BBMRI-ERIC

MAKING NEW TREATMENTS POSSIBLE

BBMRI-ERIC WEBINAR SERIES #2

NOTE

THIS WEBINAR IS BEING RECORDED!

BBMRI-ERIC

MAKING NEW TREAT MENTS POSSIBLE

ANONYMISATION/PSEUDONYMISATION UNDER GDPR

IRENE SCHLÜNDER

WHY ANONYMISE?

- **Get rid of any data protection constraints**
  - Any processing of personal data is generally prohibited, if not explicitly permitted (Art. 6, 9 GDPR)
  - Rec. 26 GDPR: "…The principles of **data protection should therefore not apply to anonymous information**, namely information which does not relate to an identified or identifiable natural person or to personal data rendered anonymous in such a manner that the data subject is not or no longer identifiable. This Regulation does not therefore concern the processing of such anonymous information, including for statistical or research purposes."
- **Comply with data minimisation principle**

  Art. 5 (c) "adequate, relevant, limited", 89 (1) GDPR

WHAT IS ANONYMISED DATA?

Art. 4 (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;”

WHAT IS ANONYMISED DATA?

Recital 26 GDPR

„… The principles of data protection should therefore not apply to **anonymous** information, **namely information which does not relate to an identified or identifiable natural person** or to personal data rendered anonymous in such a manner that the data subject is not or no longer identifiable. …"

Anonymous/anonymised data are non-personal data

(dichotomy of data protection law)

DE FACTO ANONYMITY

Rec. 26 GDPR:

"…To determine whether a natural person is identifiable, account should be taken of all the means reasonably likely to be used, such as singling out, either by the controller or by another person to identify the natural person directly or indirectly. To ascertain whether means are reasonably likely to be used to identify the natural person, account should be taken of all objective factors, such as the

- costs and time required for identification, taking into consideration
  - the available technology at the time of the processing
  - and technological developments."

„Absolute anonymity" once and forever is not possible and not required by the GDPR

Anonymity is not a static concept, but depends on context

The name „Harry Smith" will identify somebody in a classroom, but not globally.

RE-IDENTIFICATION OF GOUVERNEUR WILLIAM WELD

Publication of health insurance data (over 45.000 clients) in Massachusetts 1997

- Stripped of direct identifiers (name, address etc.)
- But containing full date of birth and zip code

Re-Identification of Gouverneur William Weld

- Collapse in live-TV show
- Publicly known to have been hospitalised
- Linkage with publicly available voter data set
- Combination of data sets lead to unique result
- More medical data could be concluded from other sources

Barth-Jones DC. The 'Re-Identification' of Governor William Weld's Medical Information: A Critical Re-Examination of Health Data Identification Risks and Privacy Protections, Then and Now (July 2012). Available at SSRN: http://ssrn.com/abstract=2076397 https://de.wikipedia.org/wiki/William_Weld

DE FACTO ANONYMITY

IMPORTANT FACTORS

- Availability of information including context knowledge

  „Harry Smith“ is not enough to identify an indiviual globally (no „singling out“), but it is in a classroom

- Goal of a potential attacker

  Counting people on the street for statistical reasons versus counting bypassing reknown actors in a certain street by the yellow press

- Effort to achieve identification

  Easy access for employees of controller without great risk?

- Technology

  This test is a dynamic one and should consider the state of the art in technology at the time of the processing and the possibilities for development during the period for which the data will be processed. …The system should be able to adapt to these developments as they happen, and to incorporate then the appropriate technical and organisational measures in due course (WP 136 concept of personal data, p. 15).

DE FACTO ANONYMITY

The crucial factor is the re-identification risk before the background of a certain context

⇒ organisational measures can influence the status of anonymity

> „Putting in place the appropriate state-of-the-art technical and organizational measures to protect the data against identification …are not the consequence of a legal obligation arising from…the Directive…, but rather a condition for the information precisely not to be considered to be personal data and its processing not to be subject to the Directive.“ (WP 136, concept of personal data, p. 17)

See also: „Reconsidering Anonymization-Related Concepts and the Term ‘Identification’ Against the Backdrop of the European Legal Framework“, Biopreserv Biobank. 2016 Apr 22. http://online.liebertpub.com/doi/full/10.1089/bio.2015.0100

WHY PSEUDONYMISE?

Comply with the data minimisation principle of Art. 5 (c) GDPR

“Personal data shall be … adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed (‘data minimisation’);”

Comply with Art. 89 (1) GDPR

“Processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, shall be subject to appropriate safeguards, in accordance with this Regulation, for the rights and freedoms of the data subject. Those safeguards shall ensure that technical and organisational measures are in place in particular in order to ensure respect for the principle of data minimisation. Those measures may include **pseudonymisation** provided that those purposes can be fulfilled in that manner. Where those purposes can be fulfilled by further processing which does not permit or no longer permits the identification of data subjects, those purposes shall be fulfilled in that manner.”

WHAT IS PSEUDONYMISED DATA?

Art. 4 (5):

“pseudonymisation’ means the processing of personal data in such a manner that the personal data

can no longer be attributed to a specific data subject

without the use of additional information,

provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person;”

WHAT IS THE DIFFERENCE BETWEEN ANONYMISATION AND PSEUDONYMISATION?

- **The key**
  - the individual remains in principle retraceable
  - by those who have access to the key

- **The level of de-identification**
  - not necessarily according to the definition
  - but very often in practice

„RELATIVE ANONYMITY“

Is pseudonymised (coded, key-coded) data anonymous in the hands of a third party having no access to the key?

„RELATIVE ANONYMITY“

WP 136, concept of personal data, p. 19/20:

The question here is whether the data used for the clinical trial can be considered to relate to "identifiable" natural persons and thus be subject to the data protection rules. … **In this case, the identification of individuals (to apply the appropriate treatment in case of need) is one of the purposes of the processing of the key-coded data.** The pharmaceutical company has construed the means for the processing, included the organisational measures and its relations with the researcher who holds the key in such a way that the identification of individuals is not only something that may happen, but rather as something that must happen under certain circumstances. The identification of patients is thus embedded in the purposes and the means of the processing. In this case, one can conclude that such key-coded data constitutes information relating to identifiable natural persons for all parties that might be involved in the possible identification and should be subject to the rules of data protection legislation. **This does not mean, though, that any other data controller processing the same set of coded data would be processing personal data, if within the specific scheme in which those other controllers are operating reidentification is explicitly excluded and appropriate technical measures have been taken in this respect**.

„RELATIVE ANONYMITY“

European Court of Justice:
C-582-14

19 October 2016
„Patrick Breyer v. Bundesrepublik Deutschland“

http://curia.europa.eu/juris/document/document.jsf?text=&docid=184668&pageIndex=0&doclang=en&mode=req&dir=&occ=first&part=1&cid=1130557

68. Just as recital 26 refers not to any means which may be used by the controller (in this case, the provider of services on the Internet), but only to those that it is likely ‘reasonably’ to use, the legislature **must also be understood as referring to ‘third parties’ who, also in a reasonable manner, may be approached by a controller seeking to obtain additional data for the purpose of identification.** This will not occur when contact with those third parties is, in fact, very costly in human and economic terms, or practically impossible or prohibited by law. Otherwise, as noted earlier, it would be virtually impossible to discriminate between the various means, since it would always be possible to imagine the hypothetical contingency of a third party who, no matter how inaccessible to the provider of services on the Internet, could — now or in the future — have additional relevant data to assist in the identification of a user.

SIDE-EFFECTS (ADVERSE EVENTS) OF ANONYMISATION

- Full (unlinked) anonymisation deprives the donor of the possibility to use their right to withdraw consent

  critical for WGS

  or other cases of weak anonymisation

- Makes feeding back research results or incidental findings impossible
- Provides the false conception, that data can be shared without safeguards (the more the data are shared and linked, the more re-identification risk increases)
- Often renders data useless for analysis (data mining)

BBMRI-ERIC®

MAKING NEW TREAT MENTS POSSIBLE

THANK YOU!

contact@bbmri-eric.eu
www.bbmri-eric.eu
@BBMRIERIC
BBMRI-ERIC

Q&A

ASK US WHAT YOU WANT TO KNOW…