Response from the Data Protection Commission's Consultation Health and Voluntary Sector Unit to Questions from the Health-Research Data Protection Network

Note: This correspondence does not purport to be a formal sanction or endorsement of the activities of a data controller, data processor or data subject and the Commissioner reserves her statutory right to investigate, or cause to be investigated, any of the provisions of the Data Protection Act 2018 and General Data Protection Regulation that have been, are being or are likely to be contravened in relation to an individual. This correspondence does not purport to represent legal advice and recipients should seek independent legal advice before acting or refraining to act upon any guidance set out herein.

Personal data from outside Ireland:

Q1. Scenario: an Irish Institution carries out a research project X using personal data originated in a third country or another European country. Question: is it sufficient that the consent and any other applicable data protection requirements of the country where the data was originated are complied with?

A. The first step to answering this question is to establish the legal basis for the processing of personal data by the Irish Institution. If the legal basis is 'explicit consent' under Articles 6(1)(a) and 9(2)(a) GDPR, the Irish institution will also have to meet the conditions of Article 7. This requires that the controller shall be able to demonstrate that valid consent has been obtained. While this does not necessarily mean re-consenting the participant, it places an onus on the Irish institution as a controller to interrogate the consent process undertaken by their partner and to satisfy themselves that it is sufficient.

If the legal basis for processing personal data by the Irish institution in explicit consent, the requirement for explicit consent as a safeguard under the Health Research Regulations will still apply. Where consent is obtained by a partner organisation in line with their country's data protection requirements, and international ethical standards in health research, there should be no necessity to obtain any further consent. However, should the Irish institution have concerns that consent has not been obtained this should be interrogated further prior to the processing of personal data.

Anonymisation:

Q2. We seek clarity on the appropriateness of the following approach:

In circumstances where an Institution/Data Controller (Institution1) wants to share data with another Institution/data recipient (Institution2), which is anonymised in the hands of Institution 2, but remains identifiable in the hands of Institution 1:

a) Institution 1 undertakes an exercise that ensures that the data is anonymised in the hands of Institution 2;

b) Institution 1 put in place a contract with Institution 2 in which:

- the Parties confirms that the data is anonymised in the hands of Institution 2;

- Institution 2 commits to only use the data only for the purposes set in the contract and not to make any attempt to reverse engineer the data and/or identify any living individuals from the data it has been given.

c) subject to a and b, the data in the hands of Institute 2 is not subject to GDPR and HRR

A. In this situation, the data controller (Institution 1) produces a pseudonymised set of personal data that they hold. It is clear that in their hand, this will remain personal data as they retain the ability to re-identify the data. Where this dataset is released to a third party, who is not provided with the key to reverse the pseudonymisation process, it is likely that this data can be considered anonymous in the third party's hands. This is contingent on a number of factors that should be carefully considered.

The establishment of anonymisation, in our view, is based upon the reasonable likelihood of re-identification. This can be in relation to the data itself i.e. the risk of "singling out" where it is possible to distinguish the data relating to one individual from all other information in a dataset, perhaps exacerbated by the rarity of the condition being researched. In certain circumstances i.e. genetic data, anonymisation may not be possible.

The likelihood of re-identification also relates to the activities that will be carried out by the recipient. As noted in our guidance document on Anonymisation and Pseudonymisation, "In academic or institutional settings, it may be possible to include binding commitments aimed at preventing re-identification in any agreement for the sharing of anonymised data. This would reduce the likelihood of identification of data subjects occurring, and would therefore permit the sharing of more detailed data than would otherwise be the case."

The first institution, in preparing the pseudonymised data for research purposes, should apply the principle of data minimisation to ensure that the minimum amount of data is processed to achieve the purposes. The second institution should carefully assess its use of the data to avoid inadvertently becoming a data controller of identifiable personal data.

Where this transfer of data takes place subject to appropriate safeguards, and with mitigation of all risks of re-identification, the second institution will be processing anonymous data outside the scope of data protection law including the HRR.

<u>Biological Samples:</u>

Q3. Clarification required on whether it is appropriate <u>not</u> to consider biological material as personal data, unless it is used to sequence the whole genome.

A. While biological material in and of itself is unlikely to be personal data as per Article 4(1) GDPR, associated health or genetic data will be personal data. Data derived from a biological sample may also constitute identifiable personal data, particular the whole genome which is a unique individual identifier.

Q4. Can a DNA sample ever be considered anonymous? What safeguards would be sufficient to render DNA anonymous?

A. The current thinking on this question is that DNA cannot be anonymised as it is in and of itself a unique individual identifier

Q5. Does the remit of the HRR cover the use of samples or only data? Is there envisaged new legislation on the transfer of biological samples?

A. The HRR covers the processing of personal data for the purposes of health research. Thus it applies to data associated with a biological sample, and data derived from a sample that constitutes personal data for the purposes of Article 4(1) GDPR. We are not aware of any intended legislation on the transfer of biological samples.

Q6. Are there any legal implications for the use in a patient information leaflet/consent form of the term "gift" or "donate" in regard to patient biological samples? It appears to imply transfer of ownership. A gift/donation is not usually revoked?

A. The conditions under which a biological sample were given to a biobank would appear to be separate and distinct from the legal basis for processing any associated data. It remains the obligation of the controller to identify an appropriate legal basis under Article 6, and condition under Article 9 GDPR, for the processing of special category personal data. The use of the terms 'gift' or 'donate' in relation to a biological sample would seem unlikely to constitute a valid consent under GDPR to process personal data as it would rely on an implication of the data subject's consent rather than a clear and unambiguous statement of their preference or intentions.

Biobanks:

Q7. The guidance on the HRCDC website regarding Biobanks is being interpreted by some that a declaration won't cover Biobanks for future sharing of data which seems to defeat the purpose of a biobank. Can you clarify if this actually means they cannot give a blanket declaration now for all future uses of the biobank but each new use (if falls outside scope of original consent) would need to apply for a declaration individually. Specifically, there are likely to be many situations where a future project wishes to use "old" (i.e. obtained with consent prior to 8th August 2018) biological samples/associated clinical data – would these be classed as "new" research and thus can apply to the HRCDC with no deadline.

A. It is important to note in the first instance that the HRCDC is an independent body with a defined statutory function and it is not within the remit of the DPC to state definitively what the scope of a consent declaration may or may not be.

We would suggest that it is not within the scope of the HRCDC to make a declaration that covers the future sharing of data by a Biobank. The HRCDC looks at applications from controllers in relation to specific research projects and has to make a determination as to the balancing of the public interest in conducting the research against the public interest in requiring explicit consent. It is not clear that such a declaration could be extended to future use for separate projects, the public interest merits of which have not been considered.

In that sense, it would seem to make sense that such projects could apply separately in the future for a separate consent declaration.

Q8. Is there a retention period for future use of data/ samples as guidance which can be given in relation to biobanks?

A. The DPC does not currently have any guidance available on the retenetion of data or samples by biobanks. In general the DPC does not give such guidance as it is the responsibility of the controller to determine a retention period in accordance with Article 5(1)(e) GDPR.

Q9. Re Biobanks – should the biobank be considered a processor if they are solely providing the material to a third party and that third party defines the purpose? Clearly, they would be a controller in their own right for the separate retention of the data/samples but they have no oversight of the third party's use of the material for their purpose?

A. It seems unlikely that a biobank would be considered to act as a data processor on behalf of a third party to which it provides data for research purposes. A data processor carries out processing strictly on behalf of and subject to the instructions of a data controller. The third party researcher does not determine the means and purposes for the collection and retention of data by the biobank and is thus not the data controller of this processing. This situation would seem to be more accurately described as a controller to controller transfer of data.

Data Controller:

Q10. Scenario: personal data (the "Data") is initially collected and used by an Institution (original data controller) (Institution 1) for a given purpose/study. The results of the study indicate that it is worthwhile to do further exploratory work. After some time (could be a significant period of time) another Institution (Institution 2) develops (independently) a plan for further research, which falls under the same general scope set by Institution 1. This plan relies on the same Data

(A common example of the above is when data collected by institution X to study the genetic causes of a disease is then shared with another Institution Y which decides to look for a specific genetic mutation. This is a very common scenario in research where the scope is defined as research progresses)

Question (a): Given that Institution 2 requires the data for the same high level purpose set by Institution 1 but for a project (specific purpose) that it defines and runs independently of Institution 1, does Institution 2 qualify as (a) joint data controller, (b) separate data controller or (c) data processor?

If (a) or (b) applies, what can be done to overcome the issue that Institution 2 is not named as data controller in the original consent form and re-consenting is not feasible?

A. This is a relatively complex scenario and it may not be feasible to formulate an answer that can be adopted in all cases – each case should be considered on its own merits and in the context of the proposed processing. Some general observations can be made.

In the first instance, the first institution should be able to clearly justify the retention of the data beyond the initial research purpose. This situation should not arise because the first institution happens to have held on to data that turns out to be useful to a third party. Where research data has been retained beyond the initial research purposes, this should be subject to Article 89(1) and Article 5(1)(e) GDPR i.e. measures should be implemented to ensure respect for the principle of data minimisation including pseudonymisation and encryption, or anonymisation.

Secondly, the second institution should be able to identify a legal basis for the processing of the personal data concerned.

The second institution must also consider its transparency requirements under Article 14 GDPR – 'Information to be provided where personal data have not been obtained from the data subject'. Article 14(5) provides an exemption from these requirements where the data is processed for scientific research purposes where the provision of

information proves impossible or would involve a disproportionate effort. As with any other exemption, this should be applied narrowly and a controller seeking to rely on it would need to clearly justify their position and document their decision making in doing so.

In the scenario that is outlined, it would not seem that a situation of joint control will arise with regard to the second project. The first institution is providing data to a third party controller for a project in which they determine neither the purposes nor the means of processing. Each project should be considered on a case-by-case basis however. The Article 29 Working Party Guidance on the concepts of Controller and Processor (WP169) may be off assistance here.

To turn to the matter of consent, the GDPR recognises in Recital 33 that,

> *"it is often not possible to fully identify the purposes 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."*

This is reflected in the HRR in regulation 3(1)(e),

> *"explicit consent has been obtained from the data subject, prior to the commencement of the health research, for the processing of his or her personal data for the purpose of specified health research,* ***either in relation to a particular area or more generally in that area or a related area of health research, or part thereof.****"*

It would be necessary therefore to carefully consider to what extent the original consent of the data subject could cover the new research project as falling within the same general or related area of health research.

<u>Consent:</u>

Q11. What is meant by explicit consent? How should this be documented for example if the consent is taken over the telephone for certain research or re-consent to research? Many biobank patients were consented knowing that they were consenting to have their samples used in multiple future studies and they were informed that the biobank would keep their identity confidential not have to be re-consented?

A. *Explicit consent is not defined as a term in the GDPR but its usage in the Regulation suggests that it extends the unambiguous and clearly affirmative aspects of consent in a manner that is stated clearly, in detail, and leaves no room for confusion or doubt. Explicit consent is often conflated with written consent but this is not necessarily the case. Where consent is provided verbally, a contemporaneous note of the conversation can provide evidence of valid consent having been obtained.*

In terms of consent provided to biobanks, we would suggest that the consideration raised in the previous question in relation to Recital 33 GDPR applies i.e. to what extent does the processing of data associated with a biological sample for a new research project relate to the particular or general area of health research to which the original consent applied?

Q12. Investigators have reported that for ICU studies, where next of kin provide consent for research as a legally acceptable representative when the patient is unconscious, they have been advised to submit an application to the Consent Declaration Committee. This seems to conflict with ICH GCP E6 (R2), ISO 14155 and the National Consent Policy, all of which recognise the validity of consent by a legally authorised or acceptable representative when the patient's condition or competence means they cannot consent on their own behalf. In situations where the patient regains capacity consent is then sought from them directly.

A. ICH GCP E6 (R2), ISO 14155 and the National Consent Policy in our understanding relate to consent to medical treatment and not to consent for the processing of personal data. Data protection law does not currently provide for consent to be given by next of kin in a situation where the data subject does not have capacity.

As it stands a deferral of the requirement for explicit consent may be sought form the HRCDC and it is our understanding that the HRCDC has made conditional declarations in this regard.

We are also aware that the Department of Health intends to imminently introduce an amendment to the HRR to deal with this issue.

Q13. In regard to the sponsor/clinical-site relationship for clinical trials and HRR requirements, which DPO should be named on the consent form (sponsor or clinical site)?

A. We would suggest that in the interests of providing the best quality of information to participants, the DPO who is in the best position to answer their questions should be named on the form. In a joint controller situation, the joint controllership agreement can set out the respective responsibilities of the controllers with regard to the provision of information to participants, and it may be appropriate that one controller's DPO takes on this responsibility.

It should be possible for a participant data subject to find out who the DPO of each of the named controllers in the project is, regardless of whether only one of them takes on the primary responsibility for provision of information and point of contact services.

<u>Withdrawal:</u>

Q14. How to deal with situations where a patient withdraws from a study but also requests that their data be deleted? Does this depend on the legal basis?

A. There are a couple of issues to be considered here, and they are contingent upon the legal basis for processing.

If we consider in the first place a research project in which the processing of personal data is based on the explicit consent of the data subjects, and no other legal basis. The GDPR is quite clear that, where processing is based on consent, the data subject shall have the right to withdraw their consent at any time. The withdrawal of consent does not affect the lawfulness of processing that took place before the withdrawal, but it does affect the processing going forward.

It is recognised in the GDPR that the purposes of scientific research may be rendered impossible or seriously impaired by the erasure of data/withdrawal of consent and provides an exemption at Article 17(3)(e). However, it should be clear that, consent

having been withdrawn, another legal basis must be identified if the controller wishes to continue to process personal data for research purposes. The Article 29 Working Party considered this in its Guidelines on Consent under GDPR,

> *"In cases where the data subject withdraws his/her consent and the controller wishes to continue to process the personal data on another lawful basis, they cannot silently migrate form consent (which is withdrawn) to this other lawful basis. Any change in the lawful basis for processing must be notified to a data subject in accordance with the information requirements in Articles 13 and 14 and under the general principle of transparency."*

It is not open to a controller to switch from consent to another legal basis retrospectively to justify processing when consent has been withdrawn, or is in doubt, without this legal basis having been made known to the data subject prior to consent being given.

WP29 further considers that, "it is important to note here that if a controller chooses to rely on consent for any part of the processing, they must be prepared to respect that choice and stop that part of the processing if an individual withdraws consent." Stopping processing would extend in this case to the erasure of data undergoing processing.

Where the controller relies on a legal basis other than consent, i.e. public interest or legitimate interest under Article 6 combined with Article 9(2)(i) or (j), the right to erasure of data shall not apply as noted above in Article 17(3)(e). Use of this exemption requires the controller to demonstrate the necessity of the continued processing of data to avoid rendering the achievement of the research objective impossible or seriously impaired.

Clinical trial regulation:

Q15. What is the status on alignment of the clinical trial regulation with GDPR?

A. The current status of this alignment is expressed by the EDPB in Opinion 3/2019 concerning the Questions and Answers on the interplay between the Clinical Trials Regulation (CTR) and the General Data Protection regulation (GDPR). This initial opinion considers the legal bases for processing personal data in connection with clinical trials. Further consideration of the Regulation is expected from the EDPB, and the EDPB may issue further guidance on the impact of the GDPR on health research in general. We are happy to keep you updated on this.