Clinical trials under the GDPR: What should sponsors consider?

Sponsors outside the European Union conducting clinical trials in the EU should consider current guidelines and the *Breyer* case to understand whether GDPR requirements will apply to them. By **Frances Stocks Allen** and **Gail E. Crawford** of Latham & Watkins.

Many sponsors of clinical trials believe that companies based outside the EU who sponsor clinical trials conducted in the EU through clinical research organisations (CROs) and/or clinical sites do not themselves need to comply with the General Data Protection Regulation (GDPR). Sponsors believe the GDPR does not apply to them as they do not conduct the research directly but only receive results in key-coded form, and only their CROs and/or clinical sites will have access to the raw data and/or the key that connects the key-coded data to individual patients. However, sponsors need to reconsider this presumption in light of current guidelines and the *Breyer* case. Similar issues arise in other fields, for example, data and market research, in which only key-coded data is received by the organisation commissioning the research. But following the GDPR and the *Breyer* decision these organisations may still be subject to the requirements of the GDPR.

Is key-coded data personal data?

The GDPR defines "personal data" broadly to include any information relating to an identified or identifiable natural person. For this purpose, an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier, or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural, or social identity of that natural person (Article 4(1) GDPR).

***Breyer* decision:** The 2016 Court of Justice of the European Union (CJEU) decision in *Breyer v. Bundersrepublik Deutschland* (which related to Directive 95/46, the predecessor legislation to the GDPR) addressed key-coded personal data. Under *Breyer*, key-coded information in the hands of a party (Party A), to which a third party (Party B) holds the key, is likely to be considered personal data in the hands of Party A if Party A has the "means likely reasonably to be used" to access the key and to combine the key with the key-coded data. For example, the CJEU noted that Party A would not have the means likely reasonably to be used to identify the person if Party A is "prohibited by law" from obtaining access to the key code. In addition, if accessing the key code would be "practically impossible on account of the fact that it requires a disproportionate effort in terms of time, cost, and manpower, so that the risk of identification appears in reality to be insignificant," then Party A would not have the means likely reasonably to be used to re-identify the data subject. Accordingly, short of a prohibition by law or a practical impossibility to access a key code, *Breyer* suggests that an entity with only key-coded data may still have means likely reasonably to be used to re-identify the person and therefore may be deemed to hold personal data — even though the data the entity holds is solely in key-coded form.

> Clinical trial data (even in key-coded form) in the hands of a sponsor is personal data.

GDPR and *Breyer*: Since *Breyer*, there has been no case law and no updated guidance on how to apply *Breyer* to reflect the GDPR coming into force in May 2018. Hence, the question of when Party A will have the means likely reasonably to be used to re-identify a data subject using information available to Party B remains unclear. However, in Opinion 4/2007 (WP 136) the Article 29 Working Party stated that key-coded clinical trial data in the hands of a sponsor should be considered personal data, because the "identification of individuals (to apply the appropriate treatment in case of need) is one of the purposes of the processing of the key-coded data". Neither the GDPR nor the *Breyer* judgment contradict this view. Therefore, we do not expect the supervisory authorities to change their view that key-coded clinical trial data in the hands of a sponsor should be considered personal data. This approach tallies with the generally accepted industry view that clinical trial data (even in key-coded form) in the hands of a sponsor is personal data.

In the context of a clinical trial, CROs and clinical sites will be subject to certain obligations of confidentiality and good clinical practice (which will impose certain limitations on a sponsor's ability to personally identify data subjects). However, it remains unclear whether these limitations are sufficiently strict or comprehensive to support a determination that a sponsor does not hold personal data (i.e., such restrictions may not constitute a prohibition by law or make access to the key code practically impossible). The lack of clarity is particularly relevant in light of the regulatory obligations a sponsor retains to report significant safety issues to regulators, or the information a sponsor may need to access in connection with litigation involving a subject injury.

Biological samples and personal data: Sponsors should keep in mind other considerations if they receive key-coded biological samples that contain

genetic data of the relevant data subject from a CRO or site. Specifically, both the Article 29 Working Party and France's supervisory authority, the CNIL, have questioned whether such data can ever be considered not to be personal data, given the unique nature of genetic data and the availability of DNA databases that facilitate re-identification. Therefore, if a sponsor receives biological samples from trial participants, the likelihood the sponsor will be considered to hold trial participants' personal data may be even higher than when only key-coded data is received in the form of study results.

Current recommendations for sponsors: On the basis of existing guidelines and case law, and subject to any forthcoming guidance, the most conservative approach for sponsors is to assume that EU supervisory authorities will view non-EU based sponsors of EU-based clinical studies as holding personal data relating to trial participants — even if sponsors receive only key-coded data or samples. Sponsors should therefore take steps to comply with GDPR requirements, whilst maintaining a watching brief for updated case law and guidance.

Sponsor as controller under the GDPR

The GDPR defines the "controller" of personal data as the entity that alone, or jointly with others, determines the purposes for and means by which the personal data, including sensitive health data, of individuals in the EU is collected, stored, analysed, transferred, and otherwise processed. A sponsor is therefore likely to be the controller in connection with a CRO or site's processing of personal data on its behalf in connection with a clinical trial, as the CRO or site processes the data for, on behalf of and at the direction of, the sponsor. However, the contractual relationship will differ from traditional processing agreements, specifically with the right to access or receive the data processed by the CRO.

Liability for Sponsors

As a controller of European personal data, a sponsor will have final responsibility for ensuring the GDPR compliance of a CRO or site's performance of processing activities on the sponsor's behalf and will be subject to significant potential liability under the GDPR, including:

- Compensating data subjects for damage caused by unlawful processing, such as a data breach
- Administrative fines for non-compliance of up to the higher of: (a) 4% of the annual turnover of a sponsor's group of companies; and (b) 20 million

What action should a sponsor take now?

In the short term, a sponsor should:

- Review its consent forms and the legal basis on which it relies to process the personal data of patients enrolled in clinical trials, to assess which supplementary notices or new consent forms will be necessary to ensure that GDPR transparency requirements are met. Member States have taken conflicting views as to whether consent is a valid legal basis under the GDPR for the processing of special category personal data of patients in these circumstances. Furthermore, different Member States may have introduced specific local derogations that allow such processing subject to documented controls or may have mandated specific consent wording. Therefore, this analysis will need to be conducted on a country-by-country basis for each trial site.
- Enter into a GDPR-compliant data-processing agreement for each EU-based study with each CRO or site that processes personal data as a processor of the sponsor, to ensure that the CRO or site processes patients' personal data from that study in compliance with the GDPR.
- Review the basis on which a sponsor relies and the protections it implements to transfer the personal data of patients enrolled in clinical trials from the EU to countries outside the EU, to ensure that these protections are adequate from a GDPR and European Commission perspective.

In addition to these priority actions, sponsors should also prepare to take more significant steps to ensure the compliance of their operations with the GDPR, including but not limited to:

- **Appointing a legal representative for GDPR purposes if they have no EU establishment** (Articles 3 and 27 GDPR and European Data Protection Board Guidelines on the territorial scope of the GDPR).
- **Completing a record of processing** (Article 30 GDPR and Article 29 Working Party Position Paper on derogations).
- **Updating its privacy governance framework** (various provisions of the GDPR, including Article 25).
- **Introducing GDPR-compliant policies and accountability** (various provisions of the GDPR, including Articles 13, 14 and 25 and the Article 29 Working Party Guidelines on transparency).
- **Assessing appropriate data retention periods** (Article 5(e) GDPR).
- **Reviewing data breach procedures** (Articles 32-24 GDPR and Article 29 Working Party Guidelines on personal data breach notification).
- **Assessing whether it will need to appoint a Data Protection Officer** (Articles 37-39 GDPR and Article 29 Working Party Guidelines on Data Protection Officers).

> As a controller of European personal data, a sponsor will have final responsibility for ensuring GDPR compliance.

AUTHORS

Frances Stocks Allen is an Associate, and Gail E. Crawford a Partner, at Latham & Watkins.
Emails: frances.stocks.allen@lw.com
gail.crawford@lw.com