Legal Insight

K&L GATES

www.klgates.com

June 19, 2012

Practice Group(s):

Health Care

Life Sciences

Data Protection in Clinical Studies – Implications of the New EU General Data Protection Regulation

By Mathias Schulze Steinen and Daniela Bohn

The European Commission published in January 2012 a proposal for a regulation setting out a general framework for data protection. The proposal, after adoption, shall supersede the current Data Protection Directive with a revised set of data protection rules that will apply directly across all Member States. Although the Regulation will continue many of the established principles of existing EU data protection law, there are significant changes in key areas that will affect the day-to-day business of companies in the life sciences and health care sectors. The practicality of some proposed changes is in question, and interested parties may wish to engage in the legislative process to ensure that the final draft takes into account the particular industry needs. The following article examines the impact of the proposed changes on clinical trials and their practicality in a global environment.

Background of the Proposal

Data protection in the European Union is currently governed by the EU Data Protection Directive (Directive 95/46/EC, "Directive") as of 1995 and the various national laws implementing the Directive in each Member State. Rapid technological developments and corresponding challenges for privacy regulation led the European Commission to introduce on January 21, 2012 a proposal for a new regulation governing the protection of individuals with regard to the processing of personal data and the free movement of such data (General Data Protection Regulation, "DPR"). The DPR, once adopted, will replace the existing Directive and the various inconsistent national data protection laws. The DPR will be directly applicable in all member states of the EU without any need of implementation in the Member States. It will provide a comprehensive and consistent EU wide data protection level that provides a uniform data protection regime and a simple but stronger enforcement framework in all Member States of the EU. The proposed regulation will now go through the EU legislation process and is expected to be adopted in 2014. Now is the time for interested parties to actively engage in the discussions on the proposal for the DPR to ensure that the final form takes account of particular needs of the industry and business operations.

Implications for Clinical Trials

Collection, processing and transfer of personal data, in particular individuals' patient records, in compliance with applicable laws are critical to the success of clinical studies. As such, the adoption of the current draft proposal will have an important impact on sponsors, investigators and other parties involved in clinical trials. The DPR, in particular, attends to the following challenges of data management:

- Unification with respect to the qualification of key-coded patient data and patient identifiers, the 'keys', as personal data and clarification of applicability of EU data protection laws for key-coded data;

- Clarification of the roles and responsibilities of sponsors and CROs as data controller;
- Definition of various additional regulatory obligations for sponsors and CROs as data controllers and data processors;
- Clarification of guidance on existing restrictions in relation to data transfers from the EU to parties resident outside of the EU;
- Introduction of EU-wide legal sanctions for violation of data protection laws including aggravation of administrative fines.

The planned amendments require international sponsors and other global participants to carefully examine the proposed DPR in order to evaluate the impact on the organization and management of clinical trials and other related business and ways of implementation.

Personal Data - Applicability of EU Data Protection Laws

Under the regime of the Directive, regulators in the various Member States have different opinions on the status of key-coded data (pseudonomyzed data where references to patient names have been changed to code numbers, with a 'key' as patient identifier showing which number corresponds to which name), i.e. whether key-coded data qualify as personal data, and with respect to data related to the health of the patients as sensitive data, and whether data protection laws apply to key-coded data. While some Member States compare key-coded data to anonymized data and do not consider key-coded data personal data, in particular if the sponsor does not have direct access to the key to re-identify the data subject or patient, other Member States apply data protection laws regardless of the possibility to re-identify the data subjects.

The DPR makes it clear in the definition of the term "personal data" that key-coded data is considered personal data. CRFs contain key-coded data that are specific to one individual who can be identified through the identification number by the investigator ("any other person") at least without unreasonable efforts, even if the sponsor or CRO does not have access to the key and/or does not de-identify the data. Indeed, under good clinical practice rules established by Directive 2001/20/EC (Clinical Trials Directive) and the GCP Directive, the CRFs have to be key-coded in a way that allows the sponsor, through the investigator, to retrieve individual persons. This clarification in the DPR harmonizes inconsistent regulations in EU Member States under the Directive by uniformly applying EU data protection laws to key-coded data in clinical trials, i.e. participants holding the CRFs. This clarification will also have a direct impact on US companies that participate in the Safe Principles. While the US Department of Commerce did not consider key-coded data subject to the Directive and did not apply Safe Principles to transfers of key-coded data from the EU (cf. Question 7 FAQ), the DPR will require US companies to apply Safe Principles if they receive key-coded data from the EU.

Who is responsible?

The data protection related qualification of the parties involved in clinical trials, in particular the qualification of the sponsor and CRO as data controller or data processor, is critical as it determines the scope of obligations and regulatory requirements applying to such party.

The DPR holds up the concepts of data controller and data processor using identical definitions as provided by the Directive. Under the definitions, the sponsor, in most cases, is considered the data controller as the sponsor is the one who initiates the trial and determines the purpose and means of processing the collected data. It is not relevant whether the sponsor is resident in the EU or has an establishment in one of the EU Member States as long as the data is collected in the EU. Due to its

control over the use of any service providers in the clinical trial, including the CRO, the sponsor will not be able to assign or pass on its function and ultimate liability as data controller to the CRO.

The position of the CRO depends to a large extent on the factual situation of the trial and the CRO's role and obligations but it comes closest to the position of a data processor. However, if a CRO takes over most of the functions of a sponsor while the involvement of the sponsor is limited to the financing of the trial, this may have consequences for the qualification under the DPR and, in this case, the CRO may be considered being a data controller. In case the sponsor is located outside of the EU, the European CRO cannot be a mere data processor and always qualifies as data controller.

Additional obligations

The DPR will impose a number of additional requirements on each data processor and data controller, over and above current requirements. For example, both data controllers and data processors will have to maintain detailed documentation on the processing operations (Art. 28). Both will be required to implement appropriate security measures to protect the data, and, where they have more than 250 employees, to appoint a data protection officer.

A sponsor established outside of the EU could also be required to designate a representative in the EU if the processing activities relate to the "offering of goods or services to such data subjects or the monitoring of their behavior." The current wording can be interpreted in a way that sponsors in clinical trials may fall under this obligation unless certain exemptions apply, such as a European Commission decision that the resident country of the controller ensures an adequate level of protection, the company has fewer than 250 employees, or the services offered to residents in the EU are only occasional. Whether authorities will consider clinical trials to be occasional services remains to be clarified.

The DPR would also ease some administrative burdens. For example, companies will no longer be required to register data processing activities with national data protection authorities, which is common practice in several Member States. Hence, sponsors of clinical trials will not have to register the clinical trial for data processing purposes with the data protection authority in the Member State where the trial is being performed or any other Member State.

However, the DPR requires that where processing operations "present specific risks to the rights and freedoms of data subjects by virtue of their nature, their scope or their purposes," the controller or processor must carry out a data protection impact assessment of the processing activity (Art. 33). The type of information potentially constituting a specific risk is broad and includes information on a person's health, race and ethnic origin. Prior to processing the data, the data controller shall be required to seek authorization from the data protection authority on the basis of the data protection impact assessment. The authority has the right to prohibit the processing or propose changes to deal with any breach of data protection laws if it thinks that the intended processing does not comply with the DPR, in particular where risks are insufficiently identified or mitigated. In addition, the controller shall seek the views of the data subjects on the intended processing. It is currently unclear how this requirement shall work in practice. Enforcement of this requirement under the current wording would have significant impact on the day-to-day activities of the parties involved in clinical trials.

International transfer of clinical data

The qualification of investigator and sponsor as data controllers under the Directive and the DPR also means that any international transfer of personal data between these parties must comply with the restrictions on transfer of personal data to non-EU countries.

The DPR does not solve the issue of data transfers from the EU to a recipient with its seat outside of the EU, e.g. transfer of clinical data from a European investigator to its US sponsor. The DPR maintains the restriction on transfers of personal data from EU Member States to other countries outside of the EU where the legal regime does not ensure an adequate level of privacy protection for individuals, for example the US. The DPR retains existing data transfer solutions, including EU standard contractual clauses and binding corporate rules. In order to force the use of binding corporate rules in global companies the DPR clarifies the definition of binding corporate rules and requirements for their approval by the authorities. The framework set by the DPR will likely give foreign companies easier guidelines on how to draft such corporate binding rules.

In addition, the DPR defines specific criteria for the EU Commission decision with respect to when a country or territory ensures an adequate level of protection. Under the regime of the Directive the EU Commission has found that the Safe Privacy Principles as adopted in the US provide adequate protection for the purposes of personal data transfers from the EU. This decision will remain valid under the DPR so that data transfers to sponsors in the US that have subscribed to the Safe Principles and adhere to these principles would be permitted and be considered compliant with the DPR. However, compared to corporate binding rules and other transfer mechanisms the Safe principles still do not provide a reliable level of data protection and high administrative burdens so that US companies should carefully consider the use of other data transfer solutions.

Notably, the DPR for the first time permits that specific sectors, e.g. the health care sector, in a certain country can be considered as having an adequate level of data protection. Industry-specific rules such as the Health Insurance Portability and Accountability Act of 1996 may form a basis for such industry-specific decisions as they partially provide stricter rules than the EU regime.

Informed Consent

Pursuant to the Clinical Trial Directive (Directive 2001/20/EC) data subjects in clinical trials conducted in the EU must provide informed consent before participating in the trial. The DPR does not bring significant practical changes in this respect.

Consent remains an important justification for processing of personal data, including sensitive health data, under the DPR (Articles 7, 9). Under the DPR unambiguous consent still requires a written form and detailed information of the patient regarding the data processing, including objectives, risks and inconveniences of the trial. Different from the Directive, the DPR now specifies in a separate Article the requirements for consent of the data subject. The controller bears the burden of proof for the data subject's consent, and if consent is given in the context of a written declaration that also concerns another matter, the requirement to give consent as the data subject must be distinguishable in its appearance from the other matter.

Legal Consequences

The DPR itself provides regulations for consequences of a violation of the data protection regime and increases fines for such violations. Penalties for non-compliance with DPR rules will rise and implementation of an effective data protection system will become more important. According to the DPR, supervisory authorities could impose fines on companies infringing data protection laws in the amount of up to EUR 1 million or 2% of the global revenue of a company. This shall apply if data protection regulations with respect to the transfer of personal data are not met or the company does not appoint a data protection officer despite an obligation to do so. In addition, and sometimes more important with respect to the success of a clinical trial, supervisory authorities could issue orders that

prevent a sponsor or CRO from using or transferring the collected personal data if such transfer or use is considered illegal. Therefore, sponsors should have a great interest in supervising their investigators and ensuring that data collection and transfer is in line with the new regulations of the DPR.

Authors:

Mathias Schulze Steinen
mathias.schulze-steinen@klgates.com
+49.69.945.196.260

Daniela Bohn
daniela.bohn@klgates.com
+49.69.945.196.265