**NKUA** Data Protection Officer regarding the Joint Data Controller Agreement document

• The reference to the Consortium Agreement (paragraph 1 of the Background) does not provide a clear description of the personal data categories or sensitive personal data that will be processed, the categories of persons, the purpose and nature of the processing (which actions and procedures of the project include processing of personal data and what it consists of) that each partner will process. These could be included in an annex

 **Added, see annex 1.**

• Since there is data exchange, the partners could be separated into data providers and data receivers, possibly specifying obligations for the latter, such as some additional technical and organisational measures they have to take or more generally when transferring and transmitting information (possibly in a second annex). An attempt is made in the text but from the wording it seems that there is some ambiguity ( e.g. in 4.3, 5, 6.3 which is the other Party?).

 **All obligations are the same for the Parties therefor there are no providers and receivers as in personal data processing agreement.**

• In the sentence of the Background section: 'The Parties agree and acknowledge that it is rarely possible, before or at the start of personal data collection for research purposes, to completely identify the aim of such personal data processing. However, the Parties shall not, as far as possible, process personal data to a greater extent or for other purposes than stated in the primary agreement" we propose to make the corresponding deletion in the text because both the retrospective data and the prospective data of the project must be collected for specific and legitimate purposes and must always be processed lawfully ( Articles 6(1) and 9(2) of the GDPR) otherwise they are unlawful.

 **See suggested change in the Background section of the JCDA. Is it OK?**

• If during the project it is envisaged to use third parties as contractors who will process personal data (processors), it would be appropriate to describe obligations for Controllers such as the existence of personal data processing contracts based on standard contractual clauses or minimum technical and organisational measures to be met, taking into account the nature of the processing they undertake.

 **Is added in the agreement under section 4 i.**

• Upon termination of the contract, for whatever reason, there may need to be provision for the return or deletion of the data by the data receiver.

 **The data that is regulated in the JCDA is a responsibility for each party who have to follow regulations regarding archiving etc. Therefore, there will be no joint data that will be returned or deleted if one party terminates the contract prematurely.**

• If all the provisions we mention are described in the required manner in the consortium agreement, or in deliverables, and you do not wish to include them in the JDCA text, there could be explicit references to them.

 **Should be resolved as per the changes in the JCDA.**

**TCD**
To add to this, there needs to be clarification about who controls what data (this will ultimately include both project partners and schools), the circumstances under which it can be transferred for processing, to whom and the expectations on the controller before transfer (such as (pseudo) anonymisation, encryption, etc). There may also be two levels of processors - those within and outside the project consortium (such as a 3rd party transcription service).

 **Added as section 3 and 4.**

Also, do we need to have a standardised mechanism to record processing activities?

**The organisational security measures should be enough, if not then it is a discussion for the project management. See below.**

This may be too granular but would be relevant under GDPR, so I would appreciate it if you could feedback on this.

One other thing. Could you ask them to confirm whether or not we need to do a data protection impact assessment, as per Article 35 of GDPR, given that we are using, or planning on using 'new' technologies.

**A DPIA would be a good security measure to implement. If the DPIA finds that it would be appropriate to include a standardized mechanism to record processing activities then this should be implemented.**