EORTC
European Organisation for Research and Treatment of Cancer
The future of cancer therapy

Avenue E. Mounier 83/11
1200 Brussels
Belgium
Tel: +32 2 774 1611
Email: eortc@eortc.be
www.eortc.org

EORTC contribution to the EMA Discussion Paper for Medicines Developers, Data Providers, Research-Performing and Research-Supporting Infrastructures entitled

"The General Data Protection Regulation: Secondary Use of Data for Medicines and Public Health Purposes Discussion Paper for Medicines Developers, Data Providers, Research-Performing and Research-Supporting Infrastructures"

10th July 2020

Prepared by EORTC Privacy team (privacy@eortc.org):
Anastassia Negrouk Head of International Policy, DPO, Roxana Albu Functional DPO, Iryna Shakhnenko Functional DPO, Teodora Lalova Legal Fellow, Izabella Jagiello International Policy Manager

Table of Contents

1 General comments

EORTC in general agrees with the arguments exposed in the introduction, the objectives and with the need and relevance of the questions and answers in this field. All our comments are relevant to the secondary use. Thus, we also touch to some aspects relevant to the primary use, which in our view are essential pre-requisites and enablers of the GDPR compliant secondary use.

Last, but not the least, we would like to point out that last documents issued by either EU commission, EDPB or EU parliament provide somehow contradictory recommendations, further increasing the confusion in the field.[1]

1.1 Need for clarity and harmonized approach

Indeed, prior and since its coming into force on 25 May 2018, the European General Data Protection Regulation (hereinafter "GDPR") has been causing significant concerns among the scientific community[2], mainly related to the diverging national implementation[3] , the uncertainty regarding the correct compliance with its provisions and perceived barriers for longer storage and re-use of already collected data as well as for the sharing of data with other researchers. In addition, GDPR interplay with other pieces of European legislation applicable to health research, such as the upcoming Clinical Trials Regulation, In Vitro Diagnostic Medical Devices Regulation, and Medical Devices Regulation has not been focused on by the authoritative EU bodies to a sufficient extent, if at all. Last, but not the least, the overall picture is further made complex through application of national highly heterogeneous legislation in relation to other matters, such as biobanks[4], registries and genetic testing.

---

[1] See e.g. *How the General Data Protection Regulation changes the rules for scientific research. Study for the European Parliament Panel for the Future of Science and Technology*, July 2019, available at: http://www.europarl.europa.eu/thinktank/en/document.html?reference=EPRS_STU(2019)634447. European Commission. DG Health and Food Safety, *Question and Answers on the interplay between the Clinical Trials Regulation and the General Data Protection Regulation* (2019), http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=611235. European Data Protection Broad (EDPB), *Opinion 3/2019 concerning the Questions and Answers on the interplay between the Clinical Trials Regulation (CTR) and the General Data Protection regulation (GDPR)*, https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_opinionctrq_a_final_en.pdf. EUROPEAN DATA PROTECTION SUPERVISOR (EDPS), *A Preliminary Opinion on data protection and scientific research*, January 6, 2020.

[2] See e.g., Negrouk A., Lacombe D. "*Does GDPR harm or benefit research participants? An EORTC point of view*", The Lancet Oncology 2018, Vol. 19, Issue 10, p. 1278-1280; Negrouk A., Lacombe D., Meunier F. "*Diverging EU health regulations: The urgent need for coordination and convergence*", Journal of Cancer Policy 2018, Vol. 17, p. 24-29; Critselis E. "Impact of the General Data Protection Regulation on Clinical Proteomics Research", Proteomics Clinical Applications March 2019, Vol. 13, Issue 2; Casali PG. "Risks of the new EU Data protection regulation: an ESMO position paper endorsed by the European oncology community", Ann Oncol, 25 (2014), p. 1458-1461; Statement by the Biomedical Alliance in Europe statement on the EU General Data Protection Regulation, available at: https://www.biomedeurope.org/images/BioMed_Alliance_statement_on_Data_protection_Regulation_-_final.pdf

[3] While the GDPR is directly applicable in all EU Member states, it still provides the possibility for derogations, where EU Member states can exercise a degree of discretion as to how certain provisions will apply.

[4] See e.g., Santa Slokenberga, Olga Tzortzatou and Jane Reichel (eds), "*GDPR and biobanking. Individual rights, public interest and research regulation across Europe"* (Springer 2020, forthcoming)

Hence, the EORTC welcomes the initiative of this document. EORTC believes that the input and answers to the questions received from different stakeholders will be highly needed and relevant to the research community and any concrete examples and solutions that are illustrative of situations relevant to the clinical research and more specifically to secondary use of data collected in context of clinical trials, is of unmet need.

Although the intended document serves information purposes only, and is thus not legally binding, it is a step forward for a more consolidated application of the relevant European legal framework.

1.2 Secondary use of data

The adoption of Opinion No 3/2019 by the European Data Protection Board (hereinafter "EDPB") was the first official guidance that sheds much needed clarity on the interpretation of the GDPR specifically in the context of clinical research. Both the EDPB and the EU Commission distinguish between primary and secondary use of clinical trial data. "Primary use" consists of all processing operations related to a clinical trials protocol during its whole lifecycle[5], while "secondary use" is any use of the clinical trial subject's data outside of the scope of the protocol exclusively for scientific purposes[6].

The similar (though slightly differently nuanced) definition of the primary and secondary use is set down in the introduction of the document. However, in our view, the line between the primary and the secondary use of data is more blurred as presented.

Introduction refers to the secondary use as:" "Secondary" (or further) purposes are those compatible with the primary purpose, that however were not explicitly stated at the time of data collection." It uses words "explicitly stated" which EORTC fully supports. In the field, many stakeholders, including EDPB and Ethics committees would replace "explicitly" by "specifically" which is sensibly different in our view and raises more ambiguity.

EORTC would also like to make a distinction between the notion of primary and secondary use as compared to the scope of the primary research project (i.e. scope of the protocol) and the extent of the information that may be presented at this occasion to the research participant. This point will be further illustrated throughout examples EORTC contribute with.

To conclude our general statements, in this contribution to the discussion, and beyond the questions asked, EORTC shares its views and possible interpretation of several aspects of the GDPR, key for clinical research and the concrete examples of implementation that solve some of the challenges linked while achieving the right balance.

For the sake of clarity, beyond this general comment section the structure of this document follows the list of questions.

Overall, EORTC would strongly recommend that any follow-up document written based on the feedback of the stakeholders should provide beyond the summary of all applicable articles and recommendations, some clear examples of possible implementations.

[5] Opinion 3/2019, p. 4 and EU Commission, Q3, p. 3
[6] Article 28(2) CTR

2 Secondary use of health data

EMA would be interested to learn from your experience and understand if there are questions on the secondary data use in the context of the GDPR and medicines and public health purposes.

First, EORTC would like to enrich examples of uses of health data in the scope of further healthcare research. EORTC regrets that examples of the secondary use of data are related exclusively to the drug development cycle. Though we understand drug approval is the main remit of EMA, other regulations such as clinical trials regulation would apply to trials aiming to improve treatment strategies rather than just obtaining an approval for the drug or any extension of the label.[7] Further, drugs are frequently co-developed with companion diagnostic tools or devices, which would require other types of re-use of already existing data[8]. Moreover, concept of personalised medicines frequently calls to the need to re-use data.

Last but not the least, examples of the further use are limited to further studies, in other words research that aims to answer a new research question in relation to the data subject or its disease.

In practice, examples of further use of data in research can also include use of data (by the same data controller or not) aiming to:

- increase the level of evidence (e.g. through meta-analysis)
- corroborate results presented (e.g. by independent body)
- support the feasibility or hypothesis of a new trial design (e.g. by looking into the number of patients that would be eligible for the new trial in databases of former trials or by checking previous treatment failure rates to add rigor to sample size calculations)
- improve methodologies (e.g. RECIST work group)
- prove and improve processes and/or procedures used in research (e.g. Artificial Intelligence use in improvement of data quality or imaging analyses)

In some of the above cases, the notion of primary and secondary use is less self-evident. All the points above can be explicitly stated upfront to the study participants but will typically not be described in the research protocol itself yet or very briefly by a general statement of intention to use data for those purposes.

Question 1: Is the term of "secondary use" a suitable term in the scope of GDPR compliance analysis for any research and what is its interplay with GDPR terms "purpose" or "processing activities"?

The term of "secondary use", routine in scientific jargon, is more and more frequently utilised interchangeably with the term of "purpose" in GDPR (term used, but not defined by the regulation). Indeed, an existence of a new purpose is almost automatically assumed to go hand in hand with the

[7] European Organisation for Research and Treatment of Cancer (EORTC). (2019). Manifesto for a new approach for better medicine in Europe—establishing treatment optimization as part of personalized medicine development. Available at: https://www.eortc.org/app/uploads/2019/06/Manifesto_EORTC_18062019.pdf;

[8] Lacombe D, Bogaerts J, Tombal B, Maignen F, Osipienko L, Sullivan R, Golfinopoulos V, "*Late translational research: putting forward a new model for developing new anti-cancer treatments that addresses the needs of patients and society"*, 13 MOL. ONCOL. 558–566, 560 (2019).

secondary use. These notions are not the same. The term "purpose" it is frequently used interchangeably with "processing activity", which is different again.

Secondary use can also be referred to as *future* research or *further* research and covers a much-diversified set of projects and situations. The word secondary can sometimes refer to the collection for a different purpose. However, it can also just refer to the fact that pre-existing research databases are being re-used with no link to the primary reason data were collected or the dataflow that brought this data to the database being used. Researchers would reason in terms of different projects (or protocols or analysis plans) which investigate one or more research questions, not yet defined at time of initial data collection.

Purpose directly points to the reasons of the collection of data from the data subjects. EDPB in its Opinion 3/2019 seems to understand clinical trials as processing activity, and not as purpose. This is supported by the wording used in footnote 12 of the document, where a single clinical trial is equalled to "individual processing".[9] In general, under the GDPR several processing activities can be performed for one purpose. The opposite is true as well: one processing activity can serve several purposes. For instance, in the context of one trial, a processing operation can be performed both to answer a research question, and to comply with a legal obligation of the marketing authorization holder.

Same purpose may be achieved through multiple secondary uses and inversely one secondary use project can potentially pursue several purposes.

Example 1: Data collected in a population-based registry over the past 10 years are used for research. From GDPR perspective this is a new purpose (a priori not incompatible). From researcher's perspective, terms may depend on the context. The registry may use terms of secondary use (or data sharing if research is not done by the registry itself). However, external researcher may consider its research as primary research as data are being used for research for the first time, specifically when research project would simultaneously use new data prospectively collected from data subjects and pre-existing sources of data.

Example 2: Clinical trials sponsors would run several clinical trials independently trying to answer the same or similar clinical question. One trial would be done in France, another in Germany and the last one in the Netherlands (taking also into account that funds could only be available nationally). After the end and publication of these trials and in order to increase the level of evidence, French sponsor would decide to further confirm the results by doing a meta-analysis on its own. This would be described in a new project being the secondary use of data, but still in the scope of the initial purpose (as there is no new research question, just the increase in the power of statistical calculations).

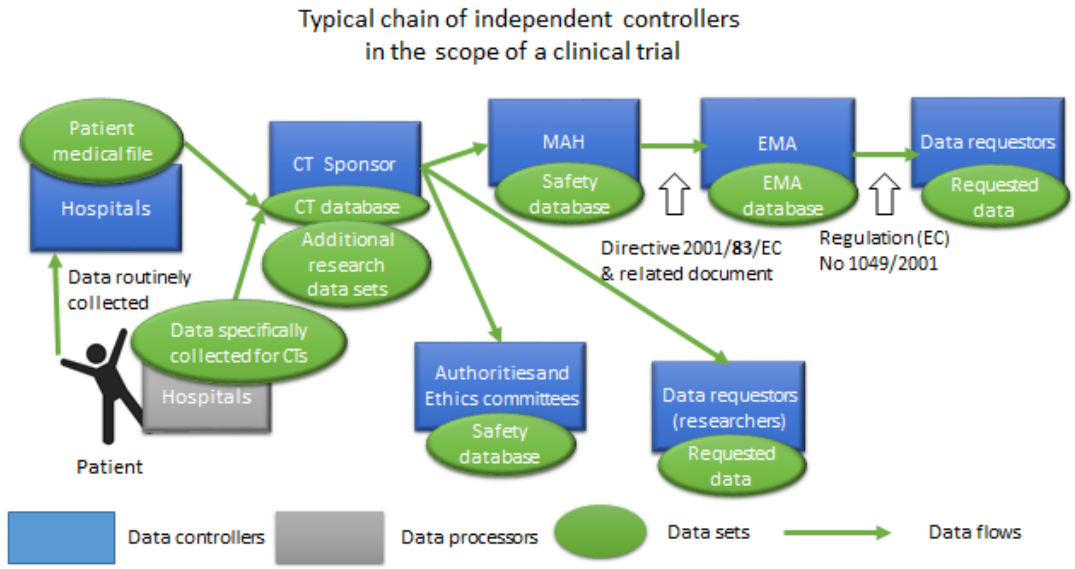
In fact, the only common element between notions of secondary use, re-use of data, future research or further research is the fact that all these types of research use exclusively data which are not being directly collected from data subjects for this project. Indeed, the controller to controller transfers (data sharing) are essential for the research and to the transparency (elaborated on later in this document).

[9] EDPB Opinion 3/2019, p. 7

Question 2: What are modalities and conditions of controller to controller transfers in the scope of scientific research and specifically clinical research?

Though controller to controller transfers are implicit in GDPR (art. 14), this transfer is not specifically named in the regulation. However, clinical research relies on chains of controllers. Data sets are shared from one independent controller to another for achievement of sensibly different purposes. Differently from the joint controllers, independent controllers do not define purposes jointly.

An example of such chain is illustrated in the figure 1.



Examples of datasets provided are either fully identified (patient medical file) or de-identified to a different degree, including to the extent to be considered as anonymous. In general, further the controller is in the chain as compared to the initial source of data, more difficult it becomes to re-identify the data subject. However, the full anonymization cannot be guaranteed at any step as the degree of de-identification depends on the needs of the activities/research at stake.

EORTC believes that clarification of the relationship between independent controllers, part of the same chain would be very helpful. EORTC applies the requirements of the Belgian law on the protection of personal data, where this relationship is clearly mentioned[10]. When transferring data to other controllers, EORTC puts in place a data transfer agreement.

Moreover, when the level of de-identification of data sets transferred, receiving controllers can easily justify that conditions of the art. 11.1 and art. 14.5.b are met, which releases them from many of GDPR obligations, EORTC puts in place additional clauses aiming to further protect data subject rights. Namely, through this agreement, EORTC requires assistance from the recipient controller in case of relevant data subject requests and prompt feed-back in case of any high-risk data breach or in case of incidental findings.

[10] Act on the protection of natural persons with regard to the processing of personal data on the 30th of July 2018.

Question 3: Does the GDPR term "purpose" have a different granularity in the scope of scientific research as compared to other sectors?

In the field of human resources, the purpose would usually be formulated on a relatively high level, such as "processing of personal data for the purpose of execution of the employment contract". This purpose will be achieved through different processing activities (payment of salaries, compliance with social laws etc...). Similarly, in marketing, the purpose would be defined as "using personal data for the marketing purpose". In the field of research however, some countries and organisations are considering each research project as different purpose, including when research projects are very similar. This approach is a clear overshoot in EORTC view.

A clarification on the acceptable granularity of the purpose would be welcome. For example, can the purpose be formulated as following "using *data for the purpose of cancer research and related diseases"?* EORTC believes that such interpretation will be consistent with the EDPB Opinion 3/2019 referred to earlier, which sees clinical trials as processing activity, and not as purpose (the purpose would be series of clinical trials performed for the similar purpose indeed).

Question 4: What is the interplay (if any) between GDPR compliance and Ethical oversight of research?

The above trend to define the purpose of research on the level of each project separately is at least partially related to amalgam made between two radically different questions:

- Is the use of data made in the scope of specific research GDPR compliant?
  and
- Is the research project ethically and scientifically sound?

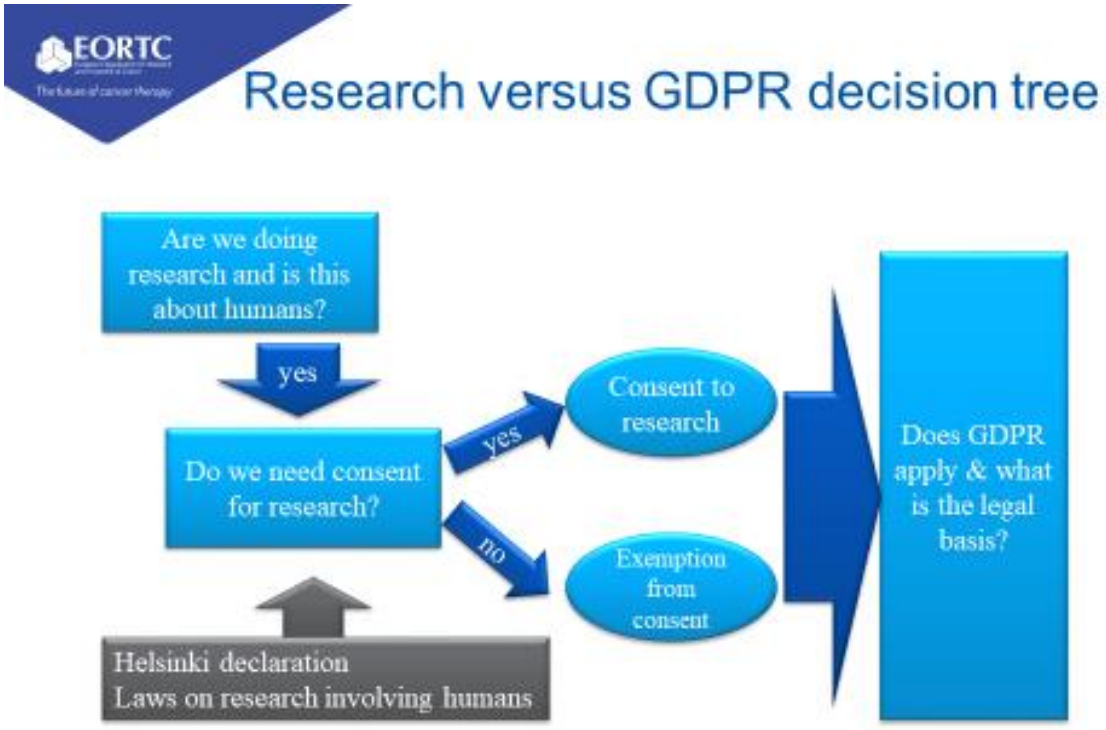
The question at stake is the following: in case the purpose would be defined on a higher level (as proposed above), and individual research projects will all fall in this larger scope and will not be considered as different purpose, does it mean that researchers would be able to do all the research without any oversight of the ethical committees and/or competent authorities? In the EORTC view, compliance with GDPR is different from the need to comply with ethical and legal framework applicable to research. In case the use of data is still done for same purpose from the perspective of the processing of persona data, but is part of a different research project, it shall be subject to the appropriate oversight as per applicable ethical and legal framework. It is important to provide the clarification to all stakeholders (entities legally responsible for research/research sponsors, regulatory bodies, ethics committees, data protection authorities, data subjects etc...) about the fact that these two aspects are independent. Current amalgam represents one of the main hurdles and barriers to the efficient implementation in this field.

This amalgam is further nourished by the fact that whether clinical trials would need consent, they may not rely on consent as legal basis. Indeed, both clinical trials (as well as health research in general) and GDPR refer to consent; thus they do not refer to the same documents in our perspective. In the table below we present some of the obvious differences.

Comparison between research consent and GDPR consent

Point of comparison	Research consent	GDPR consent
Form	written consent in many (but not all) areas, dated and signed (ICH-GCP)	any, including oral or by ticking a box or just by providing the data
Explicit/implicit	opt-out allowed in some areas (in bio-banking)	explicit (no opt-out)
Existence of exemptions	yes, provided EC approval (art 32 Helsinki declaration) or deferred consent (emergency)	no (different legal basis shall be used)

The following scheme can also help to understand the difference between both frameworks and provides a pathway to ensure compliance without confusion, it is also a perfect transition to the next section touching got the legal basis.



3 Legal basis for processing personal data

EMA would be interested to learn from your experience and understand if there are questions in establishing the legal basis for processing sensitive data in the context of the GDPR and secondary data use.

Question 1: What are comparative advantages and/or limitations of different legal basis in the scope of clinical research?

One positive contribution of the Opinion No 3/2019 by the European Data Protection Board (hereinafter "EDPB") consists in stressing out the fact that the obligation for informed consent pursuant to CTR[11] should be distinguished from consent as one of the possible grounds for the processing of personal data under the GDPR. As highlighted in other reports on Opinion 3/2019, presenting subjects with multiple consents that comply with different laws could be confusing for clinical trials participants[12], hence special attention must be paid to the communication between sponsors/investigators and patients in this regard. Moreover, the EDPB and the EU Commission show a clear preference towards the use of other legal bases for the processing of personal data in the context of clinical trial (namely, public interest or the legitimate interest of the controller) rather than relying on consent. And the limits of consent as a legal basis for processing data in clinical research were clearly highlighted (not granular enough, not feasible for research, patient population is vulnerable, consent requires active yes/no tick-boxes, etc..)

However, several crucial topics that are related to the matters discussed in the documents, have been omitted. Among those falls the importance of the One-stop-shop mechanism (hereinafter "OSS") for pan-European clinical research. More specifically, the influence that the choice of the legal basis for the processing of personal data has over whether OSS will apply, or not.

In EORTC's view, it would be a welcomed development if the EDPB choses to issue further guidance on the issues pertaining to the OSS and the choice of the legal basis for international research activities.

The GDPR is lauded for introducing the OSS. The mechanism's rationale is that controllers who conduct cross-border processing of personal data[13] benefit from dealing with a single point of contact (lead supervisory authority[14]) within the EU.

[11] Article 28-29 CTR

[12] Kessler D., Ritzer C., Jacobs S., Rudawski A., Kellogg M. "EDPB issues new opinion on interplay between Clinical Trials Regulation and the GDPR", available at the Norton Rose Fulbright Data Protection Report: https://www.dataprotectionreport.com/2019/02/edpb-issues-new-opinion-on-interplay-between-clinical-trials-regulation-and-the-gdpr/

[13] Article 4(23) GDPR defines cross-border processing of personal data as either "processing of personal data which takes place in the context of the activities of establishments in more than one Member state of a controller or processor in the Union, where the controller or processor is established in more than one Member state", or "processing of personal data which takes place in the context of the activities of a single establishment of a controller or processor in the Union but which substantially affects or is likely to affect data subjects in more than one Member state".

[14] Article 56 GDPR defines it as the Supervisory authority of the main establishment or of the single establishment of the controller or processor.

Based on further guidelines for identifying a controller or processor's leading supervisory authority[15], it is clear, a clinical trial with investigational sites open in several Member states, would fall within the scope of these provisions.

This reflects the unification and simplification which are proclaimed to be at the heart of the data protection reform.[16] The involvement of several data protection authorities (DPAs) may generally lead to confusion for controllers, conflicts of competence, and uncertainty for data subjects.[17] When analysing the possible legal bases for data processing in the context of a clinical trial, of major importance is Recital 128 GDPR, pursuant to which the rules on OSS do not apply where the processing is carried out in the public interest.[18] Further to the Recital 128 GDPR, art 55.2 specify that the notion of the lead supervisory authority (specified in the art.56) does not apply where the processing is carried out in the public interest or when processing is necessary for compliance with a legal obligation. So, choosing the public health or compliance with legal obligation as the legal basis in international trials comes with challenges. First, each member state can further specify conditions which allows to rely on this legal basis, which may not be possible to meet in all concerned countries. Secondly, such legal basis is not compatible with the OSS mechanism.

This means that the data controller would not be able to benefit from a lead supervisory authority in the following cases:

- Processing of personal data for reliability and safety purposes, where the correct legal basis has been identified unanimously by EDPB and the EU Commission as Article 6(1)(c) in conjunction with Article 9(2)(i) of the GDPR;
- Processing operations related to research activities, if one of the following legal bases is chosen by the controller: Article 6(1)(e) in conjunction with either Article 9(2)(i) or (j).

It follows from the foregoing that the legal basis that is left to be the most preferable, is Article 6(1)(f) (legitimate interest) in conjunction with Article 9(2)(j) (scientific research). By choosing it, the data controller would have access to the OSS mechanism concerning the processing of personal data when it is related to research activities.

Further, there is a need to clarify what are other consequences of choosing legal basis which does not benefit from OSS, including just for one international project. Does this means that DPO shall be notified and data breaches are to be reported to all MS's DPAs separately and this just for the sake of one project? What about transversal breaches, which will touch to several activities relying on different basis? Shall the same breach be reported through OSS and in parallel to all other MSs?

[15] Art. 29 Working Party, 13 December 2016 guidelines clarifies further the condition "substantially affects" which will be interpreted by supervisory authorities on a case by case basis, taking into account the context of the processing, the type of the data, the purpose of the processing and factors such as whether it causes, or is likely to cause, damage, loss or distress to individuals, affects, or is likely to affect, individual's health, well-being or peace of mind, involves the analysis of the special categories of personal data, and others.

[16] Balboni P., Pelino E., Scudiero L. "Rethinking the one-stop-shop mechanism: Legal certainty and legitimate expectation". Computer Law & Security Review (2014), Vol. 30(4), p. 393-402

[17] Balboni P., Pelino E., Scudiero L. "Rethinking the one-stop-shop mechanism: Legal certainty and legitimate expectation". Computer Law & Security Review (2014), Vol. 30(4), p. 393-402

[18] It should be noted that while recitals are not legally binding, they hold a strong role when it comes to the correct compliance with the provisions of any EU Directive or Regulation. This is so because the Court of Justice of the EU (CJEU) refers to them when establishing the meaning of a specific piece of legislation in the context of a concrete case, see eg. C-131/12 Google Spain SL, Google Inc. v Agencia Española de Protección de Datos, Mario Costeja González. This is even more so in the case of GDPR because not only the CJEU, but also the EDPB will use the recitals when ensuring the consistent application of the Regulation in all Member states.

In case of the use of consent as legal basis, more clarification is needed in relation to the interpretation of the 14.2.d which states that in case of withdrawal, "the lawfulness of processing based on consent before its withdrawal" is not affected. However, in research some processing activities cannot stop – such as safety reporting or archiving for several years after the end of the study... These activities can be based on a different legal basis. However, if processing of data in a clinical trial is based on the consent and patients withdraw consent at the late stage of data maturation, can data be still included in the final analysis? Or, can the results of the interim analysis still be re-done to verify the correctness of it using the same dataset if some patients withdrew consent thereafter. Can this dataset be used for some types of the secondary use based on a different legal basis? For example, in the scope of inspection or audit, which is a different processing activity?

Question 2: Who decides on the legal basis?

In our understanding of the law, when an entity is the Sponsor of research (or legal responsible) it also becomes the data controller of the processing of personal data in scope of the research (or at least one of data controllers whether joint or independent). Under the GDPR, the obligation to set up the legal ground for processing personal data resides with the data controller. Nevertheless, this is one aspect which we have faced during initial submissions to regulatory bodies, as of May 2018: ethics committees (hereinafter ECs) that impose the legal basis (frequently consent) for processing personal data in scope of research and in particular requested collection of consent of the patient in case of secondary use. Sometimes the opinion of ECs is even in contradiction with the recommendations of EDPB and/or national experts in the field (including DPAs).

In EORTC opinion, it is not up to the ECs to decide on a specific legal basis.

In EORTC understanding of the law (and in line with the EDPB Opinion No 3/2019), the consent researchers ask to the patient when ask if he/she would like to participate in a clinical study/ research is actually the consent from the ethical perspective, specifically according to the Helsinki declaration, any research on human beings or their data requires the ethical review and the consent of the patient to participate to such research.

In regards to the use of consent as legal basis for secondary use of data, this is not always possible (patients are either lost to follow-up, dead or purely not interested and don't want to be contacted for this reason), hence EORTC relies on a larger legal framework, specifically Art.32 of Helsinki declaration, which allows research on data and human biological material already collected from the patient, when there is a positive ethical review. In practice however, it is sometimes challenging to obtain such a review as some ECs would consider this type of research out of the scope of their competencies.

Another aspect that needs to be considered is that too frequent communication with patients to inform about all very specific details of the research, may be overwhelming for patients and sometimes is purely not feasible (in case of a high degree of de-identification or lost to follow-up patients). What is important is that any other research is not incompatible with the initial purpose that was communicated to the patient, e.g. research in oncology. Broad consent (enough specific for patients to understand what would thus be more feasible in this context.

Question 3: Can the legal basis for processing of personal data in the scope of the same research be different on a country by country level?

Taking an example of a research project which will collect datasets from different EU countries (i.e. form registries) and provided the current heterogeneous interpretation, we may face situations where national subsets would be processed based of different legal basis within the same research project by the same data controller. In this case, not only it became more and more challenging to conduct international studies, but it creates inequalities between patients from different countries in the way their rights are executed. Indeed, different legal basis comes with different application of rights for the data subjects.

Question 4: Is a separate legal basis even allowed for the secondary use of data?

Some stakeholder believe that it is not possible for secondary uses of data to rely on a legal basis different from the initial one. This is based on the fact that GDPR states that processing of personal data for purposes other than those for which the personal data were initially collected should be allowed only where the processing is compatible with the purposes for which the personal data were initially collected. Furthermore, it is specified that in such a case (i.e. processing for a compatible secondary purpose), no separate legal basis from that which allowed the collection of the personal data is required.

EORTC understands this as a possibility to continue with the same legal basis, not an obligation. Indeed, we believe that secondary uses may rely on a different legal basis as well. For example, in case of investigation (different from the patient claim) which requires access to coded trial data (from the trial relying on consent), such a purpose would be considered as compatible and processing will not rely on consent anymore. This point of view is supported by the position of the Commission which states on the p. 8 of the Questions & Answers on the interplay CTR-GDPR, that a new valid ground will be needed for secondary purposes, and that the chosen basis "may or may not differ from the legal basis of the primary use".

This position is among others illustrated by the Recital 47 GDPR which seems to consider compatibility of purposes together with legitimate interest as legal basis for further processing “At any rate the existence of a legitimate interest would need careful assessment including whether a data subject can reasonably expect at the time and in the context of the collection of the personal data that processing for that purpose may take place. The interests and fundamental rights of the data subject could in particular override the interest of the data controller where personal data are processed in circumstances where data subjects do not reasonably expect further processing.”

More clarity on this point with some clear examples relevant to research would be welcome.

Question 5: How to explain the legal basis and all this complexity in a lay language to patients?

GDPR concepts are quite challenging to explain in a lay language, specifically in the context where each EC has its own interpretations of elements that must be explained and how. For example, after more than two years in continued debates with ECs across all EU countries, EORTC has produced the following wording which we believe enables the patient to understand the legal basis in a lay language, ensures Sponsor’s compliance with its own obligations under GDPR and reasonably satisfy ECs. This text can further be improved based on the experience we will accumulate in the upcoming years, with feedbacks from regulatory bodies and patients themselves:

"What will your data be used for?

[SPONSOR]'s mission is to coordinate and conduct international translational and clinical research (type of scientific research). [SPONSOR] conducts scientific research in compliance with ethical norms and more specifically the Declaration of Helsinki, which requires your consent to be part of research. It is not possible to perform the research in compliance with ethical and legal requirements and answer research questions without processing of personal data.

If you agree to participate to the research conducted by the [SPONSOR], it will require using (processing) of your data to meet legitimate interest of the [SPONSOR] to conduct the scientific research explained to you.

Depending on the choices you make, [SPONSOR] may use your data for further research projects performed in compliance with applicable ethical standards. Prior to starting any further research, [SPONSOR] will evaluate the compatibility of this further research with the scope of this Study, the information you received and choices you previously expressed."

EORTC believes that providing and sharing examples of lay language on the EU level would be very helpful for researchers.

4 Presumption of compatibility

EMA would be interested to learn from your experience and understand if there are questions on the secondary use of data and the presumption of compatibility.

Question 1: Is the compatibility test even needed prior to the start of the secondary use?

In EORTC understanding, GDPR provides two key mechanisms for further processing:

- Consent
- Union and/or National law (which itself can provide legal basis for further processing as per Recital 50 GDPR)
- Compatibility of purposes

Given that re-consenting is not always feasible in clinical research context, due to the -mentioned reasons, compatibility of purposes can serve as another option. This, in EORTC view, implies that the controller, in order to enable further processing, is required to justify the compatibility of the initial and secondary purposes of processing.

However, this aspect still raises debate in the view of the statement of the art. 5.1.b as some interpretations suggest it releases data controllers from the need to perform the compatibility test. This point of view is supported by the Recital 50 GDPR which states that in case of successful compatibility test, separate legal basis is not required, but at the same time clarifies that "further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes should be considered to be compatible lawful processing operations". Clarification of this element would help sponsors to understand applicable requirements.

Last but not least, the Recital 50 GDPR may suggest that the need for compatibility test may differ from the legal basis used initially (not required in case of the initial consent followed by important objectives of general public interest versus required in case of legitimate interests initially used).

Moreover, similarly to the chain of controllers, we may describe a chain of purposes and the initial legal basis may not be clearly known to the last in chain controller. While this specific challenge may be overcome today by providing relevant information in the agreement, the notion of legal basis was not clearly present before GDPR and it may be impossible to deduct the legal basis for pre-existing databases.

EORTC would propose that in case of doubt, compatibility test would apply.

Question 2: What can be considered in the compatibility test when it comes to the secondary use for research?

EORTC believes that even though the GDPR lists all the elements to be considered for compatibility assessment, researchers struggle to understand what precise aspects they shall evaluate as part of the compatibility test. More detailed health research specific guidance would be very useful and shall provide as many examples and case scenarios as possible. Here below we share some of the elements EORTC considers for the performance of compatibility test, several aspects should be considered as described below.

General remarks:

In our view, presumption of compatibility does not necessarily mean the authorisation to further processing. When evaluating the compatibility between initial and secondary purposes, all five above mentioned criteria should be sufficiently justified. Fair, transparent processing and ability to justify the intent for further processing mean that the principle if purpose limitation is not violated.

Compatibility test cannot be purely quantitative. Qualitative assessment should be performed case-by-case by DPO or a privacy expert. There are no generic assessment / criteria.

While consent for further processing leaves the decision to the data subject, presumption of compatibility gives controller more freedom and flexibility. Though, given this, controller is not exempted from respecting data processing principles.

The positive outcome of the compatibility test does not by itself ensures full compliance with GDPR. Other requirements still apply.

A link between initial and secondary purposes of processing:

The term 'link between purposes may have different interpretations and seems to be quite broad and vague. From the EORTC point of view, establishing a link between initial and secondary purposes can be a major indication of their compatibility and thus the main criterion in the compatibility methodology. The more purposes are related and connected to each other, the bigger chance they are compatible, regardless four following criteria.

This topic is in relation to the previous considerations about the granularity of purposes. The question that arises here is how different the purposes should be, in order to measure the "distance" between them. In the research environment, it is not always possible to predict further projects of research and thus the need for further processing. For instance, at the stage of data collection none can anticipate what exactly tests/analyses will be performed on patient's data. Hence, 'encapsulated', broader purpose of processing should be allowed in EORTC view.

Two situations are to be considered:

- Use of data not primarily collected for research purposes
  and
- Use of data primarily collected in the scope of research for doing more research

In the EORTC view the art. 5.1.b. is very useful for the consideration of the first scenario. From our perspective, use data for research of the similar scope as compared to the one for which the data were primary collected shall be considered as compatible purpose specifically in cases where participants were informed about this possibility upfront. EORTC does not understand why many ECs prevent sponsors from informing patients about such possibility of further research with their data in the absence of detailed description as in our opinion this goes against the transparency requirement.

The use of data collected for research for doing more research shall be considered in our view as being the same purpose at least when the research is in the same field as the initial one (i.e. field of oncology) and does not change its nature (i.e. knowledge gaining research). Of course, as mentioned previously, even when considered to be the same purpose from the GDPR perspective, the Ethics committee review and/or other approvals may still be applicable to the project.

As of note, differently from the population-based collections of data, data sets constituted for a specific research can rarely be used to perform radically different types of research as they would not be appropriate for this other use.

The context of data collection:

The question to ask here is whether the further processing will take place in the same context as the data collection. EORTC believes that providing illustrative examples of contexts to be considered would be helpful to the research community. By context we understand, for example, the use of data for commercial purposes versus non-commercial purposes. Again, transparency is the key and researchers shall be able to inform data subjects from the onset about all possible processing activities that can be made, eventually providing some choices where relevant. Narrowing the scope of information provided to data subjects from the onset is not transparent and is detrimental to both data subjects and to the research and ultimately the EU capacity of innovation.

The nature of personal data:

Healthcare research always use special categories of data. However, it may also use genetic data. Currently many countries limit the possibilities of use of genetic data considerably and in a very divergent way (based on the article 9.4); this without making any distinction between the type of the data at stake (somatic mutations versus germ line mutations, primary DNA sequence versus results of analysis of the status of a single frequent mutation etc...). This approach is detrimental to research and does not always correspond to any higher protection of data subjects. In our view, there is a need to apply a risk-based approach and all genetic data shall not be treated the same, some do not present more risk as compared to any other health data, others do. On the other hand, data as rich as the primary sequence, whereby less than hundred pairs of nucleotides make it unique, are not eye readable to make any sense of them. "Reading" genetic data requires highly sophisticated specialised software, which in a way protects them.

Consequences of the intended further processing (risk assessment):

There should be a balance made between negative and positive or rather beneficial consequences for data subjects. Examples of positive consequences can be development of effective and acceptably

safe medicines or a sense of contribution to innovation aiming to improve either the condition or the knowledge about it. In a way this is a type of the risk benefit assessment well known in the field of research involving humans. In our view this is where the contribution of an ethics committee would be of a value.

Appropriate safeguards in both initial and further processing:

Safeguards used for the initial processing should be re-evaluated if they are relevant for further processing. Such safeguards as encryption and pseudonymization require extra efforts, due to constant technological developments. In many, but not all cases double pseudonymisation can be applied. However, beyond its benefits for the protection of confidentiality, it involves risks to the data accuracy and thus its implementation cannot be automatic but needs to be considered case by case considering all, including technical aspects.

5 Pseudonymization

We would be interested to learn from your experience and understand if there are questions on pseudonymisation in the context of the GDPR and secondary data use.

Question 1. Degree of pseudonymisation: is more the merrier? Shall the degree of de-identification be risk based?

GDPR requires controllers and processors to take all appropriate measures and steps to protect personal data. Among different safeguards, de-identification is frequently used. It results in a fact that data can no longer be directly attributed to a specific data subject or even not at all. Depending on the degree of de-identification, terms of pseudo-anonymization or anonymization will be used. Different methods used to achieve appropriate de-identification have distinct e advantages and disadvantages and the appropriate choice depend on many factors (the degree of risk, the way the data is processed…).

If the data is anonymized so the data subject is no longer identifiable (directly or indirectly), the GDPR simply doesn't see it as personal data anymore. However, anonymizing data can often destroy the value that data holds for the stakeholders and makes impossible for data subjects to exercise their rights, such as data access and portability.

This is why pseudonymization is a more sophisticated option since it leaves you the key to "unlock" the data and enrich it in case is needed. This way data is not considered directly identifying and it is not anonymized either. Pseudonymized allows you to indirectly identify the individual and GDPR fully applies when processing such data. Hence, its advantages include to be simple (as compared to more elaborate anonymisation techniques) and having relatively little impact on the data integrity. Pseudonymization can be simple or double.

Currently, some ECs only allow secondary use of data if samples are double pseudonymised. This approach is indeed simple and easy to implement in most of cases. However, in some specific situations, it may require manipulation of delicate samples (i.e. frozen samples), in which case double pseudonymisation may be more damaging to the integrity of samples (and so data that will be generated from these samples). In our view, the decision on the appropriate means and levels of pseudonymisation shall be left to the data controller based on the specific risk analysis.

6 Data retention

EMA would be interested to learn from your experience and understand if there are questions on data retention in the context of the GDPR and secondary data use.

Question 1: What is the minimum retention in clinical trials?

GDPR requires data to be stored for a minimum time needed. However, in the scope of clinical trials, retention period is of 25 years after the end of the clinical trial. Indeed, 25 years is the archiving period for the trial master file, which includes the trial database and source documents as it aims to allow verification of results reported. Secondary uses would potentially further prolong this period. EORTC, as many other sponsors struggle to explain this to the ECs. A clear statement on this fact would be very helpful.

7 Transparency

EMA would be interested to learn from your experience and understand if there are questions on the transparency principles in the context of the GDPR and secondary data use.

Question 1: Shall there be any limit to the explanation of the potential further use in the information provided to data subjects from the very beginning?

Many ECs severely limit the level of information allowed to be provided to patients from the onset. EORTC needs to frequently challenge EC requests to delete explanations about the intention to use data for further research, to share with other stakeholders etc… pointing to the fact that this information is not specific enough. EORTC strongly believe that this practice is against the principle of transparency. Indeed, it is preferable to inform about all these future possibilities, rather than not. In the field of oncology, some patients may not be alive when further research will be specified. This means that informing them later would not only be not relevant anymore, but in fact GDPR would not even apply anymore to their data. Willing to explain upfront as much as possible, even if in general terms shall definitely be required to respect the principle of transparency.

Question 2: What are appropriate means to comply with the requirements of the art 14.5.b?

Article 14.5.b considers the fact that sometimes the obligation to inform data subject is likely to render impossible or seriously impair the achievement of the objectives of that processing. In such cases it recommends among others making the information publicly available.

However, in the scope of research, public announcements are not always appropriate as they can be considered as advertisement. Publishing the research on the web site of the data controller will only address the issue for research done with data primarily collected by the data controller. However, article 14 is about data not directly collected. In this case, data subjects will not even know about the new controller and will not visit its site.

EORTC sees the need, which was already mentioned in many other contexts when speaking about EU health research. Instead of having one portal for searching clinical trials and another for device or IVD related studies, EU shall have one single repository where all research, prospective, retrospective, interventional or not, involving humans will be referred to with links between projects if data are re-used. This will not cover all uses of data, as some uses, as mentioned before are not research projects.

However, such repository would be beneficial to both data subjects and researchers and will help compliance with many legislations and recommendations.

Otherwise, any other recommendation of appropriate ways to make information public as per art. 14.5.b would greatly support the level of transparency in the field.

8 Rights of 'data subject'

EMA would be interested to learn from your experience and understand if there are questions on the rights of data subjects in the context of the GDPR and secondary data use.

Question 1: What is and what is not the GDPR data subject request in the field of health research?

In the field of health research data subject rights largely overlap with patients' rights, specifically when it is about getting access to the information and/or data. Thus in our experience, these requests are being positively and rapidly addressed, but they are rarely identified as being data subjects requests under GDPR. Moreover, EORTC relationship with patients is never direct, but occurs through investigators. Some requests come to investigators, able to address them directly as part of their normal doctor-patient relationship. This puts us in front of a challenge to understand whether we adequately comply with the accountability principle as only few out of all requests would be documented as actual GDPR related requests. It would be useful to clarify the difference between patients' request to their doctors (through routine relationship or the application of the legislation on patient's rights) and "GDPR requests" whereby EORTC needs to document compliance, including the timelines of reply.

Question 2: What shall be the flow of communication?

GDPR art 13 and 14 require to provide to data subjects the contact of DPO of the data controller. Insofar sponsors are not allowed to know the full identity of research participants, the largely accepted flow is that research participants shall contact their doctor or the DPO of their site, which in turn contacts the sponsor as any processor would (and as documented in the site agreements). Many ECs require however to provide the contacts of the DPO of the sponsor. In case EORTC would receive patient's request, we would need to contact site to assist us in addressing the request and in the meantime, data subject would probably already share information we do not need and which would require appropriate protection, storage and disposal, adding burden on us and risks to the patient. EORTC would welcome the recommendation to avoid putting Sponsor's DPO in the information documents, provided there is an alternative clearly defined pathway to address privacy questions and requests.

9 Registries

EMA would be interested to learn from your experience and understand if there are questions on secondary data use from registries.

EORTC has limited experience of collaboration with registries. From this limited experience, it does not seem that GDPR brought much changes. However, even prior to GDPR, rules of access to data from registries or ways to collaborate where unclear, difficult to establish and different from one registry to the other. Thus, EORTC would suggest registries from different member states develop a

unique code of conduct specifically addressing the possibility to use data for research purposes by other researchers (through data requests or projects run in collaboration).

10 International transfers

EMA would be interested to learn from your experience and understand if there are questions on international transfers in the context of the GDPR and the secondary data use e.g., in multi-national studies.

Question 1: What does 'transfer' mean under GDPR ?

The term of transfer is not defined in GDPR. Research community usually understands transfer as relocation of database or dataset to another partner or subcontractor.

Opinions of some DPAs[19] and EDPS[20] suggest use of clouds and other cloud-based IT solutions also constitutes a transfer (even though the processing at stake is limited to the hosting and resolution of IT issues and does not aim for consultation or modification of data).

In this context it would be highly important to analyse whether the database based in a cloud managed by a third country, is as such a transfer? Even if the third country entity is a processor and does not have access to the data? Clarification of these aspects and definition of the word transfer in the scope of clinical research (including if not different from the general scope) would help.

Question 2: Shall data subjects be systematically informed about possible future transfers to third countries and specifically US? Is this subject to consent?

In many of EORTC conducted prospective studies, the further use of data (further research, secondary use) is not yet defined at the time of initial submission of the study. Moreover, insofar sharing of data after the end of the study is concerned, this part cannot be fully know upfront (though we know upfront researchers would likely ask to have the access to data).

Nevertheless, there is the obligation of informing the patient on the potential recipients of data and eventual third countries of destination. Though, there is no obligation to seek consent and consent can only justify the transfer in cases where there is no other solutions and where transfer is occasional (with the need of notification to the DPA), very different approaches are seen in the field.

There are indeed a lot of inconsistencies within the research community, regulatory bodies, ECs and sites in relation to the way transfers are understood and justified.

Several requests (recently the national Biobank template in Germany) concerned addition of a tick box yes/ no for transfer to third country. We would like to the fact that most of clouds and SAASs involve at least some processing activities (i.e. resolution of bugs or security issues in relation to personal data hosted) being performed outside EU, which in our understanding constitutes a transfer (mostly to US). So, it is almost impossible not have any transfer in third country and IT-wide, 'only-EU-conducted-research' is more and more difficult to sustain. Moreover, in the scope of reporting of safety data, there may be a need for the flow of personal data to a US based MAH, due to regulatory reasons and compliance with non-EU laws in the field of clinical research and use of medicinal

[19] https://www.cnil.fr/fr/la-plateforme-des-donnees-de-sante-health-data-hub

[20] "Outcome of own-initiative investigation into EU institutions' use of Microsoft products and services", 2nd July 2020 (https://edps.europa.eu/sites/edp/files/publication/20-07-02_edps_euis_microsoft_contract_investigation_en.html)

products. As result, pseudonymous cases may be provided to outside EU areas for further regulatory reporting purposes

As such, GDPR clearly states that projects and activities shall not stop for the only reason of data protection; rather the data controller shall conduct risk assessments and balance the risks and provide clear justifications and solutions for still conducting the research while ensuring the data subjects rights and freedoms are protected. EORTC finds it very difficult to avoid any non-EU transfer and to ask the patient consent for such transfer when for instance the database relies on a US cloud (sometimes entirely, sometimes just for the backup).

Asking consent is also not consistent with the fact that most of those service providers are on the privacy shield, so currently in the scope of an adequacy shield.

In addition, some ECs ask at the opposite, to delete any reference to transfer to US as there is no US based partner currently involved (not considering IT-solution providers, nor potential future partners).

Moreover, as partners of further research are by definition not know yet, it is impossible to know upfront which transfer instrument would apply. In some cases, we may need indeed to rely on consent, which is only feasible to be asked upfront.

To over-come this challenge, EORTC position is that the patient is invited to participate in the study, but the transfer to third countries is embodied in the study itself; if the patient does not want its data to be transferred in third country (eg. US), his/her participation to the study will not be possible. Indeed, currently we cannot think about any clinical trial which would not have some level of access to data for a US entity (may be just a cloud provider). This approach may need to be further analysed insofar this type of consent can be considered as bundled. However, we do not currently found any other solution and this approach have at least the merit to be transparent to the data subject.

An example of wording proposed by EORTC in the patient information sheet and informed consent:

"EORTC may transfer patient's data to its delegates, partners and / or other researchers (from Europe or other countries outside Europe, for example, the United States). These may be universities or companies involved in health research or IT-solution providers, such as cloud providers."

Question 3: Are existing solutions (adequacy decisions and standard EU contractual clauses) addressing the relevant needs for research related transfers?

Standard contractual clauses, besides the fact that they have not been updated to GDPR compliance, are not sufficient to meet needs of research in many regards.

The EU SCC are built for transfers controller-to-controller (C-C) and controller-to-processor (C-P); we miss the processor-controller transfer[21].

Further, one clinical trial can embrace several processing activities, in the scope of which the relationship between the sponsor (controller) and the other party can be of a mixed nature. For some activities, it may be a controller to controller relationship, for others controller to processor and even processor to controller in more complicated research designs and consortiums.

The most relevant example are drug providing companies based outside EU and which need to receive from the academic study sponsor based in EU safety data (patient data) for their own compliance with

[21] See European Commission, Standard contractual clauses for data transfers between EU and non-EU countries, https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/standard-contractual-clauses-scc_en

the law (becoming controller on their own). On the other hand, the drug providing company provides the drug and is usually also processor for other study related activities. Hence the transfer mechanism will need to contain both sets of EU SCC (C-C, C-P) which makes very difficult any study set up in this context.

Another hurdle that we encounter is the applicability of transfer mechanism such as Privacy Shield or adequacy decision for Canada – which are applicable only for commercial entities; whereas academic community are no commercial entities. An alternative for them would be EU Standard Contractual Clauses (SCC), but even those are not feasible[22] (e.g., case of NIH sites in US for which signing such clauses comes in contradiction with their own laws)[23].

Question 4: Use of derogation through consent in the scope of research.

The transfer mechanisms (Privacy Shield, Adequacy Decision, EU Standard Contractual Clauses) are regularly challenged in court or soon to be completely revised. Clinical trials and further research may last for years. So, can we foresee solutions upfront to prevent that all trials will stop the day Privacy Shield is not valid anymore? One possibility would be to rely in this case on the last option: derogation through consent.

The pertinence of use of derogation through consent is also relevant to cases mentioned earlier, where the academic partner cannot rely on any adequacy decision and cannot sign contractual clauses.

But what type of consent? What granularity? Can it be collected upfront? Can it be considered as not being bundled?

According to GDPR, derogation consent can only be used as transfer mechanism to third country if the transfer is 'occasional'. What does it mean occasional in the context of a clinical trial? Transfers at stake would not be systematic, nor structural. However, are they occasional? How about several clinical trials in different stages of the conduct?

Specific guidance in this regard, would be useful for research community.

11 Other issues

Another important aspect is linked to the definition of 'genetic data'.

GDPR has one definition. EU Member States (MSs) sometimes have different definitions and impose different conditions, in relation to their own definition.

One example is to impose consent as legal basis without leaving any choice to the data controller (France, Germany, Italy). In other countries, conditions may include stricter access conditions which shall rely on biometric identification means (Italy).

EORTC would like to point that the notion of genetic data is a very rich notion, which embraces primary sequences which are unique and rich in information (but not directly readable without specialised software able to transform data into information) and the status of some frequent biomarkers.

[22] Molnár-Gábor F, Korbel JO. Genomic data sharing in Europe is stumbling-Could a code of conduct prevent its fall? EMBO Mol Med. 2020 Mar 6;12(3):e11421. doi: 10.15252/emmm.201911421. Epub 2020 Feb 18. PMID: 32072760; PMCID: PMC7059003. (https://www.ncbi.nlm.nih.gov/pmc/articles/PMC7059003/)

[23] Tania Rabesandratana, European data law is impeding studies on diabetes and Alzheimer's, researchers warn, doi:10.1126/science.aba2926 (https://www.sciencemag.org/news/2019/11/european-data-law-impeding-studies-diabetes-and-alzheimer-s-researchers-warn)

Genetic data can also come from germ cell line (and be inherited) or from the tumour (somatic mutations) which will not inform about the person, but the illness (different from a genetic disease). Therefore, there is a room for the risk approach within the large category of genetic data and one size does not fit all.

Therefore, there is an urgent need for harmonisation of definition, requirements and further risk based approach to genetic data, specifically in the scope of health research.

Last, but not the least, the understanding of roles of different partners of research (controllers, processors, and joint controllers) has become clearer with time, but is still subject to discussion and would merit clarification.

Safety reporting and security of transfers. Specifically, in relation to the safety reporting more clarifications are needed regarding ways of exchange of safety data between different stakeholders (including harmonisation of the security requirements for means used). Currently, a variety of methods to exchange individual case safety reports, periodic reports and line listings co-exist. Some parties have more detailed and/or stricter requirements and instructions, others barely anything. Sometimes a secure portal is used (i.e. Eudralink), but sometimes just an email (including unencrypted e-mails used frequently by Ethics Committees). Some entities require specific items to be in the bodies and titles of emails, which may include patient pseudonymous ID (i.e. France). In other countries authorities forbid transmission of any pseudonymous data through mails and mandate using more secure encrypted solutions which some of the Ethics Committees in that same country are unable to read and accept (i.e. Denmark). This puts clinical trial sponsors in front of a hard dilemma, to comply with GDPR and safe data through secure channels only or to comply with reporting obligations of clinical trial framework.

12 Conclusion

Since its implementation, GDPR did not lead to the failure of any of EORTC trials, studies or research projects. However, in two occasions we lost US based academic partners afraid of GDPR related risks, in one occasion a clinical trials was rejected for unjustified GDPR related reasons (where an EC was clearly acting beyond its remits) and, in general, the lack of harmonisation and/or clarity around questions we raise in this document costed EORTC numerous hours of work. Namely to its Privacy Office, Regulatory Affairs and Contract Departments. The time and efforts spent on the updates of documents, including hundreds and more contracts applicable to ongoing research (work still in progress) is in our view of a little added value as compared to yet to be proved gain of protection to data subjects. Therefore, we call all EU relevant bodies (EMA, EU Commission, EDPB, DPAs) to urgently clarify, harmonise and provide viable solutions to avoid seriously harming health research and innovation in Europe.

EORTC privacy team can be contacted at: privacy@eortc.org