Consent to research using biological samples and personal data

Sara Casati, Common Service ELSI BBMRI
a collaborative process
a participatory pact
pact of responsibility
between all of the actors involved
based on
transparency  reciprocal engagement
accountability
Innovative governance
INFORMED CONSENT AS A PROCESS

Fostering public trust based on understanding, transparency of governance, traceability of processes and publicity

Giving individuals as much choice and control in what is done with their personal data and samples

INFORMED CONSENT AS
A PARTICIPATORY INFORMATION PROCESS
A INDEX OF GOOD BIOBANKING RESEARCH PRACTICE

By understanding and supporting biomedical research as a partnership between participants and researchers, dynamic consent makes possible better research and a better research experience for both parties. The interface offers participants a responsive format through which to become involved with research; one which respects their autonomy by enabling information and consent preferences to be exercised and ultimately providing more meaningful consent. This in turn benefits researchers by facilitating more engaged participant populations, streamlining recruitment and improving public trust”

Kaye et all. “Data sharing in genomics” Nature Reviews Genetics 10, 331-335 (May 2009)
A CONTINUOUS PROCESS

BEFORE
- diffuse information environment based on different information sources and multimedia options
- biobanking proposal; making information available

DURING
- communication stages, also online, from preliminary stage to individual choice
- Final documented decision – expression of consent

AFTER
- interaction path that is understandable and accessible
- contacts
- website
- newsletter
- reporting
- to communicate and interact with the biobank and/or the Principal Investigator in the light of the decision to collaborate in biobanking
Supporting documents in order to understand and track:

- **The ethical evaluation →** Research Ethics Committee’s Opinion;
- **The reasons for biobanking →** brochure, detailed information documents;
- **Access to the samples and data, the return of results →** Material Transfer Agreement, code of ethics, dedicated policies;
- **The governance of the biobanking →** statute, code of ethics.
SHAPING INFORMATION STARTING FROM THE PATIENT/CITIZEN’S INFORMATION NEEDS

Information contents at stake

- Reasons for, objectives and nature of the research biobanking proposed
- Rights and responsibilities. Implications of participation
- Nature and methods of collection
- Benefits and risks/harms
- Management of data and their protection
- Rules for data and samples access/transfer
- Return and use of the results
- Names and contacts to communicate with


Council of Europe. Recommendation CM/Rec (2016)6 of the Committee of Ministers to member States on research on biological materials of human origin
## DATA PROTECTION AND MANAGEMENT

How will data linked/generated by materials be managed and protected?

How and for how long will samples/data be stored?

### RULES FOR DATA AND SAMPLE ACCESS AND TRANSFER

Can I have access to my data?

Who can access my data / sample and according to what rules?

Can my samples be transferred? To whom and for what purposes?

What happens if the biobank ceases its activity?

## RETURN AND USE OF RESULTS

How will I be informed of the research results?

What results will be returned to me?

Who can I contact for clarification or information about the research results?
| GOVERNANCE OF THE BIOBANK (CROSS-CONTENT) | - Rules for access and use.  
- Rules for the transfer of material/data.  
- Rules relating to the cessation of the biobank.  
- Ways of returning and sharing results.  
- Ways of involving citizens and patient communities |

Understanding the governance of the biobank and what is at stake in the biobanking process is core to the informed consent process. The governance information hubs correspond to some of the main information hubs. It is essential to make available all of the institutional documents and information that help a potential participant
GOVERNANCE, A KEY PILLAR

GDPR, a critical tool to structure flexible governance for data protection:

• affording citizens increased protection and empowerment over personal data
  “This Regulation protects fundamental rights and freedoms of natural persons and in particular their right to the protection of personal data.”
  [Art. 1(2)]

• enhancing the circulation of those data within the EU
  ”The free movement of personal data within the Union shall be neither restricted nor prohibited for reasons connected with the protection of natural persons with regard to the processing of personal data. “
  [Art. 1(3)]

from the issue of privacy, per se, to the acquisition of control over data and trust in their holders
WITHIN THE DATA PROTECTION, THE ACTORS

- **Data controller** means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law;

- **Data processor** means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller;

- **Data Subject**: “An identified or identifiable natural person”. The individual(s) within the EU who are having their personal data collected and processed.

- **Data Protection Officer (DPO)**: The person responsible for overseeing data protection strategy and implementation in compliance with the GDPR requirements.
DATA …

- **Personal data** “any information relating to an identified or identifiable natural person”

- **Genetic data**
  “Personal data relating to the inherited or acquired genetic characteristics of a natural person which give unique information about the physiology or the health of that natural person and which result, in particular, from an analysis of a biological sample from the natural person in question.”

- **Special categories of personal data**
  “Processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation shall be prohibited.

- **Pseudonymized data** is considered personal data that would be subject to the protections of the GDPR.

Data that have been fully anonymized are not covered by the GDPR.
"AUTONOMY- ACCOUNTABILITY REGIME"

- The GDPR decentralizes by delegating responsibility from national and EU authorities to data controllers (that is, the persons, companies, associations, or other entities that are in control of personal-data processing).

- Controllers are required to adopt a proactive approach toward data protection and are responsible for the ex ante assessment, the implementation, and the post hoc verification of appropriate measures to ensure and demonstrate that data processing complies with the GDPR.

  [Arts. 5(2) and 24],

→ a controller-based, case-sensitive, and context-specific approach to data protection

→ from a “paternalistic” to an “autonomy-based” regime in European data protection

The shift toward a decentralized, controller-anchored, and accountability-based model gains salience with respect to secondary research, especially considering the emergence of “dynamic knowledge repositories”
DATA PROTECTION BY DESIGN

a risk-based, context-specific approach meant to ensure that appropriate data-protection measures are designed and implemented throughout the entirety of the processing activities

(as enshrined in the “data protection by design and by default” principle, Art. 25)

Processing
“...any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction”.

Specific provisions for the processing of sensitive data (Art. 9) for scientific research purposes (Art. 89), requiring organizational and technical safeguards, such as data pseudonymization
THE COMPATIBILITY TEST

The data controller, which aims at ascertaining, on a case-by-case basis, whether the further processing of personal data (without the data subject’s consent), is compatible with the initial purpose for which data were originally collected.

Factors to be taken into account for the “compatibility test” include

- **the nature of the personal data**, in particular whether special categories of personal data are processed” [Art. 6(4)(c)];

- “any link between the purposes for which the personal data have been collected and the purposes of the intended further processing” [Art. 6(4)(a)];

- **the reasonable expectations of data subjects** on the basis of their relationship with the controller as to their further use” (Recital 50);

- “the context in which the personal data have been collected” [Art. 6(4)(b)]]
AT THE BASIS OF CONSENT
TRANSPARENCY, ACCOUNTABILITY, CONTINOUS ASSESSMENT, ACCESS

Providing information to data subjects prior to obtaining their consent is essential to enable to

- make informed decisions,
- understand what they are agreeing to,
- exercise their right to withdraw their consent.

If the controller does not provide accessible information,

Data subject control becomes illusory and consent will be an invalid basis for processing.
The controller must ensure that consent can be withdrawn by the data subject as easy as giving consent and at any given time.

*Article 7(3)*

**Obtaining consent also does not negate or in any way diminish the controller's obligations to observe the principles** of processing enshrined in the GDPR, especially Article 5 of the GDPR with regard to fairness, necessity and proportionality, as well as data quality.

*Art 29 WP. Guidelines on consent under Regulation 2016/679:2*

The controller must as part of the transparency obligation **inform the data subjects on how to exercise their rights**

*Art 29 WP. Guidelines on consent under Regulation 2016/679:22*
Consent should be given by a clear affirmative act establishing a freely given, specific, informed and unambiguous indication of the data subject's agreement to the processing of personal data relating to him or her, such as by a written statement, including by electronic means, or an oral statement. This could include ticking a box when visiting an internet website, choosing technical settings for information society services or another statement or conduct which clearly indicates in this context the data subject's acceptance of the proposed processing of his or her personal data. Silence, pre-ticked boxes or inactivity should not therefore constitute consent. Consent should cover all processing activities carried out for the same purpose or purposes. When the processing has multiple purposes, consent should be given for all of them. If the data subject's consent is to be given following a request by electronic means, the request must be clear, concise and not unnecessarily disruptive to the use of the service for which it is provided.
ELEMENTS OF VALID CONSENT

- freely given,
- specific,
- informed
- unambiguous indication of the data subject’s wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her.

Granularity: option of choice is freedom

(Recital 43) … consent is presumed not to be freely given if the process/procedure for obtaining consent does not allow data subjects to give separate consent for personal data processing operations respectively (e.g. only for some processing operations and not for others) despite it being appropriate in the individual case.

(Recital 32) “Consent should cover all processing activities carried out for the same purpose or purposes. When the processing has multiple purposes, consent should be given for all of them”.
SPECIFIC …

…to ensure a degree of user control and transparency for the data subject. This requirement has not been changed by the GDPR and remains closely linked to the requirement of 'informed' consent. At the same time it must be interpreted in line with the requirement for 'granularity' to obtain 'free' consent. In sum, to comply with the element of 'specific' the controller must apply:

(i) **Purpose specification** as a safeguard against function creep,
(ii) **Granularity in consent requests**,  
(iii) **Clear separation of information** related to obtaining consent for data processing activities from information about other matters.

*Art 29 WP. Guidelines on consent under Regulation 2016/679:10-11*
Explicit consent is required in certain situations where serious data protection risk emerge, hence, where a high level of individual control over personal data is deemed appropriate. Under the GDPR, explicit consent plays a role in Article 9 on the processing of special categories of data, the provisions on data transfers to third countries or international organisations in the absence of adequate safeguards in Article 49, and in Article 22 on automated individual decision-making, including profiling.

**Art 29 WP. Guidelines on consent under Regulation 2016/679:18**

*explicit ...the way consent is expressed by the data subject*. It means that the data subject must give an express statement of consent.

An obvious way to make sure consent is explicit would be to expressly confirm consent in a written statement. Where appropriate, the controller could make sure the written statement is signed by the data subject, in order to remove all possible doubt and potential lack of evidence in the future.
When consent is the legal basis for conducting research in accordance with the GDPR, this consent for the use of personal data should be distinguished from other consent requirements that serve as an ethical standard or procedural obligation. An example of such a procedural obligation, where the processing is based not on consent but on another legal basis, is to be found in the Clinical Trials Regulation. In the context of data protection law, the latter form of consent could be considered as an additional safeguard see Recital 161.

Art 29 WP. Guidelines on consent under Regulation 2016/679:28

For the purpose of consenting to the participation in scientific research activities in clinical trials, the relevant provisions of Regulation (EU) No 536/2014 of the European Parliament and of the Council should apply.

Recital 161
“compliance with the applicable rules for the collection, storage and future use of biological samples of the subject”

Reg UE 563/14, art 7 (h)

... the sponsor may ask the subject, or where the subject is not able to give informed consent, his or her legally designated representative at the time when the subject or the legally designated representative gives his or her informed consent to participate in the clinical trial to consent to the use of his or her data outside the protocol of the clinical trial exclusively for scientific purposes. That consent may be withdrawn at any time by the subject or his or her legally designated representative.

The scientific research making use of the data outside the protocol of the clinical trial shall be conducted in accordance with the applicable law on data protection.

Reg UE 563/14, art. 28 (2)
FLEXIBILITY:
RESEARCH PURPOSES “WELL-DESCRIBED”

“It is often not possible to fully identify the purpose of personal data processing for scientific research purposes at the time of data collection. Therefore, data subjects should be allowed to give their consent to certain areas of scientific research when in keeping with recognised ethical standards for scientific research. Data subjects should have the opportunity to give their consent only to certain areas of research or parts of research projects to the extent allowed by the intended purpose.”

Recital 33

Flexibility to the degree of specification and granularity of consent in the context of scientific research
➔ research purposes “well-described,” ought not always be “fully specified.”
➔ additional safeguards recommended
1. provision of a comprehensive research plan before commencement of a project
2. and/or increased transparency on its development to allow participants to exercise their right to withdraw consent.

when special categories of data are processed on the basis of explicit consent, applying the flexible approach of Recital 33 will be subject to a stricter interpretation and requires a high degree of scrutiny.
A controller must provide the data subject with a notice of the controller’s privacy practices. This notice must be:

(i) concise, transparent, intelligible, and easily accessible;
(ii) written in clear and plain language, particularly if addressed to a child;
(iii) free of charge.

The data subjects must also be informed of their rights to request access, rectification, erasure or restriction of processing, to object to processing, and the right to data portability.

(42) Where processing is based on the data subject’s consent, the controller should be able to demonstrate that the data subject has given consent to the processing operation. In particular in the context of a written declaration on another matter, safeguards should ensure that the data subject is aware of the fact that and the extent to which consent is given. In accordance with Council Directive 93/13/EEC (') a declaration of consent pre-formulated by the controller should be provided in an intelligible and easily accessible form, using clear and plain language and it should not contain unfair terms. For consent to be informed, the data subject should be aware at least of the identity of the controller and the purposes of the processing for which the personal data are intended. Consent should not be regarded as freely given if the data subject has no genuine or free choice or is unable to refuse or withdraw consent without detriment.
INFORMATION TO BE PROVIDED

(a) the identity and the contact details of the controller and, where applicable, of the controller’s representative;
(b) the contact details of the data protection officer, where applicable;
(c) the purposes of the processing for which the personal data are intended as well as the legal basis for the processing;
(d) … the legitimate interests pursued by the controller or by a third party;
(e) the recipients or categories of recipients of the personal data, if any;
(f) where applicable, the fact that the controller intends to transfer personal data to a third country or international organisation and the existence or absence of an adequacy decision by the Commission, ..

…to ensure fair and transparent processing:

(a) the period for which the personal data will be stored, or if that is not possible, the criteria used to determine that period;
(b) the existence of the right to request from the controller access to and rectification or erasure of personal data or restriction of processing concerning the data subject or to object to processing as well as the right to data portability;
(c) the existence of the right to withdraw consent at any time, without affecting the lawfulness of processing based on consent before its withdrawal;
(d) the right to lodge a complaint with a supervisory authority;
THE NOTICE:
WHO/WHAT/WHY/WHERE/WHEN/HOW

Generally, the notice must answer the who/what/why/where/when/how questions related to data collection and use:

- What information is being collected/processed?
- Who is collecting/processing it (including contact information)?
- How is it collected/processed?
- Why is it being collected/processed, including the lawful basis?
- How will it be used?
- How will it be stored and for how long?
- Who will it be shared with (including third-parties)?
- What will be the effect of this on the individuals concerned?
- Is the intended use likely to cause individuals to object or complain? Will it be transferred to a third country and, if so, what is the lawful basis for such transfer?

The data subjects must also be informed of their rights to request access, rectification, erasure or restriction of processing, to object to processing, and the right to data portability.
(50) The legal basis provided by Union or Member State law for the processing of personal data may also provide a legal basis for further processing. In order to ascertain whether a purpose of further processing is compatible with the purpose for which the personal data are initially collected, the controller, after having met all the requirements for the lawfulness of the original processing, should take into account, inter alia: any link between those purposes and the purposes of the intended further processing; the context in which the personal data have been collected, in particular the reasonable expectations of data subjects based on their relationship with the controller as to their further use; the nature of the personal data; the consequences of the intended further processing for data subjects; and the existence of appropriate safeguards in both the original and intended further processing operations.
(b) the provision of such information proves impossible or would involve a disproportionate effort, in particular for processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, subject to the conditions and safeguards referred to in Article 89(1) or in so far as the obligation referred to in paragraph 1 of this Article is likely to render impossible or seriously impair the achievement of the objectives of that processing. In such cases the controller shall take appropriate measures to protect the data subject's rights and freedoms and legitimate interests, including making the information publicly available;