BBMRI-ERIC
Biobanking and
BioMolecular resources
Research Infrastructure

Draft GDPR and health-related scientific research:
Where do we stand with the EU Council ?

Gauthier Chassang, Lawyer
BIOBANQUES Infrastructure, INSERM US013, France

Data Protection for health: Enabling Research for Health
Brussels, 28 January 2015

Inserm
Institut national
de la santé et de la recherche médicale

BIOBANQUES

www.bbmri-eric.eu

Where are we now?

- The amended text voted by the EU Parliament the 12 March 2014 is being revised by the Council – next Council vote: March 2015
- Ministers have an important role to play now
- Last available versions – partial readings:
  - Interinstitutional file 2012/0011 (COD),
    - November 2014 (Chap. IX)
    - December 2014 (full integrated text, except Article 81)
  - Work still in progress
- What will we tackle today:
  - Concerns and fears expressed so far by the scientific community regarding proposed LIBE amendments
  - Current but temporary Council version of the articles applying to health data processing and scientific research
  - What could we / should we do for facilitating improvements?

Concerns from the scientific community

• Expressed by several stakeholders after the draft amendments published by the Parliament (Albreicht Report):

E.g.

- Wellcome Trust, Inserm…
- EURORDIS…
- FEAM…
- Science Europe…
- PHG Foundation…

• Several warning letters and some proposals have been published in 2013-2014.

- Concerns about targeted research activities including personal sensitive data processing (health data, genetic, biometric, ethnic…):
  - Scientific, statistical, historical health-related researches *(e.g. fundamental or applied public/private researches; clinical trials; retrospective researches…)*
  - Biobanking *(human samples / DNA and RNA)*
  - Registries *(systematic and continuous processing of medico-economical data e.g cancer, HIV, CVD)* and archived data
  - Health-related ICTs
- Some topics of concerns:
  - Informed consent *(systematicity / broadness)*, and reuses of data/databases
  - High public interest *(actionable waiver of data subjects' rights)*
  - Balance between data subjects' rights and scientific legitimate processing *(e.g right to erasure / to be forgotten; portability etc.)*
  - Measures/Tools for alleviating administrative burdens
- **Do the uncertainties remain with the last available version of the GDPR dated December 2014?**

Concern 1: Informed consent…

- **Advantages of broad consent in research // ongoing debates on ELSI.**
- **Does the EU Council version of the Regulation forbids broad consent and obliges only restricted consent ?**

  - By principle, personal data must be collected for specified, explicit and legitimate purposes; for one or more specific (research) purposes, *Article 5(1)(b) and Article 6(1)(a).*
  - Consent remains an option to privilege for legitimating the processing of sensitive personal data under *Article 6(1)(a), Article 9(2)(h) and (i),* same within the *Clinical Trial Regulation n°536/2014.* Other means from National or EU law can be used.
  - "The processing of special categories of personal data concerning health may be necessary for reasons of public interest in the areas of public health, without consent of the data subject. This processing is subject to suitable and specific measures so as to protect the rights and freedoms of individuals". *Recital 42b)*
  - The Council proposes to add: "[…]as an independent legitimate legal basis and in order to facilitate scientific research, personal data can be processed for scientific purposes subject to appropriate conditions and safeguards set out in Member State or Union law. Hence consent from the data subject should not be necessary in each case", *Recital 125aa).*

Thus:

- Nothing requires to obtain data subject's consent for each and every single processing / purpose

- Nothing forbids « broad consent » practice in itself… provided that

- Conditions for a lawful (broad) consent: *(Dec.2014 version)*
  - Fairness and transparency. Information will be crucial, *Article 14*.
  - Proportionality and appropriate safeguards, *Article 5(1)(c) and 83*. Innovative governance mechanisms are already worked out to accompany broad uses of personal data in research and broad consent (e.g. dynamic consent).
  - "Consent should be given unambiguously by any appropriate method enabling a freely-given, specific and informed indication of the data subject's wishes, […]. Silence or inactivity should therefore not constitute consent. […] Consent should cover all processing activities carried out for the same purpose or purposes. When the processing has multiple purposes, unambiguous consent should be granted for all of the processing purposes. […]." *Recital 25.*
  - Right to withdraw at any time *Article 7*.

- *Article 81* on personal health data processing for health-related purposes *(medicine; health service management; public health threats)* as adopted by the EU Parliament in 2013 requires additional expertises.

  Possible full deletion by the EU Council; only general principles would be kept in *Article 9(2) and 9(4) (Dec. 2014 version)*.

Reminder: within the EU Parliament version *(March 2013)*:

- Consent was an obligation to process personal health data for scientific research *Article 81 2)* **but**
- Potential exceptions to consent were possible where justified on the ground of National law for research that serves a "high public interest", for data at least pseudonymised *Article 81 2a)* **and provided that**
- Art.83 laying down specific conditions for research processing was respected.

- Art.83 has been deeply reviewed by the Council and does not anymore contains technical rules for the management of identifiers. **Proposal:** reintroduce Art.83(1)(b) from the EU Parliament version.

…and for the reuses of data

- **Does the EU Council version allows the reuses of existing data for other purposes than the original ones ?**
  - A crucial question for biobanks and health registries to reach their full potential for research.
  - General rule: the controller, DPO, NDPA shall perform a compatibility test

    "In order to ascertain whether a purpose of further processing is compatible with the one for which the data are initially collected, the controller shall take into account, inter alia :
    - (a) any link between the purposes for which the data have been collected and the purposes of the intended further processing;
    - (b) the context in which the data have been collected;
    - (c) the nature of the personal data;
    - (d) the possible consequences of the intended further processing for data subjects;
    - (e) the existence of appropriate safeguards" . *Article 6(3a)*
  - Where the purpose of the further processing is incompatible with the one for which the data have been collected, the further processing shall have a legal basis in at least one of the grounds referred in Article 6 (1) a) to e). This include processing for protecting vital interest or for public interest.

Concern 2: High public interest

• ***Reminder:*** Within the EU Parliament version *Article 81 2a)*, MS law could fix exceptions to consent requirement in order to process personal health data for research that serves a "high public interest". This new notion was not understood and criticised as unactionable.

• The EU Council version does not yet contain Article 81 but does not anymore refers to high public interest. It keeps the idea of exemptions but it comes back to the wording used by the Directive 95/46:

"Derogating from the prohibition on processing sensitive categories of data should also be allowed if done by a law, and subject to suitable safeguards, so as to protect personal data and other fundamental rights, where important grounds of public interest so justify and in particular for health purposes, including public health and social protection and the management of health-care services […], or for historical, statistical and scientific (...) purposes". *Recital 42*

- Therefore it makes quite clear that scientific research is an important public interest that can be recognised by the law and that must be subject to suitable safeguards for waiving certain data subject's rights
- Will this notion be used in the context of the new Article 81?

Concern 3: Balance between data subjects' rights / necessities of scientific research

- **Does the EU Council version keeps data subjects' rights in research settings as strong as they were perceived?**

- The EU Council keeps the risk-based approach to restrict processing and impose obligations/rights.
- The *new Article 83* is entirely dedicated to **specific derogations** applying to data subjects' right in the processing for archiving, scientific, statistical and historical purposes.

Conditions:

- must be necessary for the fulfilment of the specific purposes and
- be subject to appropriate safeguards fixed by EU or MS law:
  - Application of the technological and/or organisational protection measures planned by the Regulation, such as pseudonymising the data
  - Respect of the data minimisation principle
  - Respect of the proportionality and necessity principles,
  - "Unless those measures prevent achieving the purpose of the processing and such purpose cannot be otherwise fulfilled within reasonable means". *Article 83 2)*

- **Exceptions for scientific, statistical and historical purposes:**
  - Right to information where the data have not been obtained from the data subjects *Article 14a(1) et (2)*
  - Right of access *Article 15*
  - Right to rectification *Article 16*
  - Right to be forgotten and to erasure *Article 17*
  - Right to restrict the processing *Article 17a)*
  - Right to notification regarding rectification, erasure, restriction *Article 17b)*
  - Right to data portability *Article 18*
  - Right to oppose to the processing *Article 19*

- **Additional exceptions for archiving processing in the public interest (e.g. health registries)**
  - Data protection by default and by design *Article 23*
  - Communication of personal data breach to the data subject *Article 32*
  - Data protection impact assessment *Article 33*
  - Some corrective powers to be implemented by NDPA *Article 53 (1b)(d) and (e)*

- **Are we not now in a disproportionate imbalance?**
- **Could we not agree on community-based good practices using ICTs to better balance interests and respect transparency?**

Proposals:

- Data subjects should keep, **at least, their right to object and their right to access data** in case of personal data processing for research or archiving purposes
- **(*Cost-effective*) Solutions can be found to respect transparency for archiving, as good governance practice** (e.g. public notification of personal data breaches through websites)

Concern 4: Alleviation of administrative burdens

- One stop-shop for processing taking place in several MS *Article 51(a) and (b),* NDPA cooperation *Article 54* and mutual assistance *Article 55.*
- DPIA for high risk processing; identification and mitigation of the risk. Will still be mandatory for processing sensitive data **except** if MS law deems that it is not useful, *Article 33 and 33(5).*
- Prior NDPA consultation remains for high risk processing according to DPIA results *Art34(7)(a).*
- Recording of data processing operations remains *Article 28*
- Designation of a DPO becomes a voluntary process. *Article 35*

DE, HU and AT would have preferred to define cases of a mandatory appointment in the Regulation itself and may want to revert to this issue at a later stage.
COM reservation on optional nature and deletion of points a) to c) mentioning criteria for mandatory designation.

- Code of conducts/certifications may be used to demonstrate compliance to the GDPR regarding the controller/processor/representative in the EU, *e.g. Article 22(2a) and Article 33(3a)*

Proposals:

- **Exception to DPIA for processing sensitive data should be deleted** or very restrictively specified; Article 32a of the EU Parliament version should be used in order to elaborate harmonised and practical rules.
- **Cases of a mandatory appointment of a DPO should be defined within the Regulation.** DPO must be regarded as an enabler, it is an important mean to enforce data protection, to assist researchers and to structure the ERA.

What could/should we do?

Whereas:

- The Council version of the text needs more works concerning health and research personal data processing but expressed concerns seems to have been considered.
- The role of National laws is (too much) emphasised

We could/should act:

- Towards National Ministers, Parliaments and competent authorities (information about the EU Council works and any positions adopted)
- Towards stakeholders with existing infrastructures and networks (e.g. BBMRI-ERIC) for informing but also for adopting positions before March 2015

In order to:

- Identify still existing issues (if any) and formulate concrete proposals.
- Find topics and rules on which harmonisation should be reached to structure the ERA
- Find topics where harmonisation is not desirable due to ELSI and explain how we could reach sufficient coordination.

Acknowledgements

- Anne Cambon Thomsen, INSERM, France
- Jan-Eric Litton, BBMRI-ERIC, Austria
- Michaela Mayrhofer, BBMRI-ERIC, Austria
- Declan Kirrane, Intelligence in Science (ISC), Belgium
- ISC organising staff, Belgium

Discussions?

Contact: gauthier.chassang@gmail.com

www.bbmri-eric.eu

www.biobanques.eu

THANK YOU !