It is important that the final document is not perceived merely as a restrictive interpretation of the GDPR, but also as guidance on how to enable high-quality, reproducible, internationally interoperable, and socially beneficial research in a legally secure manner.

Main comments

Area	Comment	Proposed addition / amendment
FAIRification of sensitive data	The document works with the concepts of anonymisation, pseudonymisation, secure environments and federated databases, but it does not substantially develop the relationship between the GDPR and the FAIR principles. This may lead to the erroneous conclusion that sensitive data must either be fully open or, conversely, cannot be FAIR.	Add an explicit clarification that FAIR does not automatically mean open data. For sensitive personal data, FAIRification should be implemented primarily through high-quality metadata, persistent identifiers, standardised data models, controlled vocabularies, clear access conditions, audit trails and secure analytical environments.
Sensitive health, genetic and biometric data	The document rightly emphasises that genetic data are personal data “by default” and can be considered anonymous only exceptionally, following a thorough analysis. This is essential for genetic, biomedical, psychological and forensic research at universities.	Add a practical typology of access regimes: 1. public metadata without personal data, 2. aggregated data, 3. pseudonymised data under controlled access, 4. data accessible only in a federated or secure processing environment, 5. exceptionally, identifiable data subject to strict justification.
Interoperability	The document mentions federated databases and secure access points, but it does not sufficiently emphasise that without interoperability, multicentre research,	Add that standardised interoperability may also constitute an appropriate safeguard under Article 89 GDPR: common data models, controlled terminologies, machine-readable metadata,

Area	Comment	Proposed addition / amendment
	European research infrastructures and secondary use of data cannot be effectively implemented.	harmonised data dictionaries, provenance metadata and auditable data transformations.
Data infrastructures as a positive element of protection	The document identifies secure processing environments, federated databases, role-based access controls, PETs and contractual safeguards as possible safeguards. This is correct, but it should be stated more clearly that high-quality infrastructure is not merely a “risk”, but also a means of protection.	Add wording to the effect that a well-governed research data infrastructure may provide a higher level of protection than local copies of data held by individual researchers, particularly through access management, logging, output control, separation of identifiers from research data, and prohibition of local downloading of personal data.
Long-term storage for future research	The document correctly states that the storage of personal data for future research must be delimited by a specific area of research, rather than by a generic formulation such as “for scientific purposes”.	Add examples of good practice for universities: regular review of datasets, decisions on further retention/anonymisation/pseudonymisation, linkage to a data management plan, review by an ethics committee or data access committee, and mandatory updating of metadata.
Broad consent and dynamic consent	The document appropriately allows broad consent for a certain area of research and dynamic consent for new or unexpected research directions.	Add that, for long-term university data infrastructures, it is appropriate to combine broad consent with ongoing transparent communication, a web-based project registry, the possibility to subscribe to updates, and the review of new projects by an independent body.

Area	Comment	Proposed addition / amendment
Governance and responsibility in consortia	The document provides a good description of joint controllership in consortia and federated databases. This is crucial for universities, as research often takes place in networks involving university hospitals, universities, academic institutes and commercial partners.	Add a recommendation that, in research consortia, the following should be mandatorily described already at the project or grant application stage: who is the controller/joint controller/processor, who operates the infrastructure, who approves access, who handles data subjects' rights, who maintains audit records, and who is responsible for output control.
Practical usability for universities	The document is legally detailed, but in some places difficult to translate into university processes.	Add a short annex or diagram of a "university research pathway": project proposal → DPIA/risk assessment → ethical review → DMP → legal basis and Article 9 derogation → data classification → access regime → retention/review → publication of results.