DATA PROTECTION FOR RESEARCHERS: GDPR & HRR ESSENTIALS FOR HSE RESEARCHERS AND SOME PRACTICAL IMPLICATIONS

Practical implications:
Mandatory information to provide in controller's:
- *Privacy Notice,*
- *Information Notice/Leaflets*

Sharing data with another Organisation must have explicit consent of the data subject. Processing purpose must be compatible with purpose agreed by participant

You should never be coerced into sharing personal/sensitive data with another organisation

1. to **Be Informed** by controllers at time data are obtained **on intended data processing and their rights** *(limited exemptions can apply)*
2. of **Rectification** of inaccurate data
3. of **Erasure** *('to be forgotten')*
4. to lodge a **Complaint**
5. **Data portability**
6. **To object**
7. **Not to be subject to automated processing** *incl. profiling*
8. **Not to allow you to share their data with a Third Party**

Data Subject's Rights

Apply to processing of Personal Data of data subjects based/registered in the EU

- Any data that can identify an individual
- Additional protection for special categories(e.g. Health data)

Personal Data incl. special categories or 'Sensitive Data' (*e.g. Health Data, medical records*) :
Meaning: Directly or Indirectly Identified or Identifiable Person
WHAT: Data includes: *Name, ID, location, online ID, Physical, physiological, genetic, mental, health care services identifying health status, economic, cultural, social factors (Art4.)*

NOT Processing Personal Data and/or sensitive Data :
Meaning: **NOT** Directly or Indirectly Identified or Identifiable Person
WHAT: **Epidemiological Data:** Population exposure levels and health effects values observed from samples: **Aggregated Data where no individual can be singled-out**

Practical implications:
Design of your research protocols and identify who acts as data Controller and data Processor

Data Controller : *Organisation that employs the investigator who determines the purpose and the manner in which data are processed (e.g. Why & How). Responsible for the data and highest level of compliance (GDPR, HRR). Investigator for the Controller is responsible for the day-to-day compliance to GDPR-HRR-Organisation policies*

Data Processor: *Organisation that employs the investigator who 'executes' the processing as directed by Data Controller [Data processor & Data controller can be the same person in certain cases] . Investigator for the Processor must* solely process data in compliance with protocols designed by the Controller

HSE staff with a dual academic appointment *must confirm which Organisation they represent and confirm approval with this Organisation*

⚠ *Can be complex (controller clinical data not same as controller project data; joint controllers, separate controllers…)* ***confirm findings with your HSE DDPO [link to list]. For further guidance EDPB***

Conduct a **DPIA Assessment Tool** and if required a **DPIA when drafting your protocols**
Exceptions may apply: DPIA mandatory (large scale of sensitive data; systematic/extensive profiling, some data linkage…) or DPIA not required (no risk, DPC authorisation,…) (DPC)

Privacy by design *: compliance to be factored when you design your research (means for processing) and at time of processing,* ***and by default*** *(measure only data necessary for purpose are processed*

Ethics Approval by a REC before starting your research. Project. Ethics Application covers complementary ethics-GDPR/HRR requirements

Contractual requirements to be in place before you start, incl. data processing, data sharing agreement, clinical trial agreement, etc.

GDPR *[DPC]*

'HRR' Or DPA 2018 (S36(2) (HR) Regulation

Additional measures specific to health research

Accountability

1. **DPO & DDPO**
2. **Controller (***role & legal responsibilities)*
3. **Processor** *role & legal responsibilities)*

1. **Appropriate governance to ensure compliance:**
   - *Security measures*
   - *Dealing with breaches*
   - *Code of practice*
   - *Policies & Training*
   - *Records, evidence of processing*
   - *DPIA Assessment & DPIA*
   - *Ethics approval by REC*
   - *Required contracts (processor; DSA, joint controller,….)*

Additionally:
- Be compliant with rules on data processing of data of EU data subjects outside of the EEA (European Economic Area)

Data protection **Principles**

Processing of Personal Data must:
1. be **Fair** *(information on processes, their GDPR/HRR compliance & their risks),* **Transparent (***information accessible before start & during research),* **Lawful** *(lawful basis)*
2. **for a Specific Purpose(s)** *('purpose limitation', i.e. purposes defined in your research)*
3. be **Relevant & Limited** *(to what is necessary for the purposes)* ('data minimisation')
4. be **Accurate** *(i.e. data must be up-to-date)*
5. **Permits retention solely** for the purposes and duration needed for your research *(incl. retention for publication/research audit purpose)*
6. be **Secured** *(mechanisms and processes to manage/monitor access, destruction, damages)*
7. ensure **Accountability** *& compliance Controller must demonstrate GDPR/HRR compliance)*

Practical implications:
- Processing activities shall be clearly defined in your research protocols e.g. sectioned to identify:
- data processing requirements and timescales,
- specific purposes,
- roles and responsibilities (controller/processor)
- risks (breaches) to data subjects
- information mechanisms to research participants

- Data collected for a specific purpose cannot subsequently be used for another purpose

Lawful Basis

1. **Consent:** Free, Informed, Specific, unambiguous, Explicit *(i.e.. adequately captured)*
2. **Contract** with the data subject**, legitimate activities**
3. **Legal Obligation** (on the controller)
4. **Vital interests** data subject or another person)
5. **Substantial Public interest**
6. **Legitimate interests** pursued by the controller

Practical implications:
Explicit Consent required for health research

Exceptions:
- HRR exemption, or
- HRB CDC Declaration [HRCDC] based on GPR Art 9 *(g), (h), (I), or (j) – confirm with DDPO if needed*

Consent /Ethics Algorithms

Data Algorithms: (Anonymisation & Sharing, scenario)

Laura Méchineau-Phelan, HSE R&D, Strategic Planning and Transformation