and reliability
  Purpose: ensure patient safety and reliability

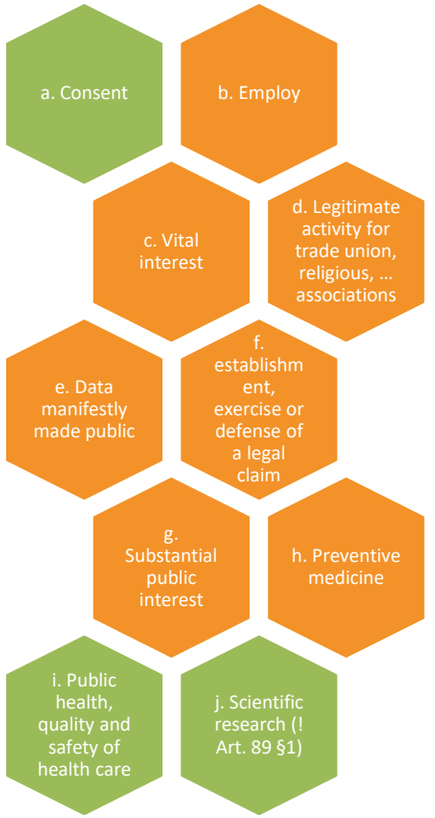
Legal basis - GDPR

Meaning of consent in CTR and GDPR differs

- Different processing for different purposes
  - Different legal bases
- GDPR Article 6 provides 6 legal grounds for processing personal data
- GDPR Article 9 forbids the processing of sensitive data (exceptions exist)
  - One legal ground under Article 6 required and one exception under Article 9 required

GDPR legal grounds and exceptions for sensitive data





Applicable Legal Grounds in GDPR (1 of 4)

a. <u>Consent</u>

The data subject has given consent to the processing of his or her personal data for one or more specific purposes

- Must be freely given, explicit, unambiguous
- Must be given for each processing activity that has a different purpose from that covered by the original consent

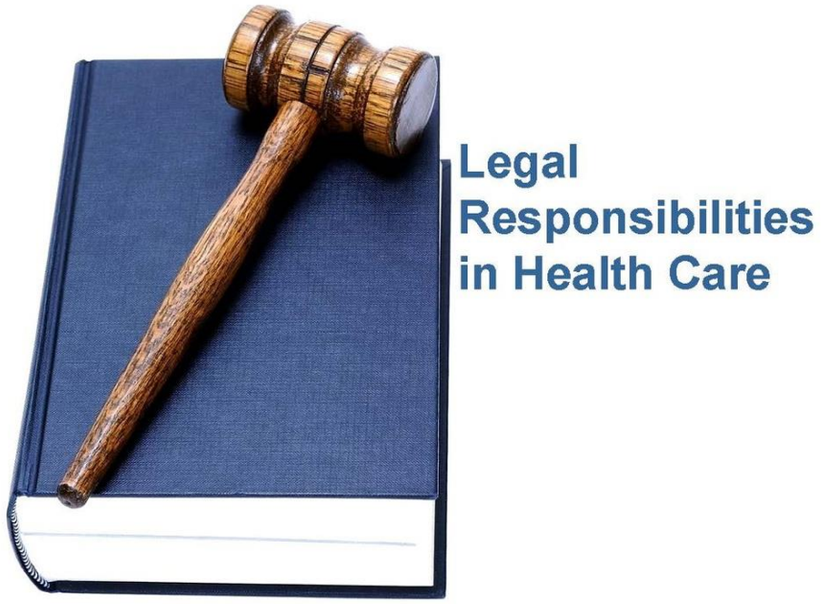
Applicable Legal Grounds in GDPR (2 of 4)

c. <u>Legal Obligation</u>

Processing is necessary for compliance with a legal obligation to which the controller is subject

- Should be used for all processing activities related to safety and reliability:

- Safety reporting to sponsor and authorities
- Reporting of CT results to authorities
- Inspections
- Archiving



Applicable Legal Grounds in GDPR (3 of 4)

e. <u>Public Interest</u>

Processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller

- Should be used for the processing of data related to research
- To be used when conduct of CT directly falls within tasks and missions vested in a public or private body by EU or national law

=> Public institutions / universities

Applicable Legal Grounds in GDPR (4 of 4)

f. <u>Legitimate Interest</u>

Processing is necessary for the purposes of the legitimate interests pursued by the controller …

- Should be used for the processing of data related to research
- When the public interest cannot be met and when consent if not the appropriate legal basis

=> Private companies

Appropriate exceptions for processing sensitive data

Legal ground	Exception for sensitive data
§6(a): Consent	§9(a): Consent
§6(c): Comply with a legal obligation	§9(i): processing is necessary for reasons of public interest in the area of public health, … ensuring high standards of quality and safety of health care and of medicinal products or medical devices, …
§6(e): Public interest	§9(i): processing is necessary for reasons of public interest in the area of public health, … ensuring high standards of quality and safety of health care and of medicinal products or medical devices, … Or §9(j): processing is necessary for …, scientific … research purposes … in accordance with Article 89(1)
§6(f): Legitimate interest	

Considerations about Legal Basis for Data Processing

- Imbalance of power under GDPR?
  - Consent could not be freely given for data processing => how can it be given for experimental treatment, which involves potential higher risks for patients?
- CTR in member states / Ethics Committees
  - Many Ethics Committees still consider CTR informed consent as a legal basis for data processing in clinical trials. We need to help improve their understanding of GDPR.

More considerations…

- (CTR) Consent withdrawal
  - CTR art 28 §3: ICF withdrawal does not affect data processing on data collected before its withdrawal
  - GDPR art 17 §1 (b): … when there is no other legal ground…
  - GDPR art 17 §1(c): … there are no overriding legitimate grounds for the processing…

- and the Council of Europe says (section 15.10.):
  - Where a data subject withdraws from a scientific research project, his / her health-related data processed in the context of that research should be destroyed or anonymised in a manner which does not compromise the scientific validity of the research and the data subject should be informed accordingly.
  - Is this a contradiction of both CTR and GDPR? Agree for secondary use, not for primary use

Who is a data subject?

CTR

- Subjects == Patients
- Subjects are recruited to participate in a clinical trial
- Subjects participating in a clinical trial should be representative of the population addressed by the trial
- Extensive set of rules for the protection of subjects

GDPR

- Applies to the processing of personal data of data subjects who are in the EU
- Applies to all trial participants, i.e. patients, investigators, site staff, monitors, data managers, etc.
- Applies to any participant in the trial whose personal data (name, site affiliation, email, etc.) is processed during the trial

Pseudonymisation

- Consists of replacing one attribute (typically a unique attribute) in a record by another. The natural person is still likely to be identified indirectly
- Pseudonymisation reduces the linkability of a dataset with the original identity of a data subject
- Re-identification – the process of analysing data or combining it with other data with the result that individuals become identifiable

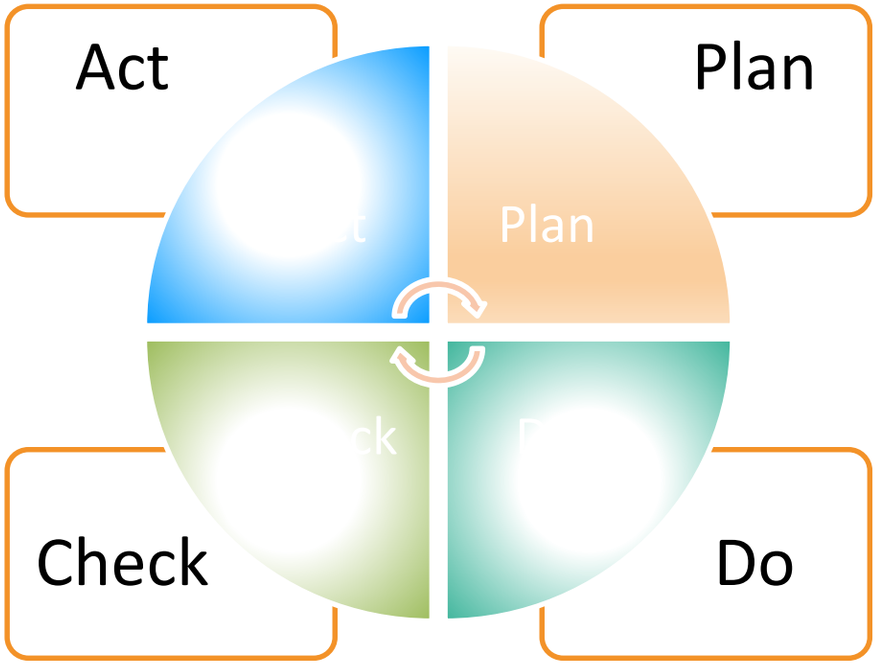
Clinical Research and Pseudonymisation

- We collect pseudonymised sensitive data (reversible pseudonymisation)
  - Sometimes with potentially high re-identification risks (prevalence of disease in standard population, extent of collected variables, …)

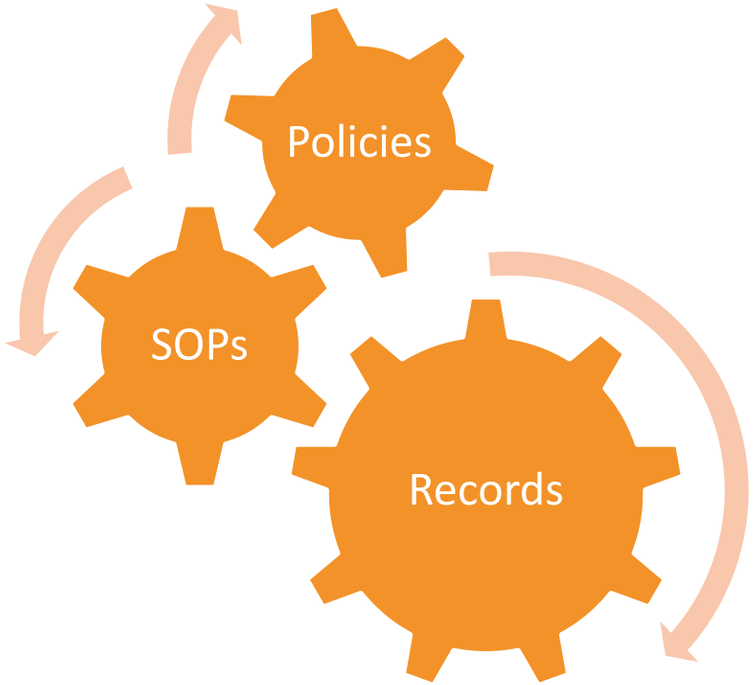
- We should employ a number of mitigation methods:
  - Always check compliance between protocol objectives and collected CRF variables.
    - Objective: limit the collected variable to strictly answer protocol (GCP and GDPR)
  - Always check the extent of collected variables
    - Example: Date of birth, medical history (dates, …)
    - Objective: minimize the re-identification risks
  - Minimise as much as possible free text comments

Accountability

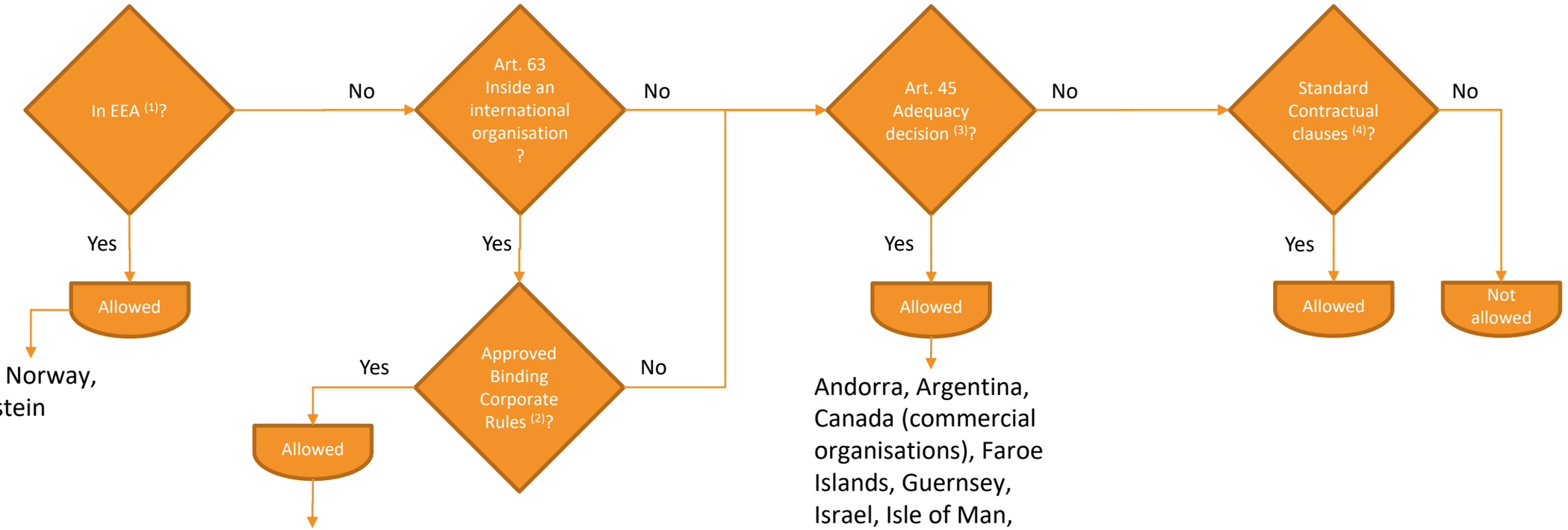
GDPR refers to a “Plan – Do – Check – Act” model



ISO27001 is the best model integrating all GDPR accountability requirements
ISMS is very similar to QMS: management review and audits



Data Transfers



See:
https://ec.europa.eu/newsroom/article29/document.cfm?doc_id=50116

Code of Conduct

- Adherence to a code of conduct is an explicit way to demonstrate GDPR compliance – promoted by GDPR
- Helps you understand what needs to be done to conduct GDPR compliant processing
- EUCROF initiative on CoC
  - EUCROF is working on a Code of Conduct for Clinical Research
  - The CoC must answer practical questions in the field of Clinical Research

EUCROF Code of Conduct

- Scope
  - Setup and conduct of clinical research studies from phase I to IV. It will also cover non regulated research and secondary use of data
- Stakeholders
  - CNIL acts as Lead DPA for all of EDPB
  - EFPIA will act as CoC reviewer of the draft version
  - Patients Association (LEEM) will review the draft version
  - Looking for MedTech Europe contact for further discussions
- Adherence
  - Adherence to the code of conduct will need to be certified by accredited independent body
- EUCROF is setting up a governance model for certification

More information about the EUCROF CoC

5th European Conference on Clinical Research

- 10-11 February 2020, Amsterdam, The Netherlands
- Session on 10-FEB-2020:
  - “GDPR in Clinical Trials, challenges in implementation” by a CNIL representative
- Session on 11-FEB-2020:
  - Stakeholder interactive (in-depth) discussions on a pragmatic implementation of the Regulation

Discussion

Alan Yeomans
Alan.Yeomans@viedoc.com