TRIAL SUBJECT GDPR CONSENT - A DO OR A DON'T?

By Jan Bjerrum Bach, Attorney-at-Law

Congratulations on your appointment as project manager of a pre-submission multinational clinical trial to be carried out at sites in, inter alia, the EEA and the UK for the purpose of generating IMP* data eventually enabling submission of a marketing authorization application for a medicinal product now to be tested.

Your employer is a private for-profit operating special purpose biotech company being run by a few CXO's* and staff, such as yourself, engaged on short term consultancy terms, and interacting digitally at a distance. Due to the limited amount of in-house resources, your responsibilities include all operational, logistical and legal aspects of the trial, often reflecting GCP* and data protection requirements.

Biotech Company GDPR Need-to-Knows:

1. The legal basis for the processing of trial derived health data.
2. The GDPR qualification of sponsor, investigators and other interests involved.
3. The need for DPA's - Who are required to enter into and sign a DPA with whom?
4. Consent required for (purpose specific) processing of protocol mandated health data?
5. GDPR de minimis data processing standards.
6. Data Protection Officer - Must sponsor have a DPO?
7. Data retention periods.

Fortunately, the trial budget authorizes engagement of a CRO*, including - on a country-by-country basis - local CRO sub-contractors, so following completion of a relatively informal tender process; you have contracted the bidder that you believe to be the most cost-effective and internationally experienced CRO available. The chosen CRO has offered to render the trial related services required on basis of a CRO developed "standard" MSA* and bi-lingual GCP (CTA*, ICF*) and GDPR* (DPIA*, DPA*) templates regulating relationships among sponsor, CROs, sub-contractors, sites, investigators, patients and EC's*, and GDPR risk assessments. The CRO expects the templates to be acceptable more or less on an "as are" basis to everybody to be contracted. So, with everything being on track for initiation of site recruitments, EC submissions, kick-off meetings, subject enrolment and initiation of the trial, you may now lean back, right?

Well, first of all your expectations that you (and sponsor) may rely on CRO templates and CRO professionals conducting the trial without involving you in the finer time-consuming details, is an illusion. The GCP requirement that CRO's may only act on specific authority and delegation implies that the negotiation process can only be executed by the CRO on basis of detailed instructions received from you on all sorts of contractual details – the templates, which sounded so promising, are no longer a solution, but merely a check list comprising a starting point for the negotiations to be concluded.

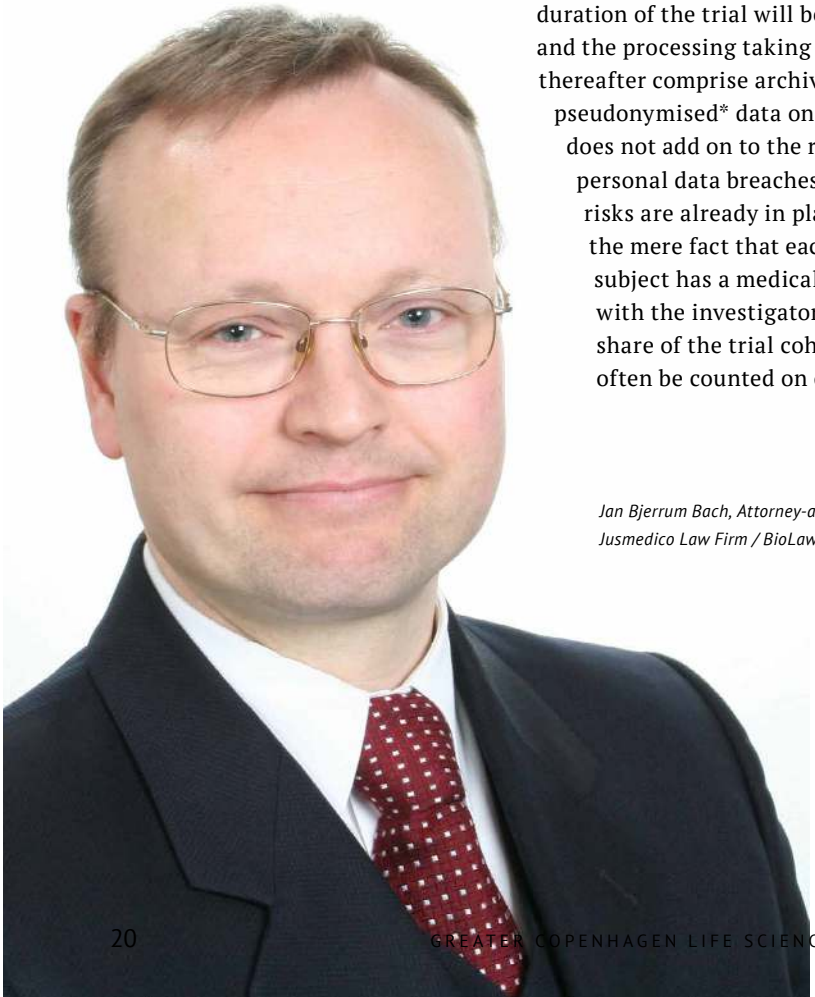
With respect to personal data processing you should, to secure regulatory consistence, implement a GDPR position policy, which addresses, among other issues, the questions raised in the appetizer above of this article, and which is consistently implemented vis-à-vis all parties involved securing that e.g. controller* and processor* roles have not been varied from site to site just to accommodate individual sites' individual institutional policies. If the GDPR roles are not consistently implemented on all sites, investigators, CROs, etc. involved, the data package ultimately compiled will comprise a GDPR patchwork vesting different GDPR rights in different trial subjects. Such end result would be a nightmare to administrate as some data may have been obtained on a no consent basis, as research data should be, and other on a trial subject consent made to the site as controller which the site should not be, implying that transfer to sponsor would be consent based and hence subject to withdrawal risks and re-consent procedures being neglected, potentially jeopardizing the entire data bank.

Considering the vast amount of GDPR advice available from a comprehensive number of sources, including the EU Data Protection Board* and national data protection agencies, it should be straightforward to agree on a GDPR interpretation paving the way

for a smooth implementation of template-based contracts. However, experience has shown that involved interests often take different views on what is the right answer to a variety of GDPR related questions, such as those raised above, and especially on GDPR consents, the need for a Data Protection Officer, DPA closing and retention periods.

GDPR Consents: Some sites insist that the sponsor – side by side with the GCP required consent comprising the ICF - must obtain a GDPR consent from the trial subjects in order for the health data generated as per the protocol to be processed. When challenged, the argument sustaining this requirement is "better safe than sorry". Ironically, the policy does the opposite – rather than being safer and better-off, such policy actually and unnecessarily vests (some) control over the health data in the trial subject and moreover a need for the subject to re-consent every one or two years. Hence, nothing is achieved, but an increase of the risk of losing data due to, e.g., withdrawal requests.

DPO* / Data Protection Officer: As per GDPR Art. 37 a data protection officer must be designated when the core activities of an enterprise consist of processing operations which, by virtue of their nature, their scope and/or their purposes, require regular and systematic monitoring of trial subjects on a large scale or where the core activities consist of processing on a large scale of health data. In this case sponsor's core activity does not comprise processing operations requiring regular and systematic monitoring on a large scale basis, nor processing on a large scale of health data. Partly sponsor's core activity is not data processing, but IMP development and partly the trial subject cohort is traditionally very limited in terms of number of trial subjects. Moreover the duration of the trial will be limited and the processing taking place thereafter comprise archiving of pseudonymised* data only, which does not add on to the risk for personal data breaches as such risks are already in place by the mere fact that each trial subject has a medical record with the investigator, whose share of the trial cohort may often be counted on one hand.



Jan Bjerrum Bach, Attorney-at-Law, Jusmedico Law Firm / BioLawEurope

DPAs / Investigator Processing: Not infrequently, sites refuse to sign Data Protection Agreements otherwise called for as per Art. 28 (3) of the GDPR on the basis that the site has to adhere to an institutional policy stipulating that investigator – by site definition – will not be "processing" data, merely "transferring" same, in spite of the CTA and the protocol requiring investigator to, inter alia, collect, record, organise, structure, store and retrieve health data. Apparently, the position reflects a kind of wishful thinking that if we call "processing" something else, then it will not be "processing" and no GDPR obligations will be vested in the processor or at least they will be less onerous. In our perspective such policy is nothing more than exactly wishful thinking, which has no bearing.

Health Data Retention Periods: Health data controlled by sponsor, i.e. data generated as per the protocol, comprise Essential Documents* as per GCP. However, the trial subject's medical record will be maintained by investigator, who as per the CTA – considering both medical confidentiality* and data minimisation* principles – will only be required to transfer pseudonymised data to sponsor. Considering that sponsor will only be in a position to cause trial subjects to be (re-)identified via the investigator's own records, sponsor is required to impose data retention periods on the investigators, which enable sponsor to comply with GCP. Hence, the CTA must impose an obligation for the investigator to keep on record the health data, including the codes required to identify a trial subject, for as long as required by GCP. The retention period duration depends on whether a marketing authorization is eventually obtained or not, but as

a general principle the investigators should be required to keep the data on file for at least 25 years after study completion, it being noted that sponsor is obligated to inform investigator, when the data may be erased. Were investigator to erase data, including the re-identification codes, prior to elapse of the retention period, such action may jeopardize sponsor's ability to comply with the CTR, when taking effect presumably later this year.

Even in cases where the parties have been capable of finding pragmatic solutions to inconsistencies between an institutional policy and sponsor's GDPR obligations, the mere disagreement on the positions will impose a severe delay on sponsor's trial execution and in effect sponsor needs to consider upfront if sites raising the above or similar objections, which may clearly be rejected on basis of the GDPR, should simply be excluded from the site selection process at a very early stage, as it may be quicker for the CRO to find alternative sites than for sponsor to try to fight institutional policies the result of which fight is likely to assemble the result of Don Quixote's fight against windmills. ■

Seven Need-to-Knows - *Answers*

1. The legal basis* for the processing of i) pre-submission trial data related to e.g. safety (legal obligation vested in sponsor) comprises Article 6(1)(c) in conjunction with Article 9(1)(i) of the GDPR, and ii) Article 6(1)(f) - Sponsor's legitimate interests - in conjunction with Article 9(2)(j) supplemented by 89(1) of the GDPR, when the data comprise other data.
2. GDPR consent as per Article 6(1)(a) and 9(2)(a) of the GDPR should under no circumstances be used as legal basis for the processing.
3. GDPR qualification: For data required to be collected and processed as per the protocol, sponsor is controller, whereas the investigator, and other parties handling the data as per sponsor's protocol derived instructions, are processors.
4. DPAs between sponsor on the one side and each processor on the other, e.g. the CRO, the CRO sub-contractors, the investigators (or sites) and laboratories handling biological samples.
5. Irrespective of GDPR consents being superfluous, GDPR de minimis data processing standards comprising DPIA completion, data minimisation, data security and the communication of a suitable privacy statement in the ICF must be observed.
6. Biotech companies will seldom have to appoint a DPO, and may name any CXO or the project manager, irrespectively of professional GDPR qualifications, in case of personal data breaches.
7. The investigators must undertake to store all health data generated as per the protocol for the shorter of 25 years after study completion and sponsor confirming that erasure may take place.

*References: See http://www.jusmedico.com/news-and-publications.

Acknowledgements: With special thanks of gratitude to Messr. Francis Davey, Barrister and Associate, & Mark Anderson, Solicitor and Managing Partner, both of Anderson Law LLP, who on basis of their valuable insights into the subject matter hereof, kindly provided helpful feedback and proof reading of this article.