Part 2: GDPR Compliance - Improving Your Position

In Part 1 of our series, we surveyed certain challenges in the negotiation of indemnification language in clinical trial agreements. That article, https://iceglobalconsulting.com/insights/, explored solutions when clinical trial sites, inclusive of academic and state-funded institutions in the United States, are unwilling to mutually indemnify the sponsor. For Part 2 of our series, we shift gears and wade through some of the critical aspects of compliance in contracting across the Atlantic. This article will focus on the basics of evaluating compliance with the General Data Protection Regulation ("GDPR") within the evolving framework of guidelines and court opinions. In order to narrow the scope, we will concentrate primarily on basic considerations of a U.S.-based sponsor doing business in a European Union country.

The data protection and privacy landscape in the U.S. continues to shift, as California and Virginia laws went into effect on January 1, 2023. However, the most complex compliance regulation for transatlantic business continues to be the GDPR. Specifically, if your clinical trial involves companies or clinical trial sites in Europe, or the broader European Economic Area, then this article serves as a reminder that you may need to review your compliance with the GDPR.

Personal Data

Most privacy professionals consider the GDPR to be the widest-reaching data privacy regulation to date. If your business handles any information that is related to an identified or identifiable natural person, you handle personal data. If you handle personal data of a European citizen or resident, then it is almost guaranteed that you need to pay careful attention to what the GDPR means for your business. In the context of this article, the reference to "personal data" means the defined term from the GDPR.

More specific to clinical research, a U.S. CRO doing business with a European company is likely to have additional compliance requirements to navigate when handling personal data – and not just patient data, but that of site personnel as well. Likewise, even if you receive what you consider to be "de-identified" patient data, you should strive to understand the difference between truly anonymous data and "pseudonymized" data under the GDPR. It is safe to say that if re-identification of the person is possible in any way, then the data is still governed as personal data under the GDPR. If this does not make clear the potential compliance requirements surrounding your handling of personal data, then consider that most privacy professionals believe that achieving true anonymization may be effectively impossible under the GDPR and the guidelines published by the European Data Protection Board.

ICE GLOBAL
CONSULTING

Processing Personal Data

The GDPR specifically uses the word "processing" to capture the many ways personal data is handled, and an analysis of processing activities must be at the core of your compliance considerations. The GDPR assigns certain obligations depending on which company controls the purposes and means of processing (a "controller") and which company handles the actual "processing" activities (a "processor"). For that reason, as a company, you must determine what your obligations are and whether you are in fact the "controller" or the "processor". Further, your company may also have obligations to ensure that personal data is adequately safeguarded when processed and transferred from the European Union – even if this data originated in the U.S. and is returned to the U.S. The GDPR is expansive in its reach and applicability to U.S. businesses working with European companies and it is imperative that you understand the risks of infringements of the GDPR.

Why you need to have a Data Processing Agreement

There are both legal and contractual requirements to have a Data Processing Agreement ("DPA") if personal data is being processed. The two simple rules to follow are that (a) you must have a DPA in place with every party that has access to the personal data, and (b) that both the controller and processor have obligations under the GDPR which necessitate a DPA. The GDPR is very prescriptive when it comes to DPA requirements, and outlines these (in part) in Article 28(3). Generally, you should expect to define (i) the scope and purpose of the processing, (ii) the relationship between the parties, and (iii) the obligations of each party. Most often, you will see DPA terms in some format with the 2021 Standard Contractual Clauses ("SCCs") appended as an exhibit or addendum. The DPA and SCCs, and how to manage their implementation, are indeed requisite of their own entire series of articles.

When it comes to incorporating DPA requirements into the clinical trial agreement ("CTA"), you have options. It is not uncommon to see terms woven into the CTA itself, added as an addendum, or incorporated via a standalone agreement – and lest we forget the Standard Contractual Clauses and the overlap these may have with your DPA terms.

As with most intricate regulation, there are exceptions to the general information in this article. ICE Global Consulting's team of attorneys and experienced global negotiators work with sponsors, CROs, and sites to resolve common and complex issues unique to clinical trial agreements requiring Data Processing Agreements and/or the Standard Contractual Clauses every day.

If you are looking to navigate these issues or learn how our team prepares our partners to understand the impact of the GDPR, we encourage you to contact us at info@iceglobalconsulting.com and visit our website at www.iceglobalconsulting.com.