CONTROLLING PERSONAL DATA – THE CASE OF CLINICAL TRIALS

By: Kristof Van Quathem
Data Protection Compliance Advisor, Covington & Burling[1]

Since its adoption in 1995, Directive 95/46/EC, commonly known as the *Data Protection Directive*, has aroused debate and controversy.[2] While the Directive seeks to ensure the free circulation of personal data in the EU by creating a level playing field of protection, in fact, it has proved more of a headache with its numerous arcane provisions and inadequate Member State implementation.

For those working with personal data in clinical trials, the problems can be even worse. First, clinical trials by definition deal with health data, which are sensitive data. Second, the pharmaceutical industry and the activities of physicians are highly regulated, which often increases the complexity from a data protection point of view. Third, there are a large number of parties involved in clinical trials who all, in some way, deal with this sensitive personal data. And fourth, clinical trials are conducted on a large scale with personal data of thousands of patients being processed. In short, masses of sensitive data are processed in a plethora of circumstances within a complex regulatory environment.

According to Article 3(2)c of the EC Clinical Trials Directive[3], a trial may be undertaken only if "the rights of the subject to physical and mental integrity, to privacy and to the protection of the data concerning him in accordance with Directive 95/46/EC are safeguarded." In other words, clinical trials can only be conducted in line with data protection laws. Data protection laws supplement other rules governing trials, such as the Clinical Trials Directive and its implementing rules, and the Good Clinical Practices (GCP).

Even though most aspects of the Data Protection Directive affect clinical trials, two elements significantly complicate the conduct of clinical trials that are undertaken in several Member States: the definition of "data controller," and the definition of "personal data," (particularly key-coded data). Discussing these issues is especially timely because the Article 29 Working Party, which consists of representatives from the national data protection authorities (DPAs), is poised to

---

[1] The opinions expressed in this article are only those of the author and do not bind the firm. Readers should take legal advice before applying the information contained in this article to specific issues or transactions.

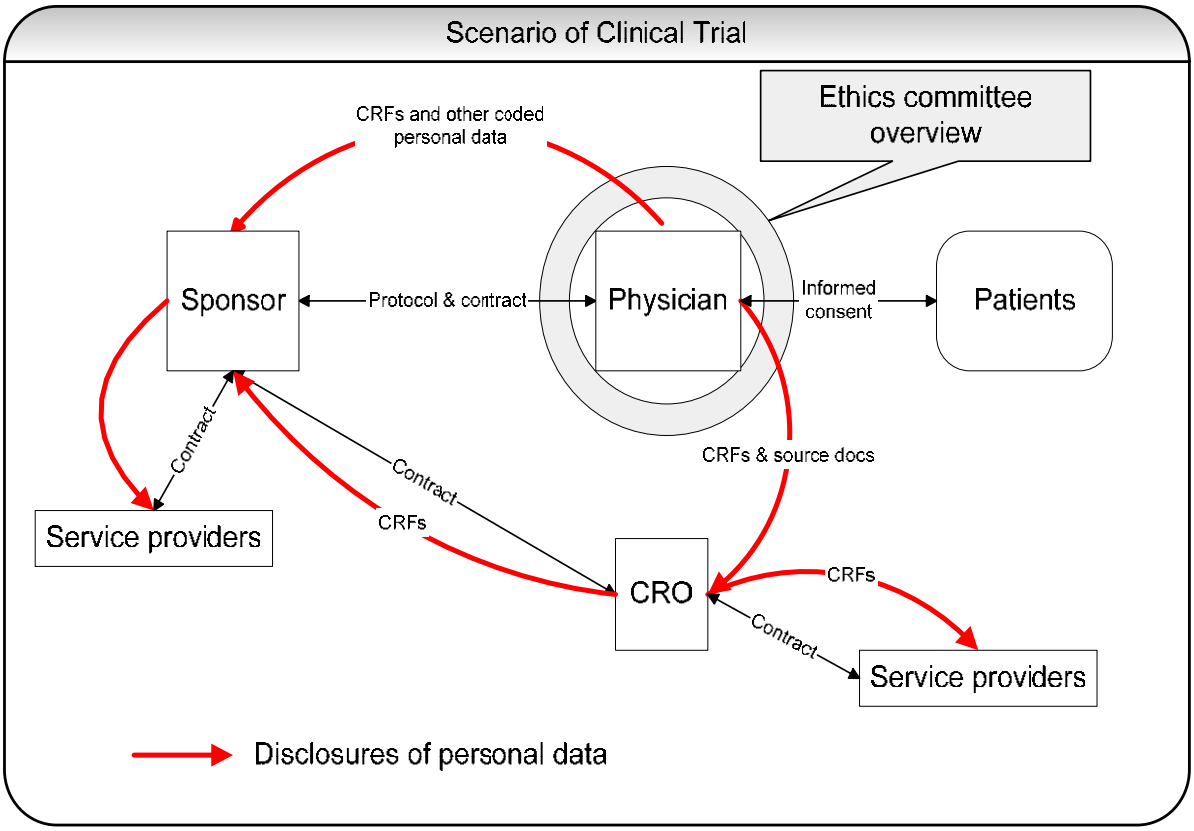
[2] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data., *OJ L 281*, 23 November 1995, pp. 0031 – 0050.

[3] Directive 2001/20/EC of the European Parliament and of the Council of 4 April 2001 on the approximation of the laws, regulations and administrative provisions of the Member States relating to the implementation of good clinical practice in the conduct of clinical trials on medicinal products for human use. *OJ L 121,* 1 May 2001, pp. 34 – 44. For a more detailed description of the Directive see: Joanne Beesley, The EU Clinical Trials Directive., *Regulatory Affairs Journal, Pharma*, January 2004, pp. 12 – 17.

consider a "Pharmaceutical Code of Conduct" that will deal with the issues surrounding the key-coding of personal data.

This article will focus on these two elements of the Directive and their impact on clinical trials. The first section briefly discusses the data flows in a classical clinical trial, then the application of data protection law and the implications for sponsors and investigators are discussed.

Data Flows in Clinical Trials



It is not our intention to provide an in-depth analysis of the different types of clinical trials that exist or the different procedures that apply. To help us structure our arguments we will use a practical scenario. The scenario is based on clinical trials performed according to the "Guidelines for good clinical practices for trials on pharmaceutical products" (GCP)[4] requirements, and is a somewhat simplified representation of how clinical trials ordinarily take place. Very often, clinical trials are organized as indicated in the picture above. [5]

---

[4] These guidelines have been developed on the basis of the Helsinki Declaration, and national regulations that exist in most developed countries for this type of research. In the EU, the implementation of good clinical practices has been harmonized by Directive 2001/20/EC of 4 April 2001. This Directive mandates the observance of the principles of good clinical practice.

[5] Truth be told, the above scenario is a simplification of reality. The role of the sponsor, CRO and investigator is not always as clear cut. For example, investigators may lead clinical trials and act as a sponsor, while the private company only finances the research. The application of data protection rules will always depend on the specific circumstances in which a clinical trial is conducted. However, we believe that the basic concepts we discuss in this article are relevant in most variations of clinical trails that occur in practice.

The "sponsor" in our case is a pharmaceutical company that wants to have one of its experimental medicines tested.[6] The sponsor relies on physicians (investigators[7]) to perform the trials. Generally those physicians are specialist in their field and linked to a (university) hospital.

The relationship between the physician and the sponsor is governed by a "protocol" and a research contract. The protocol is verified and approved by the independent ethics committee of the country where the investigator is established. The protocol sets forth in great detail what the physician should do.[8] For example, it contains information on the trial design (duration, dosage regime, use of placebo, etc.), the selection and number of patients, the treatment, the quality control and assurance, but also on data handling and record keeping, and on the information that the physician has to record for the sponsor.

The physician keeps detailed reports, called case report forms (CRFs), on each patient.[9] Here again, the protocol sets forth how these CRFs should be kept, what information they should contain, how the CRFs can be completed, how corrections can be made, and how the CRFs are to be transmitted to the sponsor. The CRFs contain all sorts of information on how patients react to medicines, their test results and the treatment they received.

On the basis of GCP and the protocol, the physician key-codes the data in the CRF and sends the key-coded CRF to the sponsor.[10] The key of the code remains with the investigator and is covered by his or her confidentiality obligation. The sponsor keeps a level of control over the physician, but often outsources this control to a clinical research organization (CRO).[11] The CRO monitors on behalf of the sponsor whether the physician performs the trials in conformity with the protocol. To do this properly, the CRO must have access to all information, including non-coded source documents. Finally, it should be noted that the sponsor and the CRO may rely on other companies or consultants to perform specific operations (tests, statistical analysis, etc.) on the information it receives.

---

[6] Directive 2001/20/EC, Article 2(e), defines sponsor as "an individual, company institution or organization which takes responsibility for the initiation, management and/or financing of a clinical trial."

[7] Directive 2001/20/EC, Article 2(f), defines investigator as "a doctor or a person following a profession agreed in the Member State for investigations because of the scientific background and the experience in patient care it requires. The investigator is responsible for the conduct of a clinical trial at a trial site. If a trial is conducted by a team of individuals at a trial site, the investigator is the leader responsible for the team and may be called the principal investigator."

[8] Directive 2001/20/EC, Article 2(h), defines protocol as "a document that describes the objective(s), design, methodology, statistical considerations and organization of a trial. […]." On the content of a protocol see GCP, Section 6.

[9] GCP, 1.11.

[10] GCP, 1.58 and 5.5.5. In addition to the CRFs, patients are often also required to fill out questionnaires on how the medicine or trial affected their quality of live. This information is also key-coded and transmitted to the sponsor.

[11] GCP, 5.1.2 and 5.15.1.

Definition of personal data applied to key-coded CRFs

Even though, and to some extent actually because, there are strict rules on clinical trials, the application of data protection laws to the personal data generated by clinical trials raises many problems. One of the main difficulties relates to the nature of the collected personal data and, in particular, the status of key-coded (personal) data contained in CRFs. The Data Protection Directive defines "personal data" as:

"any information relating to an identified or identifiable natural person ('data subject'); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity."[12]

At first reading, the Directive's definition of personal data seems clear: the key-coded CRFs contain data that are specific to one individual who can be identified through a random "identification number," and thus, remain personal data covered by the Data Protection Directive. As a result, the sponsors or CROs holding the CRFs are subject to the obligations imposed by the law. However, a number of authors and regulators have pointed to Recital 26 of the Directive, which, in their opinion, introduces an important nuance: [13]

"Whereas the principles of protection must apply to any information concerning an identified or identifiable person; whereas, to determine whether a person is identifiable, account should be taken of all the means likely reasonably to be used either by the controller or by any other person to identify the said person;[…]" *(emphasis added)*.

In essence, the recital suggests that data may not be considered personal data if it would take unreasonable efforts to identify a person. In our opinion, this interpretation wears thin in the case of key-coded personal data because of the addition of the terms "either by the controller or by any other person." The very nature of key-coded data is that someone holds the key, and thus, that someone ("any other person") can de-code the data and quite easily so. Therefore, in the case of clinical trials, the sponsor holds key-coded CRFs, which are still personal data covered by the law, because the investigator holds the key to the CRFs and can de-code the CRFs without unreasonable efforts.[14] Indeed, under GCP rules, the CRFs have to be key-coded in a way that allows the sponsor, through the investigator, to retrieve individual patients.[15]

---

[12] Directive 95/46/EC, art. 2(a).

[13] E-B van Veen, Gecodeerde gegevens bij wetenschappelijk onderzoek: een begripsverheldering, *Privacy & Informatie*, Nr. 6, December 2003, p. 261.

[14] This has already been indicated by other authors, for example, M.C. Ploem, Medisch-wetenschappelijk onderzoek met gecodeerde gegevens. De toepassing van de privacy wetgeving, *Computerrecht*, 2000/2, p. 72.

[15] GCP, 5.5.5.

National regulators, nevertheless, have adopted divergent positions on the qualification of key-coded data under data protection law. In particular, DPAs are divided on the question whether the CRO or the sponsor holds personal data if they only receive and keep key-coded data without having access to the key. Some DPAs adopt the literal reading of the Directive as we did above, and consider that whenever "any other person" than the holder of the key-coded data can identify the data subject, the data are subject to the data protection law (the holistic approach). Other Member States, however, only consider relevant the possibility of the holder to identify the data subject, and do not believe that the possibility of others to identify the data subject should have a bearing on the qualification of the data in the possession of the holder (the individual approach). Below, we provide some illustrative examples of each of these positions.

Holistic **approach to personal data**

Belgium

The Belgian legislature adopted a very broad definition of personal data that covers key-coded data and extends to entities who do not even hold the key. At the time of the law's adoption, the Belgian DPA indicated in an opinion that such a broad definition could raise difficulties in its application.[16] However, the legislature disregarded the opinion**.** Having lost the argument, the DPA supported the broad definition in an opinion of 2000 and stated that "the data subject does not necessarily have to be identifiable by the controller, but by *any person* using whatever means likely reasonably to be used by that person."[17]

France

France only recently enacted the EU Data Protection Directive. The new law leaves little doubt on the status of key-coded data. Indeed, the Directive's Recital 26 reference to "any other person" has been included in the actual definition of personal data in the law.[18] This position does not present a radical shift. In a 1999 report on the mandatory registration of AIDS patients, for example, the DPA indicated that "nowadays many electronic data processing operations conducted in the framework of epidemiologic research are "indirectly identifiable" […], and, as such, subject to the law."[19]

---

[16] Parliamentary documents, 1566/1/97/98 – p. 12.

[17] Commission de la protection de la vie privée, *Avis (2000/34) d'initiative relatif à la protection de la vie privée dans le cadre du commerce électronique.*, p. 6. For Austria, see: W. Dohr and E. M. Weiss, *Kommentar Datenschutzrecht.*, Manzsche Verlags- und Universitätsbuchhandlung, p. 42.

[18] Loi du 6 janvier 1978 modifiée relative à l'informatique, aux fichiers et aux libertés, Art. 2.

[19] CNIL, *Rapport relative aux modalités d'information de la surveillance épidémiologique du sida.*, 1999, p. 14.

Sweden

In Sweden, the DPA also adopted a position of principle that key-coded data are personal data. In a report of 2003 on the use of sensitive data for research purposes, the DPA states that "key-coded data are covered by the law, as long as a key exists with the help of which it is possible to identify single individuals. It is of no significance where the key is kept or who is in possession of it. The same applies to encrypted data. As long as the key exists, the data are not anonymized in the sense of the Personal Data Act."[20]

Individual **approach to personal data**

Netherlands

In the Netherlands, the DPA adopted a diametrically different position from the above countries. In 2002, the DPA approved a code of conduct proposed by Nefarma, the national organization of pharmaceutical companies. The code deals specifically with the processing of personal data in the context of clinical trials. In the comments to the code, the DPA explicitly states that "key-coded data processed in the context of clinical trails, conducted in accordance with the GCP, are not covered by the data protection law." The code is up for revision in 2007.[21]

United Kingdom

The UK Data Protection Act contains a simple definition of personal data, with a clear position on the question at hand: ""personal data" means data which relate to a living individual who can be identified: (a) from those data, or (b) from those data and other information which is in the possession of, or is likely to come into the possession of, the data controller, […]."[22] Thus only data in the possession of the controller is being considered, not the possibility of "any other person" to identify the individual.

Safe Harbor Agreement Between the EU and US

In 2000, the EU and US negotiated the Safe Harbor Agreement as a mechanism to legalize transfers of personal data from the EU to the US. US companies certifying to the Safe Harbor Agreement commit to upholding a level of protection accepted as adequate by the EU. As a result, transfers of personal data to such companies are not subject to additional restrictions.

Also**,** the Safe Harbor Agreement addresses the issue of key-coded data in clinical trials. FAQ 14, an integral part of the Agreement, provides:

---

[20] Datainspektionen, *Behandling av känsliga personuppgifter i forskningen.*, Report 2003:1, p. 5.

[21] Nefarma Code, Explanation to Article 2.1.), *Staatscourant*, 2 September 2002, p. 18.

[22] Data Protection Act: 1998, Part I, 1(1).

"7. Q: Invariably, research data are uniquely key-coded at their origin by the principal investigator so as not to reveal the identity of individual data subjects. Pharmaceutical companies sponsoring such research do not receive the key. The unique key code is held only by the researcher, so that he/she can identify the research subject under special circumstances (*e.g.* if follow-up medical attention is required). Does a transfer from the EU to the United States of data coded in this way constitute a transfer of personal data that is subject to the Safe Harbor Principles?
7. A: No. This would not constitute a transfer of personal data that would be subject to the Principles."[23]

In other words, key-coded data are not considered personal data, and, thus, are not covered by EU data protection law. The Safe Harbor Agreement has been approved by all EU Member States.

Summary

The divergence of positions on the status of key-coded data can be summed up into two categories: (1) the *holistic* approach, emphasizing that if "anyone" can de-code the data with reasonable means, this data must remain "personal data" (Belgium, France, Sweden), and (2) the *individual* approach, which only considers the possibility for the holder of key-coded data to de-code that data (Netherlands, UK, Safe Harbor Agreement). In our experience, countries such as Germany, Finland, Hungary, Lithuania, and Italy seem to prefer the individual approach, even though the DPAs often decline taking strong positions.

The practical consequences of these different views can be very significant. Indeed, the status of key-coded data determines whether or not the data protection law applies to entities holding key-coded data. The qualification of key-coded data has an impact on the identification of the "data controller" of a clinical trial, and, for pan-European trials, on the determination of the applicable national data protection law.

Who controls whom and what?

The Data Protection Directive distinguishes between two different key actors. First, there is the "data controller," defined as "the natural or legal person […] which alone or jointly with others determines the purposes and means of the processing of personal data; […]."[24] The identification of the data controller is important because most of the obligations under data protection law fall on the controller, and because, according to the Directive, the country of establishment of the controller determines the applicable data protection law. Hence, a controller established in the UK must comply only with the UK Data Protection

[23] Commission Decision of 26 July 2000 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the safe harbour privacy principles and related frequently asked questions issued by the US Department of Commerce. *OJ L 217*, 25 August 2001, p. 24.

[24] Directive 95/46/EC, art. 2(d).

Act, even if this controller collects data in other EU countries. However, if this controller has establishments in, for example, France and Belgium, then the data processing by these establishments must comply with French or Belgian data protection law respectively.

Second, the Data Protection Directive created the concept of a "data processor," defined as "a natural or legal person […], which processes personal data on behalf of the controller."[25] Whenever a controller outsources the processing of personal data to a data processor, the controller must ensure that this activity is governed by a data processing contract. This contract must define the role of the processor and the security measures to be implemented by the processor.[26]

How can these concepts be applied in the framework of a clinical trial? In particular, who is considered the data controller of the personal data generated by a clinical trial? What is the status of the investigator, the sponsor, and the CRO? Only when we have answers to these questions can we determine which data protection laws apply to the processing of key-coded CRFs, if any.

Sponsor

In the majority of cases, the sponsor in our clinical trial scenario is considered a data controller, subject to the relevant data protection laws. Conceptually, this qualification is based on one or more of the following three arguments.

(1) The sponsor processes personal data.

As indicated above, DPAs disagree on this point. If key-coded CRFs contain personal data (as in Belgium, France and Sweden), it is obvious that the sponsor who receives key-coded data becomes the data controller, subject to relevant data protection laws. On the other hand, if key-coded data are not considered personal data, then the sponsor may not be a data controller because he or she never receives personal data. This is the position taken by the Netherlands under the Nefarma code. To us, this reasoning is somewhat superficial because, as we demonstrate below, there are other reasons why a sponsor can be considered a data controller.

(2) The sponsor has access to source documents.

Sponsors and/or their CRO, on the basis of informed consent from the patient, often have access to non-coded source documents held by the investigator to monitor the investigator's compliance with the protocol. This access to source documents seriously affects the key-coded nature of the CRFs. It seems clear that it would not be difficult for a sponsor to identify patients, if at one point in time he or she has access to the patient's medical file. In other words, the sponsor can identify patients using "reasonable means" at his or her disposal.

[25] Idem, art. 2(e).

[26] Idem, art. 17.

The data contained in the key-coded CRFs thus become personal data, and the sponsor becomes a data controller. This is apparently the main reason why the Italian and German DPAs generally consider sponsors as data controllers.[27] In the Netherlands, by contrast, this element does not seem to affect the sponsor's position under the Nefarma code.

The Italian DPA, however, pointed to an interesting "solution" to this problem. According to the DPA, the sponsor could avoid being considered a data controller if the access to the source documents occurs under the supervision of the investigator. In other words, the sponsor would become a "data processor" of the investigator when accessing non-coded medical files. The processing of the key-coded CRFs by the sponsor could then fall outside the scope of the data protection law because they would not be considered to contain personal data.[28]

(3) The sponsor determines the purpose and means of processing.

Strictly speaking, the definition of data controller does not imply that the controller must receive or hold personal data. In principle, an entity can "determine the purpose and means" of a data processing operation without ever receiving personal data. The UK and Italian DPAs seem to share this opinion. Although they do not seem to consider key-coded CRFs as personal data as a matter of principle, the DPAs encourage sponsors to consider themselves data controllers because of their important role in determining processing activities in a clinical trial. [29]

Indeed, one could argue that the sponsor is the data controller because the sponsor is the one who initiates the trial and writes the protocol, which *determines the purposes and means of the processing*. Without the sponsor, the trial and the data processing operations generated by it would not take place at all. In addition, the regulatory framework in which clinical trials occur seem to confer obligations on the sponsor that are very similar to the role generally attributed to a data controller. For example, the Good Clinical Practices provide:

- GCP 1.5.3: the sponsor "takes responsibility for the initiation, management and/or financing of a clinical trial";
- GCP 4.9.3: sponsors should provide guidance to investigators on how to fill out and correct CRFs;
- GCP 5.1.1: "[t]he sponsor is responsible for implementing and maintaining quality assurance and quality control systems with written SOPs to ensure that trials are conducted and data are generated, documented (recorded), and reported in compliance with the protocol, GCP, and the applicable regulatory requirement(s)";

---

[27] Garante per la protezione dei dati personali, *Cittadini e Società dell'informazione*, Bollettino 13, August 2000, p. 33.

[28] Idem.

[29] Idem.

- GCP 5.1.2: "[t]he sponsor is responsible for securing agreement from all involved parties to ensure direct access to all trial related sites, source data/documents, and reports for the purpose of monitoring and auditing by the sponsor, and inspection by domestic and foreign regulatory authorities";
- GCP 5.5: sponsors should establish and implement security safeguards; and
- GCP 5.7: "[p]rior to initiating a trial, the sponsor should define, establish, and allocate all trial related duties and functions."

Investigator

Most DPAs agree that the investigator is a data controller.[30] Beyond the fact that physicians process non-coded health data, the main justification for this position seems to be that the investigator is subject to legal, professional, and ethical obligations that presuppose a level of control over the data processing operations. It is the investigator who seeks informed consent from the patients, and it is also the investigator who needs authorization from his or her ethics committee to perform the trial. These ethical committees and the investigators are considered to evaluate the sponsor's research proposal independently, and, thus, exert real control over the way personal information of patients will be processed and disclosed to the sponsor.[31]

To us, this argument is not self-evident. Again, through the protocol, the sponsor has a high degree of control over who collects what data and how. One could also argue that the investigator does little more than processing personal data on behalf and under instruction of the sponsor. The protocol governing the trial is usually sufficiently detailed to be considered a data processing contract, and the GCPs clearly limit the control of investigators over the conduct of clinical trails to the advantage of the sponsor:

- GCP 4.1.4: the investigator "should permit the monitoring and auditing by the sponsor […]";
- GCP 4.5.1: the investigator should conduct the trial in compliance with the protocol agreed to by the sponsor […]. The investigator and the sponsor should sign the protocol, or an alternative contract, to confirm agreement";
- GCP 4.5.2: the investigator should not implement any deviation from, or changes of the protocol without agreement by the sponsor and prior review and documented approval/favourable opinion from [ethics committees] of an amendment […].

[30] We use the term "investigator" here in a broad sense. Often, investigators are linked to a hospital, and the question arises who in this context should be considered the data controller: the investigator or the hospital.

[31] We have found no published reference of these positions; however, we base our statements on numerous contacts we have had with DPAs and the written statements they have made to us.

It is correct that the obligations of an investigator are stricter and better spelled out by law than for a "normal" processor (*i.e.*, a marketing service). To us this only means that a physician or CRO could not sign a protocol or processing contract that violates his or her legal, ethical or commercial obligations.[32] The fact that the investigator is subject to these obligations does not exclude him or her from being a data processor, provided the contract respects the investigator's obligations. Finally, we do not see why the investigator could not be considered a processor for the activities set forth by the protocol, but a controller for the activities that fall outside the scope of the protocol, such as unrelated diagnosis and care, or the maintenance of the patient's medical file.

CRO

The position of the CRO depends**,** to a large extent, on the factual situation of each trial. The CRO works on behalf of the sponsor, even though the "ultimate responsibility for the quality and integrity of the trial data always resides with the sponsor."[33] Based on the GCP, the trial related duties and functions of the CRO have to be specified in writing, often in the form of a contract.[34]

In terms of the data protection law, the position of the CRO comes closest to that of a "data processor." However, there seems to be a tendency for sponsors to increase the role of CROs in clinical trials. In many cases, CROs take over most of the functions of the sponsor, while the involvement of the sponsor is often limited to the financing of the trial. This can have important consequences in the application of data protection law. The more control a CRO exerts over the processing of CRFs, the greater the chance that DPAs would consider the CRO as a data controller, rather than a data processor for the sponsor. In fact, the French DPA has considered, a number of times, the CRO to be a data controller because of the CRO's sizable leverage over the way the CRFs were processed.

Applicable law

Only once the data controller of the data generated by a trial is identified**,** can we determine which data protection law applies. In particular, for trials conducted in several jurisdictions, this question is very important. As indicated above, the place of establishment of the data controller determines which data protection law applies. If there is no agreement on who the data controller(s) is/are, there can be no agreement on the applicable law(s).

For example, a sponsor established only in the Netherlands conducts a clinical trail with investigators in Belgium and France. In each country, the sponsor contracted with a CRO to perform a general monitoring function on behalf of the

---

[32] The European Commission's standard contract clauses for international transfers to processors actually recognize this in Clause 5 (a) and (b). If for some reason the processor is of the opinion that it cannot abide by the terms of the contract, the processor informs the controller and the contract can be ended.

[33] GCP, 5.2.1.

[34] GCP, 5.2.2.

sponsor (a data processor function). The investigators in Belgium and France send key-coded CRFs to the Dutch sponsor and the CROs.

- The investigators are considered data controllers and have to apply their respective data protection laws.

- The Dutch sponsor, pursuant to the Nefarma code, is not considered to process personal data and is not subject to the Dutch data protection law. As the sponsor has no establishments in France nor Belgium, he or she cannot be subject to these data protection laws either.

- The CROs in Belgium and France are bound by a contract with the Dutch sponsor, who is not subject to Dutch data protection law. Can the CROs be considered a data processor for someone that is not a data controller? Do the CROs then become data controllers in Belgium and France only because the sponsor happens to be established in the Netherlands, and even though they do not determine the purpose and means of the processing?

  The same scenario with a sponsor established in France leads to completely different results for the sponsor and CRO. The sponsor receives key-coded CRFs, considered to be personal data, and is subject to French data protection law. The CROs in Belgium and France contract with a data controller and can be considered data processors.

  The conclusion is clear: In the EU, even with the Data Protection Directive, there is little or no harmonization. Sponsors conducting trials in many Member States face a patchwork of legal requirements in the field of data protection. Transfers of key-coded CRFs from one country to another raise enormous difficulties. Where in one country they are not subject to the data protection law, in others they are. Where in one country sponsors are considered controllers, in another they are not.

Towards a Solution ?

As shown above the current situation is far from ideal. This patchwork of rules reduces legal certainty, increases regulatory complexity and the risk of non-compliance. However, finding a solution to these problems is not an easy endeavour. According to its 2005 Work Plan, the Article 29 Working Party will be working on an EU code of conduct for clinical trials governing the key-coding of personal data.[35] But what would such code look like?

For one we believe the code should find agreement on the definition of personal data, and, in particular, on the status of key-coded data. Based on the Data Protection Directive, it seems to us that key-coded personal data should be considered personal data, even for those who do not hold the key to the code. This is not the most pragmatic interpretation and it can lead to burdensome

[35] See: http://europa.eu.int/comm/justice_home/fsj/privacy/docs/wpdocs/2005/wp109_en.pdf.

results. However, a solution can be found in adapting the obligations of the controller to the nature of the controlled personal data.

Processing adequately key-coded data should entail less obligations than processing nominative data. Good examples of this approach can be found in the Austrian Data Protection Act[36] and, to a lesser extent, in the new French Act. In principle, key-coded data remain personal data in Austria also for entities that do not have access to the code, but most provisions in the Act do not apply.[37] For example, controllers of key-coded personal data do not have to grant data subjects access to their personal data, and requirements on notification to the DPA, and restrictions on international transfers and disclosures are dropped. In France, Art. 61 of the new Law provides that non-coded health data processed in the context of bio-medial research is subject to the restrictions on international transfers. To us, this logically implies that key-coded health data is not subject to restrictions, and thus, that lesser protections are applied to key-coded data than to non-coded data.

In contrast, Austrian data controllers do have to apply security and confidentiality requirements, and supervision by the data protection authority is maintained. This makes sense because adequate security of both the key and the coded data further prevents accidental disclosure and de-coding of the data.

Finally, this principle of less obligations for controllers of key-coded data will only be acceptable if regulators and industry can agree on a method of key-coding that adequately protects data subjects. It is quite clear today that the key-coding methods in countries following the holistic approach are weaker than in those that follow the individual approach. The reason is simple: in the holistic approach the key-coding does not affect the status of the data under data protection law, and thus receives less attention. However, in order to accept that less obligations should apply for the controller of key-coded data, higher demands will be placed on the method of key-coding. This is very much a sector-specific matter that should be dealt with in a code of conduct.

The possible discussion on creating a code is a good opportunity to seek an agreement on the status of key-code data, the coding standard, and the responsibilities attached to the processing of such data. The code will also have to take into account other legal obligations that sponsor and investigators have (*i.e.*, pharmacovigilance, other reporting to authorities, etc.), and which we have not fully considered here. Unfortunately, past experience with negotiations of EU-wide codes of conduct is not very encouraging. We can only hope that the DPAs will be able to reach an agreement on some of the issues raised above. However, a workable solution can only be achieved in cooperation with the pharmaceutical industry. The industry will also have to evaluate the benefits of a more harmonized regime against the risk of this regime being more burdensome than the current regimes in some Member States. In our opinion, the above solution

[36] Datenschutzgesetz 2000 – DSG 2000, Bundesgesetzblatt, 17 August 1999.

[37] W. Dohr and E. M. Weiss, *Kommentar Datenschutzrecht.*, Manzsche Verlags- und Universitätsbuchhandlung, p. 42.

of limited obligations for adequately key-coded data strikes a middle ground for regulators and industry that is worth exploring.